IWT - International Workshop on Telecommunications
Sponsored by
Instituto Nacional de Telecomunicações (Inatel), Brazil
Rio de Janeiro, Brazil

Capacity-Approaching Low-Density Parity-Check Codes: Recent Developments

Shu Lin

Department of Electrical and Computer Engineering
University of California, Davis
Davis, CA 95616, U.S.A.

May 3 - 6, 2011

I. Introduction

- The ever-growing needs for cheaper, faster, and more reliable communication and storage systems have forced many researchers to seek means to attain the ultimate limits on reliable information transmission and storage.
- Low-density parity-check (LDPC) codes are currently the most promising coding technique to achieve the Shannon capacities (or limits) for a wide range of channels.
- Discovered by Gallager in 1962 [1].
- A brief visit by Tanner in 1981 - graphical representation and message-passing concepts were introduced.

- Resurrected in the late 1990's by MacKay, Ruby and others.
- Ever since, a great deal of research effort has been expended in design, construction, encoding, decoding algorithms, structure, performance analysis, generalizations and applications of these remarkable codes.
- Numerous papers and patents have been published on these subjects.

- Many LDPC codes have been chosen as the standard codes for various next generations of communication systems, such as wireless, optical, satellite, space, digital video broadcast (DVB), multi-media broadcast (MMB), 10G BASE-T Ethernet, NASA's LANDSAT and other space missions.
- Applications to data storage systems, such as hard disk drives and flash memories are now being seriously considered.
- This rapid dominance of LDPC codes in applications is due to their capacity-approaching performance which can be achieved with practically implementable iterative decoding algorithms.

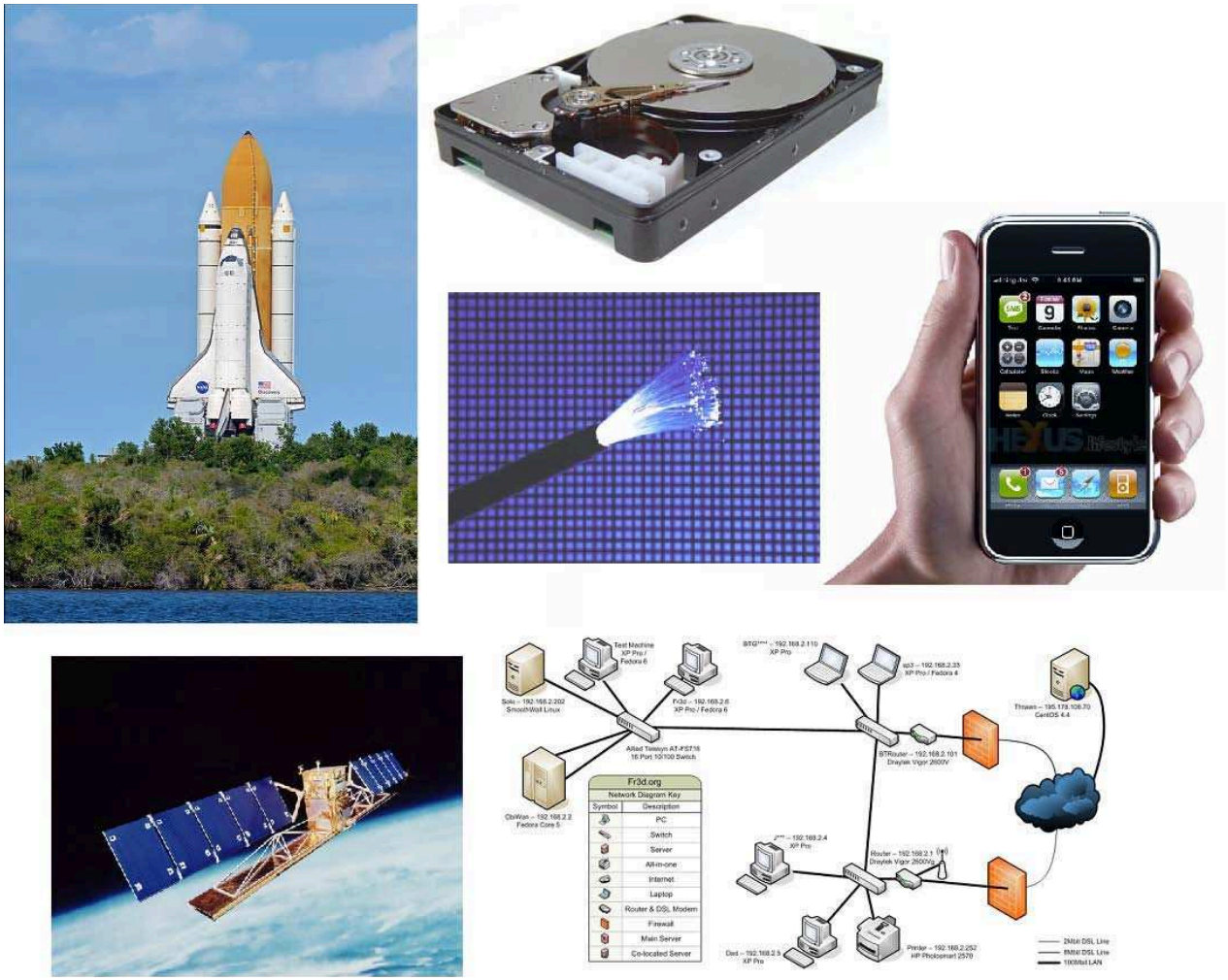

Figure 1: Picture of communication and storage systems.

- More applications are expected to come.
- Future is promising.
- However, there are still many things unknown about these codes, especially their fundamental structure. Further study is needed.
- The most urgent need are methods to design and construct efficient encodable and decodable codes that can achieve very low error rates, say a BER of 10^{-15}, for very high speed communications and very high density data storage.

Theme

This presentation is to give an overview of LDPC codes and their recent developments.

II. Definition and Classifications of LDPC Codes

- An LDPC code over GF(q), a finite field with q elements, is a q-ary linear block code given by the **null space** of a **sparse parity-check matrix** $\mathbf{H}$ over GF(q).
- An LDPC code is said to be **regular** if its parity-check matrix $\mathbf{H}$ has constant column weight, say γ, and constant row, say ρ. Such a q-ary LDPC code is said to be (γ,ρ)-regular.
- If the columns and/or rows of the parity-check matrix $\mathbf{H}$ have **multiple weights**, then the null space over of $\mathbf{H}$ gives an **irregular** LDPC code.

- If $\mathbf{H}$ is an **array** of **sparse circulants** of the same size over GF(q), then the null space over of $\mathbf{H}$ gives a q-ary **quasi-cyclic** (QC)-LDPC code.
- If $\mathbf{H}$ consists of a single sparse circulant or a column of sparse circulants, then the null space of $\mathbf{H}$ gives a **cyclic** LDPC code.
- For $q = 2$, the null space of $\mathbf{H}$ over the binary field GF(2) gives a **binary** LDPC code.
- At the present, only binary LDPC codes are being used for applications.
- Non-binary LDPC codes and their (efficient) decoding are now being seriously investigated.

- LDPC codes can be classified into two general categories:
  1) **random** or **pseudo-random** codes, and
  2) **Algebraic** codes.
- Random or pseudo-random codes are constructed using **computer-based algorithms or methods**.
- Algebraic codes are constructed using algebraic or combinatorial tools such as **finite fields, finite geometries and combinatorial designs**.

- Codes in these two categories can be classified into two types:
  1) codes whose parity-check matrices possess **little structure** and
  2) codes whose parity-check matrices have **structures**.
- A code whose parity-check matrix possesses no structure beyond being a linear code is **problematic** in that both encoding and decoding implementations become quite complex.
- A code whose parity-check matrix has structures beyond being a linear code is in general more easily implemented.

- Two desirable structures for hardware implementation of encoding and decoding of LDPC codes are cyclic and quasi-cyclic structures.
- A cyclic LDPC code can be **efficiently** and **systematically** encoded using a single feedback shift-register with complexity linearly proportional to the number of parity-check symbols (or information symbols).
- Encoding of a QC-LDPC code can also be efficiently implemented but requires multiple shift-registers. It is in general more complex than encoding of a cyclic code but still enjoys linear complexity.

- However, QC-LDPC codes enjoy some **advantages** in hardware implementation of decoding in terms of wire routing. Furthermore, the QC structure allows partially to full parallel decoding which offers a trade-off between decoding complexity and decoding speed.
- A cyclic LDPC code can be put in QC form through column and row permutations. As a result, a cyclic LDPC code enjoys both encoding and decoding implementation advantages.
- Encoding is carried out in cyclic form while decoding is carried out in QC form.

Well Known Structured LDPC Codes

1. Finite geometry codes
2. Finite field codes
3. Algebraic geometry codes
4. Codes based on combinatorial (or experimental) designs
5. Superimposed codes
6. Graph-theoretic codes (including **proto-graph** codes, **PEG-ACE** codes, and **trellis-based** codes)
7. Multi-edge-type codes
8. Accumulator-based codes (including **repeat-accumulate** (RA) codes, **irregular repeat-accumulate** (IRA) codes, and **accumulate-repeat-accumulate** (ARA) codes)
9. Generalized and doubly generalized LDPC codes

- Codes in the first five classes are constructed using finite or algebraic geometries, finite fields and combinatorial mathematics.
- Finite geometry LDPC codes are the first class of structured codes ever constructed (2000 at the AAECC Conference in Hawaii and published in *IEEE Trans. Inform. Theory*, Nov. 2001). They are cyclic LDPC codes.
- Recently, a large class of cyclic LDPC codes has been constructed based on cyclic finite geometry codes.
- Codes in the next four classes are constructed using computer-based algorithms or methods.
- Proto-graph, multi-edge-type, generalized and doubly generalized LDPC codes are actually superimposed LDPC codes.

IV. Row-Column Constraint

- In almost all of the proposed constructions of LDPC codes, the following **constraint** is imposed on the rows and columns of the parity-check matrix $\mathbf{H}$ of an LDPC code:
  No two rows (or two columns) can have more than one place where they both have 1-components.
- This constraint on the rows and columns of $\mathbf{H}$ and is referred to as the **row-column** (RC)**-constraint**.
- The RC-constraint ensures that the Tanner graph of an LDPC code is **free** of cycles of length 4 and hence has a **girth** of at least 6.

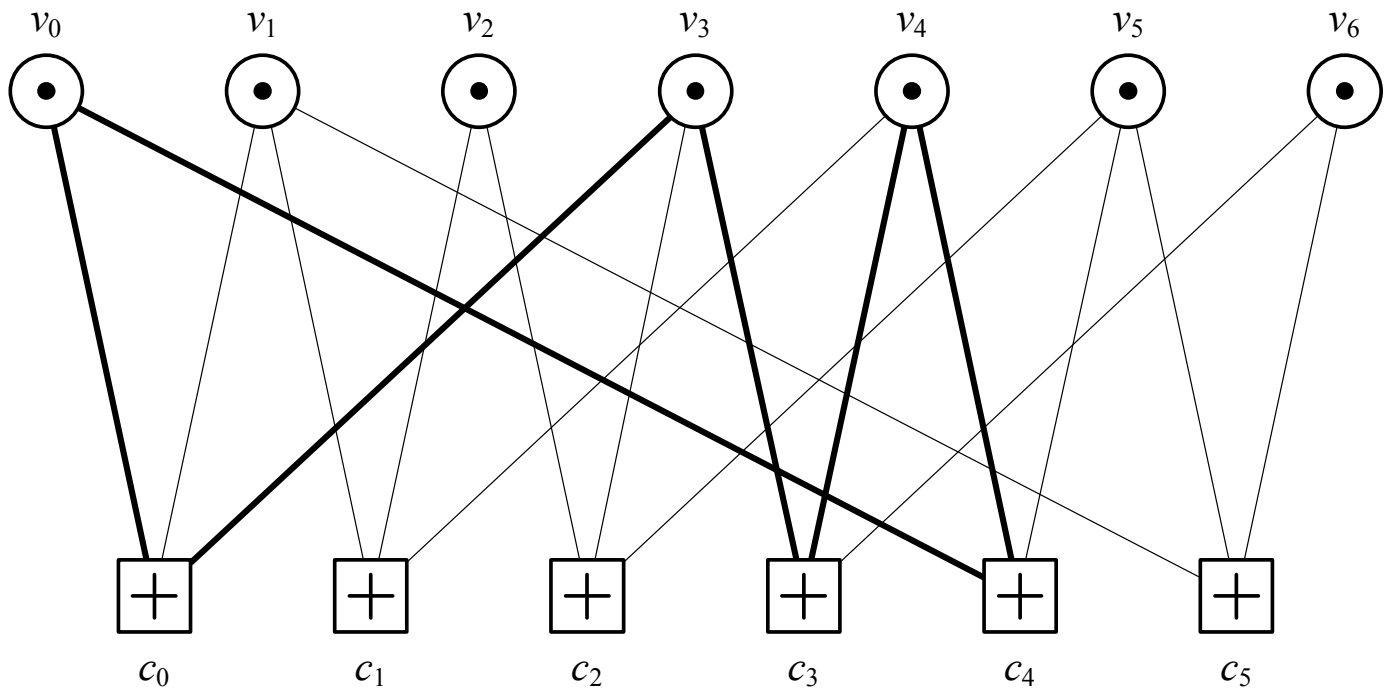

Figure 2: A Tanner graph to demonstrate its cycles.

