



## TYPE-II APM-LDPC CODES WITH GIRTH 6

Mohammad Gholami<sup>1</sup> and Zahra Gholami<sup>2</sup>

<sup>1</sup> Department of Applied Mathematics and Computer Science  
Faculty of Mathematics and Statistics, University of Isfahan, Iran

<sup>2</sup> Department of Mathematics  
Shahrekord University, Shahrekord, Iran

ORCID IDs: Mohammad Gholami  
Zahra Gholami

 <https://orcid.org/0000-0002-3174-0138>  
 N/A

**Abstract.** In this paper, for the first time, *Type-II APM-LDPC codes* are presented as a class of APM-LDPC codes whose parity-check matrices (PCMs) include blocks comprising by combining two non-overlapping APMs. Then, some conditions are provided to give Type-II APM-LDPC codes with girth at least 6 and a table containing of the 4-cycle free constructed codes with will be given.

**Keywords:** LDPC codes, girth, affine permutation matrix.

### 1. Introduction

Low-density parity-check (LDPC) codes [2], as a main class of error correcting linear codes, can be specified by their sparse parity-check matrices (PCM's) and their associated Tanner graphs. Although the minimum-distance of LDPC codes is less than that of the best known linear codes, due to their structures, they are suitable for low-complexity iterative decoding methods, such as *Pearl's belief propagation (BP) algorithm*, adopted in many practical applications. The performance of LDPC codes of small length may be strongly affected by their cycle properties such as *girth*. In fact, the girth, i.e. the shortest cycles in the Tanner graph, is one important factor [5, 4, 3, 6, 1] to design LDPC codes with good error-correcting properties.

---

Received August 14, 2023, accepted: September 07, 2024

Communicated by Mojtaba Bahramian, Amirhossein Nokhodkar and Predrag Stanimirović

Corresponding Author: Mohammad Gholami. E-mail addresses: gholamimoh@gmail.com (M. Gholami), zghbaba123@gmail.com (Z. Gholami)

2020 *Mathematics Subject Classification*. Primary 11H71; Secondary 11T71, 14G50

© 2024 BY UNIVERSITY OF NIŠ, SERBIA | CREATIVE COMMONS LICENSE: CC BY-NC-ND

*Quasi-cyclic* (QC) LDPC codes [1] are the most promising class of structured LDPC codes due to their ease of hardware implementation using simple shift registers and excellent performance over noisy channels when they are decoded by message-passing algorithms. The PCM's of QC-LDPC codes are comprised of blocks of circulant matrices, classified by the researchers as *type-I*, *type-II* and *type-III* QC-LDPC codes, if each block is a combination of at-most one, two and three circulant permutation matrices (CPMs), respectively. On the other hand, recently, some attention have been paid on a class of low-density parity-check codes from affine permutation matrices, called (Type-I) APM-LDPC codes, in [5, 4, 3], where they have some advantages than QC-LDPC codes in terms of minimum-distance, cycle distributions, girths and error-rate performances. In this paper, for the first time, we deal about the construction of *Type-II APM-LDPC codes* as a class of APM-LDPC codes whose parity-check matrices (PCMs) include blocks which combine two non-overlapping APMs. Then, we give some conditions to attain 4-cycle free Type-II APM-LDPC codes. Finally, some constructed Type-II APM-LDPC codes with girth at least 6 will be provided as a table.

