On the Construction and Decoding of Cyclic LDPC Codes

Chao Chen

Joint work with Prof. Baoming Bai from Xidian University

April 30, 2014

Outline

1. Introduction
2. Construction based on Idempotents and Modular Golomb Rulers
3. Construction based on $(n, 2)$ Pseudo-Cyclic MDS Codes
4. Iterative Decoding Using Automorphism Group of Cyclic Codes
5. Simulation Results

Cyclic LDPC codes form an important class of structured LDPC codes.

- As cyclic codes, they can be simply encoded with shift register.
- As LDPC codes, they provide good performance under iterative decoding with a reasonable decoding complexity.
- They have relatively large minimum distance.
- Some codes can be transformed into quasi-cyclic (QC) codes through row and column permutations on the parity-check matrix.

Some Known Constructions

- Construction based on finite geometries (Lin et al.)
- Construction based on idempotents (Shibuya et al., Tomlinson et al.)
- Construction based on matrix decomposition (Lin et al.)

Code Features

- The defining parity-check matrix is a circulant matrix or a column of circulant matrices.
- The party-check matrix is highly redundant.
- The column weight γ is relatively large.
- The corresponding Tanner graph is free of length-4 cycles.
- The minimum distance of the code is at least $\gamma + 1$. (Massey bound)

Idempotent

Definition: Let R_n be the ring of residue classes of $F_q[x]$ modulo $x^n - 1$. Then a polynomial $e(x)$ of R_n is called an *idempotent* if $e^2(x) = e(x)$.

Properties:

- For a cyclic code C, there exists a unique idempotent $e(x)$ that generates C, called the generating idempotent of C.
- Let $e^{\perp}(x)$ be the generating idempotent of $C^{\perp}$, the dual code of C, then $e^{\perp}(x) = 1 - x^n e(x^{-1})$.

Modular Golomb Ruler

Definition: A set of integers $\{a_i : 0 \leq a_i < n, 1 \leq i \leq \gamma\}$ is called a *Golomb ruler modulo n with* γ *marks*, if the differences $(a_i - a_j)$ mod n are distinct for all ordered pairs (i, j) with $i \neq j$.

An example:

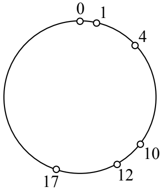


Figure: A Golomb ruler modulo 31 with 6 marks.

An inherent constraint: $\gamma \times (\gamma - 1) \leq (n - 1)$.

Three Algebraic Constructions of Modular Golomb Rulers

- Singer construction (projective geometry plane)
- Bose construction (Euclidean geometry plane)
- Ruzza construction

Code Definition

Consider a cyclic LDPC code C of length n over F_q, whose parity-check matrix is an $n \times n$ circulant

$$\mathbf{H} = \begin{bmatrix} c_0 & c_1 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & \cdots & c_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & \cdots & c_0 \end{bmatrix}.$$

The above code is specified by the polynomial

$$\begin{aligned} c(x) &= c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \\ &= c_{a_1} x^{a_1} + c_{a_2} x^{a_2} \cdots + c_{a_\gamma} x^{a_\gamma}, \end{aligned}$$

where γ is the row weight of $\mathbf{H}$ and $c_{a_i} \neq 0$ $(i = 1, \cdots, \gamma)$.

Main Results

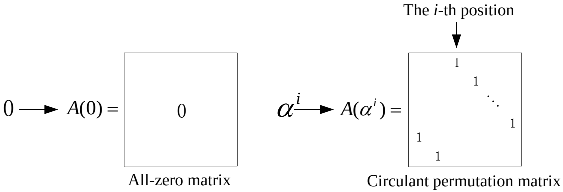
- If $c(x)$ is an idempotent, then the minimum distance of C satisfies

$$d_{min} \leq \begin{cases} \gamma+1, & \text{if } c_0 = 0; \\ \gamma-1, & \text{if } c_0 = 1; \\ \gamma, & \text{otherwise.} \end{cases}$$

- The Tanner graph corresponding to $\mathbf{H}$ is free of length-4 cycles if and only if $\{a_1, a_2, \cdots, a_\gamma\}$ is a Golomb ruler modulo n with γ marks.
- According to Massey bound, if the Tanner graph is free of length-4 cycles, then $d_{min} \geq \gamma + 1$.
- If $c(x)$ is an idempotent and $\{a_1, a_2, \cdots, a_\gamma\}$ is a modular Golomb ruler, then the minimum distance of C is exactly $\gamma + 1$.

