Construction of Quasi-Cyclic Low-Density Parity-Check Codes Using Hamming Codewords

Haijing Zhong*, Shancheng Zhao†, Li Chen* and Xiao Ma‡

*School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou, China
†School of Information Science and Technology, Jinan University, Guangzhou, China
‡School of Data and Computer Science, Sun Yat-sen University, Guangzhou, China
Email: zhonghj6@mail2.sysu.edu.cn, zhaoday@mail2.sysu.edu.cn, chenli55@mail.sysu.edu.cn, maxiao@mail.sysu.edu.cn

***Abstract*—In this paper, we propose a new approach to construct quasi-cyclic low-density parity-check (QC-LDPC) codes using Hamming codewords of weight three, namely the HM-QC-LDPC codes. Thanks to the distance property of Hamming codes, length four cycles are avoided from the Tanner graph of the constructed codes, resulting in codes of girth six. This approach can be further extended to construct QC-LDPC codes of girth eight. Our numerical results show that the proposal has a better cycle profile than the progressive-edge-growth (PEG) constructed codes, and consequently prevails in performance. Moreover, the constructed QC-LDPC code prevails the LDPC code of the IEEE802.22 standard by 0.2 dB at the bit error rate (BER) of 10^{-8} when the codeword length is within hundreds of bits, making it a promising candidate for scenarios where strict decoding latency is imposed.**

***Key words*: QC-LDPC codes, short codes, Hamming codes.**

I. Introduction

Low-density parity-check (LDPC) codes [1] are competent channel codes that can achieve performance closed to the Shannon limit. So far, various construction and decoding algorithms for LDPC codes have been proposed, maturing the code. The code has already been adopted by various standards, such as DVB-S2, IEEE802.16e, IEEE802.22. LDPC codes can be mainly categorized into two types, random codes and structured codes, which had been investigated in [2-3] and [4], respectively. It is well known that random codes can approach channel capacity with relatively long codeword length. However, random codes are not implementation friendly. In contrast, structured codes often possess cyclic or quasi-cyclic (QC) structure in their parity-check matrices and therefore have low encoding complexity [5]. These codes with short-to-medium length can achieve a similar performance as the random codes.

In practice, the short-to-medium length channel codes play an important role in the communication scenarios that have a strict latency tolerance. The progressive-edge-growth (PEG) approach [6] can construct good LDPC codes with moderate codeword length. It yields a large girth code and can be applied to generate linear time encodable LDPC codes. Subsequent research [7-8] had been proposed to improve the performance of the PEG constructed codes. In this paper, we propose a new approach to construct QC-LDPC codes with flexible length utilizing Hamming codewords of weight three. Utilizing the distance property of Hamming codes, it avoids length four cycles from the Tanner graph [9] of the constructed codes, resulting in girth six for the codes. This approach can be further extended to construct codes of girth eight. For simplicity, we name the proposed codes as Hamming (HM)-QC-LDPC codes. Extensive simulation has been conducted and our numerical results show that the constructed short codes have a better cycle profile than the PEG constructed codes. Consequently, they yield a better decoding performance. Moreover, with a smaller length and a higher rate, the HM-QC-LDPC code of length 378 bits can outperform the IEEE802.22 standard code by 0.2 dB at the bit error rate (BER) of 10^{-8} over the additive white Gaussian noise (AWGN) channel using BPSK modulation.

II. Preliminary

This section introduces the preliminaries for the proposed work, including QC-LDPC codes, Hamming codes and its equivalent codeword class.

A. *QC-LDPC Codes*

QC-LDPC codes are a class of LDPC codes whose parity-check matrices are formed using the zero matrices and the circulant permutation matrices (CPMs). Both the encoding and decoding of QC-LDPC codes are easy to be implemented. Therefore, they have a promising prospect in communication systems. The conventional parity-check matrix of an (I , J) QC-LDPC code with codeword length $N = J \times s$ can be defined by

$$\mathbf{H} = \begin{bmatrix} \mathbf{P}_{1,1} & \mathbf{P}_{1,2} & \cdots & \mathbf{P}_{1,J} \\ \mathbf{P}_{2,1} & \mathbf{P}_{2,2} & \cdots & \mathbf{P}_{2,J} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{P}_{I,1} & \mathbf{P}_{I,2} & \cdots & \mathbf{P}_{I,J} \end{bmatrix}, \qquad (1)$$

where $\mathbf{P}_{i,j}$ ($1 \leq i \leq I$, $1 \leq j \leq J$, $I < J$) is either a $s \times s$ CPM or a zero matrix with the same size. CPM has the cyclic structure while its row weight and column weight are both one. In particular, a CPM can be obtained by cyclically shifting an identity matrix.

