# Minimum Distance Bounds for Irregular QC-LDPC Codes and their Applications

**Min-Ho Shin, Joon-Sung Kim, Hong-Yeop Song**

**July 1, ISIT 2004, Chicago**

**Coding & Information Theory Laboratory**
**Dept. of Electrical and Electronic Engineering**
**Yonsei University Seoul, Korea**

# Contents

- **Introduction**
- **Tanner's Minimum Distance Bounds**
- **Quasi-Cyclic LDPC Codes**
- **Minimum Distance Bounds for QC-LDPC Codes**
  - Bit-Oriented Bound
  - Parity-Oriented Bound
- **Code Construction Examples**
- **Simulation Results**
- **Conclusions**

# Introduction

- **Tanner's minimum distance bounds**
  - Minimum distance bound for regular codes
  - Using these bounds, we can find good regular LDPC codes which are good in terms of the distance property.
  - Applicable only to regular LDPC codes

- **Quasi-Cyclic LDPC codes**
  - Constructed from circulant submatrices
  - The encoding complexity is almost as low as cyclic codes.

=> We will derive minimum distance bound for irregular QC-LDPC codes using a similar technique to Tanner's bound.

# Tanner's Minimum Distance Bounds

- **Tanner's minimum distance bounds**
  - Minimum distance bound for a regular code with an $m \times n$ parity check matrix **H**
  - Let $\gamma$ be the fixed column weight and $\rho$ be the fixed row weight of **H.**
  - Let $\mu_1, \mu_2$ be the largest and the second largest eigenvalues of $\mathbf{HH}^T$.
  - bit-oriented bound

$$d \geq \frac{n(2\gamma - \mu_2)}{\mu_1 - \mu_2}$$

  - parity-oriented bound

$$d \geq \frac{2n(2\gamma + \rho - 2 - \mu_2)}{\rho(\mu_1 - \mu_2)}$$

  - Tanner set up a heuristic rule that a code with a smaller ratio of second to first eigenvalues will have a good distance property.

- **Example**
  - A rate 4/9 (9,2,3)-regular LDPC code with $\mu_1 = 6$ and $\mu_2 = 3$
  - The bit-oriented bound gives $d \geq 3$
  - The parity-oriented bound gives $d \geq 4$
  - The actual minimum distance is $d = 4$
  - In this case, the parity-oriented bound gives the true minimum distance.

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

## QC-LDPC Codes

- A block code is said to be quasi-cyclic if a cyclic shift of any codeword by $p$ places is still a codeword
- We consider QC codes with following structure

$$\mathbf{H} = [\mathbf{H}_1, \mathbf{H}_2, \cdots, \mathbf{H}_p]$$

  where $\mathbf{H}_1, \mathbf{H}_2, \cdots, \mathbf{H}_p$ are $m \times m$ circulant matrices

- Each circulant matrix $\mathbf{H}_i$ is described by the associated polynomial

$$h_i(x) = \sum_{j=0}^{m-1} (\mathbf{H}_i)_{0j} x^j$$

  corresponding to the top row of $\mathbf{H}_i$

$$\mathbf{H}_i = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix} \Leftrightarrow h_i(x) = 1 + x^2 + x^3$$

# Minimum Distance Bounds for QC-LDPC Codes

## Theorem 1. Bit-oriented bound

- Let $\mu_1 > \mu_2 > \cdots > \mu_s$ be the ordered distinct eigenvalues of real valued matrix $\mathbf{H}^T\mathbf{H}$, where $\mathbf{H} = [\mathbf{H}_1, \mathbf{H}_2, \cdots, \mathbf{H}_p]$ and $\mathbf{H}_i$ is an $m \times m$ circulant matrices which has constant row weight $\omega_i$ ,$1 \le i \le p$, with $\omega_1 \le \cdots \le \omega_p$

  Then the minimum distance of the code satisfies

$$d \ge \frac{(2\omega_1 - \mu_2)\sum_{i=1}^{p} \omega_i^2 \cdot m}{(\sum_{i=1}^{p} \omega_i^2 - \mu_2) \cdot \omega_p^2}$$

- **Proof**
  - The first eigenvector of $\mathbf{H}^T\mathbf{H}$

$$\mathbf{e}_1 = (\omega_1, \cdots \omega_1, \omega_2, \cdots \omega_2, \cdots, \omega_p, \cdots \omega_p)^T / \sqrt{m \cdot \sum_{i=1}^{p} \omega_i^2}$$

with corresponding eigenvalue $\mu_1 = \sum_{i=1}^{p} \omega_i^2$

  - Let **c** be a minimum-weight codeword of weight $d$.

