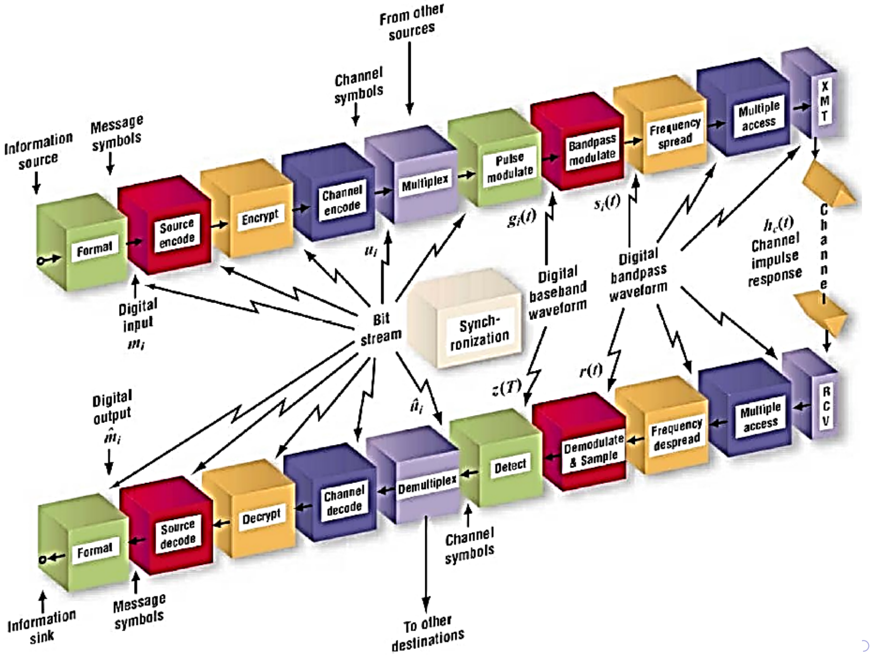
Capacity-Approaching Low-Density Parity-Check Codes: Recent Developments and Applications

Shu Lin

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


From other sources
Channel symbols
Message symbols
Information source
Format
Source encode
Encrypt
Channel encode
Multiplex
Pulse modulate
Bandpass modulate
Frequency spread
Multiple access
X M T
u_i
$g_i(t)$
$s_i(t)$
Digital input m_i
Bit stream
Synch-ronization
Digital baseband waveform
Digital bandpass waveform
$h_c(t)$ Channel impulse response
Channel
$z(T)$
$r(t)$
$\hat{u}_i$
Digital output $\hat{m}_i$
Format
Source decode
Decrypt
Channel decode
Demultiplex
Detect
Demodulate & Sample
Frequency despread
Multiple access
R C V
Information sink
Message symbols
Channel symbols
To other destinations

I. Introduction

- Channel coding is an important element in every communication or data storage system.
- The objective of channel coding is to provide reliable information transmission and storage.
- Shannon Channel Coding Theorem (1948).
- Over the last 60 years, various types of codes and methods for correcting transmission errors over a wide spectrum of communication and storage channels have been constructed and devised.

- 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 [2].

[1] R. G. Gallager, "Low density parity-check codes," *IRE Trans. Inf. Theory*, vol. 8, no. 1, pp. 21-28, Jan. 1962.

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

- Resurrected in the late 1990's by MacKay [3],[4], Luby [5] and others [6],[7],[8].
- 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.

[3] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *Electro. Lett.*, vol. 32, no. 2, pp. 1645–1646, Aug. 1996.

[4] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 399–431, Mar. 1999.

[5] J. Byers, M. Luby, M. Mitzenmacher, and A. Rege, "A digital fountain approach to reliable distribution of bulk data," *Proc. ACM SIGCOMM '98*, Vancouver, BC, Canada, Jan. 1998, pp. 56-67.

[6] Y. Kou, S. Lin, and M. Fossorier, "Low density parity check Codes based on finite geometries: A rediscovery," in *Proc. IEEE Int. Symp. Inf. Theory*, Sorrento, Italy, June 25-30, 2000.

[7] Y. Kou, S. Lin, and M. P. C. Fossorier, "Low-density parity-check codes based on finite geometries: A rediscovery and new results," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2711-2736, Nov. 2001.