- For a (γ,ρ)-regular LDPC code, the RC-constraint on its parity-check matrix $\mathbf{H}$ ensures that the **minimum distance** (or **weight**) of the code is at least $\gamma + 1$.
- This lower bound on the minimum distance is tight for a regular LDPC code whose parity-check matrix $\mathbf{H}$ has a relatively large column weight γ, such as a finite geometry LDPC code or finite field LDPC codes.

V. Iterative Decoding of LDPC Codes

- Decoding algorithms devised for LDPC codes are **iterative** in nature. These decoding algorithms are also referred to as **message-passing decoding (MPD) algorithms**.
- They are **practically implementable**.
- The **low-density nature** of the parity-check matrix of an LDPC code facilitates iterative decoding.
- An iterative decoder consists of a collection of low-complexity decoders working cooperatively in a distributed fashion to decode a received codeword which may be corrupted by noise.

Well Known Iterative Decoding Algorithms For Binary LDPC Codes

- **Sum-product algorithm** (SPA)
- **Min-sum algorithms** (MSA)
- **Binary message-passing** (BMP) **algorithms**
- **Bit-flipping** (BF) **algorithm**
- **Weighted-BF** (WBF) **algorithms**

- The SPA is a **suboptimal** (soft-decision) decoding algorithm which gives the best error performance but requires the highest computational complexity.
- An MSA is a simplified version of the SPA. It may cause some performance degradation.
- BMP- and WBF-algorithms are **reliability-based** decoding algorithms that provide effective trade-off between error performance and decoding complexity.
- The BF-algorithm is a hard-decision decoding algorithm that requires the least decoding complexity but offers the least coding (or performance) gain over an uncoded system.

For Non-binary LDPC Codes

- Q-ary SPA (QSPA)
- FFT-QSPA
- Reliability-Based Message-Passing Algorithms

VI. Measure of Performance

- The performance of an LDPC code with iterative decoding using algorithms such as the **sum-product algorithm** (SPA) and the **min-sum algorithm** (MSA), is measured by:
  1) The bit and block error performance (how close to the Shannon limit or sphere packing bound),
  2) The rate of decoding convergence,
  3) Error-floor,

Error-Floor

- LDPC codes perform amazingly well with **iterative decoding based on belief propagation**.
- However, with iterative decoding, most LDPC codes have a common **severe weakness**, known as **error-floor**.
- The error-floor of an LDPC code is characterized by the phenomenon of an **abrupt decrease in the slope** of the code's error performance curve from the moderate SNR water-fall region to the high SNR floor region, i.e., the error probability of a code in the high SNR region suddenly drops at a rate **much slower** than that in the region of low to moderate SNR (or even **stops to drop**).

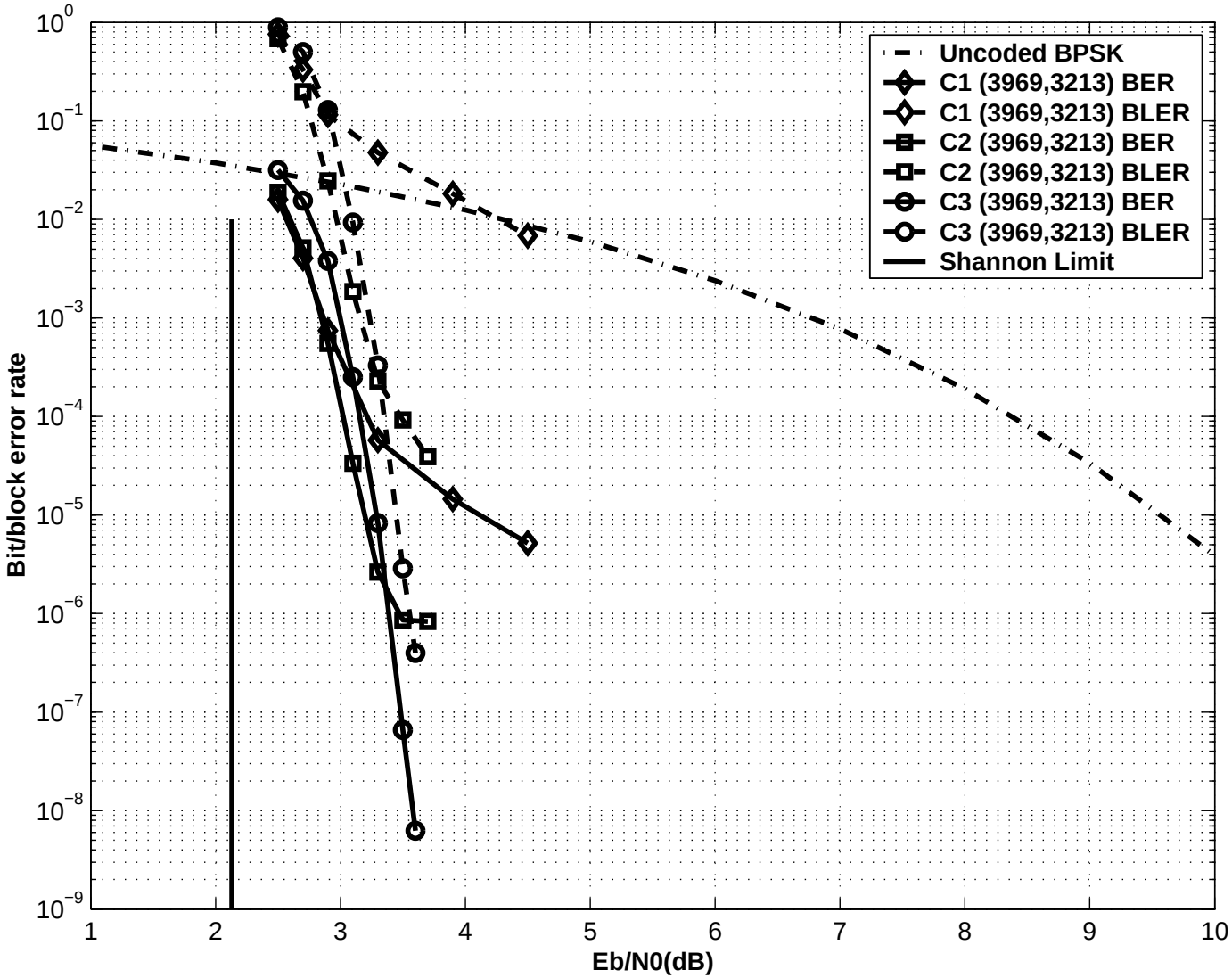

Figure 3: A figure to demonstrate the error floor phenomenon.

- For the AWGN channel, the error-floor of an LDPC code is mostly caused by an undesirable structure, known as **trapping-set**, in the Tanner graph of the code based on which the decoding is carried out.
- Error-floor may preclude LDPC codes from applications requiring very low error rates.
- High error-floors most commonly occur for random or pseudo-random LDPC codes.
- Structured LDPC codes constructed algebraically, in general, have much lower error-floors.

- Constructing (or designing) codes to avoid **harmful** trapping sets to mitigate error-floor problem is a combinatorial problem, **hard but challenging**.
- Several subclasses of finite geometry and finite field LDPC codes have been proved that their Tanner graphs do not contain small harmful trapping sets.
- The error-floor of an LDPC can be lowered by taking a **decoder-based strategy** to remove or reduce the effect of harmful trapping sets on error-floor.
- Several such decoder based strategies have been recently proposed. Among them, the most effective decoding strategy is the **backtracking iterative decoding algorithm** proposed recently.

Summary

- The performance of an LDPC code is determined by a number of structural properties **collectively**:
  1. minimum distance (or minimum weight);
  2. **girth** of its Tanner graph;
  3. **cycle distribution** of its Tanner graph;
  4. **cycle connectivity** (or structure);

5. parity-check matrix **row redundancy**;
6. **trapping set** distribution of its Tanner graph;
7. **degree distributions** of variable and check nodes of its Tanner graph; and
8. other unknown structures.

- No single structural property dominates the performance of a code.
- It is still unknown how the code performance depend on the above structural properties analytically as a function.

Remarks Based on Extensive Simulation Results

- Error-floor performance of an LDPC is mostly determined by its trapping set distribution and minimum distance.
- Large girth does not necessarily give good error performance. In fact, for finite geometry and finite field LDPC codes, a girth of 6 is all that needed.
- Large row redundancy of the parity-check matrix of an LDPC code makes the decoding of the code converging faster.
- Parity-check matrices of finite geometry and several classes of finite field LDPC codes have large row redundancies. Their decoding converges very fast.

New Results

- For algebraically constructed regular LDPC codes, RC-constraint and large row redundancy ensure that their Tanner graphs do not contain harmful trapping sets of sizes smaller than the column weights of their parity-check matrices.
- More specifically, the Tanner graph of an RC-constrained (γ, ρ)-regular LDPC code contains no harmful trapping sets with sizes γ or less.

VII. Algebraic Constructions of Structured LDPC Codes

- Construction based on finite geometries such as Euclidean and projective geometries
- Construction based algebraic geometries (not published yet)
- Constructions based on finite fields: 1) additive subgroups; 2) cyclic subgroups; and 3) primitive elements
- Construction based on combinatorial designs: 1) Latin squares; and 2) balanced incomplete block designs (BIBDs)

- Construction based on Reed-Solomon (RS) codes
- Superposition construction (including product)
- Transform domain construction (new powerful approach)
- Algebraic constructions mostly result in cyclic and quasi-cyclic LDPC codes.

The rest of This Talk

- Two algebraic constructions including new results.

VIII. Finite Geometry LDPC Codes

- There are two classes of finite geometry (FG) LDPC codes, one class constructed based on finite Euclidean geometries and the other based on projective geometries.
- Based each type of geometries, both cyclic and QC-LDPC codes can be constructed.
- They have large minimum distances and their Tanner graphs have girth of at least 6.
- Their parity-check matrices have large row redundancy.
- They have very low error-floors.

Binary Cyclic Euclidean Geometry (EG) LDPC Codes

- In the following, we only consider construction of binary LDPC codes based on Euclidean geometries over finite fields.
- Let the m-dimensional Euclidean geometry, EG(m, q), over GF(q) be the code construction geometry.
- The parity-check matrix $\mathbf{H}_{EG}$ of a binary EG-LDPC code $\mathcal{C}_{EG}$ is formed by the binary **incidence vectors** of all the lines in EG(m, q) not passing through the origin.
- $\mathbf{H}_{EG}$ can be arranged as a column of circulants of size $(q^m - 1) \times (q^m - 1)$.

- $\mathbf{H}_{EG}$ satisfies the RC-Constraint.
- The null space of $\mathbf{H}_{EG}$ gives a binary cyclic EG-LDPC code $\mathcal{C}_{EG}$ whose Tanner graph has a girth at least 6.
- Its minimum distance is at least $(q^m - 1)/(q - 1) + 1$.

A Special Subclass of Cyclic EG-LDPC Codes

- For $m = 2$, the parity check matrix $\mathbf{H}_{EG}$ constructed based on the two-dimensional (2-D) Euclidean geometry, EG$(2, q)$, over GF(q) is a single $(q^2 - 1) \times (q^2 - 1)$ circulant with both column and row weights q.
- The null space of $\mathbf{H}_{EG}$ gives a cyclic EG-LDPC codes of length $n = q^2 - 1$ with minimum distance at least $q + 1$.
- Its Tanner graph contains no small trapping sets of sizes smaller than $q + 1$.

- For $m = 2$ and $q = 2^s$, the cyclic EG-LDPC code $\mathcal{C}_{EG}$ has the following parameters:
  Length $n = 4^s - 1$,
  Number of parity bits $n - k = 3^s - 1$,
  Minimum distance $d_{min} = 2^s + 1$.
- It parity-check matrix $\mathbf{H}_{EG}$ has $4^s - 3^s$ dependent rows and hence has large row redundancy.
- Its Tanner graph contains no trapping sets of sizes small than the minimum distance d_{min}.

Decoding

- Besides decoding with the SPA and the MSA, EG-LDPC codes are quite effective for other types of decoding such as: 1) **one-step majority-logic decoding** (OSMLGD) (not iterative), 2) BF-decoding, 3) WBF-decoding, 4) soft-reliability-based binary message-passing (SRB-BMP) decoding, and 5) hard-reliability-based binary message-passing (HRB-BMP) decoding.
- Various methods of decoding provide a wide spectrum of trade-offs between error performance and decoding complexity.
- Dual-mode decoder, SPA (MSA) plus (OSMLGD), can be designed to improve error performance.

Example 1

- Construction geometry: EG(2,2^6) over GF(2^6).
- Parity-check matrix $\mathbf{H}_{EG}$: a 4095×4095 circulant with both column and row weights 64.
- Code: a (4095,3367) cyclic LDPC code with minimum distance 65.
- The error-floor of the code is very low.
- The error performances of this code with various decoding methods are shown in Figure 1.