$$\mathbf{c}^T\mathbf{c} = \|\mathbf{c}\|^2 = d \quad (3)$$

  - Let $d_i$ be the number of nonzeros of **c** in each $m$-portion corresponding to $\mathbf{H}_i$, and let $\mathbf{c}_i$ be the projection of **c** onto the $i$th eigenspace.

$$\|\mathbf{c}_1\|^2 = \|\mathbf{c} \cdot \mathbf{e}_1\| = \frac{(\sum_{i=1}^{p} d_i \omega_i)^2}{m \cdot \sum_{i=1}^{p} \omega_i^2} \le \frac{d^2 \omega_p^2}{m \cdot \sum_{i=1}^{p} \omega_i^2} \quad (4)$$

# Minimum Distance Bounds for QC-LDPC Codes

- Let $x_i$ be the weight on the $i$th parity defined by $\mathbf{Hc}$. Then

$$\|\mathbf{Hc}\|^2 = \sum_{i=1}^{m} x_i^2 \geq 2\sum_{i=1}^{m} x_i = 2\sum_{i=1}^{m} \omega_i d_i \geq 2\omega_1 d \qquad (5)$$

- Using the eigenspace representation

$$\|\mathbf{Hc}\|^2 = \sum_{i=1}^{s} \mu_i \|\mathbf{c}_i\|^2 \leq (\mu_1 - \mu_2)\|\mathbf{c}_1\|^2 + \mu_2\|\mathbf{c}\|^2 \qquad (6)$$

- Finally substituting (3),(4),(5) into (6) gives

$$2\omega_1 d \leq (\mu_1 - \mu_2)\|\mathbf{c}_1\|^2 + \mu_2\|\mathbf{c}\|^2 \leq \left(\sum_{i=1}^{p} \omega_i^2 - \mu_2\right)\frac{d^2\omega_p^2}{m \cdot \sum_{i=1}^{p} \omega_i^2} + \mu_2 d$$

$$\Rightarrow \; d \geq \frac{(2\omega_1 - \mu_2)\sum_{i=1}^{p} \omega_i^2 \cdot m}{\left(\sum_{i=1}^{p} \omega_i^2 - \mu_2\right) \cdot \omega_p^2}$$

## Theorem 2. Parity-oriented bound

- Let $\mu_1 > \mu_2 > \cdots > \mu_s$ be the ordered distinct eigenvalues of real valued matrix $\mathbf{HH}^T$, where $\mathbf{H} = [\mathbf{H}_1, \mathbf{H}_2, \cdots, \mathbf{H}_p]$ and $\mathbf{H}_i$ is a $m \times m$ circulant matrices which has weight $\omega_i, 1 \le i \le p$, with $\omega_1 \le \cdots \le \omega_p$