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

- Many LDPC codes have been adopted 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 2: 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.

- 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.
- Based on quasi-cyclic structure, a reduced complexity iterative decoding algorithm can be devised, which significantly reduces the hardware implementation complexity of a QC-LDPC decoder in terms of the number of message processing units and the number of wires required to connect the message processing units.
- A cyclic LDPC code can be put in QC form through column and row permutations [9]. 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.

[9] Q. Huang, Q. Diao, S. Lin, and K. Abdel-Ghaffar, “Cyclic and quasi-cyclic LDPC codes on constrained parity-check matrices and their trapping sets,” *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2648-2671, May 2012.

Well Known Structured LDPC Codes

1. Partial geometry codes
2. Finite field codes
3. Algebraic geometry codes
4. Codes based on combinatorial (or experimental) designs
5. Superimposed codes

Well Known Structured LDPC Codes

6. Graph-theoretic codes: **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 partial or algebraic geometries, finite fields and combinatorial mathematics.
- Partial geometry LDPC codes constructed based on Euclidean and projective geometries are the first class of structured codes ever constructed. They are cyclic LDPC codes [7],[8].
- Recently, a large class of cyclic LDPC codes has been constructed based on cyclic finite geometry codes by decomposition [9].
- 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.

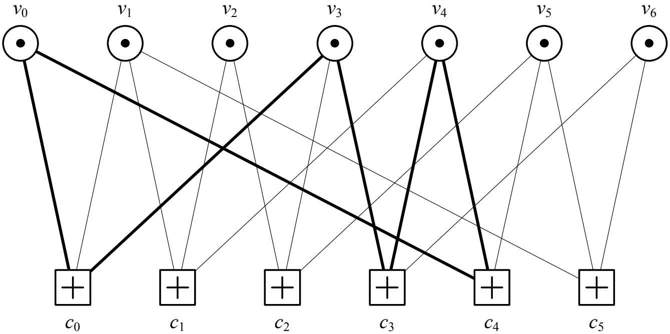


Figure 3: A Tanner graph to demonstrate its cycles.

- 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 algorithm** (MSA)
- **Revolving iterative decoding** (RID) **algorithm** (New)
- **Binary message-passing** (BMP) **algorithm**
- **Iterative majority-logic decoding** (IMLGD) **algorithm**
- **Bit-flipping** (BF) **algorithm**
- **Weighted-BF** (WBF) **algorithm**

- 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.
- The RID is devised for decoding LDPC codes whose parity-check matrices have block cyclic structure to reduce decoder complexity with no or small 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
- FFT-RID
- Reliability-Based Message-Passing Algorithms
- Min-Max Algorithm

VI. Measure of Performance

- The performance of an LDPC code with iterative decoding 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 (how fast the decoding process terminates),
  3) Error-floor (how low the error rate can achieve).

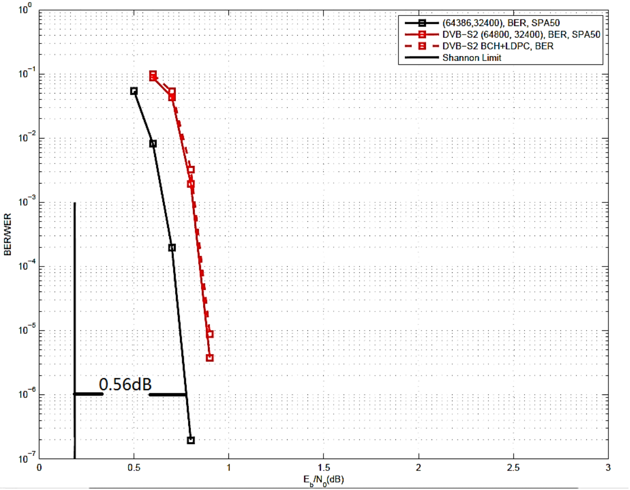


Figure 4: Error performances of a masked (64386,32193) QC-LDPC code and the DVB-S2 code over the AWGN channel.

