

Construction of Regular Quasi-Cyclic LDPC Codes Based on Cosets

Pengcheng Chen, Yuansheng Tang, Zhanghua Cao and Tingsu Yan

College of Mathematical Sciences

Yangzhou University

Yangzhou, Jiangsu, 225002 China

Email: pengchengchen@yahoo.com, ystang@yzu.edu.cn

Abstract—We propose a construction method for constructing quasi-cyclic low-density parity-check (QC LDPC) codes based on subgroup's coset. Our construction method is available not only for the prime circulants size, but also for the nonprime circulants size in some conditions. And it is showed that these conditions are easy to satisfy. Regular QC LDPC codes with various lengths and rates can be easily constructed with girth at least 6. Simulation results show that they are have almost the same performance as random regular LDPC codes over AWGN channel.

I. INTRODUCTION

Low-density parity-check (LDPC) codes were first discovered by Gallager in 1962 [1] and were rediscovered recently that they can achieve near Shannon limit performance with sum-product algorithm [2]. It is well known that an LDPC code with girth equal to 6 performs quite well. Here the girth is the minimum length of cycles in the Tanner graph of the given parity-check matrix of the LDPC code. In various LDPC codes, quasi-cyclic (QC) LDPC codes were extensively studied because they can be encoded using simple shift-registers with linear complexity and require a small memory space to store the code graph for decoding, especially compared with randomly constructed codes.

Many construction methods have been proposed to construct QC LDPC codes with girth at least 6. Fan [3] proposed a class of algebraically constructed LDPC codes from a family of array codes. To construct an array LDPC code with girth at least 6, the circulant permutation matrices (shortly, circulants) size has to be prime to eliminate the short cycles. A modified construction to array LDPC codes was presented for supporting arbitrary circulants size by Abematsu *et al.* [4], while such codes probably contain a few short cycles. In [5], Tanner *et al.* proposed a construction method for QC LDPC codes based on the multiplicative structure of a group. Such codes are called SFT codes and have been investigated widely.

In this paper, we propose a novel method for constructing QC LDPC codes based on subgroup's coset. A modified version is also presented. These methods can easily ensure the code's girth larger than or equal to 6 if the circulants size is a prime. Moreover, we derive the sufficient conditions of girth at least 6 when the circulants size is a nonprime, and show that these conditions are easily satisfied. Thus the codes constructed by our methods have a wide range of codeword lengths and code rates.

II. QC LDPC CODES

A (J, L, m) -regular QC LDPC code is characterized by the parity-check matrix

$$\mathbf{H} = \begin{pmatrix} \mathbf{P}^{c_{0,0}} & \mathbf{P}^{c_{0,1}} & \cdots & \mathbf{P}^{c_{0,L-1}} \\ \mathbf{P}^{c_{1,0}} & \mathbf{P}^{c_{1,1}} & \cdots & \mathbf{P}^{c_{1,L-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{P}^{c_{J-1,0}} & \mathbf{P}^{c_{J-1,1}} & \cdots & \mathbf{P}^{c_{J-1,L-1}} \end{pmatrix} \quad (1)$$

where $c_{i,j} \in \{0, 1, \dots, m-1\}$ and $\mathbf{P} = (P_{ij})$ is the $m \times m$ circulant obtained by cyclically shifting the rows of the $m \times m$ identity matrix to the right by one position. Clearly, \mathbf{P}^0 is the identity matrix. The exponent matrix $E(\mathbf{H})$ of \mathbf{H} in (1) is defined by

$$E(\mathbf{H}) = \begin{pmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,L-1} \\ c_{1,0} & c_{1,1} & \cdots & c_{1,L-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{J-1,0} & c_{J-1,1} & \cdots & c_{J-1,L-1} \end{pmatrix}. \quad (2)$$

Notice that \mathbf{H} can be obtained by extending the $J \times L$ exponent matrix $E(\mathbf{H})$ in (2) into a $Jm \times Lm$ matrix with \mathbf{P} . $E(\mathbf{H})$ is also called the exponent matrix of the code. The cycles of QC LDPC codes may be easily analyzed in an algebraic way due to their structured parity-check matrices.

