4-CYCLE FREE APM-LDPC CODES WITH AN EXPLICIT CONSTRUCTION

Z. GHOLAMI AND M. GHOLAMI*

ABSTRACT. Recently, attention has been focused on a class of low-density parity-check codes from affine permutation matrices, called APM-LDPC codes, having some advantages than quasi-cyclic (QC) LDPC codes in terms of minimum-distance, cycle distribution and error-rate performance. Moreover, some explicit constructions for exponent matrices of conventional APM-LDPC codes with girth at least 6 have been investigated. In this paper, a class of 4-cycle free APM-LDPC codes is constructed by a new explicit method such that the constructed codes have better cycle distributions rather than the recently proposed APM codes with girth 6. As simulation results show, the constructed codes outperform PEG and random-like LDPC codes with the same rates and lengths.

1. PRELIMINARIES

For given positive integer $m$, let $\mathbb{Z}_m = \{0, 1, \ldots, m - 1\}$ be the ring of integers modulo $m$ and $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \gcd(a, m) = 1\}$ be the set of elements in $\mathbb{Z}_m$ which are relatively prime to $m$. Now, for each $(s, a) \in \mathbb{Z}_m \times \mathbb{Z}_m^*$, define affine permutation (AP) matrix $\mathcal{I}_{s,a}^m$, briefly $\mathcal{I}_{s,a}$ when $m$ is known, to be the $m \times m$ binary matrix $(p_{i,j})_{0 \leq i,j \leq m-1}$ in which $p_{i,j} = 1$ if and only if $i = aj + s \mod m$. In fact, in $\mathcal{I}_{s,a}$, the row-index of 1 in the first column is $s$ and each column is shifted down...
by a with respect to the previous column. Some of the properties of AP matrices can be seen easily as follows [3].

1. \( I^{s_1,a_1} \times I^{s_2,a_2} = I^{s_1+s_2,a_1a_2} \).
2. \( I^{s_1,a_1}/I^{s_2,a_2} = I^{s_1-s_2a_1a_2^{-1},a_1a_2^{-1}} \).
3. \( (I^{s,a})^{-1} = (I^{s,a})^T = I^{-s^{-1},a^{-1}} \).
4. \( (I^{s,a})^n = \begin{cases} I^{s+n,1}/a^n & a \neq 1 \\ I^{sn,1} & a = 1 \end{cases} \).

By the above relations, it is clear that the set of all APs of size m, i.e. \( \{I^{s,a} : (s,a) \in \mathbb{Z}_m \times \mathbb{Z}_m^* \} \), with the multiplication operation, forms a non-abelian group of order \( m \times \phi(m) \), where \( \phi(m) = |\mathbb{Z}_m^*| \) is the phi-Euler’s function.

Now, for a given \( J \times L \) fully-one matrix \( B \), let \( E = (e_{i,j})_{0 \leq i \leq J-1, 0 \leq j \leq L-1} \) be a \( J \times L \) array on \( \mathbb{Z}_m \times \mathbb{Z}_m^* \), i.e. each element \( e_{i,j} \) is a pair \((s_{i,j}, a_{i,j}) \) \in \( \mathbb{Z}_m \times \mathbb{Z}_m^* \). The \((J, L)\) APM-LDPC code with base matrix \( B \), APM-size \( m \) and exponent matrix \( E \) can be defined as an LDPC code having the following parity-check matrix.

\[
H_{m,E} = \begin{pmatrix}
I^{s_0,0,a_0,0} & \cdots & I^{s_0,L-1,a_0,L-1} \\
\vdots & \ddots & \vdots \\
I^{s_{J-1},0,a_{J-1},0} & \cdots & I^{s_{J-1,L-1},a_{J-1},L-1}
\end{pmatrix} \quad \text{(1.1)}
\]

In the literature, the \( J \times L \) matrices \( S = (s_{i,j})_{0 \leq i \leq J-1, 0 \leq j \leq L-1} \) and \( A = (a_{i,j})_{0 \leq i \leq J-1, 0 \leq j \leq L-1} \) are called slope and shift matrices, respectively. It is noticed that, if an element of \( E \) is greater than \( m \), in construction of \( H_{m,E} \), such element is considered to be modulo \( m \). Especially, if \( a_{i,j} = 1 \) for each \( 0 \leq i \leq J-1 \) and \( 0 \leq j \leq L-1 \), then \( H_{m,E} \) in (1.1) can be considered as the parity-check matrix of a QC-LDPC code with circulant permutation matrix (CPM) size \( m \). Moreover, after some elementary row (column) operations on \( H_{m,E} \), it may be considered as the parity-check matrix of a QC-LDPC code. The following theorem gives a necessary condition such that \( H_{m,E} \) is the parity-check matrix of a QC-LDPC code.