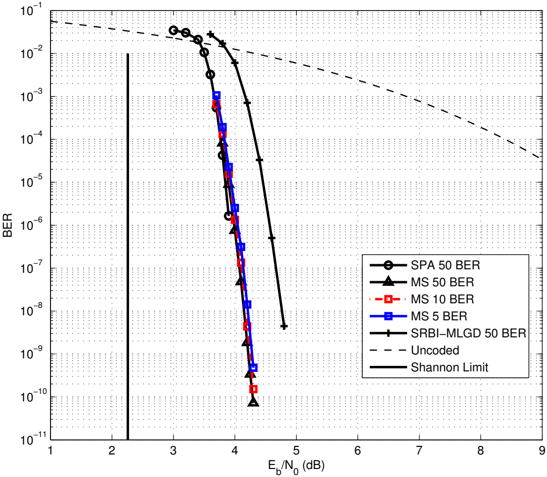


Figure 5: Bit error performances of the binary (4095,3367) cyclic EG-LDPC code decoded with the SPA and the scaled MS-algorithm.

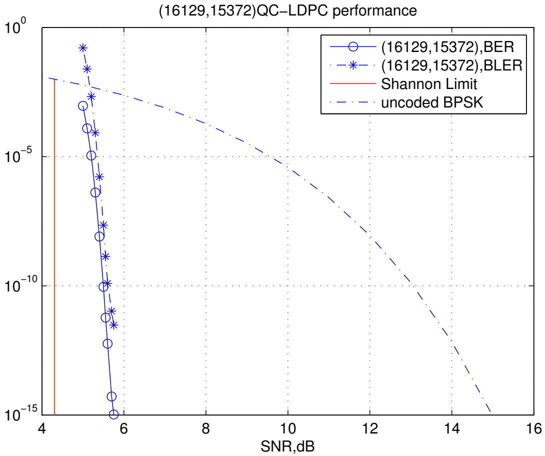


Figure 6: The bit and block error performances of a binary QC-LDPC code with rate 0.953.

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**).

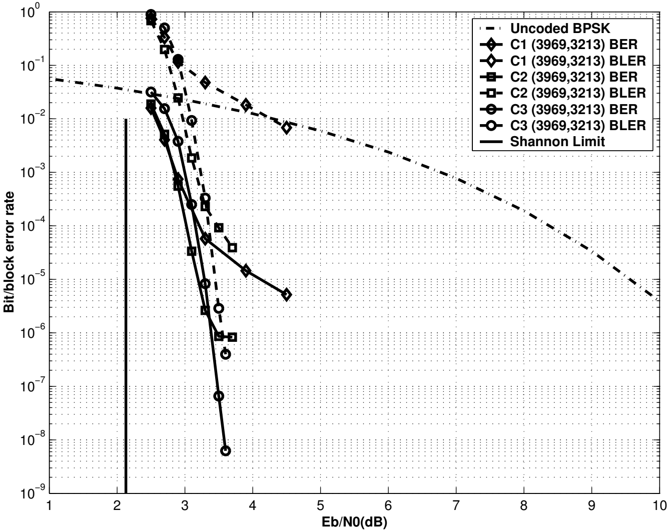


Figure 7: A figure to demonstrate the error floor phenomenon.

- 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, such as optical communication and flash memory.
- 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. **variable node (VN) connectivity** (or structure);

5. **row redundancy** of the parity-check matrix;
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 (partial geometries in a broad sense)
- Construction based algebraic geometries
- 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 integer sequences

- 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.
- Algebraic LDPC codes in general have lower error-floor and their decoding converges faster than graph-theoretic-based LDPC codes.

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 two-dimensional Euclidean geometries over finite fields.
- Let the 2-dimensional Euclidean geometry, EG(2,q), over GF(q) be the code construction geometry.
- This geometry consists of q^2 point and $q^2 + q$ lines. Each line consists of q points. Any two points are connected by a unique line. Two lines are either parallel or they intersect at one and only one point. Any point is intersected by $q + 1$ lines.

- 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$(2, q)$ not passing through the origin.
- $\mathbf{H}_{EG}$ can be arranged as a column of circulants of size $(q^2 - 1) \times (q^2 - 1)$.
- $\mathbf{H}_{EG}$ satisfies the RC-Constraint.

A Special Subclass of Cyclic EG-LDPC Codes

- 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 $q+1$.
- 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 $q = 2^s$, 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 $d_{min} = 2^s + 1$.
- Its 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 $2^s + 1$.

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, 5) hard-reliability-based binary message-passing (HRB-BMP) decoding, and 6) RID.
- 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 8.