Preliminaries: Finite Field based Construction of QC-LDPC Codes (Lin et al.)

Let α be a primitive element of F_q, then $0, \alpha^0, \cdots, \alpha^{q-2}$ give all elements of F_q. Let $\beta \in F_q$, then it can be mapped to a $(q-1) \times (q-1)$ binary matrix $A(\beta)$, as shown below.



The matrix $A(\beta)$ is called the *matrix dispersion* of β over F_2.

Procedure for Finite Field based Construction

- First construct an $m \times n$ matrix over F_q, called the *base matrix*.

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

- Then replace each entry of $\mathbf{W}$ by its matrix dispersion and form the following matrix as the parity-check matrix

$$\mathbf{H}(\mathbf{W}) = \begin{bmatrix} A(w_{0,0}) & A(w_{0,1}) & \cdots & A(w_{0,n-1}) \\ A(w_{1,0}) & A(w_{1,1}) & \cdots & A(w_{1,n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ A(w_{m-1,0}) & A(w_{m-1,1}) & \cdots & A(w_{m-1,n-1}) \end{bmatrix}.$$

Design Constraint on $\mathbf{W}$

For $0 \leq i, j \leq m-1, i \neq j$ and $0 \leq h, k \leq q-2$,

$$d(\alpha^h \mathbf{w}_i, \alpha^k \mathbf{w}_j) \geq n-1,$$

where d denotes the Hamming distance.

The constraint is called the α*-multiplied row distance (RD) constraint*, which guarantees that the Tanner graph corresponding to $\mathbf{H}(\mathbf{W})$ is free of length-4 cycles.

Pseudo-Cyclic Code and MDS Code

Definition: A linear block code of length n is a *pseudo-cyclic* code with parameter $\beta \in F_q$, if for any codeword $(c_0, c_1, \cdots, c_{n-1})$, its pseudo-cyclic $(\beta c_{n-1}, c_0, \cdots, c_{n-2})$ also forms a codeword.

Definition: An (n, k) linear block code is a *maximum-distance-separable* (MDS) code, if the minimum distance $d_{min} = n - k + 1$.

Code Construction

Consider the the following $n \times n$ matrix over F_q

$$\mathbf{W} = \begin{bmatrix} w_0 & w_1 & \cdots & w_{n-2} & w_{n-1} \\ \alpha w_{n-1} & w_0 & \cdots & w_{n-3} & w_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha w_2 & \alpha w_3 & \cdots & w_0 & w_1 \\ \alpha w_1 & \alpha w_2 & \cdots & \alpha w_{n-1} & w_0 \end{bmatrix},$$

where the rows are codewords of a $(n, 2)$ pseudo-cyclic MDS code with $\beta = \alpha$.

It can be proved that the $\mathbf{W}$ satisfies the α-multiplied RD constraint.

Through matrix dispersion, the obtained $\mathbf{H}(\mathbf{W})$ defines a QC-LDPC code.

Main Result

From the above QC-LDPC code, a cyclic LDPC code can be obtained by transforming $\mathbf{H}(\mathbf{W})$ to a circulant parity-check matrix through row and column permutations.

Automorphism Group of a Code

Definition: Let C be a binary linear block code of length n. The set of coordinate permutations that map C to itself forms a group under composition operation. The group is called the *automorphism group* of C, denoted by $Aut(C)$.

