# A simple construction for QC-LDPC codes of short lengths with girth at least 8

**Inseon Kim and Hong-Yeop Song**

Yonsei University

The 11th International Conference on ICT Convergence

In this paper, we propose a simple construction for quasi-cyclic low density parity-check codes with girth at least 8 by selecting 3 consecutive rows of a square base matrix over a finite field of size prime $p = t^2 + 1$ for some $t$. The bit error rate performance of the codes of lengths 1200 and 2400 are Monte-Carlo simulated.

## 1. QC-LDPC codes and Cycle Property

- **QC-LDPC Codes – the finite field approach**
  - Every non-zero element of $GF(p)$ appears once in square matrix $B$ when $p = t^2 + 1$

$$\mathrm{B} = \begin{bmatrix} 1 & \alpha^t & \cdots & \alpha^{(t-1)t} \\ \alpha & \alpha^{t+1} & \cdots & \alpha^{(t-1)t+1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{t-1} & \alpha^{2t-1} & \cdots & \alpha^{t^2-1} \end{bmatrix}$$

  - Parity matrix of QC-LDPC code by choosing any $m$ rows of $B$

$$\mathrm{H} = \begin{bmatrix} \mathbf{H}_{0,0} & \mathbf{H}_{0,1} & \cdots & \mathbf{H}_{0,t-1} \\ \mathbf{H}_{1,0} & \mathbf{H}_{1,1} & \cdots & \mathbf{H}_{1,t-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{H}_{m-1,0} & \mathbf{H}_{m-1,1} & \cdots & \mathbf{H}_{m-1,t-1} \end{bmatrix}$$

    - $H_{i,j}$ : $p \times p$ CPM cyclically shifting by $(i,j)-th$ entry of $B$
    - Rate : $\frac{t-m}{t}$ and QC-LDPC codes have girth at least 6 [8] .

- **Cycle property of QC-LDPC codes**
  - 2 by 2 submatrix of $B$ : $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$
  - $a - b - c + d \equiv 0 \ (mod\ p)$ iff ∃ a cycle of length 4 in parity-check matrix

## 2. Simple construction of QC-LDPC codes with girth at least 8

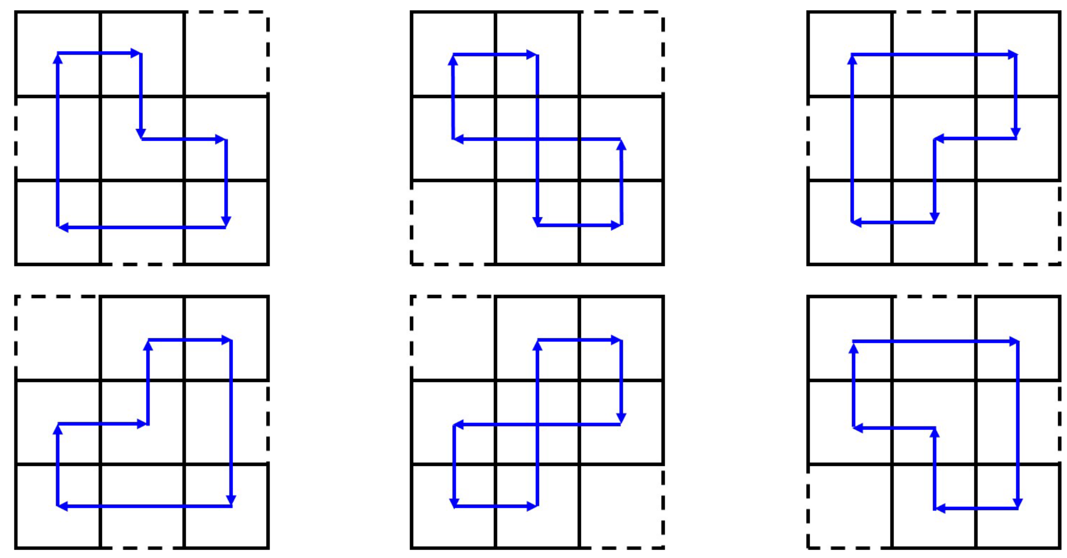
- **Construction Methods**
  - Select 3 consecutive rows of square matrix $B$

$$\mathbf{B}_s = \begin{bmatrix} \alpha^0 & \alpha^t & \alpha^{2t} & \cdots & \alpha^{(t-1)t} \\ \alpha^1 & \alpha^{t+1} & \alpha^{2t+1} & \cdots & \alpha^{(t-1)t+1} \\ \alpha^2 & \alpha^{t+2} & \alpha^{2t+2} & \cdots & \alpha^{(t-1)t+2} \end{bmatrix}$$