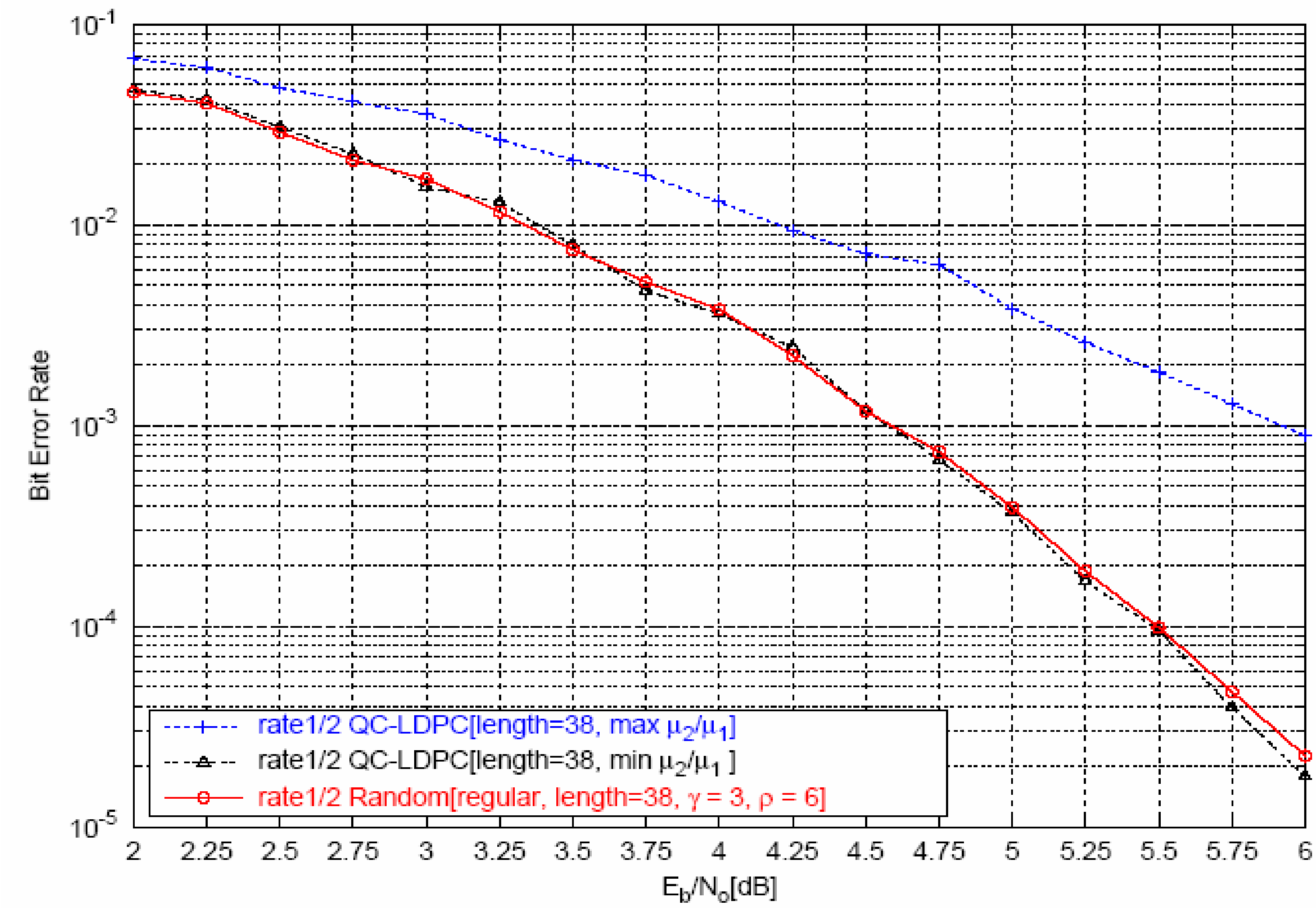
Then the minimum distance of the code satisfies

$$d \ge \frac{2m(2\omega_1 + \sum_{i=1}^{p} \omega_i - 2 - \mu_2)}{\omega_p(\sum_{i=1}^{p} \omega_i^2 - \mu_2)}$$

# Code Construction Examples

- **A rate 1/2 irregular QC-LDPC code of length 38**
  - Let $\mathbf{H} = [\mathbf{H}_1 \ \ \mathbf{H}_2]$ and $m = 19$
  - The best case
    - ✓ $h_1(x) = 1 + x + x^8, \ h_2(x) = 1 + x^2 + x^6 + x^{16}$
    - ✓ Eigenvalues $\mu_1 = 25, \ \mu_2 = 6 \ (\mu_2/\mu_1 = 0.24)$
    - ✓ The bit and the parity-oriented bound gives $d \geq 0$ and $d \geq 2.5$
    - ✓ The actual minimum distance is $d = 7$
  - The worst case
    - ✓ $h_1(x) = 1 + x^5 + x^{12}, \ h_2(x) = 1 + x^2 + x^7 + x^{14}$
    - ✓ Eigenvalues $\mu_1 = 25, \ \mu_2 = 22.29 \ (\mu_2/\mu_1 = 0.89)$
    - ✓ The actual minimum distance is $d = 4$
  - We can increase the minimum distance of a code by minimizing the second largest eigenvalue.