B. *Hamming Codes*

Hamming code is one of the earliest linear block codes. For any positive integer $m \geq 3$, there exists a Hamming code with the following parameters [10]. The codeword length is

$$n = 2^m - 1 \tag{2}$$

and the dimension of the code is

$$k = 2^m - m - 1. \tag{3}$$

Hence, the number of parity-check bits is $n - k = m$. The code maintains the minimum distance $d_{min} = 3$, and it can correct one bit error.

Moreover, weight distribution of Hamming codes is known in literature. We can obtain the weight enumerator according to the MacWilliams identity [11]

$$A(x) = \frac{1}{n+1}((1+x)^n + n(1-x)(1-x^2)^{(n-1)/2}). \tag{4}$$

$A(x)$ can also be presented as

$$A(x) = \sum_{z=0}^{n} A_z x^z, \tag{5}$$

where A_z indicates the number of Hamming codewords with weight z. By expanding (4), we can determine $A_3 = n(n-1)/6$.

Hereafter, we will utilize weight three Hamming codewords for the design of HM-QC-LDPC codes.

C. *Codeword Equivalent Class*

The proposed construction will utilize the cyclic property of Hamming codes. Hence, the following preliminaries are necessary to be introduced.

***Definition I*:** Given an n-tuple codeword $\overline{c} = (c_0, c_1, \cdots, c_{n-1})$, we can obtain the following n-tuple codeword $\overline{c}^{(\beta)}$ by cyclically shifting $\overline{c}$ to the right by β $(0 \leq \beta < n)$ positions

$$\overline{c}^{(\beta)} = (c_{n-\beta}, c_{n-\beta+1}, \cdots, c_{n-1}, c_0, c_1, \cdots, c_{n-\beta-1}). \tag{6}$$

$\overline{c}^{(\beta)}$ is cyclically equivalent to $\overline{c}$.

Definition II: Let $S_{\overline{c}}$ denote the set of all codewords that are cyclically equivalent to $\overline{c}$. We call $S_{\overline{c}}$ as a codeword equivalent class.

Note that codeword $\overline{c}$ can also be expressed as a polynomial by

$$C(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}. \tag{7}$$

Assuming there exists a weight three Hamming codeword $\overline{c}$, its corresponding polynomial $C(x)$ is

$$C(x) = x^e + x^b + x^a, \tag{8}$$

where $0 \leq e < b < a < n$. We cyclically shift the codeword by β positions and the polynomial of such a shifted codeword can be written as [10]

$$C^*(x) = x^\beta C(x) \bmod (x^n + 1). \tag{9}$$

Lemma 1 Given Hamming codewords in the form of $C(x) = 1 + x^{n/3} + x^{2n/3}$, they can be obtained again by cyclically shifting it to the right by $n/3$ positions.

Proof: We can elaborate $x^\beta C(x)/(x^n + 1)$ for the proof. First of all, if

$$(x^\beta C(x) - C^*(x))/(x^n + 1) = x^{a+\beta-n},$$

then

$$C^*(x) = x^{a+\beta-n} + x^{e+\beta} + x^{b+\beta}.$$

We have

$$x^\beta(x^e + x^b + x^a) = x^{a+\beta-n}(x^n + 1) + x^{a+\beta-n} + x^{e+\beta} + x^{b+\beta}.$$

Further based on (8), in order to let $C^*(x) = C(x)$, we need

$$\begin{cases} a + \beta - n = e, \\ e + \beta = b, \\ b + \beta = a. \end{cases}$$

The above equation group implies $\beta = n/3$. That says we can trace back the codeword by cyclically shifting it to the right by $n/3$ positions. Let $e = 0$, we have $b = n/3$ and $a = 2n/3$. The code polynomial is $C(x) = 1 + x^{n/3} + x^{2n/3}$ and $|S_{\overline{c}}| = n/3$.