## 2. Type-II APM-LDPC Codes

Let  $m, s, a$  be some positive integers with  $0 \leq s, a < m$  and  $\gcd(m, a) = 1$ . In fact, if  $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$  and  $\mathbb{Z}_m^* = \{i \in \mathbb{Z}_m \mid \gcd(i, m) = 1\}$ , then  $(s, a) \in \mathbb{Z}_m \times \mathbb{Z}_m^*$ . By the *APM matrix*  $\mathcal{I}_m^{s,a}$ , or  $\mathcal{I}^{s,a}$  when  $m$  is known, with *slope value*  $s$  and *shift value*  $a$ , we mean the  $m \times m$  permutation matrix  $(e_{i,j})_{0 \leq i, j \leq m-1}$ , for which  $e_{i,j} = 1$  if and only if  $i = aj + s \pmod m$ . For example, for  $m = 7$ , we have

$$\mathcal{I}^{3,4} = \begin{pmatrix} \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{pmatrix}.$$

In continue, we need the summation of two arbitrary APMs to be non-overlapping, i.e. they have not any common non-zero element in the same position. In other words, if  $\mathcal{I}^{s,a} = (e_{i,j})_{0 \leq i, j \leq m-1}$  and  $\mathcal{I}^{s',a'} = (e'_{i,j})_{0 \leq i, j \leq m-1}$  are such APMs, then  $e_{i,j} \times e'_{i,j} \neq 1$ , for each  $0 \leq i, j \leq m-1$ . Now, the following lemma guarantee the non-overlap condition by choosing proper slope and shift values.

**Lemma 2.1.** *Two APMs  $\mathcal{I}^{s,a}$  and  $\mathcal{I}^{s',a'}$  have not any overlap, if and only if*

$$\gcd(a - a', m) \nmid s - s'.$$

*Proof.* Clearly, for each two matrices  $\mathcal{I}^{s,a}$  and  $\mathcal{I}^{s',a'}$ , the nonzero elements do not coincide if and only if the equations  $x = ay + s \pmod m$  and  $x = a'y + s' \pmod m$  are not hold simultaneously which is true, if  $\gcd(a - a', m) \nmid s - s'$ .  $\square$

For the case that  $m$  is prime, Lemma 2.2 is hold iff  $a = a'$ . Moreover, for each  $m$ , if  $a = a'$ , then Lemma 2.2 is true if  $s \neq s'$ . In general, for the case that  $s = s'$ , Lemma 2.2 does not hold.

Now, for given integers  $v, k, v < k$ , a type-II APM-LPC code with APM-size  $m$  is defined by giving the following parity-check matrix:

$$(2.1) \quad \mathcal{H} = \begin{pmatrix} \mathcal{I}^{s_{1,1}, a_{1,1}} + \mathcal{I}^{s'_{1,1}, a'_{1,1}} & \mathcal{I}^{s_{1,2}, a_{1,2}} + \mathcal{I}^{s'_{1,2}, a'_{1,2}} & \dots & \mathcal{I}^{s_{1,k}, a_{1,k}} + \mathcal{I}^{s'_{1,k}, a'_{1,k}} \\ \mathcal{I}^{s_{2,1}, a_{2,1}} + \mathcal{I}^{s'_{2,1}, a'_{2,1}} & \mathcal{I}^{s_{2,2}, a_{2,2}} + \mathcal{I}^{s'_{2,2}, a'_{2,2}} & \dots & \mathcal{I}^{s_{2,k}, a_{2,k}} + \mathcal{I}^{s'_{2,k}, a'_{2,k}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{I}^{s_{v,1}, a_{v,1}} + \mathcal{I}^{s'_{v,1}, a'_{v,1}} & \mathcal{I}^{s_{v,2}, a_{v,2}} + \mathcal{I}^{s'_{v,2}, a'_{v,2}} & \dots & \mathcal{I}^{s_{v,k}, a_{v,k}} + \mathcal{I}^{s'_{v,k}, a'_{v,k}} \end{pmatrix}$$