Theorem 1 ([6]): A necessary and sufficient condition for a (J, L, m) -regular QC LDPC code obtained by (2) to have girth at least 6 is

$$\Delta_{j_1, j_2}(l_1) - \Delta_{j_1, j_2}(l_2) \not\equiv 0 \pmod{m} \quad (3)$$

for any $0 \leq j_1 < j_2 \leq J-1$, $0 \leq l_1 < l_2 \leq L-1$, where $\Delta_{j_1, j_2}(l_i) = c_{j_1, l_i} - c_{j_2, l_i}$, $i = 1, 2$.

III. CONSTRUCTION OF QC LDPC CODES BY COSETS

A. Subgroup and Coset

Suppose that m is a positive integer. Then $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ is a ring under addition and multiplication modulo m and $\mathbb{Z}_m^* = \{z \in \mathbb{Z}_m | z^{-1} \text{ exists}\}$ is a multiplication group. In fact, \mathbb{Z}_m^* is the set consisting of all nonnegative integers which are less than and prime to m . All the operations carried out in \mathbb{Z}_m are modulo m unless otherwise specified. It is clear that if $z \in \mathbb{Z}_m^*$, then $-z \in \mathbb{Z}_m^*$. Let $\#\mathbb{Z}_m^*$ denote the order of \mathbb{Z}_m^* and $\varphi(\cdot)$ denote the Euler function, then

$\#\mathbb{Z}_m^* = \varphi(m)$. We denote the order of $\sigma \in \mathbb{Z}_m^*$ in \mathbb{Z}_m^* by $\delta_m(\sigma)$, sometimes abbreviated as δ_m , i.e., δ_m is the smallest positive integer d with $\sigma^d \equiv 1 \pmod{m}$. Throughout this paper, we require that $\delta_m \neq \#\mathbb{Z}_m^*$, i.e., σ is not a primitive root modulo m . With this convention, we obtain $\delta_m \mid \#\mathbb{Z}_m^*$ and $\langle \sigma \rangle = \{1, \sigma, \dots, \sigma^{\delta_m-1}\}$ is a proper subgroup of \mathbb{Z}_m^* . The proper subgroup $\langle \sigma \rangle$ can partition \mathbb{Z}_m^* into $\varepsilon = \#\mathbb{Z}_m^*/\delta_m$ disjoint cosets: $[\tau_s] = \tau_s \langle \sigma \rangle = \{\tau_s \sigma^i \mid i = 0, 1, \dots, \delta_m - 1\}$, $s = 1, \dots, \varepsilon$, where ε is called the index of $\langle \sigma \rangle$ in \mathbb{Z}_m^* and $\tau_1, \dots, \tau_\varepsilon$ are called ε distinct coset leaders with respect to the ε disjoint cosets. Notice that any element in a coset can be the leader of the coset.

B. Construction of QC LDPC by Cosets

Let $\mathbf{E} = (e_{ij})$ and $\mathbf{F} = (f_{ij})$, where $e_{ij} = \sigma^{i+j}$, $f_{ij} = \sigma^{-i+j}$, $1 \leq i, j \leq \delta_m$. And let $S = \{s_1, s_2, \dots, s_{\#S}\}$ be a subset of $S_{\max} = \{0, 1, \dots, \delta_m - 1\}$. We denote the matrix by \mathbf{E}_S (resp., \mathbf{F}_S) which is obtained from the matrix \mathbf{E} (resp., \mathbf{F}) by deleting the rows whose indices are not in S . Here the row index begins with zero. A triple (σ, m, S) is said to be matching if $\sigma^{j_1} - \sigma^{j_2} \in \mathbb{Z}_m^*$ for any $j_1, j_2 \in S$, $j_1 \neq j_2$. This is equivalent to saying that $\sigma^{j_1} - \sigma^{j_2}$ and m are relatively prime for any $j_1, j_2 \in S$, $j_1 \neq j_2$.