Secondly, if

$$(x^\beta C(x) - C^*(x))/(x^n + 1) = x^{b+\beta-n} + x^{a+\beta-n},$$

then

$$C^*(x) = x^{b+\beta-n} + x^{a+\beta-n} + x^{e+\beta},$$

and therefore

$$\begin{aligned} x^\beta(x^e + x^b + x^a) =& (x^{b+\beta-n} + x^{a+\beta-n})(x^n + 1) + x^{b+\beta-n} \\ &+ x^{a+\beta-n} + x^{e+\beta}. \end{aligned}$$

Hence, if

$$\begin{cases} b + \beta - n = e, \\ a + \beta - n = b, \\ e + \beta = a, \end{cases}$$

then $C^*(x) = C(x)$. Again, the above equation group implies $\beta = 2n/3$. In other words, after cyclically shifting $\overline{c}$ to the right by $2n/3$ positions, we can obtain $\overline{c}$ again. Let $e = 0$, then $b = n/3$ and $a = 2n/3$. The code polynomial is $C(x) = 1 + x^{n/3} + x^{2n/3}$ and $|S_{\overline{c}}| = n/3$.

Finally, if

$$(x^\beta C(x) - C^*(x))/(x^n + 1) = x^{e+\beta-n} + x^{b+\beta-n} + x^{a+\beta-n},$$

then

$$C^*(x) = x^{e+\beta-n} + x^{b+\beta-n} + x^{a+\beta-n},$$

and therefore

$$\begin{aligned} x^\beta(x^e + x^b + x^a) =& (x^{e+\beta-n} + x^{b+\beta-n} + x^{a+\beta-n})(x^n + 1) \\ &+ x^{e+\beta-n} + x^{b+\beta-n} + x^{a+\beta-n}. \end{aligned}$$

Furthermore, if

$$\begin{cases} e + \beta - n = e, \\ b + \beta - n = b, \\ a + \beta - n = a, \end{cases}$$

$C^*(x) = C(x)$. Therefore, $\beta = n$. It conforms that any codeword $\overline{c}$ can trace back to itself by cyclically shifting it to the right by n positions. The above proof shows that if $e = 0$, $b = n/3$ and $a = 2n/3$, $|S_{\overline{c}}| = n/3$. ■

The above proof however indicates that n should be divided by three. Based on (2), we know that this will only happen when m is even. Together with Definition II, we have the following Corollary that describes the characteristics of $|S_{\overline{c}}|$.

Corollary 2 When m is even, there exists a Hamming codeword in the form of $C(x) = 1 + x^{n/3} + x^{2n/3}$ and its equivalent class has a cardinality of $|S_{\overline{c}}| = n/3$. The rest of Hamming codewords have an equivalent class of cardinality $|S_{\overline{c}}| = n$.

III. Construction of HM-QC-LDPC Codes

In this section, we will present our approaches to construct HM-QC-LDPC codes of girth six and eight. Parameterization of the codes will also be described.

A. *HM-QC-LDPC Codes of Girth Six*

For the construction, the following Lemmas need to be introduced.

Lemma 3 Given any positive integer $m \geq 3$, let all the weight three Hamming codeword $\overline{c}$ belong to a set B_3, where $|B_3| = n(n-1)/6$. We can choose l distinct codewords from B_3 and denote them as $\overline{c}_1$, $\overline{c}_2$, $\cdots$, $\overline{c}_l$. Parity-check matrix $\mathbf{H}$ can be formed by placing the l codewords column wise as

$$\mathbf{H} = [\overline{c}_1^T \;\; \overline{c}_2^T \;\; \cdots \;\; \overline{c}_l^T]. \tag{10}$$

Matrix $\mathbf{H}$ is free from cycles of length four.

Proof: Given any positive integer $m \geq 3$, let us assume that there exists length four cycles in matrix $\mathbf{H}$. A length four cycle in the matrix corresponds to two codewords (in two columns of $\mathbf{H}$). Since Hamming codes are linear block codes, linear combination of the two codewords will produce a third Hamming codeword. However, this combination would produce a codeword of weight less than three. This contradicts to the fact that the minimum distance of Hamming codes is three. Therefore, matrix $\mathbf{H}$ is free from cycles of length four. ■

Lemma 4 Given a matrix $\mathbf{H}$ without length four cycles, we can obtain several submatrices of the same size by decomposing $\mathbf{H}$ as

$$\mathbf{H} = \mathbf{H}_1 + \mathbf{H}_2 + \cdots + \mathbf{H}_\gamma, \tag{11}$$

and $\mathbf{H}_1, \mathbf{H}_2, \cdots, \mathbf{H}_\gamma$ do not possess the common nonzero entry in the same column or the same row. By combining these submatrices as

$$\mathbf{H}^* = \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \\ \vdots \\ \mathbf{H}_\gamma \end{bmatrix}, \tag{12}$$

$\mathbf{H}^*$ is also free from cycles of length four.