**Theorem 1.1.** If \( (s_i^{(r)}, a_i^{(r)}) \) \in \( \mathbb{Z}_m \times \mathbb{Z}_m^* \), \( 0 \leq i \leq J-1 \), and \( (s_j^{(c)}, a_j^{(c)}) \) \in \( \mathbb{Z}_m \times \mathbb{Z}_m^* \), \( 0 \leq j \leq L-1 \), are given such that for each \( i, j \), \( a_i^{(r)} a_j^{(c)} a_{i,j} = 1 \) mod \( m \), then \( H_{m,E} \) can be considered as the parity-check matrix of a QC-LDPC code.

**Proof.** For \( 0 \leq i \leq J-1 \) and \( 0 \leq j \leq L-1 \), multiplying the \( i \)th row-block of \( H_{m,E} \) by \( I^{(s_i^{(c)}, a_i^{(r)})} \) and then multiplying the \( j \)th column-block of \( H_{m,E} \) by \( I^{(s_j^{(r)}, a_j^{(c)})} \), the matrix \( H_{m,E'} \) with exponent matrix
For given positive integers \(1 \leq p \leq \text{gcd}(v_0, v_1)\), each \(i, j\) in \(\{1, 2, \ldots, r\}\), we have
\[
\mathcal{H}_{m, E'} = \left(\left(\sum a_{i,j}^{(p)} s_{i,j} + s_{i,j}^{(v)} a_{i,j}^{(v)} \right) a_{i,j}^{(v)} a_{i,j}^{(v)} \right) \in \mathbb{Z}_m \times \mathbb{Z}_m^*.
\]
Now, if \(a_{i,j}^{(p)} a_{i,j}^{(v)} = 1\), for each \(i, j\), then \(\mathcal{H}_{m, E'}\) is the parity-check matrix of a QC-LDPC code and the proof is completed. \(\Box\)

**Example 1.2.** For given positive integers \(J\) and \(L\), and prime number \(m > JL\), the matrix \(A = (a_{i,j})\), \(a_{i,j} = (i + 1)(j + 1)\), \(0 \leq i \leq J - 1\), \(0 \leq j \leq L - 1\), can be considered as a \((J, L)\)-shift matrix of an APM-LDPC code \(\mathcal{C}\), because for each \(i, j\) we have \(\text{gcd}(a_{i,j}, m) = 1\). Now, substituting \(a_{i,j}^{(p)} = (i + 1)^{-1} (\text{mod } m)\) and \(a_{i,j}^{(v)} = (j + 1)^{-1} (\text{mod } m)\) in Theorem 1.1, we have \(a_{i,j}^{(p)} a_{i,j}^{(v)} = 1 (\text{mod } m)\), and so \(\mathcal{C}\) is equivalent to a QC-LDPC code.

The following theorem gives a necessary and sufficient condition for the existence of a 2\(l\)-cycle in the Tanner graph of a \((J, L)\) APM-LDPC code with the parity-check matrix \(\mathcal{H}_{m, E}\).

**Theorem 1.3.** ([3]) A 2\(l\)-cycle in \(\text{TG}(\mathcal{H}_{m, E})\) exists if and only if there is a chain \((i_0, j_0); (i_1, j_1); \ldots; (i_{l-1}, j_{l-1}); (i_l, j_l) = (i_0, j_0)\), \(0 \leq i_k \neq i_{k+1} \leq J - 1\) and \(0 \leq j_k \neq j_{k+1} \leq L - 1\), such that one of the following relations holds:

1. \(p_0 = 1\) and \(A = 0\).
2. \(\text{gcd}(p_0 - 1, m)\)\(|A\).

in which \(p_h = \prod_{k=0}^{l-1} a_{i_k,j_k}^{-1} a_{i_{k+1},j_{k+1}}^{-1} \mod \, m\), \(0 \leq h \leq l - 1\), \(p_l = p_0\), and \(A = \sum_{k=0}^{l-1} (p_k s_{i_k,j_k} - p_{k+1} s_{i_{k+1},j_{k+1}}) \mod \, m\).