Theorem 2: Suppose (σ, m, S) is matching, $0 \leq u \leq v \leq \varepsilon$ and τ_1, \dots, τ_v are distinct coset leaders. Let

$$E(\mathbf{H}_1(\sigma, m, S, u, (\tau_1, \dots, \tau_v))) = (\tau_1 \mathbf{E}_S \ \dots \ \tau_u \mathbf{E}_S \ -\tau_{u+1} \mathbf{F}_S \ \dots \ -\tau_v \mathbf{F}_S). \quad (4)$$

Then $\mathbf{H}_1(\sigma, m, S, u, (\tau_1, \dots, \tau_v))$ is of girth at least 6.

Proof: By Theorem 1, it suffices to prove that (3) holds for any $j_1, j_2 \in S$, $j_1 \neq j_2$, $1 \leq l_1, l_2 \leq v\delta_m$, $l_1 \neq l_2$. Let $l_1 = q_1\delta_m + \bar{l}_1$ and $l_2 = q_2\delta_m + \bar{l}_2$ with $\bar{l}_1, \bar{l}_2 \in S_{\max}$. Then $\bar{l}_1 \neq \bar{l}_2$. By symmetry, we need to consider the cases

- (a) $0 \leq q_1, q_2 \leq u - 1$,
- (b) $u \leq q_1, q_2 \leq v - 1$,
- (c) $0 \leq q_1 < u \leq q_2 \leq v - 1$.

In case (a), the left-hand side of (3) is

$$(\sigma^{j_1} - \sigma^{j_2}) \left(\tau_{q_1+1} \sigma^{\bar{l}_1} - \tau_{q_2+1} \sigma^{\bar{l}_2} \right).$$

Since (σ, m, S) is matching we have that $\sigma^{j_1} - \sigma^{j_2}$ is prime to m . Thus it is enough to check that the inequality $\tau_{q_1+1} \sigma^{\bar{l}_1} - \tau_{q_2+1} \sigma^{\bar{l}_2} \not\equiv 0 \pmod{m}$ holds. Assume first that $q_1 \neq q_2$. It holds since the left-hand side of the inequality is the difference between an element of $[\tau_{q_1+1}]$ and an element of $[\tau_{q_2+1}]$, obviously, not congruent to 0 modulo m . Now suppose $q_1 = q_2$. The inequality also holds since $\bar{l}_1 \neq \bar{l}_2$ and (σ, m, S) is matching. In case (b), the left-hand side of (3) is

$$-\sigma^{-(j_1+j_2)} (\sigma^{j_1} - \sigma^{j_2}) \left(\tau_{q_1+1} \sigma^{\bar{l}_1} - \tau_{q_2+1} \sigma^{\bar{l}_2} \right).$$

The proof is analogous to that of case (a) since $-\sigma^{-(j_1+j_2)} \in \mathbb{Z}_m^*$. Finally, in case (c), the left-hand side of (3) is

$$(\sigma^{j_1} - \sigma^{j_2}) \left(\tau_{q_1+1} \sigma^{\bar{l}_1} - \tau_{q_2+1} \sigma^{\bar{l}_2 - (j_1+j_2)} \right).$$

Similarly, the difference $\tau_{q_1+1} \sigma^{\bar{l}_1} - \tau_{q_2+1} \sigma^{\bar{l}_2 - (j_1+j_2)}$ is not congruent to 0 modulo m since $q_1 \neq q_2$. We have shown (3) holds in all cases. ■

Remark: The LDPC codes obtained from choosing different leaders for the same submatrices in (4) are mutually equivalent.

C. About the Triple (σ, m, S)

Theorem 3: Let $m = p_0^{a_0} p_1^{a_1} p_2^{a_2} \dots p_l^{a_l}$ and $m' = p_0^{a'_0} p_1^{a'_1} p_2^{a'_2} \dots p_l^{a'_l}$, where $p_0 = 2$, p_1, p_2, \dots, p_l are different odd primes and $0 \leq a_e \leq a'_e$, $e = 0, 1, \dots, l$. Then following propositions hold.

- (1) If m is a prime, then (σ, m, S_{\max}) is matching.
- (2) If (σ, m, S) is matching, then $\#S$ at most equal to δ_{\min} , where $\delta_{\min} = \min_{1 \leq e \leq l} \{\delta_{p_e}\}$ and δ_{p_e} is the order of σ in $\mathbb{Z}_{p_e}^*$.
- (3) If (σ, m, S) is matching, then (σ, m', S) is also matching.