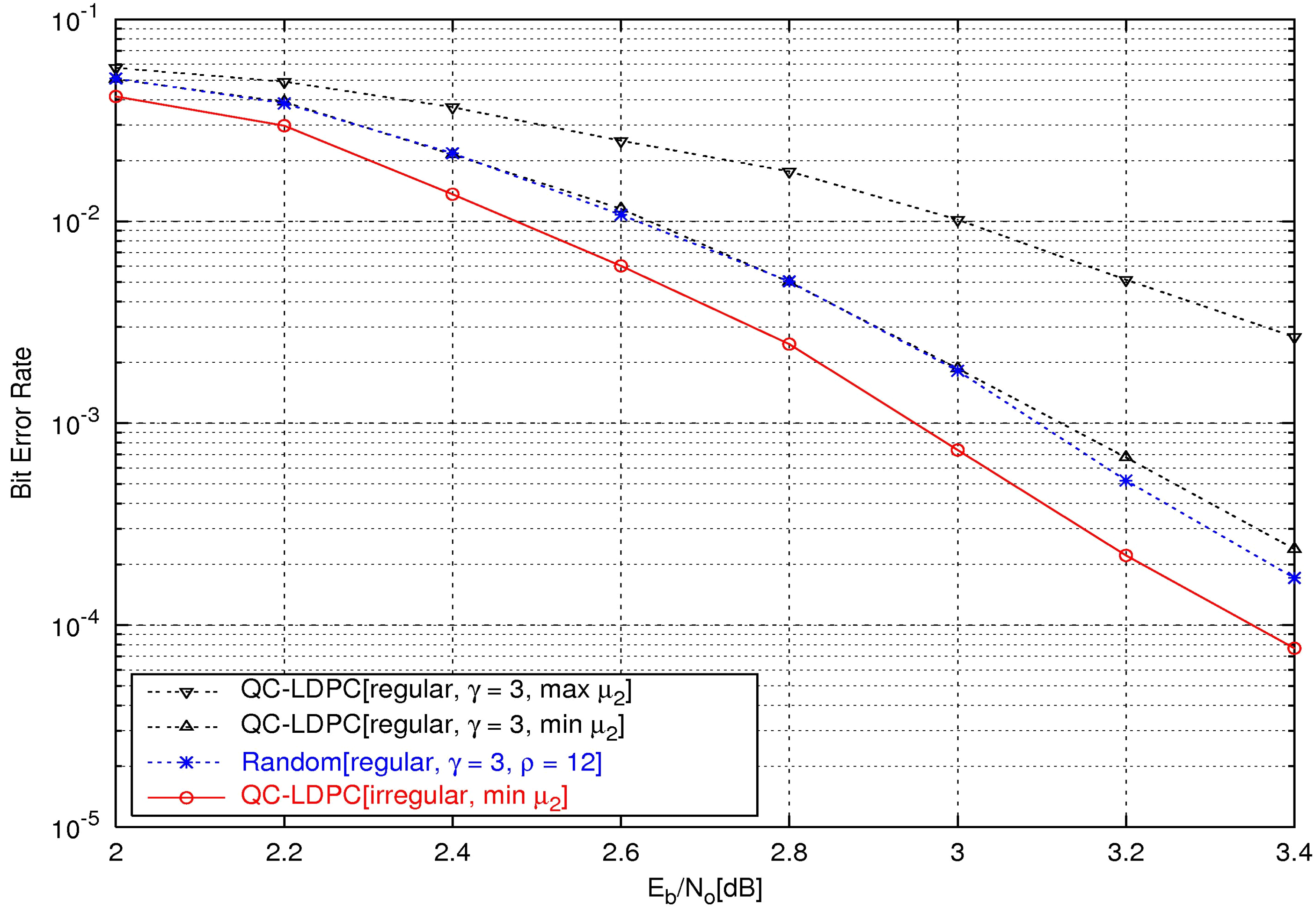
# Simulation Results



# Code Construction Examples

| Code Description | | Eigenvalue ratio | # of 6-cycle |
|---|---|---|---|
| Random | [868,3,12] Random LDPC code | $\mu_2/\mu_1 = 0.5926$ | 1,792 |
| Regular QC-LDPC | $h_1(x) = x^{78} + x^{121} + x^{137}$ $h_2(x) = 1 + x^{8} + x^{107}$ $h_3(x) = 1 + x^{11} + x^{86}$ $h_4(x) = x^{29} + x^{64} + x^{198}$ | $\mu_2/\mu_1 = 0.9543$ (maximum) | 6,727 |
| | $h_1(x) = 1 + x^{121} + x^{137}$ $h_2(x) = x^{8} + x^{79} + x^{85}$ $h_3(x) = 1 + x^{11} + x^{100}$ $h_4(x) = x^{29} + x^{165} + x^{207}$ | $\mu_2/\mu_1 = 0.5469$ (minimum) | 1,085 |
| Irregular QC-LDPC | $h_1(x) = x^{67} + x^{88}$ $h_2(x) = x^{18} + x^{78} + x^{121}$ $h_3(x) = 1 + x^{11} + x^{144}$ $h_4(x) = x^{B_5}$ | $\mu_2/\mu_1 = 0.5764$ (maximum) | 28,220 |
| | $h_1(x) = x + x^{149}$ $h_2(x) = 1 + x^{18} + x^{137}$ $h_3(x) = 1 + x^{144} + x^{190}$ $h_4(x) = x^{B_5}$ | $\mu_2/\mu_1 = 0.3830$ (minimum) | 23,002 |

# Simulation Results



# Conclusions

- **Summary**
  - Minimum distance bounds for irregular QC-LDPC codes using a similar technique to Tanner's bound

- **Further work**
  - Derive tighter minimum distance bound