In particular case, if \(l = 2\), then Theorem 1.3 can be summarized as follows.

**Corollary 1.4.** \(\text{TG}(\mathcal{H}_{m, E})\) is free of 4-cycles if and only if for each \(0 \leq i_0 < i_1 < J - 1\) and \(0 \leq j_0 < J_1 \leq L - 1\), we have \(v \neq 0\) if \(u = 0\) or otherwise \(\text{gcd}(u, m) \nmid v\), in which \(u = a_{i_0,j_0} a_{i_1,j_1}^{-1} a_{i_1,j_0} - a_{i_1,j_1} a_{i_0,j_0} \mod \, m\) and \(v = a_{i_0,j_1} a_{i_1,j_0} (s_{i_0,j_0} - s_{i_0,j_1}) + a_{i_0,j_0} a_{i_0,j_1} (s_{i_1,j_1} - s_{i_1,j_0}) \mod \, m\).

**Proof.** Setting \(l = 2\) in Theorem 1.3, we have \(p_0 = a_{i_0,j_0} a_{i_1,j_0}^{-1} a_{i_0,j_1} - a_{i_1,j_1} a_{i_0,j_0} \mod \, m\) and \(A = a_{i_1,j_0} a_{i_0,j_0}^{-1} a_{i_0,j_1} a_{i_0,j_1}^{-1} (s_{i_0,j_0} - s_{i_0,j_1}) + a_{i_0,j_0} a_{i_0,j_1} (s_{i_1,j_1} - s_{i_1,j_0}) \mod \, m\). On the other hand, by the proof of Theorem 1.3 in [3], the existence of a 4-cycle in \(\text{TG}(\mathcal{H})\) is related to the resolvability of the equation \((p_0 - 1)x = A \mod \, m\), which can be solved if and only if \(a_{i_0,j_0} a_{i_1,j_1} (p_0 - 1)x = a_{i_0,j_0} a_{i_1,j_1} A \mod \, m\) is resolvable, because \(\text{gcd}(a_{i_0,j_0} a_{i_1,j_1}, m) = 1\). Now, this equation is simplified as \(ux = v\).
For prime $2.1$

Substituting $1.4$ is not equivalent to a QC-LDPC code, because by Theorem $\text{where}$ $e$ if and only if $a$

$a$

$i$ of two functions in terms of the variables $1$

$e$ the expression $1.1$

$\text{On the other hand, if } e < k - 2, \text{then } u \neq 0, \text{because } \nu_p(u) = e + 2 < \nu_p(m) = k$ and $(j_1 - j_0)(i_1 - i_0) \neq 0$. In this case, $\gcd(u, m) = p^{e+2}$ which is not divisible by $v$, because $\nu_p(v) = \nu_p((j_1 - j_0)(i_1 - i_0)) = e < e + 2 = \nu_p(\gcd(u, m))$. On the other hand, if $e \geq k - 2$, then $u = 0$, but $v \neq 0$, because $v = 0$ if and only if $(j_1 - j_0)(i_1 - i_0) = 0 \mod m$. However, $(j_1 - j_0)(i_1 - i_0) \neq 0 \mod m$, because $0 < (j_1 - j_0)(i_1 - i_0) \leq (J - 1)(L - 1) < p^k = m. \ □$

It is worth noticing that the APM-LDPC code constructed by Theorem 2.1 is not equivalent to a QC-LDPC code, because by Theorem 1.1, the expression $\frac{1}{(i+j)p+1}$ can not be decomposed to the multiplications of two functions in terms of the variables $i$ and $j$. On the other hand, $a_{i,j} = (i + j)p + 1$ is always prime respect to $m = p^k$, for each $i, j$. 