Proof: (1) Clearly, $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{0\}$ since m is a prime. Thus $\sigma^{j_1} - \sigma^{j_2} \neq 0$, i.e., $\sigma^{j_1} - \sigma^{j_2} \in \mathbb{Z}_m^*$ for any $j_1, j_2 \in S_{\max}$, $j_1 \neq j_2$.

(2) It is clear that $\sigma \in \mathbb{Z}_{p_e}^*$ since $\sigma \in \mathbb{Z}_m^*$. Then $\sigma^{j_1} - \sigma^{j_2} \in \mathbb{Z}_m^*$ is equivalent to $\sigma^{j_1-j_2} \not\equiv 1 \pmod{p_e}$ which in turn equivalent to $\delta_{p_e} \nmid (j_1 - j_2)$ for any $e = 0, 1, \dots, l$. Now assume that (σ, m, S) is matching, where $S = \{s_1, \dots, s_{\delta_{\min}}, s_{\delta_{\min}+1}\}$. There exist $s_{i_1}, s_{i_2} \in S$ such that $\delta_{\min} \mid s_{i_1} - s_{i_2}$ which contradicts the hypothesis. We have shown that $\#S$ can not be greater than δ_{\min} . In particular, let $S_0 = \{0, 1, \dots, \delta_{\min} - 1\}$. One can check that (σ, m, S_0) is matching.

(3) Let (σ, m, S) be matching. Then σ is not a primitive root modulo m . Since $m \mid m'$ we have that σ is also not a primitive root modulo m' . By the proof of (2), the set S is determined by the prime factors of m . Since m and m' have the same prime factors, we have that (σ, m', S) is also matching, which is as required. ■

In general, if the column weight $J < 3$, sum-product algorithm does not work well. We can add the all-zero row vector to $E(\mathbf{H}_1(\sigma, m, S, u, (\tau_1, \dots, \tau_v)))$ if $-\tau_j/\tau_i \notin \langle \sigma \rangle$ for any $u+1 \leq j \leq v$, $0 \leq i \leq u$. By the proof of Theorem 2, the code obtained by the added exponent matrix is also with girth at least 6. Obviously, it is feasible to do so for $u = 0$ or v . In particular, let m be odd and $\sigma = m - 1$. Then $\delta_m = 2$ which follows that $\delta_{p_1} = \dots = \delta_{p_l} = 2$. By Theorem 3, we get a set S with $\#S = 2$. Then we can get a parity-check matrix with column weight of 3 if the condition of adding the all-zero row vector is satisfied. Fig.1 is a histogram of “length ≤ 10000 and the cardinality of the triples (σ, m, S) with $\#S \geq 2$ ”. Here the LDPC codes are obtained by (4) with $v = \varepsilon$. As we see on Fig.1, various lengths are realizable by our construction. Certainly, the codes with specific length or rate can be obtained by choosing a part of the square matrices in (4) and some columns of other square matrices.

D. Modified Construction

Corollary 4 ([7]): Suppose m is a prime, $v < \delta_m$ and τ_1, \dots, τ_v are distinct coset leaders. Let

$$E(\mathbf{H}_2(\sigma, m, (\tau_1, \dots, \tau_v))) = \begin{pmatrix} ([\tau_1]) \\ ([\tau_2]) \\ \dots \\ ([\tau_v]) \end{pmatrix}. \quad (5)$$

Then $\mathbf{H}_2(\sigma, m, (\tau_1, \dots, \tau_v))$ is of girth at least 6, where $([\tau_j]) = (\tau_j, \tau_j\sigma, \dots, \tau_j\sigma^{\delta_m-1})$, $1 \leq j \leq v \leq \varepsilon$.