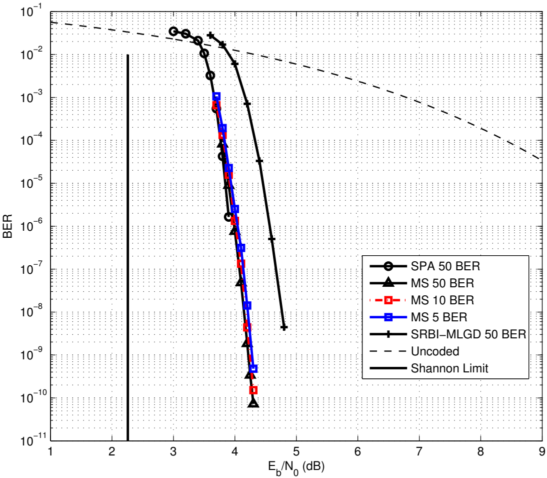


Figure 8: Bit error performances of the binary (4095,3367) cyclic EG-LDPC code given in Example 2 decoded with the SPA and the scaled MS-algorithm.

X. A 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 $\mathbf{H}_{EG,qc}$ of circulants of size $(q - 1) \times (q - 1)$.
- Each circulant in $\mathbf{H}_{EG,qc}$ 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 $\mathbf{H}_{EG,qc}$ consists of q CPMs and one zero matrix.

- The null space of $\mathbf{H}_{EG,qc}$ 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 $\mathbf{H}_{EG,qc}(\gamma, \rho)$ be a $\gamma \times \rho$ subarray of $\mathbf{H}_{EG,qc}$.
- The null space of $\mathbf{H}_{EG,qc}(\gamma, \rho)$ gives a QC-LDPC code of length $n = \rho(q-1)$.
- The above decomposition and construction give a large class of QC-EG-LDPC codes with various lengths, rates and minimum distances.

A Very Low Error Floor QC-LDPC Code

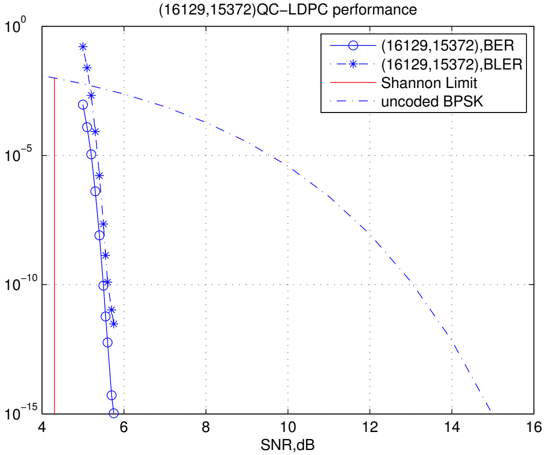


Figure 9: The bit and block error performances of a binary QC-LDPC code with rate 0.953.

Example 2

NASA Standard Code for LANDSAT and Cruise Exploration Shuttle Mission

- A (8176,7156) QC-EG-LDPC code with rate 7/8.
- The performance of this code is shown in Figure 10.
- Beautiful waterfall performance and no error-floor down to the BER of 10^{-14}.

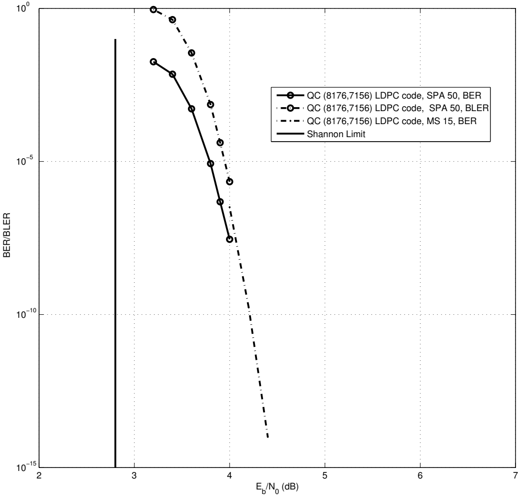
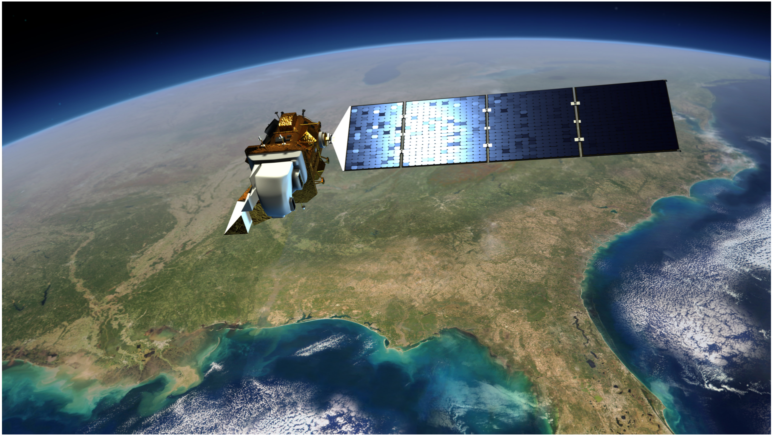