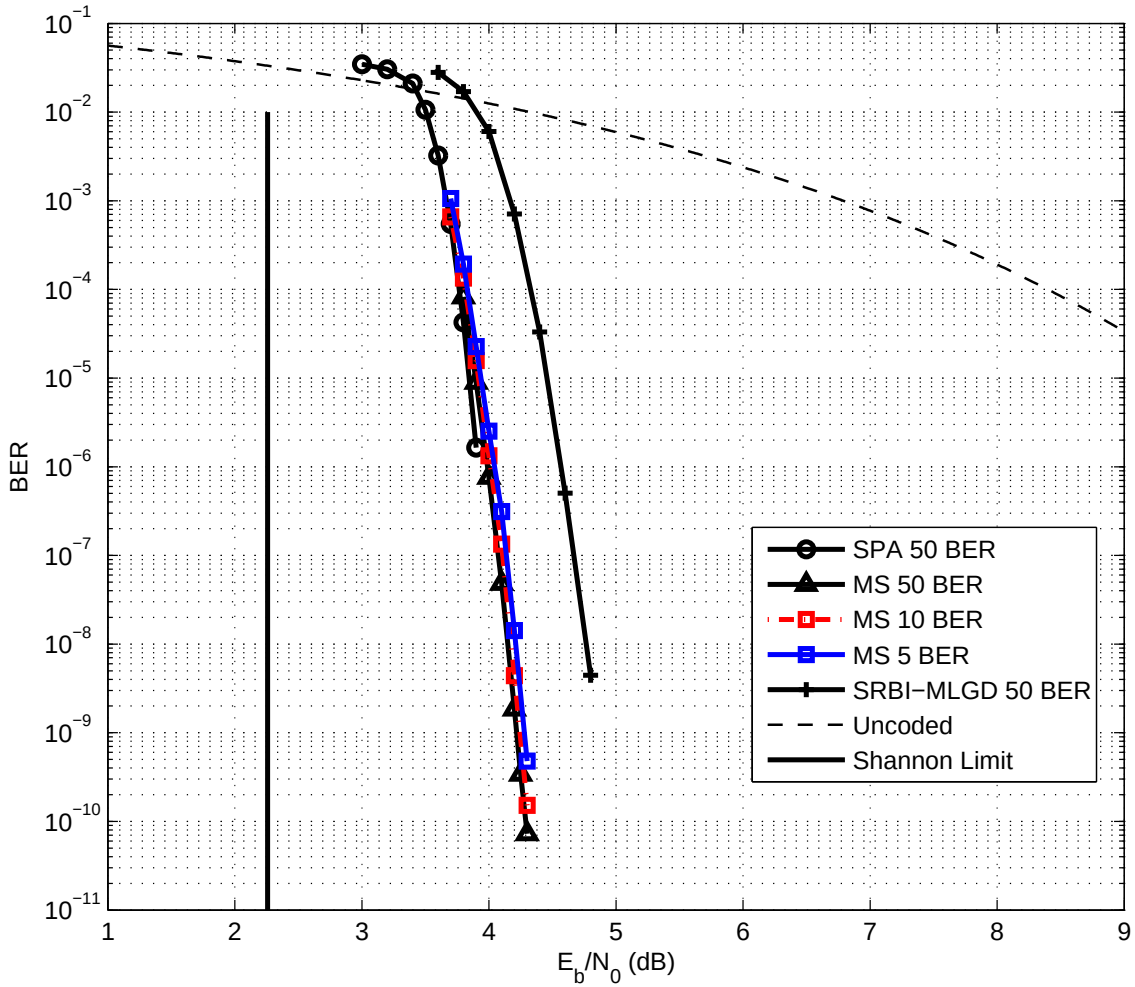

Figure 4: Bit error performances of the binary (4095,3367) cyclic EG-LDPC code given in Example 2 decoded with the SPA and the scaled MS-algorithm.

Binary QC-EG-LDPC Codes

- The incidence vectors of lines in EG(m, q) not passing through the origin can be used to form

$$K_c = (q^{m-1} - 1)/(q - 1)$$

  circulants of size $(q^m - 1) \times (q^m - 1)$, each having both column and row weights q.
- For $1 \leq k \leq K_c$, take k such circulants and arrange them in a row.
- This results in a $(q^m - 1) \times k(q^m - 1)$ matrix $\mathbf{H}_{EG,qc}$ over GF(2) with column and row weights q and kq, respectively.
- The null space of $\mathbf{H}_{EG,qc}$ gives a QC-LDPC code $\mathcal{C}_{EG,qc}$ of length $k(q^m - 1)$ with minimum distance at least $q + 1$.

Decomposition by Column and Row Splitting

- Each circulant can be decomposed into an array of $(q^m - 1) \times (q^m - 1)$ circulants using column and row splitting.
- If each circulant in $\mathbf{H}_{EG,qc}$ is decomposed into an array of the same size, say $c \times c$, we obtain a $c \times kc$ array $\mathbf{M}_{EG,qc}$ of $(q^m - 1) \times (q^m - 1)$ circulants.
- $\mathbf{M}_{EG,qc}$ is a $c(q^m - 1) \times kc(q^m - 1)$ matrix over GF(2).
- The null space of $\mathbf{M}_{EG,qc}$ gives a new QC-LDPC code.

Example 2

NASA Standard Code for LANDSAT and Cruise Exploration Shuttle Mission

- Bit error performance requirement: 10^{-12}.
- Code construction geometry: EG(3,2^3) over GF(2^3).
- Nine 511×511 circulants can be formed based on the incidence vectors of the lines in EG(3,2^3) not passing through the origin. Each circulant has both column and row weights 8.
- Take 8 such circulants and arrange them in a row to obtain a 511×4088 matrix $\mathbf{H}_{EG,qc}$.

- Decompose each circulant in $\mathbf{H}_{EG,qc}$ into a 2×2 array of four 511×511 circulants, each having both column and row weights 2.
- The decomposition results in a 2×16 array $\mathbf{M}_{EG,qc}$ of 511×511 circulants.
- $\mathbf{M}_{EG,qc}$ is a 1022×8176 matrix over GF(2) with column and row weights 4 and 32.
- The null space of $\mathbf{M}_{EG,qc}$ gives a (8176,7156) QC-LDPC code $\mathcal{C}_{qc,nasa}$ with rate 0.8752.
- The performance of this code is shown in Figure 5.
- Beautiful waterfall performance and no error-floor down to the BER of 10^{-14}.

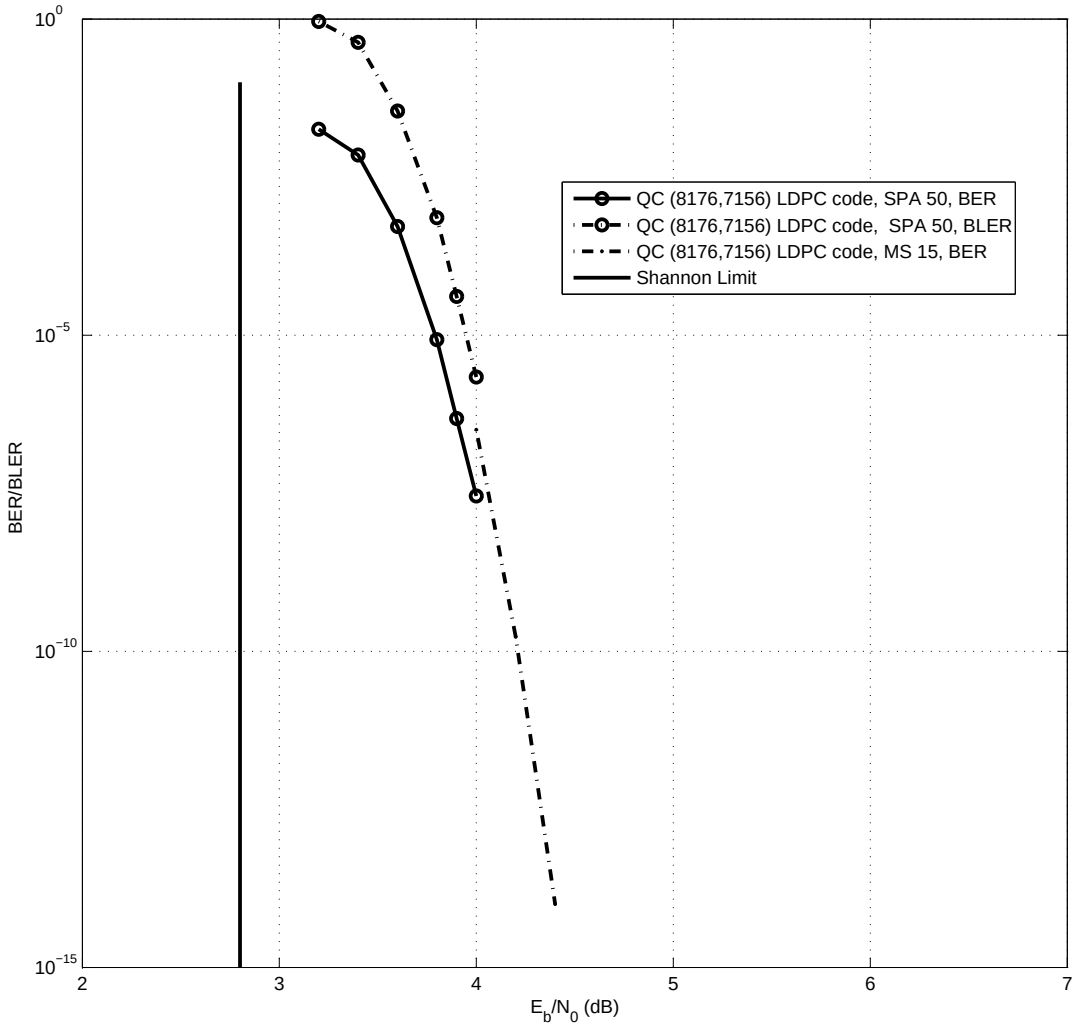

Figure 5: The error performances of the binary (8176,7156) QC-LDPC code given in Example 2.

IX. New Cyclic and QC EG-LDPC Codes

- Consider the $(q^2-1) \times (q^2-1)$ circulant $\mathbf{H}_{EG}$ constructed based on the two-dimensional Euclidean geometry EG(2,q) over GF(q).
- The null space of $\mathbf{H}_{EG}$ gives a cyclic EG-LDPC code $\mathcal{C}_{EG}$.
- Let $n = q^2 - 1$ and $\mathbf{w} = (w_0, w_1, ..., w_{n-1})$ be the first row of $\mathbf{H}_{EG}$, which is called the **generator** of the circulant $\mathbf{H}_{EG}$.
- Label the rows and columns of the circulant $\mathbf{H}_{EG}$ from 0 to $n-1$.
- Suppose n can be properly factored as a product of two positive integers, c and l, i.e., $n = c \cdot l$.

A Specific Permutation

- Let $\Gamma = \{0, 1, 2, ..., c \cdot l - 1\}$ be the set of labels for the rows and columns of $\mathbf{H}_{EG}$.
- Define the following index sets:

$$\pi^{(0)} = [0, c, 2c, \ldots, (l-1)c], \tag{1}$$

$$\pi = [\pi^{(0)}, \pi^{(0)} + 1, \ldots, \pi^{(0)} + c - 1]. \tag{2}$$

- Then, π gives a permutation of the indices in Γ.

A Circulant Decomposition

- Permuting the columns and rows of $\mathbf{H}_{EG}$ based on π, we obtain the following $c \times c$ array of circulants of size $l \times l$:

$$\Phi_{EG} = \begin{bmatrix} \Psi(\mathbf{w}_0) & \Psi(\mathbf{w}_1) & \cdots & \Psi(\mathbf{w}_{c-2}) & \Psi(\mathbf{w}_{c-1}) \\ \Psi^{(1)}(\mathbf{w}_{c-1}) & \Psi(\mathbf{w}_0) & \cdots & \Psi(\mathbf{w}_{c-3}) & \Psi(\mathbf{w}_{c-2}) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \Psi^{(1)}(\mathbf{w}_2) & \Psi^{(1)}(\mathbf{w}_3) & \cdots & \Psi(\mathbf{w}_0) & \Psi(\mathbf{w}_1) \\ \Psi^{(1)}(\mathbf{w}_1) & \Psi^{(1)}(\mathbf{w}_2) & \cdots & \Psi^{(1)}(\mathbf{w}_{c-1}) & \Psi(\mathbf{w}_0) \end{bmatrix}, \quad (3)$$

- For $0 \leq i < c$, the circulant $\Psi^{(1)}(\mathbf{w}_i)$ is obtained by simultaneously cyclically shifting all the rows of $\Psi(\mathbf{w})$ one place to the right.
- Note that $\Psi^{(1)}(\mathbf{w}_i)$ and $\Psi(\mathbf{w}_i)$ have identical set of rows and identical set of columns.
- Their **null spaces** are identical.
- Each $l \times l$ circulant in Φ_{EG} is called a **descendant** circulant of the mother circulant $\mathbf{H}_{EG}$.

- Since the array Φ_{EG} is obtained by applying the permutation π to the columns and rows of the ciruclant $\mathbf{H}_{EG}$, we write $\Phi_{EG} = \pi(\mathbf{H}_{EG})$.
- Let π^{-1} be the inverse permutation of π. Then $\mathbf{H}_{EG} = \pi^{-1}(\Phi_{EG})$.
- The null space of Φ_{EG} gives a binary QC-EG-LDPC code $\mathcal{C}_{EG,qc}$ which is **equivalent** to the cyclic EG-LDPC code $\mathcal{C}_{EG}$.

Structure of the Array $\Phi_{EG,circ}$

- Each row of $l \times l$ circulants in Φ_{EG} is a right cyclic-shift of the row above it, however, when the last circulant on the right is shifted around to the left, all its rows are cyclically shifted one place to the right within the circulant.
- This structure is referred to as the **doubly cyclic structure** which is pertinent to the construction of new cyclic LDPC codes from a given cyclic **EG-LDPC code**.