in which  $(s_{i,j}, a_{i,j})$  and  $(s'_{i,j}, a'_{i,j}), 1 \leq i \leq v, 1 \leq j \leq k$ , are some elements belong to  $\mathbb{Z}_m \times \mathbb{Z}_m^*$  such that each two matrices  $\mathcal{I}^{s_{i,j}, a_{i,j}}$  and  $\mathcal{I}^{s'_{i,j}, a'_{i,j}}$  have not any overlap, i.e. they have not any common non-zero element in the same position. On the other hand, if  $\mathcal{I}^{s_{i,j}, a_{i,j}} = (e_{s,t})_{0 \leq s, t \leq m-1}$  and  $\mathcal{I}^{s'_{i,j}, a'_{i,j}} = (e'_{s,t})_{0 \leq s, t \leq m-1}$ , then  $e_{s,t} \times e'_{s,t} \neq 1$ , for each  $0 \leq s, t \leq m-1$ . Now, the following lemma guarantee the non overlap condition by choosing proper slope and shift values.

**Lemma 2.2.** *Two APMs  $\mathcal{I}^{s,a}$  and  $\mathcal{I}^{s',a'}$  have not any overlap, if and only if*

$$\gcd(a - a', m) \nmid s - s'.$$

*Proof.* Clearly, for each two matrices  $\mathcal{I}^{s,a}$  and  $\mathcal{I}^{s',a'}$ , the nonzero elements do not coincide if and only if the equations  $x = ay + s \pmod m$  and  $x = a'y + s' \pmod m$  are not hold simultaneously which is true, if  $\gcd(a - a', m) \nmid s - s'$ .  $\square$

**Example 2.1.** For  $(s, a), (s', a') = (3, 5), (2, 7)$  and  $m = 8$ , Lemma 2.2 is hold which result the following  $8 \times 8$  matrix with row (column) weight 2.

$$\mathcal{I}^{3,5} + \mathcal{I}^{2,7} = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

For example, for positive integer  $n$ , let  $m = p^n - 1$ , and for each  $1 \leq i \leq v$  and  $1 \leq j \leq k$ , set  $s_{i,j} = (i + j - 2)p, a_{i,j} = p^{i+j-2}, s'_{i,j} = (i + j - 1)p$  and  $a'_{i,j} = p^{i+j-1}$ . Then, for each  $i, j$ , the condition of Lemma 2.2 is satisfied, because,  $\gcd(a'_{i,j} - a_{i,j}, m) = p - 1 \nmid p = s'_{i,j} - s_{i,j}$ .

In continue, we give some conditions in which the constructed APM-LDPC codes with PCM's given by Eq. 2.1 are free of 4-cycles.

**Theorem 2.1.** *For the PCM  $H$  given by Eq. 2.1, there is a 4-cycle in  $TG(H)$  if and only if one of the following conditions holds.*