Proof: Since m is a prime, by Theorem 3, we may choose the first column in the v square matrices of $E(\mathbf{H}_1(\sigma, m, S_{\max}, v, (\tau_1, \dots, \tau_v)))$ to form a new matrix. Its transposed matrix is $E(\mathbf{H}_2(\sigma, m, (\tau_1, \dots, \tau_v)))$. The result now follows by applying Theorem 2. ■

Yongmei *et al.* [7] have proposed the construction method of Corollary 4 and the relation between the codes constructed by Corollary 4 and the SFT codes, i.e., the SFT codes are special cases of the codes constructed by Corollary 4. If m is a nonprime, we have the following result.

Theorem 5: Let m be a nonprime, $v < \delta_m$ and τ_1, \dots, τ_v be distinct coset leaders. If $(\tau_{j_1} - \tau_{j_2}) \in \mathbb{Z}_m^*$ for any $1 \leq j_1, j_2 \leq v$, $j_1 \neq j_2$, then $\mathbf{H}_2(\sigma, m, (\tau_1, \dots, \tau_v))$ is of girth at least 6.

Proof: It suffices to prove that $E(\mathbf{H}_2(\sigma, m, (\tau_1, \dots, \tau_v)))$ satisfies (3). Let l_1 and l_2 be integers between 1 and δ_m with $l_1 \neq l_2$. Clearly, $-(\delta_m - 1) \leq l_2 - l_1 \leq \delta_m - 1$ and $l_2 - l_1 \neq 0$. It follows that $(1 - \sigma^{l_2 - l_1}) \not\equiv 0 \pmod{m}$. Since $(\tau_{j_1} - \tau_{j_2}) \in \mathbb{Z}_m^*$, we have $(\tau_{j_1} - \tau_{j_2})(\sigma^{l_1} - \sigma^{l_2}) \not\equiv 0 \pmod{m}$, i.e., (3) is valid and the proof is complete. ■

The conditions of Theorem 5 are easily satisfied for most cases, since the column weight v is small and it is feasible to choose a different coset leader for a coset.

IV. EXAMPLES AND SIMULATION RESULTS

Let $m = 119$, $\sigma = 38 \in \mathbb{Z}_{119}^*$. Then $\#\mathbb{Z}_{119}^* = 96$ and 38 has order $\delta_{119}(38) = 12$. We get $\varepsilon = 96/12 = 8$, i.e., \mathbb{Z}_{119}^* can be partitioned into 8 disjoint cosets with respect to $\langle 38 \rangle$. And $(\tau_1, \tau_2, \tau_3, \tau_4, \tau_5, \tau_6, \tau_7, \tau_8) = (1, 2, 3, 4, 5, 6, 8, 10)$ are distinct coset leaders. Furthermore, 38 has order $\delta_7(38) = 6$ and $\delta_{17}(38) = 4$ in $\mathbb{Z}_{p_1}^*$ and $\mathbb{Z}_{p_2}^*$ with $p_1 = 7$ and $p_2 = 17$, respectively. Then the triple $(38, 119, \{0, 1, 2, 3\})$ is matching by Theorem 3. By Theorem 2, $\mathbf{H}_1(38, 119, \{0, 1, 2, 3\}, 2, (1, 2))$ and $\mathbf{H}_1(38, 119, \{0, 1, 2, 3\}, 1, (6, 8))$ are of girth at least 6. We denote them by eg-1 and eg-2, respectively. We also choose $\sigma = 19 \in \mathbb{Z}_{119}^*$ with order $\delta_{119}(19) = 24$. Then $\langle 19 \rangle$ is a subgroup of \mathbb{Z}_{119}^* with index $\varepsilon = 96/24 = 4$. One can check $(\tau_1, \tau_2, \tau_3, \tau_4) = (1, 2, 3, 6)$ are 4 distinct coset leaders, and its pairwise differences are prime to p_1 and p_2 . Then $\mathbf{H}_2(19, 119, (1, 2, 3, 6))$, which is denoted by eg-3, is of girth at least 6 by Theorem 5. These three codes mentioned above all have the same codeword length $n = 2856$, design rate $k = 5/6$ and column weight 4.