Cycles, especially cycles of length 4, in the Tanner graph of an LDPC code degrade the performance of LDPC decoders. Therefore, design of LDPC codes free of 4-cycles is of great interest. Here, for enough large $m$, we give some exponent matrices $E$ explicitly such that $H_{m,E}$ has girth 6. In fact, an exponent matrix $E$ is constructed explicitly with the lower-bound $Q(E)$, such that $g(H_{m,E}) \geq 6$ for each $m \geq Q(E)$.

2. Explicit Constructions of APM-LDPC Codes with Girth at Most 6

In order to construct APM-LDPC codes with girth 6, we start from the following theorem. Before that, for positive integers $m$ and prime $p$, define $\nu_p(m)$ to be the largest power of $p$ which divides $m$, i.e. $\nu_p(m) = e$ if and only if $p^e | m$ and $p^{e+1} \nmid m$. Clearly, for two integers $a, b$, we have $\nu_p(ab) = \nu_p(a) + \nu_p(b)$, so $\nu_p(p^ka) = k + \nu_p(a)$, $\nu_p((kp + 1)a) = \nu_p(a)$ and if $a | b$, then $\nu_p(a) \leq \nu_p(b)$. Moreover, by the Legendre’s formula $[13]$ for the factorial of an integer number, we have $\nu_p(m!) = \sum_{i=1}^{\infty} \lfloor \frac{m}{p^i} \rfloor$, where $[x]$ is the floor function. Moreover, for each integer $m = 1 \times 3 \times 5 \times \cdots \times (2N - 1)$, we have $\nu_p(m) = \nu_p((2N)! - \nu_p(N!)$.

**Theorem 2.1.** For prime $p$ and integers $J, L$, $J < L$, let $E = (e_{i,j})$, be a $(J, L)$-exponent matrix, such that $e_{i,j} = (s_{i,j}, a_{i,j})$, in which $s_{i,j} = ij$ and $a_{i,j} = (i + j)p + 1$, $0 \leq i \leq J - 1$ and $0 \leq j \leq L - 1$. Then, for each $m = p^k$, $k > \log_p (J - 1)(L - 1)$, we have $g(H_{m,E}) \geq 6$.

**Proof.** Substituting $s_{i,j}$ and $a_{i,j}$ in Corollary 1.4, we have $u = p^2((j_1 - j_0)(i_1 - i_0)) \mod m$ and $v = (i_0 - i_1)(j_0 - j_1)(kp + 1) \mod m$, where $k = (i_0j_0 + j_0j_1)p + i_0 + j_0 + j_1$. Let $e = \nu_p((j_1 - j_0)(i_1 - i_0))$. Now, if $e < k - 2$, then $u \neq 0$, because $\nu_p(u) = e + 2 < \nu_p(m) = k$ and $(j_1 - j_0)(i_1 - i_0) \neq 0$. In this case, $\gcd(u, m) = p^{e+2}$ which is not divisible by $v$, because $\nu_p(v) = \nu_p((j_1 - j_0)(i_1 - i_0)) = e < e + 2 = \nu_p(\gcd(u, m))$. On the other hand, if $e \geq k - 2$, then $u = 0$, but $v \neq 0$, because $v = 0$ if and only if $(j_1 - j_0)(i_1 - i_0) = 0 \mod m$. However, $(j_1 - j_0)(i_1 - i_0) \neq 0 \mod m$, because $0 < (j_1 - j_0)(i_1 - i_0) \leq (J - 1)(L - 1) < p^k = m. \ □$
Table 1. A comparison between the number of 6,8-cycles of the constructed codes with some explicit QC, APM and AQC-LDPC codes in [12], [4] and [5]

<table>
<thead>
<tr>
<th>3</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>16</td>
<td>744</td>
<td>16</td>
<td>1192</td>
</tr>
<tr>
<td>6</td>
<td>16</td>
<td>1856</td>
<td>16</td>
<td>2432</td>
</tr>
<tr>
<td>7</td>
<td>16</td>
<td>3832</td>
<td>16</td>
<td>4568</td>
</tr>
<tr>
<td>8</td>
<td>16</td>
<td>7008</td>
<td>16</td>
<td>7904</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>32</td>
<td>3232</td>
<td>16</td>
</tr>
<tr>
<td>6</td>
<td>16</td>
<td>7760</td>
<td>16</td>
<td>8800</td>
</tr>
<tr>
<td>7</td>
<td>16</td>
<td>25480</td>
<td>16</td>
<td>29528</td>
</tr>
<tr>
<td>8</td>
<td>16</td>
<td>81120</td>
<td>16</td>
<td>97088</td>
</tr>
<tr>
<td>5</td>
<td>32</td>
<td>32</td>
<td>113344</td>
<td>31</td>
</tr>
</tbody>
</table>

