SCIENCE CHINA
Information Sciences

• LETTER •

October 2019, Vol. 62 209305:1–209305:3
https://doi.org/10.1007/s11432-018-9778-x

Two classes of QC-LDPC cycle codes approaching Gallager lower bound

Hengzhou XU[1,2*], Huaan LI[2], Mengmeng XU[1], Dan FENG[2] & Hai ZHU[1*]

[1]*School of Network Engineering, Zhoukou Normal University, Zhoukou* 466001*, China;*
[2]*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an* 710071*, China*

Received 18 October 2018/Revised 24 December 2018/Accepted 29 January 2019/Published online 14 June 2019

Citation Xu H Z, Li H A, Xu M M, et al. Two classes of QC-LDPC cycle codes approaching Gallager lower bound. Sci China Inf Sci, 2019, 62(10): 209305, https://doi.org/10.1007/s11432-018-9778-x

Dear editor,
Many research results show that, for equivalent bit length, short nonbinary LDPC codes outperform binary LDPC codes by about 1 dB [1–3]. Moreover, nonbinary LDPC codes have lower error-floor, fast iterative decoding convergence, and strong ability of correcting burst errors. But the roadblock to their application is the high decoding complexity. Recently, significant studies on the low-complexity decoding algorithms of nonbinary LDPC codes have been done [4]. It is noticeable that these low-complexity algorithms are under the frame of iterative decoding. Hence, it is interesting to design nonbinary LDPC codes with large minimum distance and suitable for the iterative algorithms.

For a given block length, nonbinary LDPC codes perform better and better with the increase of their finite field size. When the finite field size is sufficiently large, the increased coding gain becomes negligible, and then the column weight in the parity-check matrices of the best nonbinary LDPC codes tends to 2. In order to facilitate the hardware implementation, quasi-cyclic (QC) structure should be considered. In this study, we study a class of binary QC-LDPC codes with column weight 2 and row weight ρ. Notice that this class of codes is referred to as $(2,\rho)$-regular QC-LDPC cycle codes. By replacing 1's in the parity-check matrices of QC-LDPC cycle codes with nonzero elements of nonbinary finite fields, nonbinary LDPC cycle codes are obtained. It can be seen from [5] that the fully-connected $(2,\rho)$-regular QC-LDPC codes have girths 4, 8, and 12. The cycles of length 4 degrade the performance of the iterative decoding algorithms employed by LDPC codes. Hence, we construct two classes of QC-LDPC cycle codes, i.e., ones with girths 8 and 12, respectively. It is noticeable that the Gallager lower bound on the code length of the proposed codes is tight, and it is useful for constructing nonbinary LDPC cycle codes with large girths [6].

Binary QC-LDPC cycle codes and their short cycles. Based on isomorphism theory [5,7], we consider a binary QC-LDPC cycle code $\mathcal{C}$ of length ρL whose exponent matrix is

$$\boldsymbol{P}=\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ p_0(=0) & p_1 & p_2 & \cdots & p_{\rho-1} \end{bmatrix}, \tag{1}$$

where $p_0=0$ and $1\leqslant p_s\leqslant L-1$ for $1\leqslant s\leqslant \rho-1$. The lifting size (or lifting degree) is L.

According to [5], a cycle of length $2i$, called $2i$-cycle, in the Tanner graph of $\mathcal{C}$ can be represented by a sequence of CPMs, i.e.,

$$\boldsymbol{I}(0),\boldsymbol{I}(p_{k_1}),\boldsymbol{I}(p_{k_2}),\boldsymbol{I}(0),\ldots,\boldsymbol{I}(p_{k_{i-1}}),\boldsymbol{I}(p_{k_i}),\boldsymbol{I}(0)$$

with $0\leqslant k_s\leqslant \rho-1$ and $k_s\neq k_{s+1}$. The type of this $2i$-cycle is denoted by $(p_{k_1},p_{k_2},\ldots,p_{k_i})$.