For a binary cyclic code of odd length n, the automorphism group contains the following two cyclic subgroups:

- S_0: The set of permutations $\tau^0, \tau^1, \cdots, \tau^{n-1}$, where

$$\tau^k : j \rightarrow (j + k) \, mod \, n.$$

- S_1: The set of permutations $\zeta^0, \zeta^1, \cdots, \zeta^{m-1}$, where

$$\zeta^k : j \rightarrow (2^k \cdot j) \, mod \, n,$$

  and m is the smallest positive integer such that $2^m \equiv 1 \, mod \, n$.

Properties of $Aut(C)$

- Let $C^{\perp}$ be the dual code of C, then $Aut(C^{\perp}) = Aut(C)$.
- Let $\pi \in Aut(C)$. If $\mathbf{H}$ is a parity-check matrix of C, then $\pi\mathbf{H}$ also forms a parity-check matrix of C.

Decoder Diversity

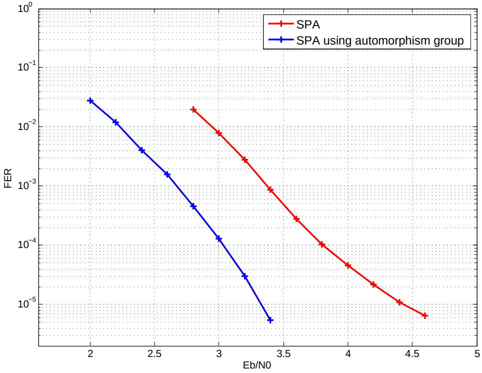
- Two party-check matrices are called *non-equivalent* if they cannot be obtained from each other only by row permutations.
- The basic idea is to construct multiple non-equivalent parity-check matrices based on $Aut(C)$. Different decoding attempts can be made on these parity-check matrices, thus providing decoder diversity gain.

Main Results

- For cyclic LDPC codes constructed from idempotents and modular Golomb rulers, S_0 and S_1 cannot be used to generate non-equivalent parity-check matrices.
- For cyclic LDPC codes constructed from pseudo-cyclic MDS codes with two information symbols, S_1 can be used to generate non-equivalent parity-check matrices.

Simulation Results

A $(341, 160)$ cyclic LDPC code is constructed from $(31, 2)$ pseudo-cyclic MDS code over F_{32}. The BPSK modulation over AWGN channel is assumed. The maximum number of iterations is set to be 100.



References

- 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.
- T. Shibuya and K. Sakaniwa, "Construction of cyclic codes suitable for iterative decoding via generating idempotents," *IEICE Trans. Fundamentals,* vol. E86-A, no. 4, pp. 928-939, Apr. 2003.
- R. Horan, C. Tjhai, M. Tomlinson, M. Ambroze, and M. Ahmed, "Idempotents, Mattson-Solomon polynomials and binary LDPC codes," *IEE Proc. Commun.,* vol. 153, no. 2, pp. 256-262, Apr. 2006.
- Q. Huang, Q. Diao, S. Lin, and K. Abdel-Ghaffar, "Cyclic and quasi-cyclic LDPC codes on row and column constrained parity-check matrices and their trapping sets," *IEEE Trans. Inf. Theory,* vol. 58, no. 5, pp. 2648-2671, May 2012.

References

- C. Chen, B. Bai, Z. Li, X. Yang, and L. Li, "Nonbinary cyclic LDPC codes derived from idempotents and modular Golomb rulers," *IEEE Trans. Commun.*, vol. 60, no. 3, pp. 661-668, Mar. 2012.
- L. Lan, L.-Q. Zeng, Y. Y. Tai, L. Chen, S. Lin, and K. Abdel-Ghaffar, "Construction of quasi-cyclic LDPC codes for AWGN and binary erasure channels: A finite field approach," *IEEE Trans. Inf. Theory,* vol. 53, no. 7, pp. 2429-2458, Jul. 2007.
- C. Chen, B. Bai, X. Yang, L. Li, and Y. Yang "Enhancing iterative decoding using their automorphim groups," *IEEE Trans. Commun.*, vol. 60, no. 3, pp. 661-668, Mar. 2012.

Thanks!