Cyclic LDPC Descendant Codes of a Cyclic EG-LDPC Code

- From the array Φ_{EG}, we can construct new cyclic EG-LDPC codes of three different types.
- These new cyclic EG-LDPC codes are called **cyclic descendant codes** (simply descendants) of the cyclic EG-LDPC code $\mathcal{C}_{EG}$.
- The cyclic code $\mathcal{C}_{EG}$ itself is called the **mother code**.

Type-1 Cyclic Descendant LDPC Codes

- For $0 \leq i < c$, if $\Psi(\mathbf{w}_i)$ is a nonzero circulant, the null space of $\mathbf{H}_i^{(1)} = \Psi(\mathbf{w}_i)$ gives a cyclic descendant of $\mathcal{C}_{EG}$, denoted by $\mathcal{C}_i^{(1)}$, of length l.
- This descendant code is referred to as a type-I descendant of $\mathcal{C}_{EG}$.

Type-2 Cyclic Descendant LDPC Codes

- From the array Φ_{EG}, we see that each column consists of the circulants in the first row of Φ_{EG}.
- For $0 \leq i < c$, each circulant $\Psi(\mathbf{w}_i)$ or its cyclic shift $\Psi^{(1)}(\mathbf{w}_i)$ appears once and only once in each column.
- Since a circulant $\Psi(\mathbf{w}_i)$ and its cyclic shift $\Psi^{(1)}(\mathbf{w}_i)$ differ only in permutation of their rows and hence their null spaces are identical.
- Consequently, the null spaces of all the columns of Φ_{EG} are the same.

- In fact, the null space of each column of Φ_{EG} is identical to the null space of the $cl \times l$ matrix

$$\begin{bmatrix} \Psi(\mathbf{w}_0) \\ \Psi(\mathbf{w}_1) \\ \vdots \\ \Psi(\mathbf{w}_{c-1}) \end{bmatrix}.$$

- For $1 \leq k < c$, let $i_1, i_2, ..., i_k$ be k distinct integers such that $0 \leq i_1, i_2, ..., i_k < c$. Let

$$\mathbf{H}_{col,k}^{(2)} = \begin{bmatrix} \Psi(\mathbf{w}_{i_1}) \\ \Psi(\mathbf{w}_{i_2}) \\ \vdots \\ \Psi(\mathbf{w}_{i_k}) \end{bmatrix}, \tag{4}$$

- $\mathbf{H}_{col,k}^{(2)}$ is a $kl \times l$ matrix over GF(2) whose null space gives a cyclic LDPC code of length l, denoted by $\mathcal{C}_k^{(2)}$, which is referred to as a type-2 cyclic descendant of the mother cyclic EG-LDPC code $\mathcal{C}_{EG}$.

Type-3 Cyclic Descendant LDPC Codes

- Construction of cyclic descendant LDPC codes of type-3 depends on the doubly cyclic structure of the array

$$\Phi_{EG} = \begin{bmatrix} \Psi(\mathbf{w}_0) & \Psi(\mathbf{w}_1) & \Psi(\mathbf{w}_2) & \cdots & \Psi(\mathbf{w}_{c-1}) \\ \Psi^{(1)}(\mathbf{w}_{c-1}) & \Psi(\mathbf{w}_0) & \Psi(\mathbf{w}_1) & \cdots & \Psi(\mathbf{w}_{c-2}) \\ \Psi^{(1)}(\mathbf{w}_{c-2}) & \Psi^{(1)}(\mathbf{w}_{c-1}) & \Psi(\mathbf{w}_0) & \cdots & \Psi(\mathbf{w}_{c-3}) \\ \vdots & \vdots & & \ddots & \vdots \\ \Psi^{(1)}(\mathbf{w}_1) & \Psi^{(1)}(\mathbf{w}_2) & \Psi^{(1)}(\mathbf{w}_3) & \cdots & \Psi(\mathbf{w}_0) \end{bmatrix},$$

- For $1 \leq k < c$, let $i_1, i_2, ..., i_k$ be a set of distinct integers such that $0 \leq i_1, i_2, ..., i_k < c$.
- Suppose we replace the descendant circulants, $\Psi(\mathbf{w}_{i_1}), \Psi(\mathbf{w}_{i_2}), ..., \Psi(\mathbf{w}_{i_k})$ and all their cyclic shifts in the array Φ_{EG} by zero matrices of size $l \times l$.
- By doing this, we obtain a $c \times c$ masked array $\mathbf{H}^{(3)}_{qc,mask} = [\Phi_{EG}]_{mask}$ of circulants and zero matrices of size $l \times l$.

- The masked array $[\Phi_{EG}]_{mask}$ still retains the doubly cyclic structure.
- Applying the inverse permutation π^{-1} to the columns and rows of the $c \times c$ array $\mathbf{H}^{(3)}_{qc,mask} = [\Phi_{EG}]_{mask}$, we obtain a new circulant matrix

$$\mathbf{H}^{(3)}_{circ,mask} = \pi^{-1}([\Phi_{EG}]_{mask}).$$

- Then the null space of $\mathbf{H}^{(3)}_{circ,mask}$ gives a cyclic LDPC code $\mathcal{C}^{(3)}_{mask}$ which is referred to as a type-3 cyclic descendant of the cyclic EG-LDPC code $\mathcal{C}_{EG}$.

- The replacement of a set of circulants in the array Φ_{EG} is called masking.
- Different masking patterns results in different cyclic descendants of the cyclic EG-LDPC code $\mathcal{C}_{EG}$.
- The results developed above show that decomposition of the circulant parity-check matrix of a cyclic EG-LDPC code $\mathcal{C}_{EG}$ gives a family of cyclic LDPC codes.
- Circulant decomposition enlarge the repertoire of cyclic LDPC codes.

Quasi-Cyclic LDPC Descendants of a Cyclic EG-LDPC Code

- For any pair (s, t) of integers with $1 \leq s, t \leq c$, let $\Phi_{EG}(s, t)$ be a $s \times t$ sub-array of Φ_{EG}.
- Since $\Phi_{EG}(s, t)$ is an array of circulants and satisfies the RC-constraint, its null space gives a QC-LDPC code.
- This QC-LDPC code is called a QC descendant of the cyclic EG-LDPC code $\mathcal{C}_{EG}$.
- Therefore, decomposition of a cyclic EG-LDPC code $\mathcal{C}_{EG}$ gives a family of QC-LDPC codes.

Example 3

- Consider the 4095x4095 circulant $\mathbf{H}_{EG}$ constructed based on the two-dimensional Euclidean geometry, EG(2,2^6) over GF(2^6).
- Factor 4095 as the product of $c = 3$ and $l = 1365$.
- Then the 4095x4095 circulant $\mathbf{H}_{EG}$ can be decomposed into a 3x3 doubly cyclic array of circulants of size 1365×1365 in the form as shown below:

$$\Phi_{EG} = \begin{bmatrix} \Psi_0 & \Psi_1 & \Psi_2 \\ \Psi_2^{(1)} & \Psi_0 & \Psi_1 \\ \Psi_1^{(1)} & \Psi_2^{(1)} & \Psi_0 \end{bmatrix}.$$

- Both descendant circulants Ψ_0 and Ψ_2 have column and row weights 24.
- The descendant circulant Ψ_1 has both column and row weights 16.
- Consider the 1365×1365 descendant circulant Ψ_1. Its rank is 600.
- The null space of Ψ_1 gives a (1365,765) type-1 cyclic descendant LDPC code $\mathcal{C}_{EG}^{(1)}$ of the (4095,3367) cyclic EG-LDPC code $\mathcal{C}_{EG}$ with rate 0.56 and minimum distance at least 17.

- The error performance of the code over the AWGN channel using BPSK signaling decoded with 50 iterations of SPA (or MS) is shown in Figure 6.
- At the block error rate (BLER) of 10^{-5}, the code perform 1.6 dB from the sphere packing bound.

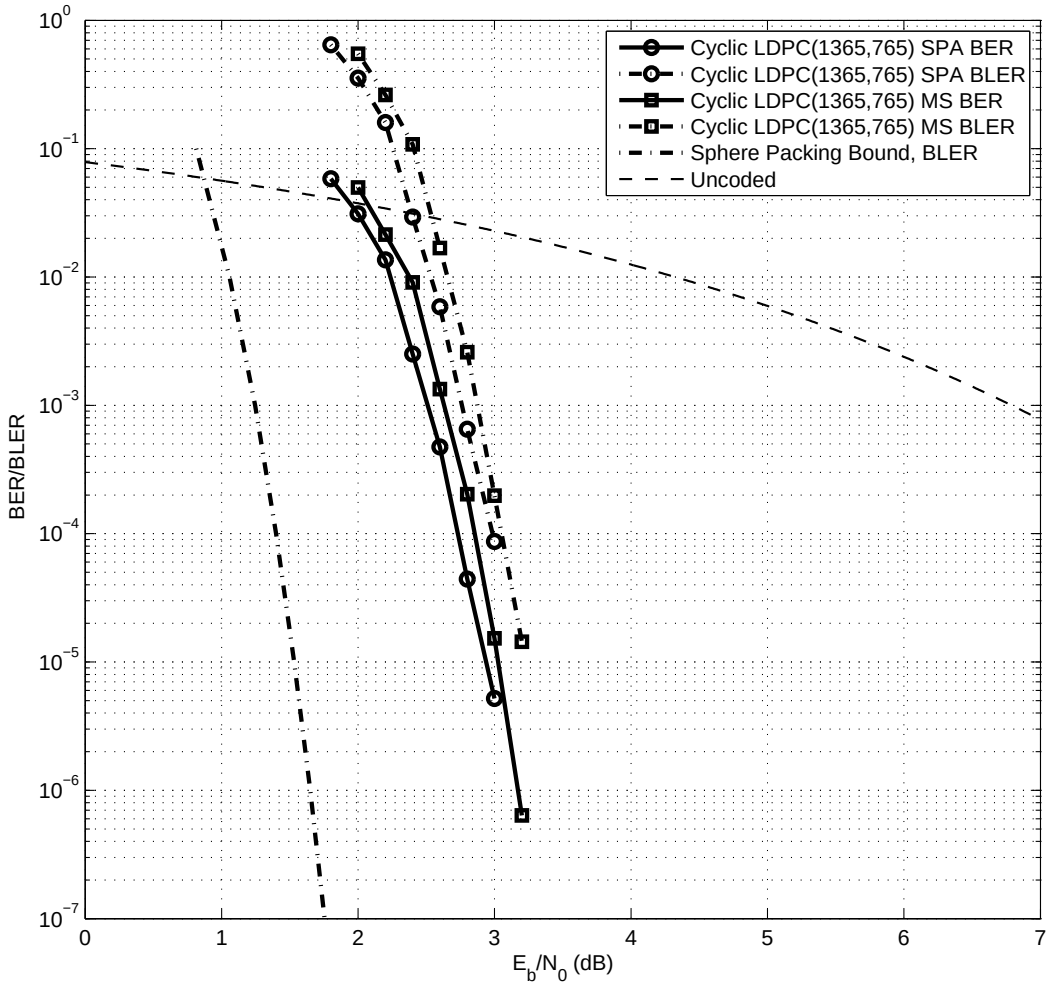

Figure 6: The error performances of the binary (1365,765) cyclic EG-LDPC code given in Example 3 decoded with 50 iterations of the SPA and the MS-algorithm.

Example 4

- Suppose we replace Ψ_2 and its cyclic-shift $\Psi_2^{(1)}$ in the decomposed array $\Phi_{EG,qc}$ given in Example 3 by two 1365×1365 zero matrices. We obtain the following 3×3 masked array:

$$[\Phi_{EG}]_{mask} = \begin{bmatrix} \Psi_0 & \Psi_1 & \mathbf{O} \\ \mathbf{O} & \Psi_0 & \Psi_1 \\ \Psi_1^{(1)} & \mathbf{O} & \Psi_0 \end{bmatrix}.$$

- The masked array $[\Phi_{EG}]_{mask}$ still has the doubly cyclic structure.

- Applying the inverse permutation π^{-1} to $[\Phi_{EG}]_{mask}$, we obtain a masked 4095×4095 circulant $\mathbf{H}^{(3)}_{circ,mask} = \pi^{-1}([\Phi_{EG}]_{mask})$ with both column and row weights 40.
- The null space of $\mathbf{H}^{(3)}_{circ,mask}$ gives a (4095,2703) type-3 cyclic descendant LDPC code of the (4095,3367) cyclic EG-LDPC code.
- The code has rate 0.66 and minimum distance at least 41.
- The error performances of this cyclic descendant LDPC code decoded with 3, 5, and 50 iterations of the SPA is shown in Figure 7.