Proof: Since $\mathbf{H}$ does not have any cycle of length four, neither do submatrices $\mathbf{H}_1, \mathbf{H}_2, \cdots, \mathbf{H}_\gamma$. Moreover, since the submatrices do not share a common nonzero entry in the same column or the same row, $\mathbf{H}^*$ will also be free from cycles of length four. ■

Now, it is sufficient to propose our construction approach for HM-QC-LDPC codes of girth six. In following algorithm, we will only choose the weight three Hamming codewords whose equivalent classes have size n, i.e., $\overline{c}_v \in B_3$ and $|S_{\overline{c}_v}| = n$.

```
Algorithm 1 HM-QC-LDPC Codes of Girth Six
• Initialization: Choose parameter $m$, and the codeword length $N$, where $N \leq n(n-1)/6$ and $N \bmod n = 0$. Let $g = N/n$ and $v = 1$;
• Step 1: Search for $\overline{c}_v \notin S_{\overline{c}_1}, S_{\overline{c}_2}, \cdots, S_{\overline{c}_{v-1}}$;
• Step 2: Define $S_{\overline{c}_v} = \{\overline{c}_v^{(0)}, \overline{c}_v^{(1)}, \cdots, \overline{c}_v^{(n-1)}\}$;
• Step 3: Generate matrix $\mathbf{\Omega}_v$ as $\mathbf{\Omega}_v = [\overline{c}_v^{(0)^T} \; \overline{c}_v^{(1)^T} \; \cdots \; \overline{c}_v^{(n-1)^T}]$;
• Step 4: Decompose $\mathbf{\Omega}_v$ into three CPMs $\mathbf{P}_{1,v}$, $\mathbf{P}_{2,v}$, $\mathbf{P}_{3,v}$ as $\mathbf{\Omega}_v = \mathbf{P}_{1,v} + \mathbf{P}_{2,v} + \mathbf{P}_{3,v}$;
• Step 5: Generate matrix $\mathbf{\Lambda}_v$ as
      $\mathbf{\Lambda}_v = \begin{bmatrix} \mathbf{P}_{1,v} \\ \mathbf{P}_{2,v} \\ \mathbf{P}_{3,v} \end{bmatrix}$;
• Step 6: Let $v = v + 1$;
• Step 7: If $v \leq g$, go to Step 1; Else, generate matrix $\mathbf{H}_{\mathrm{HM-QC-LDPC}}$ as $\mathbf{H}_{\mathrm{HM-QC-LDPC}} = [\mathbf{\Lambda}_1 \; \mathbf{\Lambda}_2 \; \cdots \; \mathbf{\Lambda}_g]$ and terminate the construction.
```

In the above construction, parameter g can be understood as among all the available codeword equivalent classes, the number we choose to constitute $\mathbf{H}_{\mathrm{HM-QC-LDPC}}$. It is a parameter that defines the code rate, which will be discussed in Section III.C. Note that the above construction requires $|S_{\overline{c}_v}| = n$. Hence, the Hamming codeword $C(x) = 1 + x^{n/3} + x^{2n/3}$ and their cyclically equivalent codewords are excluded. Secondly, when $v = 1$, **Step 1** can be skipped. We will simply choose a codeword $\overline{c}_1$ from B_3 with $|S_{\overline{c}_1}| = n$. Finally, Lemmas 3 and 4 help ensure that $\mathbf{\Lambda}_v$ is free from cycles of length four. Since $\mathbf{P}_{1,v}$, $\mathbf{P}_{2,v}$, $\mathbf{P}_{3,v}$ are CPMs and $\overline{c}_v \notin S_{\overline{c}_1}, S_{\overline{c}_2}, \cdots, S_{\overline{c}_{v-1}}$, $\mathbf{H}_{\mathrm{HM-QC-LDPC}}$ will also be free from cycles of length four.