According to [5], the Tanner graph of $\mathcal{C}$ contains a 4-cycle if and only if the following equation

* Corresponding author (email: hzxu@zknu.edu.cn, zhu_sea@163.com)

is satisfied:

$$\sum_{s=0}^{1}(-1)^s(0-p_{k_s}) = p_{k_1} - p_{k_0} = 0 \pmod{L} \quad (2)$$

with $k_0 \neq k_1$. Furthermore, an 8-cycle exists in the Tanner graph of $\mathcal{C}$ with girth 8 if and only if

$$\sum_{s=0}^{3}(-1)^s(0-p_{k_s}) = 0 \pmod{L} \quad (3)$$

with for $0 \leqslant s \leqslant 3$, $k_s \neq k_{s+1}$ and $k_0 = k_4$.

Gallager lower bound. A lower bound, called Gallager lower bound, on the code length N of (γ, ρ)-regular QC-LDPC codes was given in [8]. When $\gamma = 2$, the next theorem follows.

Theorem 1. For a $(2, \rho)$-regular QC-LDPC cycle code of length $N = \rho L$ whose exponent matrix is given by (1) and lifting size is L, the Gallager lower bound becomes

$$N \geqslant \begin{cases} \rho^2, & g = 8, \\ \rho(\rho-1)^2 + \rho(\rho-1) + \rho, & g = 12, \end{cases}$$

where g is the girth value.

Two classes of QC-LDPC cycle codes approaching Gallager lower bound. In this section, we will construct two classes of QC-LDPC cycle codes approaching Gallager lower bound, i.e., codes with girths 8 and 12, respectively. It can be observed that the Gallager lower bound $N \geqslant \rho^2$, in fact, is tight for $g = 8$. For $(\rho - 1)$ being a power of a prime and $g = 12$, the Gallager lower bound $N \geqslant \rho(\rho-1)^2 + \rho(\rho-1) + \rho$ is also tight. For the other QC-LDPC cycle codes with girth 12, the tight lower bound on the block length N is unknown.

First, we can directly construct a QC-LDPC cycle code $\mathcal{C}_8$ of length ρL based on the following exponent matrix:

$$\boldsymbol{P}_8 = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 2 & \cdots & \rho-1 \end{bmatrix},$$

where the lifting size is L for $L \geqslant \rho$ and $\rho \geqslant 3$. We can see from (2) that the Tanner graph of the constructed code $\mathcal{C}_8$ is free of 4-cycles. That is, the code $\mathcal{C}_8$ has girth at least 8. In the Tanner graph of $\mathcal{C}_8$, there exist L 8-cycles of type $(0, 1, 2, 1)$ [5]. Therefore, the girth of $\mathcal{C}_8$ is 8 for $L \geqslant \rho$ and $\rho \geqslant 3$.

Next, we will construct another class of QC-LDPC cycle codes with girth 12 based on difference sets. As a subclass of difference sets, Singer perfect difference sets had been used to construct QC-LDPC cycle codes [8]. We first give some definitions and notations about difference sets.

Definition 1. Let G be an additive group of order v. For a given positive integer λ, a k-subset D of G is a (v, k, λ)-difference set if every nonzero element of G can be precisely represented by λ differences $x - y$ with $x, y \in D$. If the group G is abelian (or cyclic), we say the k-subset D is a (v, k, λ)-cyclic difference set. The difference sets with $\lambda = 1$ are called planar difference sets.

In order to facilitate a better understanding of difference sets, some examples are provided in Appendix A. In combinatorial mathematics, the next theorem follows.

Theorem 2. For q being a prime power, there exists a $(q^2 + q + 1, q + 1, 1)$-planar difference set.

Consider an additive group G of order $((\rho-1)^2 + (\rho-1) + 1)$ where $(\rho - 1)$ is a prime power. Under Theorem 2, let the ρ-subset $D = \{d_1, d_2, \ldots, d_\rho\}$ of G be a $((\rho-1)^2 + (\rho-1) + 1, \rho, 1)$-planar difference set. We employ the following exponent matrix

$$\boldsymbol{P} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ d_1 & d_2 & d_3 & \cdots & d_\rho \end{bmatrix}$$

to construct a QC-LDPC cycle code $\mathcal{C}_{12}$ with lifting size $((\rho-1)^2 + (\rho-1) + 1)$. In the following, we will prove that the girth of $\mathcal{C}_{12}$ is 12.