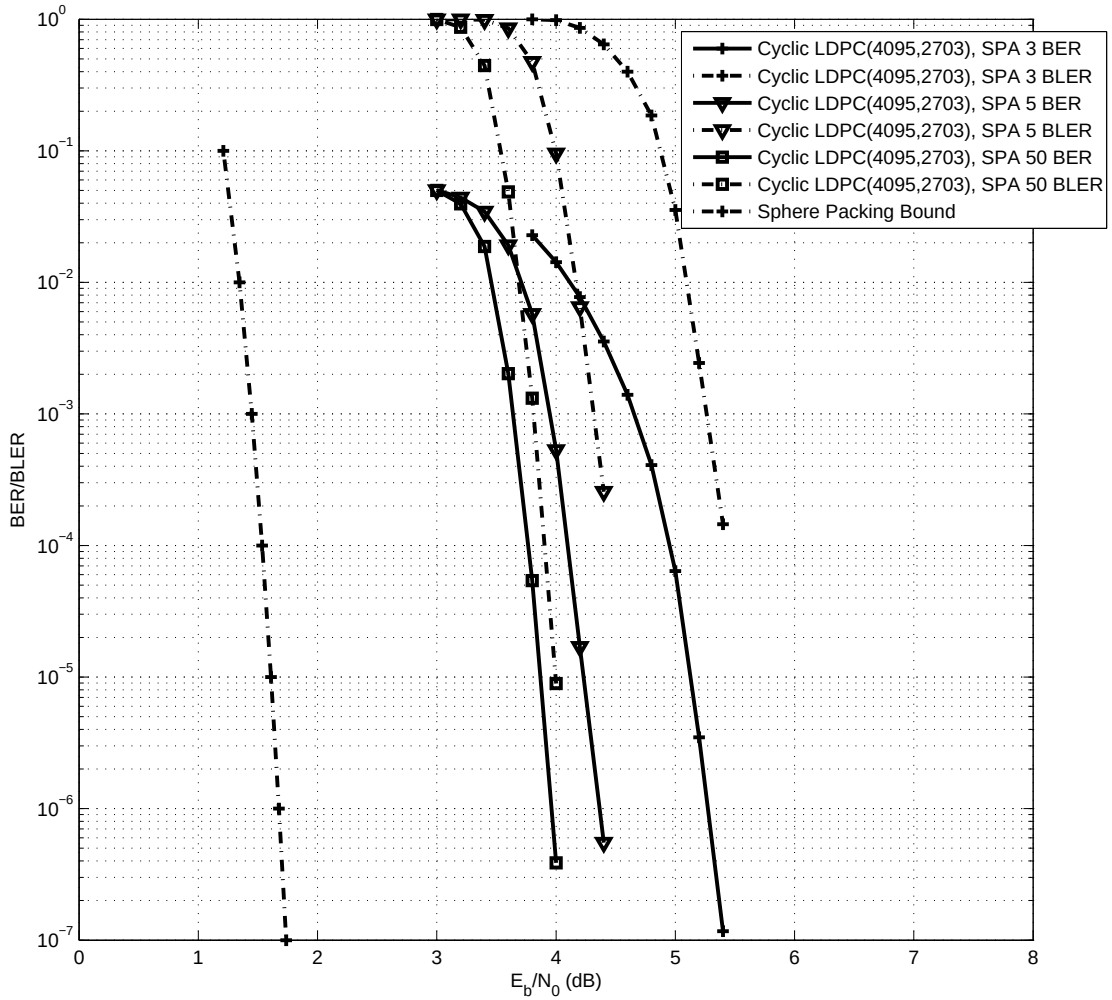

Figure 7: (c) The bit and block error performances of the binary (4095,2703) cyclic EG-LDPC code given in Example 4.

X. A New Class of QC-LDPC Codes

- Suppose we factor q^2-1 as the product of $c=q+1$ and $l=q-1$.
- Then, the $(q^2-1)\times(q^2-1)$ circulant $\mathbf{H}_{EG}$ constructed based on EG(2,q) over GF(q) can be decomposed into a $(q+1)\times(q+1)$ doubly cyclic array $[\Phi_{EG}]_{cpm}$ of circulants of size $(q-1)\times(q-1)$.
- Each circulant in $[\Phi_{EG}]_{cpm}$ is either a $(q-1)\times(q-1)$ **circulant permutation matrix** (CPM) or a $(q-1)\times(q-1)$ zero matrix (ZM). Each row (or column) block of Φ_{EG} consists of q CPMs and one zero matrix.

- The null space of $[\Phi_{EG}]_{cpm}$ gives a QC-EG-LDPC code $\mathcal{C}_{EG,qc}$ which is equivalent to the cyclic EG-LDPC code $\mathcal{C}_{EG}$ constructed based on EG(2,q).
- For any pair of integers, (γ, ρ) with $1 \leq \gamma, \rho \leq q+1$, let $[\Phi_{EG}(\gamma, \rho)]_{cpm}$ be a $\gamma \times \rho$ subarray of $[\Phi_{EG}]_{cpm}$.
- The null space of $[\Phi_{EG}(\gamma, \rho)]_{cpm}$ gives a descendant QC-LDPC code of the cyclic EG-LDPC code $\mathcal{C}_{EG}$.
- The above decomposition and construction give a large class of QC-EG-LDPC codes with various lengths, rates and minimum distances.

Example 5

- Consider the 4095×4095 circulant $\mathbf{H}_{EG}$ over GF(2) constructed based on the 2-D Euclidean geometry EG(2,2^6) over GF(2^6) given in Example 1.
- We factor 4095 as the product of $c = 65$ and $l = 63$.
- Decompose the 4095×4095 circulant $\mathbf{H}_{EG}$ into a 65×65 array $[\Phi_{EG}]_{cpm}$ of CPMs and ZMs of size 63×63.
- The null space of $[\Phi_{EG}]_{cpm}$ gives a (4095,3367) QC-EG-LDPC code which is equivalent to the cyclic EG-LDPC code constructed based on EG(2,2^6).

- Suppose we choose the first 6 rows of $[\Phi_{EG}]_{cpm}$ to from a 6×65 subarray $[\Phi_{EG}(\gamma, \rho)]_{cpm}$ of $[\Phi_{EG}]_{cpm}$
- It is a 378×4095 matrix over GF(2) with constant row weight 64 and two column weights, 5 and 6.
- The null space of this matrix gives a (4095,3771) descendant QC-EG-LDPC code with rate 0.921.
- Its error performance with 50 iterations of the SPA is shown in Figure 8.
- At the BLER of 10^4, the code performs 0.75 dB from the sphere packing bound.

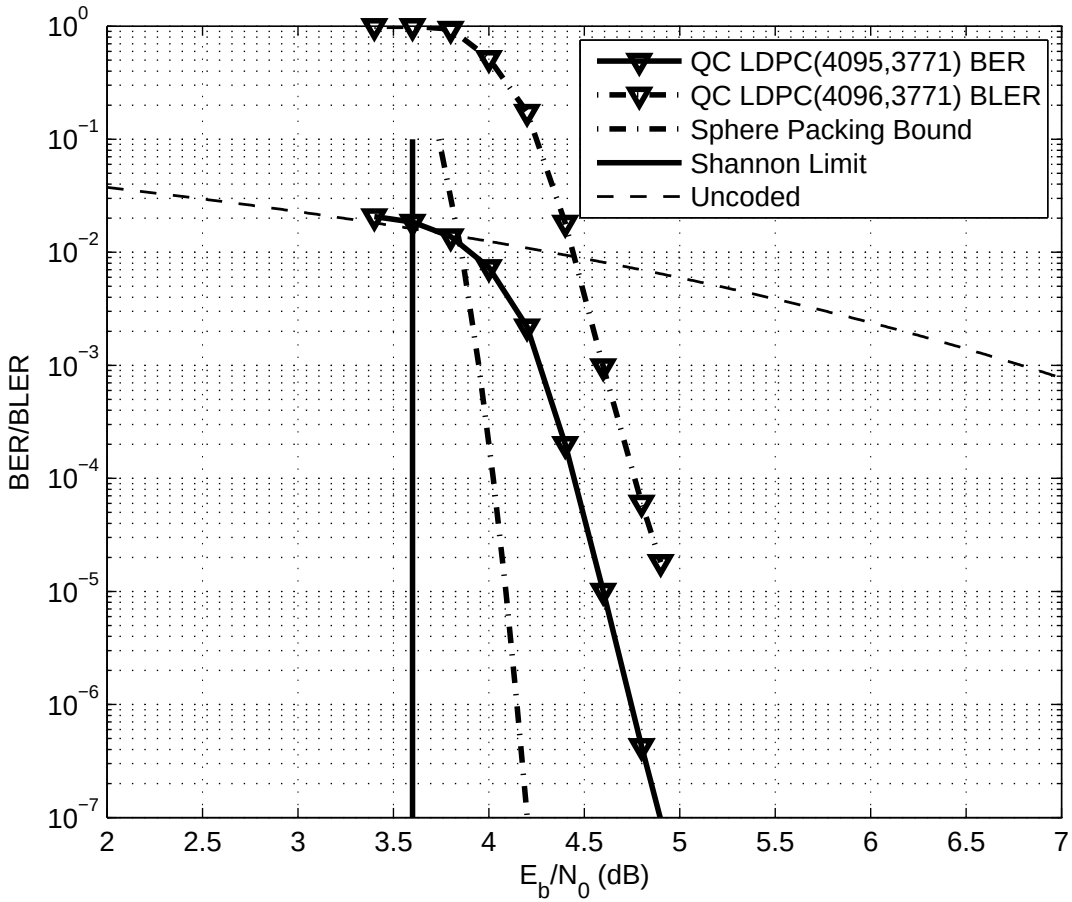

Figure 8: The bit and block error performance of the binary (4095,3771) QC-LDPC code given in Example 5.

A Very Low Error Floor QC-LDPC Code

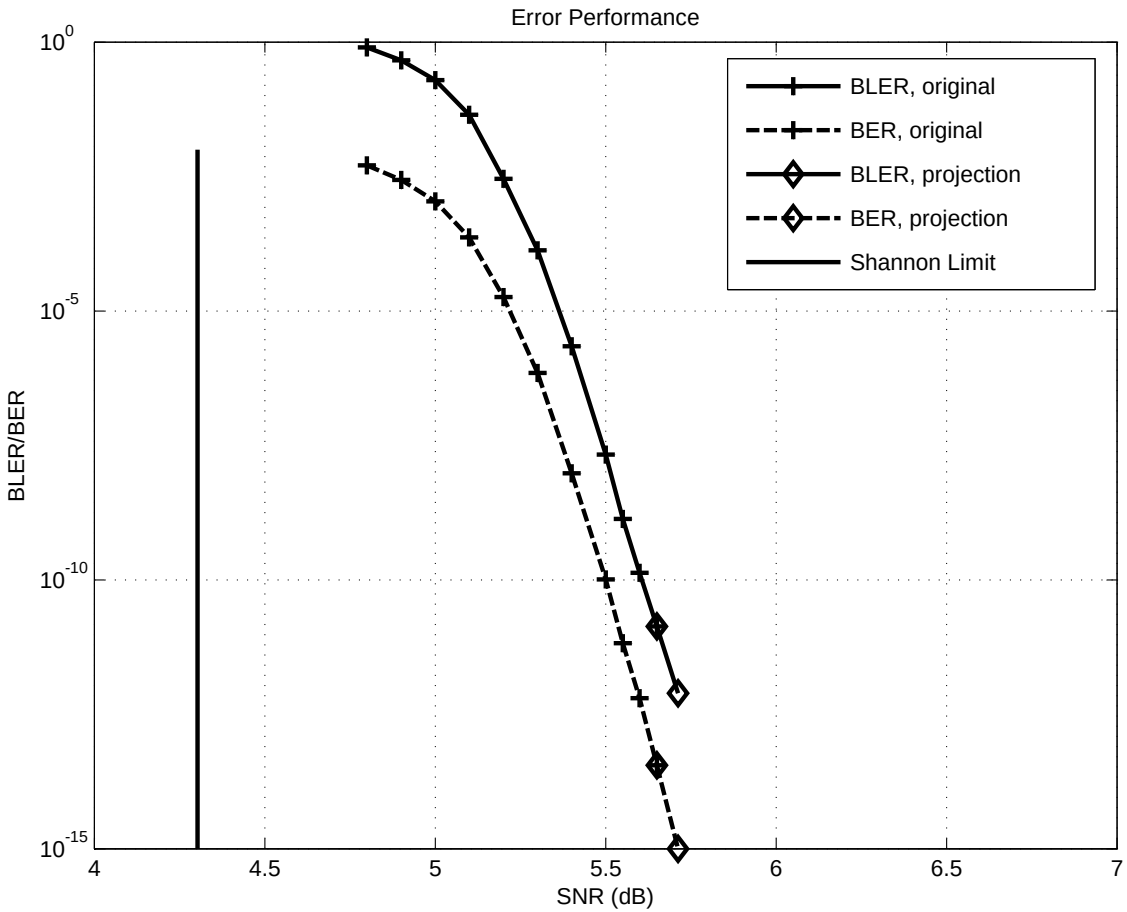

Figure 9: The bit and block error performances of the binary QC-LDPC code.

Algebraic LDPC Codes

- From late 1950's to early 1970's, finite fields were successfully used to develop algebraic coding theory and construct linear block codes, especially cyclic codes, with large minimum distances for hard-decision algebraic decoding, such as BCH codes, RS codes, Reed-Mueller codes, FG codes, quadratic codes, self-dual, Goppa codes and many others. These codes are called **classical codes**.
- Finite fields can also be used to construct Shannon capacity approaching LDPC codes, called **modern codes**.
- For any finite field GF(q), it is possible to construct a family of structurally compatible QC-LDPC codes of various lengths, rates and minimum distances, whose Tanner graphs have a girth of at least 6.
- Codes in the same family can be encoded with the same encoding circuit and decoded with the same decoding circuit.

A General Construction
Binary Matrix Dispersions of Field Elements

- Consider the Galois field GF(q). Let α be a primitive element of GF(q). Then,

$$\alpha^{-\infty} = 0, \alpha^0 = 1, \alpha, \alpha^2, \cdots, \alpha^{q-2}$$

  give all the q elements of GF(q) and $\alpha^{q-1} = 1$.