Example 2.2. For \( p = 5 \), let \( E \) be the following \( 5 \times 7 \) exponent matrix given by Theorem 2.1.

\[
\begin{pmatrix}
(0, 1) & (0, 6) & (0, 11) & (0, 16) & (0, 21) & (0, 26) & (0, 31) \\
(0, 6) & (1, 11) & (2, 16) & (3, 21) & (4, 26) & (5, 31) & (6, 36) \\
(0, 11) & (2, 16) & (4, 21) & (6, 26) & (8, 31) & (10, 36) & (12, 41) \\
(0, 16) & (3, 21) & (6, 26) & (9, 31) & (12, 36) & (15, 41) & (18, 46) \\
(0, 21) & (4, 26) & (8, 31) & (12, 36) & (16, 41) & (20, 46) & (24, 51)
\end{pmatrix}
\]

For \( k \geq \lceil \log_5(5 - 1)(7 - 1) \rceil = 2 \), we have \( g(H_{m,E}) \geq 6 \). It is note that each element of \( E \) is reduced in modulo \( m \). For example, for \( m = 25 \), the element \((24, 51)\) in the above exponent matrix is reduced to \((24, 1)\).

3. Outputs

Table 1 provides some comparisons between the 6,8-cycle multiplicities of the constructed codes with block-size \( m \), on one hand, and some QC-LDPC codes [12] with CPM-size \( m_1 \), APM-LDPC codes [4] with APM-size \( m_2 \) and AQC-LDPC codes [5] with block size \( m_3 \) with some explicit constructions, on the other hand. All of the codes considered in this comparison have girth at least 6. In the table, \( n_{6,8} \) is the summation of 6,8 cycle multiplicities of the corresponding codes. As Table 1 shows, the constructed codes have better \( n_{6,8} \) rather than QC and AQC-LDPC codes, although, they have a close comparisons with the APM-LDPC codes in [4].

4. Simulation Results

For simulation results, we have used an additive white Gaussian noise (AWGN) channel, using software available online [7]. The decoding algorithm is sum-product with iteration number 50 and block number 1000. Figure 1 shows a bit error performance comparison between two
Figure 1. The constructed APM codes with different girths against Random and PEG LDPC codes

QC-LDPC codes with different girths having lifting degree 9600 lifted from the base matrix of the (3, 6) APM-LDPC code constructed explicitly, on one hand and a 4-cycle free randomly constructed LDPC code and an LDPC code from progressive edge growth (PEG) [9] with target girth 14, on the other hand. As the figure confirms, the constructed codes outperform random and PEG codes with the same lengths, rates and girths.

Acknowledgments

This work was supported in part by the research council of Shahrekord University.

REFERENCES

8. ⟨http://www.cs.toronto.edu/Radford/ldpc.software.html⟩.

**Zahra Gholami**
Department of Mathematics, University of Shahrekord, P.O. Box 8818634141, Shahrekord, Iran.
Email: zghbaba123@gmail.com

**Mohammad Gholami**
Department of Mathematics, University of Shahrekord, P.O. Box 8818634141, Shahrekord, Iran.
Email: gholami-m@sci.sku.ac.ir, gholamimoh@gmail.com
4-CYCLE FREE APM-LDPC CODES WITH AN EXPLICIT CONSTRUCTION

Z. GHOLAMI AND M. GHOLAMI

کده‌ای خلوت آفین فاقد دور به طول ۴ با یک ساختار صریح

زهرا غلامی و محمد غلامی

1) دانشگاه علوم ریاضی، دانشگاه شهید کیامیار، ایران

کلمات کلیدی: کده‌ای خلوت آفین، ساختارهای صریح، کمر.