B. *HM-QC-LDPC Codes of Girth Eight*

Algorithm 1 can be further modified to construct HM-QC-LDPC codes of girth eight. We now let $\mathbf{H}_{\mathrm{HM-QC-LDPC}}(w, u)$ donate the parity-check matrix's entry of row w and column u, where $0 \leq w < 3n$ and $0 \leq u < N$. Identifying any six nonzero entries in $\mathbf{H}_{\mathrm{HM-QC-LDPC}}$, they will constitute a length six cycle in the corresponding Tanner graph if they appear as in one of the six patterns shown in Fig. 1. Note that

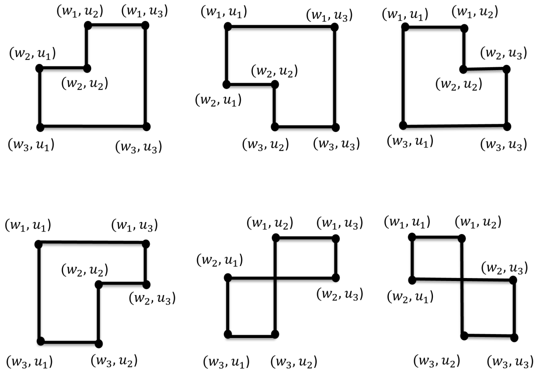

Fig. 1. Patterns of length six cycles in the parity-check matrix.

the entry coordinates are assigned following $w_1 < w_2 < w_3$ and $u_1 < u_2 < u_3$.

In **Algorithm 1**, $\mathbf{H}_{\mathrm{HM-QC-LDPC}}$ is formed by generating $\mathbf{\Lambda}_1, \mathbf{\Lambda}_2, \cdots, \mathbf{\Lambda}_g$ one by one. The above description implies that we should be selective when introducing $\mathbf{\Lambda}_v$ into $[\mathbf{\Lambda}_1 \mathbf{\Lambda}_2 \cdots \mathbf{\Lambda}_{v-1}]$ in order to avoid length six cycles. In general, when $v \geq 3$, we will generate six possible $\mathbf{\Lambda}_v$ by permuting $\mathbf{P}_{1,v}$, $\mathbf{P}_{2,v}$, $\mathbf{P}_{3,v}$ as

$$\mathbf{\Lambda}_{v_1} = \begin{bmatrix} \mathbf{P}_{1,v} \\ \mathbf{P}_{2,v} \\ \mathbf{P}_{3,v} \end{bmatrix}, \mathbf{\Lambda}_{v_2} = \begin{bmatrix} \mathbf{P}_{1,v} \\ \mathbf{P}_{3,v} \\ \mathbf{P}_{2,v} \end{bmatrix}, \mathbf{\Lambda}_{v_3} = \begin{bmatrix} \mathbf{P}_{2,v} \\ \mathbf{P}_{1,v} \\ \mathbf{P}_{3,v} \end{bmatrix},$$

$$\mathbf{\Lambda}_{v_4} = \begin{bmatrix} \mathbf{P}_{2,v} \\ \mathbf{P}_{3,v} \\ \mathbf{P}_{1,v} \end{bmatrix}, \mathbf{\Lambda}_{v_5} = \begin{bmatrix} \mathbf{P}_{3,v} \\ \mathbf{P}_{1,v} \\ \mathbf{P}_{2,v} \end{bmatrix}, \mathbf{\Lambda}_{v_6} = \begin{bmatrix} \mathbf{P}_{3,v} \\ \mathbf{P}_{2,v} \\ \mathbf{P}_{1,v} \end{bmatrix}.$$

We will then pick up one that does not create any of the length six cycle patterns in $[\mathbf{\Lambda}_1 \ \mathbf{\Lambda}_2 \ \cdots \ \mathbf{\Lambda}_{v-1} \ \mathbf{\Lambda}_v]$. Note that there can be plural choices for $\mathbf{\Lambda}_v$. In this case, we will pick up the one that imposes the least number of cycles of length eight in $[\mathbf{\Lambda}_1 \ \mathbf{\Lambda}_2 \ \cdots \ \mathbf{\Lambda}_{v-1} \ \mathbf{\Lambda}_v]$. Also notice that it is possible that all of the above six $\mathbf{\Lambda}_v$ will impose length six cycles in $[\mathbf{\Lambda}_1 \ \mathbf{\Lambda}_2 \ \cdots \ \mathbf{\Lambda}_{v-1} \ \mathbf{\Lambda}_v]$. In this case, we will abandon all the $\mathbf{\Lambda}_v$ and generate a new $\mathbf{\Lambda}_v$ based on another Hamming codeword from B_3. Therefore, when $v \geq 3$, we will integrate this selection process into **Step 5** of **Algorithm 1**. This will enable us to construct HM-QC-LDPC codes of girth eight.