- For $0 \leq i < q-1$, let $\mathbf{P}^i$ denote the $(q-1) \times (q-1)$ circulant permutation matrix (CPM) over GF(2) whose top row has its single 1-component at the ith position. There are exactly $q-1$ CPMs over GF(2) and $\mathbf{P}^0$ is the $(q-1) \times (q-1)$ identity matrix.

- For the nonzero element α^i with $0 \leq i < q-1$, we represent it by the $(q-1) \times (q-1)$ CPM $\mathbf{P}^i$.

- This matrix representation is referred to as the $(q-1)$**-fold binary matrix dispersion** (or simply binary matrix dispersion) of α^i.
- The binary matrix dispersions of two different nonzero elements in GF(q) are different.
- Since there are exactly $q-1$ different $(q-1) \times (q-1)$ CPMs over GF(2), there is a **one-to-one correspondence** between a nonzero element of GF(q) and a $(q-1) \times (q-1)$ CPM. Therefore, each nonzero element of GF(q) is uniquely represented by a $(q-1) \times (q-1)$ CPM.
- For a nonzero element δ in GF(q), we use $\mathbf{B}(\delta)$ to denote its binary matrix dispersion. If $\delta = \alpha^i$, then $\mathbf{B}(\delta) = \mathbf{P}^i$.
- For the 0-element of GF(q), its matrix dispersion is defined as the $(q-1) \times (q-1)$ zero matrix.

A Row-Distance Constrained Matrix over a Finite Field

- Consider an $m \times n$ matrix over GF(q),

$$\mathbf{W} = \begin{bmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_{m-1} \end{bmatrix} = \begin{bmatrix} w_{0,0} & w_{0,1} & \cdots & w_{0,n-1} \\ w_{1,0} & w_{1,1} & \cdots & w_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ w_{m-1,0} & w_{m-1,1} & \cdots & w_{m-1,n-1} \end{bmatrix} \quad (1)$$

- We require the rows of $\mathbf{W}$ to satisfy the following constraint: For $0 \leq i, j < m$, $i \neq j$ and $0 \leq k, l < q - 1$, the Hamming distance between the two q-ary $(n-1)$-tuples, $\alpha^k \mathbf{w}_i$ and $\alpha^l \mathbf{w}_j$, is at least $n - 1$, (i.e., $\alpha^k \mathbf{w}_i$ and $\alpha^l \mathbf{w}_j$ differ in at least $n - 1$ places).
- The above constraint on the rows of matrix $\mathbf{W}$ is called the **α-multiplied row-distance (RD)-constraint**.
- $\mathbf{W}$ is called an **α-multiplied RD-constrained matrix**.

Binary Array Dispersion

- For $0 \leq i < m$ and $0 \leq j < n$, dispersing each nonzero entry $w_{i,j}$ of $\mathbf{W}$ into a binary $(q-1) \times (q-1)$ CPM $\mathbf{B}_{i,j} = \mathbf{B}(w_{i,j})$ over GF(2) and zero entry into a $(q-1) \times (q-1)$ zero matrix, we obtain the following $m \times n$ array of $(q-1) \times (q-1)$ CPMs and/or zero matrices over GF(2):

$$\mathbf{H}_b = \begin{bmatrix} \mathbf{B}_{0,0} & \mathbf{B}_{0,1} & \cdots & \mathbf{B}_{0,n-1} \\ \mathbf{B}_{1,0} & \mathbf{B}_{1,1} & \cdots & \mathbf{B}_{1,n-1} \\ \vdots & & \ddots & \vdots \\ \mathbf{B}_{m-1,0} & \mathbf{B}_{m-1,1} & \cdots & \mathbf{B}_{m-1,n-1} \end{bmatrix} \tag{2}$$

- $\mathbf{H}_b$ is called the binary $(q-1)$-fold array dispersion of $\mathbf{W}$. It is an $m(q-1) \times n(q-1)$ matrix over GF(2).

- The RD-constraint imposed on $\mathbf{W}$ ensures that $\mathbf{H}_b$ satisfies the RC-constraint. Hence, the associated Tanner graph of $\mathbf{H}$ has a girth of at least 6.

Binary QC-LDPC Codes

- For any pair (γ,ρ) of integers with $1 \leq \gamma \leq m$ and $1 \leq \rho \leq n$, let $\mathbf{H}_b(\gamma, \rho)$ be a $\gamma \times \rho$ subarry of $\mathbf{H}_b$.
- $\mathbf{H}_b(\gamma, \rho)$ is a $\gamma(q-1) \times \rho(q-1)$ matrix over GF(2) and satisfies the RC-constraint.
- The null space of $\mathbf{H}_b(\gamma, \rho)$ gives a binary QC-LDPC code $C_{b,qc}$ of length $\rho(q-1)$ with rate at least $(\rho - \gamma)/\rho$, whose Tanner graph have girth of at least 6.
- If $\mathbf{H}_b(\gamma, \rho)$ has constant column and row weights, then $C_{b,qc}$ is a regular binary QC-LDPC code.

Masking

- A set of CPMs in a chosen $\gamma \times \rho$ subarray $\mathbf{H}_b(\gamma, \rho) = [\mathbf{B}_{i,j}]$ of the array $\mathbf{H}_b$ given by (2) can be **replaced by a set of zero matrices**.
- This replacement is referred to as **masking**.
- Masking results in a sparser matrix whose associated Tanner graph has fewer edges and hence fewer short cycles and probably a larger girth than that of the associated Tanner graph of the original $\gamma \times \rho$ subarray $\mathbf{H}_b(\gamma, \rho)$.
- To carry out masking, we first design a sparse $\gamma \times \rho$ matrix $\mathbf{Z}(\gamma, \rho) = [z_{i,j}]$ over GF(2).

- Then take the following matrix product:

$$\mathbf{M}_b(\gamma, \rho) = \mathbf{Z}(\gamma, \rho) \times \mathbf{H}_b(\gamma, \rho) = [z_{i,j}\mathbf{B}_{i,j}],$$

  where $z_{i,j}\mathbf{B}_{i,j} = \mathbf{B}_{i,j}$ for $z_{i,j} = 1$ and $z_{i,j}\mathbf{B}_{i,j} = \mathbf{O}$ (a $(q-1) \times (q-1)$ zero matrix) for $z_{i,j} = 0$.

- We call $\mathbf{Z}(\gamma, \rho)$ the **masking matrix**, $\mathbf{H}_b(\gamma, \rho)$ the **base array** and $\mathbf{M}_b(\gamma, \rho)$ the **masked array**.

- Since the base array $\mathbf{H}_b(\gamma, \rho)$ satisfies the RC-constraint, the masked array $\mathbf{M}_b(\gamma, \rho)$ also satisfies the RC-constraint, **regardless** of the masking matrix.

- Hence, the associated Tanner graph of the masked matrix $\mathbf{M}_b(\gamma, \rho)$ has a girth of at least 6.

- The null space of the masked array $\mathbf{M}_b(\gamma, \rho)$ gives a new binary QC-LDPC code.

Classes of α-Multiplied RD-Constrained Matrices

- Suppose that $q-1$ can be factored as a product of two integers, c and n, that are relatively prime. Then $q-1=cn$.
- Let $\beta=\alpha^c$ and $\delta=\alpha^n$. Then the orders of β and δ are n and c, respectively.
- The sets $G_1=\{\beta^0=1,\beta,...,\beta^{n-1}\}$ and $G_2=\{\delta^0=1,\delta,...,\delta^{c-1}\}$ form two cyclic subgroups of the GF(q).
- $G(1)\cap G(2)=\{1\}$.
- If $q-1$ is a prime, we set $c=1$ and $n=q-1$ (or $c=q-1$ and $n=1$).

First Class

- For $0 \leq i, j < c$ and $\delta^{j-i} \in G_2$, form the following $n \times n$ matrix $\mathbf{W}_{i,j}$ over GF(q):

$$\mathbf{W}_{i,j} = \begin{bmatrix} \delta^{j-i}\beta^0 - \beta^0 & \delta^{j-i}\beta^0 - \beta^1 & \cdots & \delta^{j-i}\beta^0 - \beta^{n-1} \\ \delta^{j-i}\beta^1 - \beta^0 & \delta^{j-i}\beta^1 - \beta^1 & \cdots & \delta^{j-i}\beta^1 - \beta^{n-1} \\ \vdots & & \ddots & \vdots \\ \delta^{j-i}\beta^{n-1} - \beta^0 & \delta^{j-i}\beta^{n-1} - \beta^1 & \cdots & \delta^{j-i}\beta^{n-1} - \beta^{n-1} \end{bmatrix}. \quad (3)$$

The matrix $\mathbf{W}_{i,j}$ of has the following structural properties:

- The entries are formed based on one element δ^{j-i} in the cyclic subgroup G_2 and all the elements of the cyclic subgroup G_1.
- Each row is the right cyclic-shift of the row above it **multiplied** by β and the first row is the right cyclic-shift of the last row multiplied by β.
- Each column is the **downward** cyclic-shift of the column on its left multiplied by β and the first column is the downward cyclic-shift of the last column multiplied β.
- All the entries in a row (or a column) are distinct elements of GF(q).
- Any two rows (or columns) differ in every position.
- For $i \neq j$, all the entries in $\mathbf{W}_{i,j}$ are nonzero elements of GF(q).
- For $i = j$, the entries on the main diagonal of $\mathbf{W}_{i,i}$ are zeros and all the other entries are nonzero.

- $\mathbf{W}_{i,j}$ is an $n \times n$ β-multiplied circulant matrix over GF(q).

  Theorem 1: For $0 \leq i, j < c$, the $(q-1) \times (q-1)$ matrix $\mathbf{W}_{i,j}$ satisfies the α-multiplied RD-constraint.

- By array dispersion of $\mathbf{W}_{i,j}$ given by (3), we obtain the following $n \times n$ array of binary $(q-1) \times (q-1)$ CPMs and zero matrices:

$$\mathbf{H}_{i,j} = \begin{bmatrix} \mathbf{B}_{0,0}^{i,j} & \mathbf{B}_{0,1}^{i,j} & \cdots & \mathbf{B}_{0,n-1}^{i,j} \\ \mathbf{B}_{1,0}^{i,j} & \mathbf{B}_{1,1}^{i,j} & \cdots & \mathbf{B}_{1,n-1}^{i,j} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{B}_{n-1,0}^{i,j} & \mathbf{B}_{n-1,1}^{i,j} & \cdots & \mathbf{B}_{n-1,n-1}^{i,j} \end{bmatrix}. \tag{4}$$

- $\mathbf{B}_{0,0}^{i,j} = \mathbf{B}_{1,1}^{i,j} = \cdots = \mathbf{B}_{n-1,n-1}^{i,j} = \mathbf{O}$

Second Class

- For $0 \leq i, j < c$, use the $n \times n$ matrices $\mathbf{W}_{i,j}$'s as the building blocks to form the following $c \times c$ array:

$$\mathbf{W} = \begin{bmatrix} \mathbf{W}_{0,0} & \mathbf{W}_{0,1} & \cdots & \mathbf{W}_{0,c-1} \\ \mathbf{W}_{1,0} & \mathbf{W}_{1,1} & \cdots & \mathbf{W}_{1,c-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{W}_{c-1,0} & \mathbf{W}_{c-1,1} & \cdots & \mathbf{W}_{c-1,c-1} \end{bmatrix}, \tag{5}$$

  where for or $0 \leq i, j < c$, $\mathbf{W}_{i,j}$ is given by (7).

- $\mathbf{W}$ is composed of a $c \times c$ array of β-multiplied circulants over GF(q).

- It is an $n \times n$ matrix over GF(q) with entries on its main diagonal equal to zeros.

- **Theorem 2:** $\mathbf{W}$ satisfies the α-multiplied RD-constraint.

A Class of Binary QC-LDPC Codes

- By array dispersion of $\mathbf{W}$ given by (5), we obtain the following $c \times c$ array of $n \times n$ subarrays of binary $(q-1) \times (q-1)$ CPMs and zero matrices:

$$\mathbf{H}_b = \begin{bmatrix} \mathbf{H}_{0,0} & \mathbf{H}_{0,1} & \cdots & \mathbf{H}_{0,c-2} \\ \mathbf{H}_{1,0} & \mathbf{H}_{1,1} & \cdots & \mathbf{H}_{1,c-2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{H}_{c-1,0} & \mathbf{H}_{c-2,1} & \cdots & \mathbf{H}_{c-2,c-2} \end{bmatrix} \tag{6}$$

- $\mathbf{H}_b$ is a $(q-1) \times (q-1)$ array of $(q-1) \times (q-1)$ CPMs and zero matrices with zero matrices on the main diagonal of $\mathbf{H}_b$. The zero matrices are on the main diagonal $\mathbf{H}_b$.
- $\mathbf{H}_b$ is a $(q-1)^2 \times (q-1)^2$ matrix over GF(2) with both column and row weights $q-1$.
- Since $\mathbf{W}$ satisfies the α-multiplied RD-constrained, $\mathbf{H}_b$ satisfies the RC-constraint.
- Consequently, the associated Tanner graph of $\mathbf{H}_b$ has a girth of at least 6.
- The rank of $\mathbf{H}_b$ is $3^m - 3$.