Firstly, we show that the elements $d_1, d_2, \ldots, d_\rho$ are different from each other. Suppose that, for $1 \leqslant i \neq j \leqslant \rho$, there are two elements $d_i, d_j \in D$ such that $d_i = d_j$. For any element $d_k \in D$ such that $d_k \neq d_i$ $(\neq d_j)$, there exists a nonzero element $x = (d_k - d_i)$ of G. It can be expressed as a difference at least twice, i.e., $(d_k - d_i)$ and $(d_k - d_j)$. This contradicts the definition of the planar difference set. Hence, for $1 \leqslant i \neq j \leqslant \rho$, $d_i \neq d_j$. Based on (2), it can be proved that the Tanner graph of $\mathcal{C}_{12}$ is free of 4-cycles.

Secondly, we prove that there is no 8-cycle in the Tanner graph of $\mathcal{C}_{12}$. For any nonzero element x of G, there are two elements $d_a, d_b \in D$ such that $x = d_a - d_b$, and then $-x = d_b - d_a$. Since $\lambda = 1$, there is not a pair (d_s, d_t) $(d_s, d_t \in D)$ apart from (d_b, d_a) such that $-x = d_s - d_t$. That is, for two different pairs (d_a, d_b) and (d_s, d_t) (i.e., $(d_s, d_t) \neq (d_b, d_a)$), the equation $d_a - d_b + d_s - d_t = 0$ is not satisfied. Because of the random selection of d_a, d_b, d_s, d_t, we can see that, based on (3), the Tanner graph of $\mathcal{C}_{12}$ does not contain 8-cycles.

Hence, the girth of the code $\mathcal{C}_{12}$ is 12. It is clear that the code length of $\mathcal{C}_{12}$ achieves the Gallager lower bound. In the following, we will discuss all girth-12 QC-LDPC cycle codes whose code lengths achieve the Gallager lower bound.

Theorem 3. Let $\mathcal{C}$ be a girth-12 QC-LDPC cycle code of length $\rho\upsilon$ whose exponent matrix is

$$\boldsymbol{P}_{12} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ p_1 & p_2 & p_3 & \cdots & p_\rho \end{bmatrix}.$$

The lifting size of this code is $\upsilon = (\rho-1)^2 + (\rho-1) + 1$. For a group $G = Z_\upsilon$ under modulo-υ addition, the ρ-subset $D = \{p_1, p_2, \ldots, p_\rho\}$ of G is a $(\upsilon, \rho, 1)$-difference set (or $(\upsilon, \rho, 1)$-planar difference set).

Proof. Based on (2), we can see that the Tanner graph of the code $\mathcal{C}$ does not contain 4-cycles, since $p_1, p_2, \ldots, p_\rho$ are different from each other. There also do not exist 8-cycles of type (a, b, c, d) in the Tanner graph of $\mathcal{C}$ with $a, b, c, d \in D$. That is, the following equation is not satisfied:

$$a - b + c - d = 0 \ (\mathrm{mod}\ \upsilon).$$

Assume that D is not a $(\upsilon, \rho, 1)$-planar difference set. There exist $2 \cdot \binom{\rho}{2} = \rho(\rho-1)$ nonzero differences $x - y$ with $x, y \in D$. If these $\rho(\rho-1)$ differences are different from each other, then they can form the group G by adding the element 0. According to the definition of difference set, the ρ-subset D of G is a $(\upsilon, \rho, 1)$-planar difference set. This contradicts the assumption. Therefore, there are at least two same differences such that $p_{k_1} - p_{k_2} = p_{k_4} - p_{k_3} \neq 0$ with $(p_{k_1}, p_{k_2}) \neq (p_{k_4}, p_{k_3})$ and $1 \leqslant k_1, k_2, k_3, k_4 \leqslant \rho$. Hence, the following equation holds:

$$p_{k_1} - p_{k_2} + p_{k_3} - p_{k_4} = 0 \ (\mathrm{mod}\ \upsilon). \tag{4}$$

It is clear that $k_1 \neq k_2$ and $k_3 \neq k_4$. We consider the following three cases.