$(v, k)$	$g$	$m$	$S$
(2,3)	8	12	[3,1,10,11,0,11,11,1,9,11,5,11,8,1,11,11,6,11]
(2,4)	8	16	[1,13,3,7,13,3,9,13,9,3,7,7,13,13,15,7,11,7,12,1,5,3,10,15]
(2,5)	8	20	[7,17,7,9,0,17,15,17,4,17,12,17,3,17,1,1,5,1,13,13,16,17,3,9,16,1,18,13,15,9]
(2,6)	8	24	[15,11,6,13,14,13,2,1,18,13,13,23,1,19,1,7,11,7,9,19,10,13,8,13,18,1,20,13,9,7,7,11,23,23,0,13]
(2,7)	8	28	[15,1,24,9,27,23,3,15,21,9,11,9,18,1,0,23,17,9,17,15,4,23,16,23,12,15,10,9,9,9,9,15,22,23,2,23,24,1,7,9,12,23]
(2,8)	8	32	[31,3,23,3,9,15,14,5,15,19,21,23,24,1,4,25,0,1,6,21,17,15,18,13,13,23,11,11,19,11,4,9,26,13,25,15,26,13,1,15,30,5,23,3,22,5,7,3]
(2,9)	8	36	[13,13,19,11,29,5,26,25,3,35,20,5,34,31,1,11,21,35,7,13,2,5,31,11,4,13,25,29,10,11,15,1,0,35,13,11,10,31,35,23,23,5,24,19,18,35,16,11,32,7,12,17,34,11]
(2,10)	8	40	[21,33,0,33,26,37,18,9,4,13,30,37,11,37,2,17,23,21,32,21,29,29,33,29,29,13,12,33,27,21,10,9,8,13,16,13,24,21,24,13,15,1,33,13,28,13,34,17,36,21,22,17,9,29,14,29,13,29,7,21]
(3,4)	6	19	[12,1,18,13,10,13,18,5,1,5,13,1,7,13,1,13,3,5,0,5,9,1,5,13,15,13,12,5,16,5,1,1,13,13,17,13,7,5,13,5]
(3,5)	6	25	[11,21,6,18,10,23,4,12,10,7,8,11,3,8,9,3,17,22,11,2,18,11,15,23,23,8,9,12,21,2,16,21,24,3,14,3,13,17,24,12,3,11,21,18,12,13,0,7,18,17]
(3,6)	6	31	[28,1,17,4,7,4,2,6,1,6,4,1,0,4,22,4,21,6,27,6,24,1,27,4,12,4,11,6,29,6,26,1,3,4,1,4,25,6,15,6,6,1,11,4,28,4,13,6,10,6,2,1,13,4,2,4,18,6,4,6]
(3,7)	6	37	[15,1,2,32,27,32,0,30,26,30,16,1,10,32,0,32,5,30,29,30,34,1,20,32,11,32,32,30,1,30,17,1,1,32,34,32,2,30,27,30,10,1,22,32,23,32,16,30,23,30,1,1,9,32,25,32,14,30,18,30,32,1,7,32,29,32,13,30,22,30]
(3,8)	6	41	[6,1,39,5,21,5,3,14,23,14,5,1,20,5,13,5,18,14,27,14,22,1,31,5,15,5,14,14,12,14,3,1,12,5,22,5,11,14,29,14,17,1,14,5,19,5,9,14,25,14,14,1,30,5,33,5,31,14,26,14,37,1,6,5,23,5,0,14,7,14,31,1,18,5,40,5,19,14,20,14]
(3,9)	6	47	[10,1,22,17,12,17,42,26,12,26,41,1,18,17,7,17,38,26,30,26,36,1,29,17,4,17,5,26,43,26,42,1,6,17,23,17,37,26,25,26,3,1,31,17,17,17,20,26,24,26,4,1,46,17,42,17,4,26,29,26,24,1,41,17,1,17,1,26,28,26,32,1,37,17,19,17,8,26,13,26,1,1,2,17,5,17,2,26,18,26]
(3,10)	6	53	[38,1,8,43,28,43,21,49,8,49,41,1,15,43,34,43,39,49,0,49,5,1,51,43,9,43,51,49,7,49,49,1,11,43,5,43,25,49,3,49,29,1,21,43,38,43,19,49,22,49,31,1,7,43,39,43,37,49,20,49,33,1,45,43,35,43,16,49,26,49,44,1,16,43,14,43,6,49,33,49,1,1,26,43,40,43,43,49,11,49,37,1,44,43,13,43,24,49,28,49]

Table 2.1: The slope-shift vectors  $S$  corresponding to some  $(v, k)$  Type-II APM-LDPC codes with girth  $g$  and APM-size  $m$