Figure 10: The error performances of the binary (8176,7156) QC-LDPC code.

- This code is used by NASA-USA in the Landsat Data Continuity Mission. The satellite was successfully launched on February 13, 2013. The code is used for downlink data transmission in the X-band.
- This 384 Mbps data rate communications link is NASA's first operational use of an LDPC and is the first use of an LDPC code for a space to ground link for any agency or company.
- The next mission to use this LDPC code is IRIS: http://science.nasa.gov/missions/iris/.
- It will be launched in April, 2013.
- Goes-R will follow in 2015: http://www.goes-r.gov/.



Other Applications

- New NASA Tracking and Data Relay Satellite Service (TDRSS): high-rate 1.0 and 1.5 Gbps return link Service.
- The 1.0 Gbps Deformation, Ecosystem Structure and Dynamics of Ice (DESynl) mission.
- Surface Water Ocean Topography (SWOT).
- Hyperspectral Infrared Imager (HyspIRI).

IX. QC-LDPC Codes on Finite Fields

- From late 1950s to early 1960s, 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-Muller 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.

Code Construction by Binary Matrix Dispersions of Field Elements

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

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

  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 i-th 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 that the rows of $\mathbf{W}$ satisfies the following constraint: every 2×2 submatrix of $\mathbf{W}$ contains at least one zero entry or is non-singular.
- This constraint is referred to as 2×2 submatrix constraint.

Binary Array Dispersion

- For $0 \le i < m$ and $0 \le j < n$, 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):

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

- $\mathbf{H}_b$ 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).

Binary Array Dispersion(Continued)

- The 2×2 submatrix constraint on the base matrix $\mathbf{W}$ ensures that $\mathbf{H}_b$ satisfies the RC-constraint. Hence the Tanner graph of the code given by the null space of $\mathbf{H}_b$ 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 $\gamma \times \rho$ subarray 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 codes $\mathcal{C}_{b,qc}$ of lenth $\rho(q-1)$ with rate at least $\frac{\rho-\gamma}{\rho}$, whose Tanner graph have girth of at least 6.
- If $\mathbf{H}_b(\gamma, \rho)$ has constant column and row weights, then $\mathcal{C}_{b,qc}$ 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.

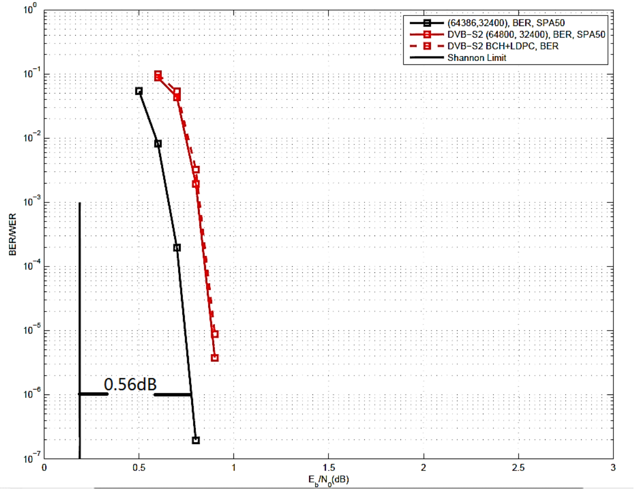


Figure 11: Error performances of a masked (64386,32193) QC-LDPC code and the DVB-S2 code over the AWGN channel.