Case 1: $k_2 = k_3$. Then $p_{k_2} = p_{k_3}$. Eq. (4) becomes $p_{k_1} = p_{k_4}$. This contradicts the fact that $(p_{k_1}, p_{k_2}) \neq (p_{k_4}, p_{k_3})$.

Case 2: $k_1 = k_4$. Then $p_{k_1} = p_{k_4}$. Eq. (4) becomes $p_{k_2} = p_{k_3}$, contradicting the fact that $(p_{k_1}, p_{k_2}) \neq (p_{k_4}, p_{k_3})$.

Case 3: $k_2 \neq k_3$ and $k_1 \neq k_4$. Let $p_{k_1} = a, p_{k_2} = b, p_{k_3} = c$, and $p_{k_4} = d$. Based on (3) and (4), we can see that there exist 8-cycles of type $(p_{k_1}, p_{k_2}, p_{k_3}, p_{k_4})$ in the Tanner graph of $\mathcal{C}$, clearly a contradiction.

This completes the proof. So the ρ-subset D of G is a $(\upsilon, \rho, 1)$-planar difference set.

From Theorem 3, we can see that, for $\upsilon = ((\rho-1)^2 + (\rho-1) + 1)$ and $(\rho-1)$ being a prime power, all girth-12 QC-LDPC cycle codes of length $\rho\upsilon$ whose exponent matrices are given by (1) are (or isomorphic to) the proposed ones constructed based on $(\upsilon, \rho, 1)$-planar difference sets. That is, there exists only one isomorphic QC-LDPC cycle code with girth 12, i.e., the proposed codes [7]. Notice that Theorems 2 and 3 can be also proved based on the difference matrices in [9].

Conclusion. In this study, we studied two classes of QC-LDPC cycle codes approaching Gallager lower bound, i.e., codes with girths 8 and 12, respectively. Numerical simulation results in Appendix B show that the proposed nonbinary LDPC cycle codes perform well over the AWGN channel under iterative decoding. Furthermore, according to these two classes of QC-LDPC cycle codes, some tight lower bounds on code length (or lifting size) of QC-LDPC cycle codes are given in Appendix C, and it will be helpful for constructing nonbinary LDPC cycle codes with large girths.

Acknowledgements This work was supported in part by National Natural Science Foundation of China (Grant Nos. 61801527, 61701368, U1504601).

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Chen C, Bai B, Shi G, et al. Nonbinary LDPC codes on cages: structural property and code optimization. IEEE Trans Commun, 2015, 63: 364–375

2 Li J, Liu K, Lin S, et al. A matrix-theoretic approach to the construction of non-binary quasi-cyclic LDPC codes. IEEE Trans Commun, 2015, 63: 1057–1068

3 Zhao S, Huang X, Ma X. Structural analysis of array-based non-binary LDPC codes. IEEE Trans Commun, 2016, 64: 4910–4922

4 Huang Q, Song L, Wang Z. Set message-passing decoding algorithms for regular non-binary LDPC codes. IEEE Trans Commun, 2017, 65: 5110–5122

5 Xu H, Chen C, Zhu M, et al. Nonbinary LDPC cycle codes: efficient search, design, and code optimization. Sci China Inf Sci, 2018, 61: 089303

6 Kim S, No J, Chung H, et al. Quasi-cyclic low-density parity-check codes with girth larger than 12. IEEE Trans Inform Theor, 2007, 53: 2885–2891

7 Tasdighi A, Banihashemi A H, Sadeghi M R. Efficient search of girth-optimal QC-LDPC codes. IEEE Trans Inform Theor, 2016, 62: 1552–1564

8 Chen C, Bai B, Wang X. Construction of nonbinary quasi-cyclic LDPC cycle codes based on singer perfect difference set. IEEE Commun Lett, 2010, 14: 181–183

9 Amirzade F, Sadeghi M R. Lower bounds on the lifting degree of QC-LDPC codes by difference matrices. IEEE Access, 2018, 6: 23688–23700