$$\begin{aligned}
1. & a_{i_0, j_0}^{(t_0)} a_{i_1, j_1}^{(t_2)} = a_{i_1, j_0}^{(t_1)} a_{i_0, j_1}^{(t_3)}, \quad a_{i_0, j_1}^{(t_3)} (s_{i_1, j_0}^{(t_1)} - s_{i_1, j_1}^{(t_2)}) = a_{i_1, j_1}^{(t_2)} (s_{i_0, j_0}^{(t_0)} - s_{i_0, j_1}^{(t_3)}) \\
2. & a_{i_0, j_0}^{(t_0)} a_{i_1, j_1}^{(t_2)} \neq a_{i_1, j_0}^{(t_1)} a_{i_0, j_1}^{(t_3)}, \\
& \gcd(a_{i_0, j_0}^{(t_0)} a_{i_1, j_1}^{(t_2)} - a_{i_1, j_0}^{(t_1)} a_{i_0, j_1}^{(t_3)}, m) | a_{i_1, j_0}^{(t_1)} a_{i_0, j_1}^{(t_3)} s_{i_0, j_0}^{(t_0)} + a_{i_0, j_0}^{(t_0)} a_{i_0, j_1}^{(t_3)} (s_{i_1, j_1}^{(t_2)} - s_{i_1, j_0}^{(t_1)}) - \\
& a_{i_0, j_0}^{(t_0)} a_{i_1, j_1}^{(t_2)} s_{i_0, j_1}^{(t_3)}
\end{aligned}$$

For type-II APM-IDPC codes with PCMs  $\mathcal{H}$  given by Eq. 2.1, without loss of generality, we set  $(s_{1,i}, a_{1,i}) = (0, 1)$ , for each  $1 \leq i \leq k$ . Because, otherwise, under the equivalence relations between the codes, the  $i$ th column block of  $\mathcal{H}$  can be multiplied by  $(\mathcal{I}^{s_{1,i}, a_{1,i}})^{-1} = \mathcal{I}^{-s_{1,i}, a_{1,i}^{-1}, a_{1,i}^{-1}}$ .

Then, other slopes and shifts of  $\mathcal{H}$  are arranged column-by-column from top to the bottom, briefly as the following slope-shift vector.

$$S = (s'_{1,1}, a'_{1,1}, s_{2,1}, a_{2,1}, s'_{2,1}, a'_{2,1}, \dots, s_{v,1}, a_{v,1}, s'_{v,1}, a'_{v,1}, s'_{1,2}, a'_{1,2}, s_{2,2}, a_{2,2}, s'_{2,2}, a'_{2,2}, \dots, s_{v,k}, a_{v,k}, s'_{v,k}, a'_{v,k})$$

Now, applying Theorem 2.1, Table 2.1 has provided some slope-shift vectors corresponding to  $(v, k)$  type-II APM-LDPC codes which are free of 4-cycles.

### 3. Conclusion

This paper discusses about the construction of fully connected type-II APM-LDPC codes with girth at least 6. In fact, a necessary and sufficient condition is provided to have 4-cycles in the Tanner graph of these codes. Finally, for  $v = 2, 3$  and  $k \leq 10$ , the paper provides some  $(v, k)$  type-II APM-LDPC codes given by Table 2.1.

### Acknowledgement

This work was supported in part by the research council of the University of Isfahan. The authors were supported in part by the research council of Shahrekord university.

### REFERENCES

1. M. P. FOSSORIER: *Quasi-cyclic low density parity-check codes from circulant permutation matrices*. IEEE Transactions on Information Theory, **50**(8) (2004), 1788–1793.
2. R. GALLAGER: *Low-density parity-check codes*. IRE Transactions on information theory, **8**(1) (1962), 21–28.
3. M. GHOLAMI and M. ALINIA: *Explicit APM-LDPC codes with girths 6, 8, and 10*. IEEE Signal Processing Letters, **24**(6) (2017), 741–745.
4. M. GHOLAMI and M. ALINIA: *High-performance binary and non-binary low-density parity-check codes based on affine permutation matrices*. IET Communications, **9**(17) (2015), 2114–2123.
5. S. MYUNG, K. YANG and D.S. PARK: *A combining method of structured LDPC codes from affine permutation matrices*. In 2006 IEEE International Symposium on Information Theory, (2006), 674–678.
6. M. E. O’SULLIVAN: *Algebraic construction of sparse matrices with large girth*. IEEE Transactions on Information Theory, **52**(2) (2006), 718–727.