Construction of QC-LDPC Codes Based on Latin Squares over Finite Fields

Definition: A Latin square of order n is an $n \times n$ array in which each row and each column contains every element of a set of n distinct objects. The following $q \times q$ array is a Lain square over $GF(q)$:

$$\mathbf{W} = \begin{bmatrix} \alpha^0 - \alpha^0 & \alpha^0 - \alpha & \dots & \alpha^0 - \alpha^{q-2} & \alpha^0 - 0 \\ \alpha - \alpha^0 & \alpha - \alpha & \dots & \alpha - \alpha^{q-2} & \alpha - 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha^{q-2} - \alpha^0 & \alpha^{q-2} - \alpha & \dots & \alpha^{q-2} - \alpha^{q-2} & \alpha^{q-2} - 0 \\ 0 - \alpha^0 & 0 - \alpha & \dots & 0 - \alpha^{q-2} & 0 - 0 \end{bmatrix}. \quad (3)$$

This matrix satisfies the 2×2 submatrix constraint and hence can be used as a base matrix for constructing RC-Constrained QC-LDPC code.

- Construct a $q \times q$ RC-constrained array H of circulant permutation and zero matrices of size $(q-1) \times (q-1)$.
- From this array, a family RC-constrained QC-LDPC code can be constructed. They are suitable for various types of message-passing decoding and OSMLGD to provide a wide range of trade-offs between performance and decoding complexity.
- For $q = 2^r$, the rank of $\mathbf{H}$ is $3^r - 1$. $\mathbf{H}$ has a large row redundancy, $4^r - 3^r - 2^r + 1$ redundant rows.
- The code given by the null space of $\mathbf{H}$ has the following parameters: length $n = 2^r(2^r - 1)$, dimension $k = 4^r - 3^r - 2^r + 1$, minimum distance at least 2^r. Again, its Tanner graph has no trapping set with size smaller than 2^r.

Example

- Code Construction Field: GF(181).
- Code: a (6,90)-regular (16200,15125) QC-LDPC code with rate 0.9336.
- Performance: See Figure 12. There is no error-floor down to 10^{-12}.
- Possible application: being considered for application in two high-rate and low error-rate systems.

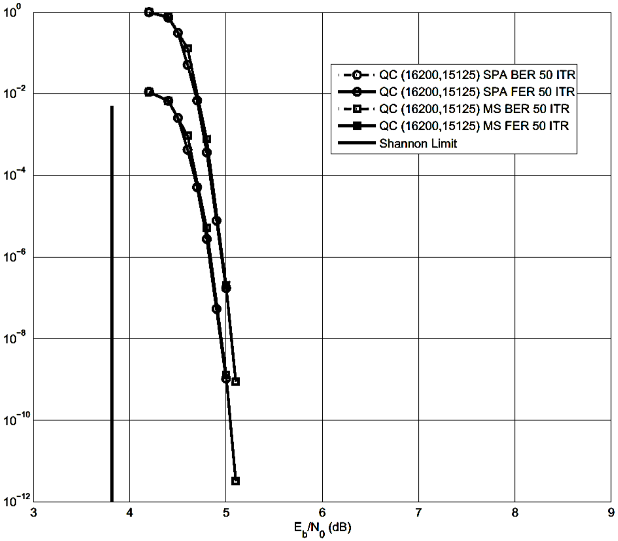


Figure 12: Error performances of (6,90)-regular (16200,15125) QC-LDPC code.

X. Possible Research Directions

- Further structure analysis for better understanding of algebraic LDPC codes, especially the structural properties that affect the error performance of an algebraic LDPC code and facilitate the implementation complexity of its decoder.
- Further performance analysis, especially the rate of decoding convergence and error-floor.
- Nonbinary LDPC codes and effective decoding algorithms
- Decoder design to reduce power consumption and to increase decoding throughput.

X. Possible Research Directions

- Effective iterative decoding algorithms for Reed-Solomon codes.
- Concatenation with LDPC codes as inner codes.
- Graph-theoretic approach to the construction LDPC codes from combinatorial point of view (codes on graph).
- LDPC codes vs. polar codes.
- Application to flash memory.

白雲
許家尚寫
於庚午之夏

Thank you!