  - Generate parity-check matrix whose base matrix is selected matrix
  - These **QC-LDPC codes has girth at least 8**
  - For some case, the QC-LDPC codes has girth at least 10
- **Its cycle property**
  - Consider $3 \times 3$ submatrix of $\mathbf{B}_s$

$$\begin{bmatrix} \alpha^{it} & \alpha^{jt} & \alpha^{kt} \\ \alpha^{it+1} & \alpha^{jt+1} & \alpha^{kt+1} \\ \alpha^{it+2} & \alpha^{jt+2} & \alpha^{kt+2} \end{bmatrix}$$

  - $\alpha^{it} - \alpha^{jt} + \alpha^{jt+1} - \alpha^{kt+1} + \alpha^{kt+2} - \alpha^{it+2} \equiv 0 \ (mod\ p)$ iff ∃ a cycle of length 6
  - Patterns of cycle of length 6



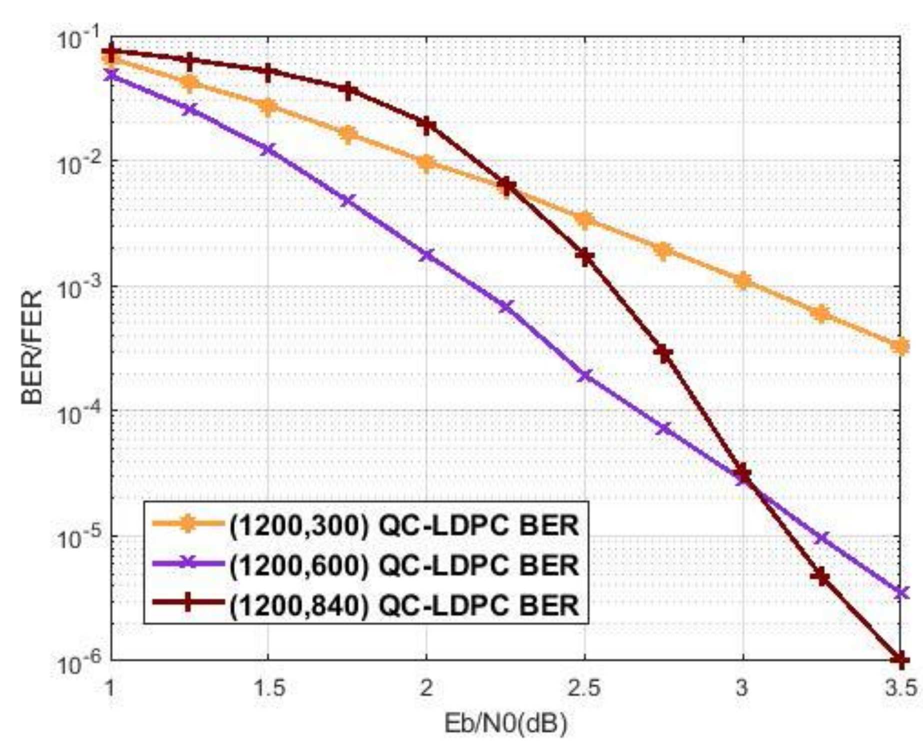
- Length and rate of constructed QC-LDPC

| $p$ | code rate | code length |
|---|---|---|
| $t^2+1$ | $\frac{t-3}{t}$ | $t(p+l)$ where $l = 0, 1, 2, \cdots$ |
| $4^2+1$ | $\frac{1}{4}$ | $4(p+l) = 68, 72, 76, \cdots$ |
| $6^2+1$ | $\frac{1}{2}$ | $6(p+l) = 222, 228, 234, \cdots$ |
| $10^2+1$ | $\frac{7}{10}$ | $10(p+l) = 1010, 1020, 1030, \cdots$ |
| $14^2+1$ | $\frac{11}{14}$ | $14(p+l) = 2758, 2772, 2786, \cdots$ |
| $16^2+1$ | $\frac{13}{16}$ | $16(p+l) = 4112, 4128, 4144, \cdots$ |
| $\vdots$ | $\vdots$ | $\vdots$ |

- Proposed construction gives QC-LDPC codes with
  1. **Very short length as a few hundreds**
  2. **High code rate approaching 1**

## 3. Simulation Results

- To compare the performance of QC-LDPC codes, we choose three case : $t = 4, 6, 10$
- Code length : 1200 (set $l_1 = 283, l_2 = 163, l_3 = 19$)
- Code length : 2400 (set $l_1 = 563, l_2 = 363, l_3 = 139$)
- Assume BPSK modulation and AWGN channel
- Decoding algorithm : SP algorithm




- Surprisingly, higher code rate codes have better decoding performance

CHANNEL CODING
채널코딩연구실