- For any pair (γ, ρ) of integers with $1 \leq \gamma, \rho < q$, let $\mathbf{H}_b(\gamma, \rho)$ be a $\gamma \times \rho$ subarray of $\mathbf{H}_b$. $\mathbf{H}_b(\gamma, \rho)$ is a $\gamma(q-1) \times \rho(q-1)$ matrix over GF(2) and it also satisfies the RC-constraint.
- The null space of $\mathbf{H}_b(\gamma, \rho)$ gives a binary QC-LDPC code $C_{b,qc}$ of length $\rho(q-1)$ with rate at least $(\rho - \gamma)/\rho$ and minimum distance at least $\gamma + 1$,whose Tanner graph has a girth of at least 6.
- If $\mathbf{H}_b(\gamma, \rho)$ does not contains any zero matrix of $\mathbf{H}_b$, it has constant column and row weights, γ and ρ, respectively. Then $C_{b,qc}$ is a binary (γ,ρ)-regular QC-LDPC code.
- For a given finite field GF(q), the above construction gives a family of structurally compatible binary QC-LDPC codes.

A Special Sub-Class of Binary QC-LDPC Code

- For $q = 2^m$, the binary QC-LDPC code given by the null space of the entire array $\mathbf{H}_b$ has:

  Length = $(2^m - 1)^2$

  Dimension = $(2^m - 1)^2 - 3^m + 3$

  Minimum distance $\geq 2^m$

- This code denoted by $C_{b,qc,f}$, not only performs well with iterative decoding using the SPA but also offers effective trade-offs between error performance and decoding complexity when it is decoded with **bit-flipping** (BF), **weighted BF** (WBF) and other **reliability-based binary message-passing** (BMP) decoding algorithms.

Example 3

- Let GF(2^6) be the field for code construction. Let α be a primitive element of GF(2^6).
- Factor $2^6 - 1 = 63$ as the product of $c = 7$ and $n = 9$. Let $\beta = \alpha^7$ and $\delta = \alpha^9$.
- Let $\mathbf{G}_1 = \{\beta^0 = 1, \beta, ..., \beta^8\}$ and $\mathbf{G}_2 = \{\delta^0 = 1, \delta, ..., \delta^6\}$ be two cyclic subgroups of GF(2^6) generated by β and δ, respectively.
- Based on (3) and (6), we form a α-multiplied RD-constrained 64×64 matrix $\mathbf{W}$ over GF(2^6) which consists of 7×7 array of 9×9 submatrices $\mathbf{W}_{i,j}$'s over GF(2^6).
- Dispersing the entries of $\mathbf{W}$, we obtain a 63×63 array $\mathbf{H}_b$ of 63×63 CPMs and zero matrices.

- For any pair (γ, ρ) of positive integers, with $1 \leq \gamma, \rho \leq 64$, the null space of any $\gamma \times \rho$ subarray $\mathbf{H}_b(\gamma, \rho)$ of $\mathbf{H}_b$ gives a binary QC-LDPC code of length 63ρ.

- Choose $\gamma = \rho = 63$.
- $\mathbf{H}_b(63, 63) = \mathbf{H}_b$ is a 3969×3969 RC-constrained matrix over GF(2) with both column and row weights equal to 62. The rank of this matrix is $3^6 - 3 = 726$.
- The null space of $\mathbf{H}_b$ gives a (3969,3243) QC-LDPC code with minimum distance at least 63.
- The performance of this code with 5, 10 and 50 iterations of the SPA is shown in Figure 3.
- Decoding of this code converges very fast.

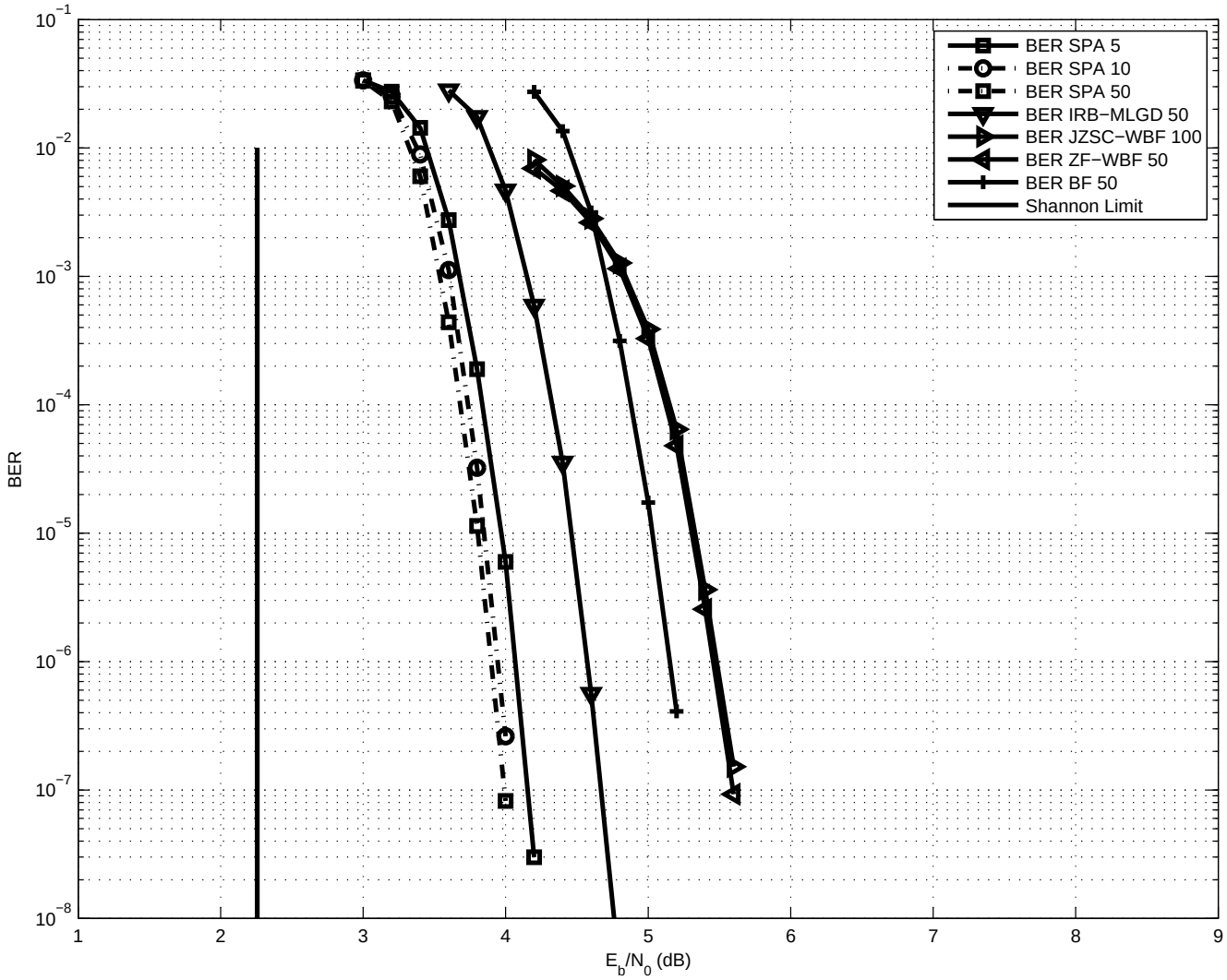

Figure 3: Error performance of (3969,3243) QC-LDPC code.

Example 4

- Let GF(2^9) be the code construction field. Let α be a primitive element of GF(2^6).
- Factor $2^9 - 1 = 511$ as the product of $c = 7$ and $n = 73$. Let $\beta = \alpha^7$ and $\delta = \alpha^{73}$.
- Based on (4) to (7), we construct a 511×511 array $\mathbf{H}_b$ of 511×511 CPMs and zero matrices.
- Choose $\gamma = 63$ and $\rho = 126$. Take a 63×126 subarray $\mathbf{H}_b(63, 126)$ from $\mathbf{H}_b$, avoiding the zero matrices.

- Construct a masking matrix $\mathbf{Z}(63, 126)$ with column and row weight distributions closed to the following variable- and check-node degree distributions of the Tanner graph of a code designed for rate 1/2 using density evolution (with adjustment).

$$\gamma(X) = 0.4524X + 0.3492X^2 + 0.1587X^7 + 0.0397X^9$$

$$\rho(X) = 0.1746X^7 + 0.8254X^8$$

- Masking $\mathbf{H}_b(63, 126)$ with $\mathbf{Z}(63, 126)$, we obtained a masked array $\mathbf{M}_b(63, 126)$ of 511×511 CPMs and zero matrices.
- $\mathbf{M}_b(63, 12)$ is a 32193×64386 matrix over GF(2).
- The null space of $\mathbf{M}_b(63, 128)$ gives a (64386,32193) QC-LDPC code whose performance over the AWGN channel decoded with 50 iterations of the SPA is shown in Figure 2(a).
- At the BER of 10^{-8}, the code performs 0.55 dB from the Shannon limit.

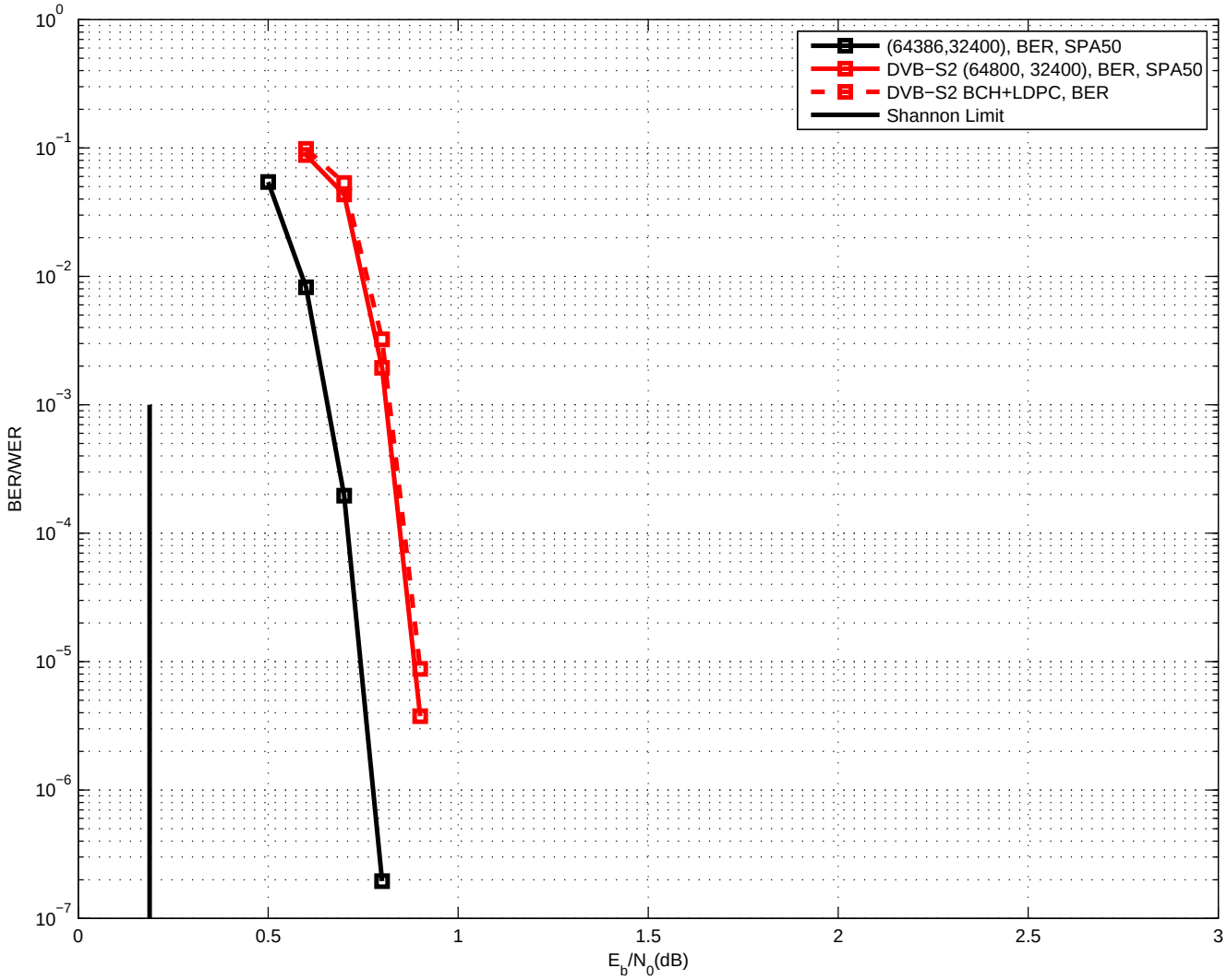

Figure 4: Error performance of (64386,32193) LDPC code over AWGN channel.

- Also included in Figure 4 is the performance of the DVB S-2 standard (64800,32400) LDPC code with and without a BCH outer code.
- The DVB S-2 LDPC code is an **IRA** (irregular repeat-accumulated) code. The BCH code is a (32400,32208) shortened BCH code with error-correction capability 12.
- The BCH outer code is used to push down the error-floor of the DVB S-2 code.
- The (64386,32193) QC-LDPC code outperforms DVB S-2 code by 0.15 dB with or without the BCH outer code.

- The performance of the (64386,32193) QC-LDPC code over the BEC is shown in Figure 5.
- At the unresolved erasure bit rate (UEBR) of 10^6, the code performs 0.053 bit per channel usage from the Shannon limit 0.5.