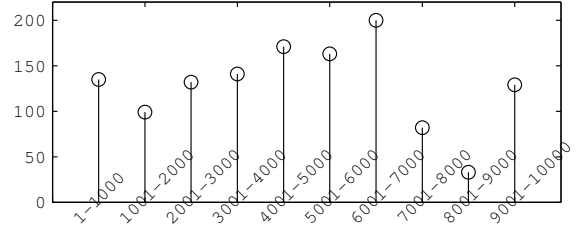


Fig. 1. Histogram of lengths and Numbers of triples

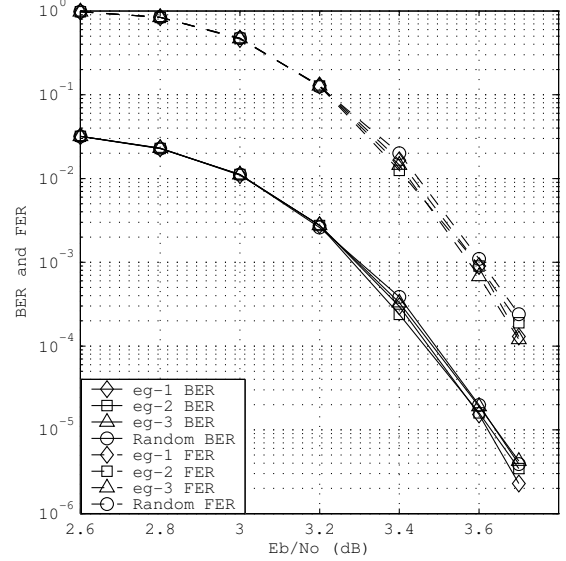


Fig. 2. Performance of the three regular QC LDPC codes constructed from subgroup's coset with codeword length $n = 2856$, design rate $k = 0.83$ and column weight 4.

The performance of the three codes was analyzed by computer simulations over AWGN channel. They were decoded by the sum-product algorithm with 50 iterations. Fig.2 shows the bit error rate (BER) and frame error rate (FER) performance of these three codes and a Mackay random code with the same codeword length, code rate, column weight. The simulation result shows that the LDPC codes constructed in our methods are comparable to the random one in error-correcting performance. In the case that the column weight is 4, there are no serious error floors at $\text{FER} = 10^{-4}$.

V. CONCLUSION

A method for constructing regular QC LDPC codes based on subgroup's coset has been proposed. A modified version have also been presented. QC LDPC codes with girth at least 6 are easily constructed by our methods if the circulants size m is a prime. The sufficient conditions with girth at least 6 when m is a nonprime have also been discussed. And these conditions are easy to satisfy. The LDPC codes with various lengths and rates can be obtained. The simulation results show that the proposed QC LDPC codes perform as well as the Mackay random constructed LDPC codes.

ACKNOWLEDGMENT

This work was supported by the Natural Science Foundation of China Grant (No. 60473018), the Key Project of Chinese Ministry of Education Grant (No. 208045), the Natural Science Foundation of Jiangsu Province (No. BK2008208), and the Open Foundation of NCRL of Southeast University.

REFERENCES

- [1] R. G. Gallager, "Low-density parity-check codes," *IRE Transaction Information Theory*, vol. IT-8, pp. 21–28, Jan. 1962.
- [2] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *Electronics Letters*, vol. 33, pp. 457–458, 1997.
- [3] J. L. Fan, "Array codes as low-density parity-check codes," in *Proc. Int'l. Symp. on Turbo Codes*, Brest, France, 2000, pp. 543–546.
- [4] D. Abematsu, T. Ohtsuki, S. P. W. Jarot, and T. Kashima, "Size compatible (SC)-array LDPC codes," in *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, 2007, pp. 1147–1151.
- [5] R. M. Tanner, D. Sridhara, A. Sridharan, T. E. Fuja, and D. J. Costello, Jr., "LDPC block and convolutional codes based on circulant matrices," *Information Theory, IEEE Transactions on*, vol. 50, pp. 2966–2984, 2004.
- [6] M. P. C. Fossorier, "Quasicyclic low-density parity-check codes from circulant permutation matrices," *Information Theory, IEEE Transactions on*, vol. 50, pp. 1788–1793, 2004.
- [7] D. Yongmei, Y. Zhiyuan, and C. Ning, "Optimal overlapped message passing decoding of quasi-cyclic LDPC codes," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, vol. 16, pp. 565–578, 2008.