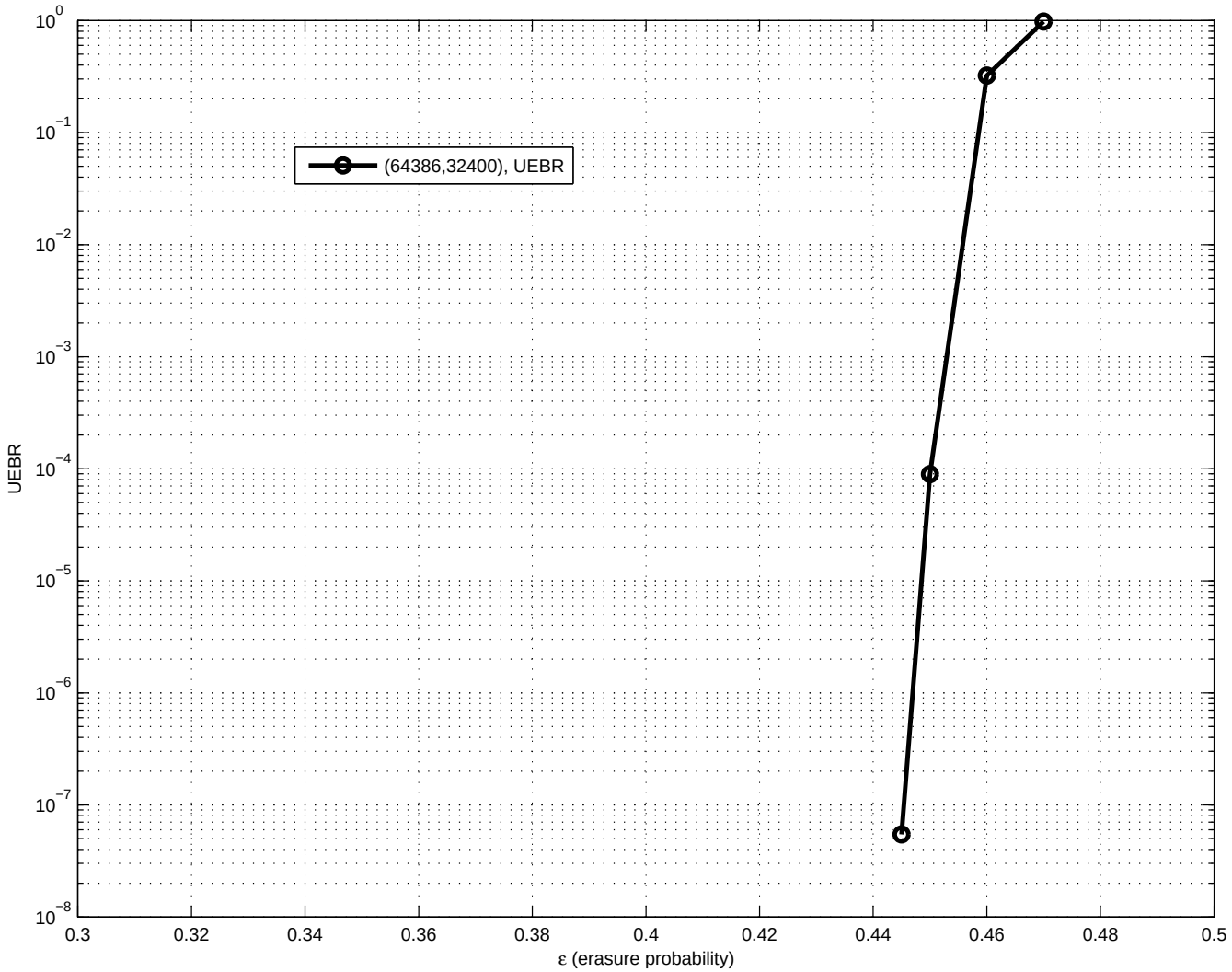

Figure 5: Error performance of (64386,32193) LDPC code over BEC.

A Special Case

- Consider the special case for which $c = 1$ and $n = q - 1$. In this case, $\beta = \alpha, \delta = 1$ and the RD-constrained α-multiplied matrix has the following form

$$\mathbf{W} = \mathbf{W}_{0,0} = \begin{bmatrix} 1-1 & 1-\alpha & \cdots & 1-\alpha^{q-2} \\ \alpha-1 & \alpha-\alpha & \cdots & \alpha-\alpha^{q-2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{q-2}-1 & \alpha^{q-2}-\alpha & \cdots & \alpha^{q-2}-\alpha^{q-2} \end{bmatrix}. \quad (7)$$

Example 5

- Code construction field: GF(73).
- Base matrix for array dispersion $\mathbf{W}$: 72×72 matrix over GF(73).
- Disperse $\mathbf{W}$ into a 72×72 array $\mathbf{H}_b$ of 72×72 CPMs.
- Take a 32×64 subarray $\mathbf{H}_b(32, 64)$ from $\mathbf{H}_b$.
- Construct a 32×64 masking matrix $\mathbf{Z}(32, 64) = [\mathbf{G}_1 \mathbf{G}_2]$ over GF(2) which consists of two 32×32 circulants with generators,

$$\mathbf{g}_1 = (10100100000000000000000000000000),$$

$$\mathbf{g}_2 = (10000010000000100000000000000000).$$

- Masking $\mathbf{H}_b(32, 64)$ with $\mathbf{Z}(32, 64)$ results in a 32×64 masked array $\mathbf{M}_b(32, 64)$ which is a 2304×4608 matrix with column and row weights 3 and 6, respectively.
- The null space of $\mathbf{M}_b(32, 64)$ gives a (3,6)-regular (4608,2304) QC-LDPC code.
- The performance of the code is shown in Figure 6.
- No error-floor down to the BER of 5×10^{-10}.

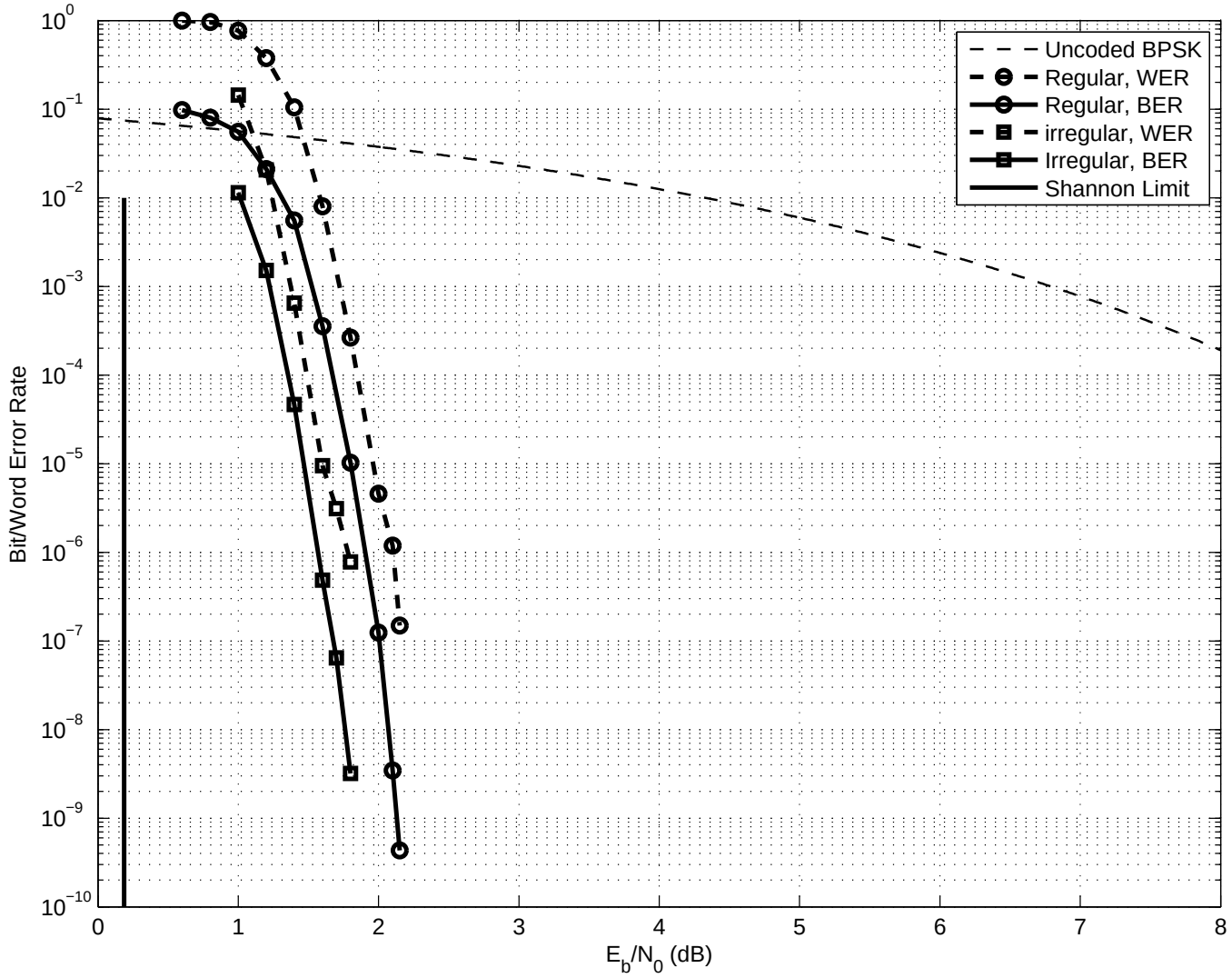

Figure 6: Error performance of (3,6)-regular (4608,2304) QC-LDPC code.

- An irregular version of this code will be used as the MMB T-2 standard code.

Example 6

- Code construction field: GF(271).
- Code: a (6,90)-regular (16200,15125) QC-LDPC code with rate 0.9336.
- Performance: See Figure 7. There is no error-floor down to 10^{-12}.
- Possible applications: being considered for applications in two high-rate and low error-rate systems.

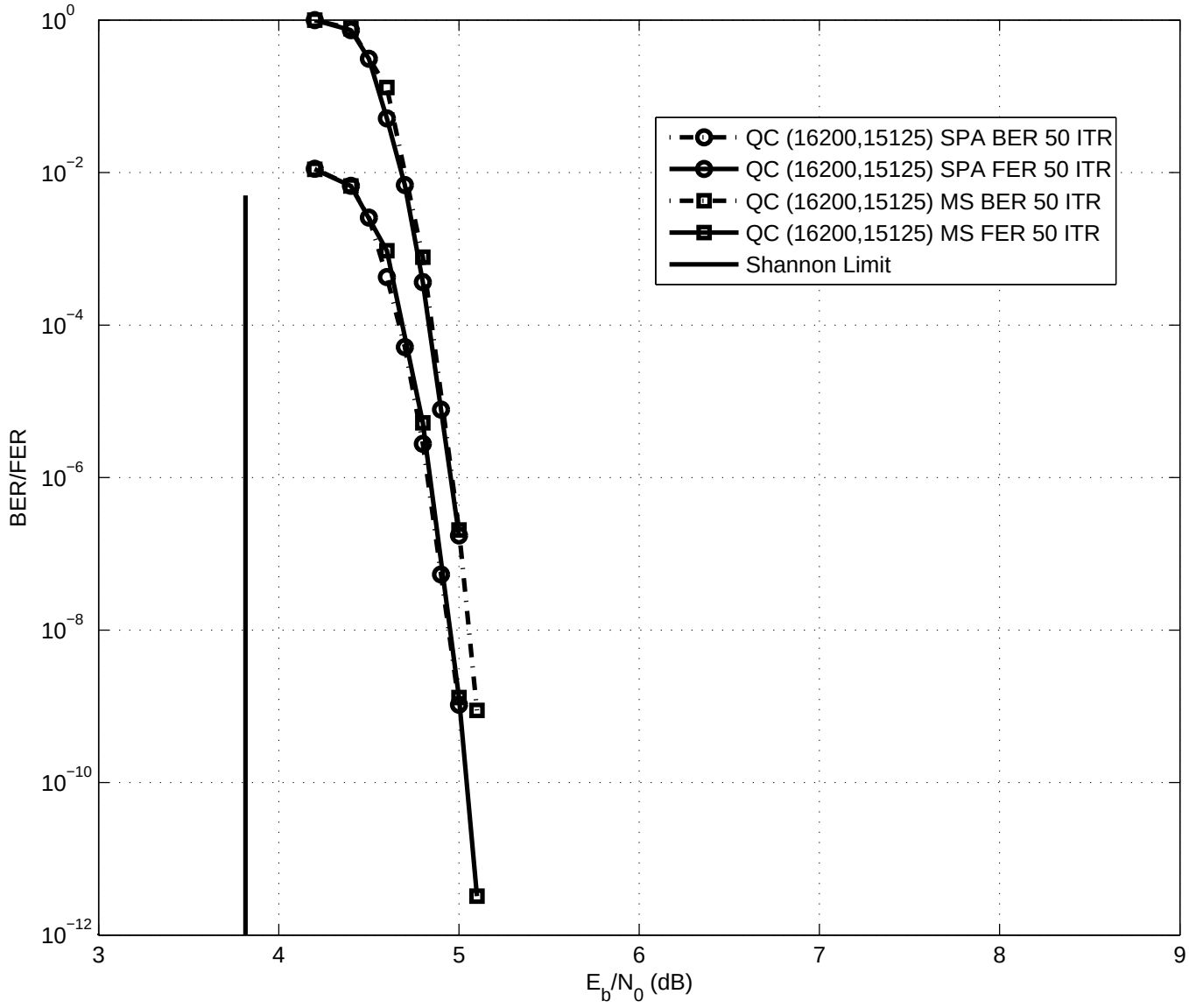

Figure 7: Error performance of (6,90)-regular (16200,15125) QC-LDPC code.

Conclusion and Remarks

- Conclusion and Remarks