C. Parameterization of HM-QC-LDPC Codes

Based on Section II, we know that there are $n(n-1)/6$ weight three Hamming codewords, i.e. $|B_3| = n(n-1)/6$, where $n = 2^m - 1$. Recalling Corollary 2, we further know that if m is odd, these codewords can be categorized into $(n-1)/6$ equivalent classes, each of which has size n. Hence, **Algorithm 1** and its variant of Section III.B can produce a HM-QC-LDPC code with the maximal length of $(2^m-1)(2^m-2)/6$. However, if m is even, there are $n(n-1)/6 - n/3 = n(n-3)/6$ codewords that belong to equivalent classes of size n. In this case, the constructed code's maximal length will be $(2^m-1)(2^m-4)/6$. In general, a larger Hamming code will lead to a larger HM-QC-LDPC code.

The actual length of the constructed code can however be more flexible as it can be controlled by parameter g. It indicates the number of classes that we choose to constitute $\mathbf{H}_{\mathrm{HM-QC-LDPC}}$. Hence, if m is odd, $g \leq (n-1)/6$, and if m is even, $g \leq (n-3)/6$. The actual length of the constructed code will be $gn = g(2^m-1)$.

Finally, the designed rate of constructed code will be $(gn - 3n)/gn = (g-3)/g$. But notice that due to the parity-check matrix's cyclic feature, it will not be full rank and actual code rate will be greater than the designed one. Table I summarizes the above parameterization of HM-QC-LDPC codes.

TABLE I
PARAMETERIZATION OF HM-QC-LDPC CODES

m	maximum length	actual length	rate
odd	$(2^m-1)(2^m-2)/6$	$g(2^m-1)$	$> (g-3)/g$
even	$(2^m-1)(2^m-4)/6$	$g(2^m-1)$	$> (g-3)/g$

TABLE II
CYCLE PROFILE OF CODES WITH LENGTH 378 BITS

	Length six cycles	Length eight cycles	Length ten cycles
Proposed code with girth six	63	2709	12033
Proposed code with girth eight	0	1638	11151
PEG code with girth eight	0	1749	13986

TABLE III
CYCLE PROFILE OF CODES WITH LENGTH 762 BITS

	Length six cycles	Length eight cycles	Length ten cycles
Proposed code with girth six	254	2794	10414
Proposed code with girth eight	0	1397	9906
PEG code with girth eight	0	1484	12003

IV. SIMULATION RESULTS AND ANALYSES

In our simulations, the codewords are BPSK modulated and transmitted over the AWGN channel. The sum-product algorithm (SPA) [12] is employed for decoding and the maximum number of iterations is 100. The codes' BER performance is measured against E_b/N_0, where E_b is the energy per information bit and N_0 is the noise power.

Given $m = 6$, we constructed the HM-QC-LDPC codes with girth six and eight, respectively. For comparison, we have also constructed an LDPC code of girth eight using the PEG approach. Both the proposed codes and PEG constructed code have the same codeword length of 378 bits and rate of 0.52. In Fig. 2, it can be seen that the HM-QC-LDPC code of girth eight outperforms the one of girth six. This mainly thanks to the former has a better cycle profile that lists the number of cycles of various length for a given code. Table II shows that the cycle profile of the proposed codes and the PEG constructed code, all of which are 378 bits long. Fig. 2 also shows that the proposed code of girth eight outperforms the PEG constructed code with a coding gain of 0.3 dB at the BER of 10^{-8}. Table II reveals that with girth eight the HM-QC-LDPC code has a better cycle profile than the PEG constructed code. Fig. 2 also compares the proposed codes with the IEEE802.22 standard LDPC code that is 384 bits long and has a rate of 0.5. It can be observed that even with a smaller length and a higher rate, the proposed code of girth eight can outperform the standard code by 0.2 dB at the BER of 10^{-8}. Fig. 3 demonstrates the decoding convergence of the proposed codes, which is exhibited by the average number of SPA iterations. It shows the proposed codes converge better than the PEG code.

Similarly, we constructed the HM-QC-LDPC codes with girth six and eight when $m = 7$. They are compared with the PEG constructed code of girth eight. They have the same length of 762 bits and rate of 0.51. Table III again shows the above mentioned codes' cycle profile. Moreover, the IEEE802.22 standard LDPC code with length of 768 bits and rate of 0.5 is also used as a comparison benchmark. Fig. 4 shows that the proposed code with girth eight outperforms the

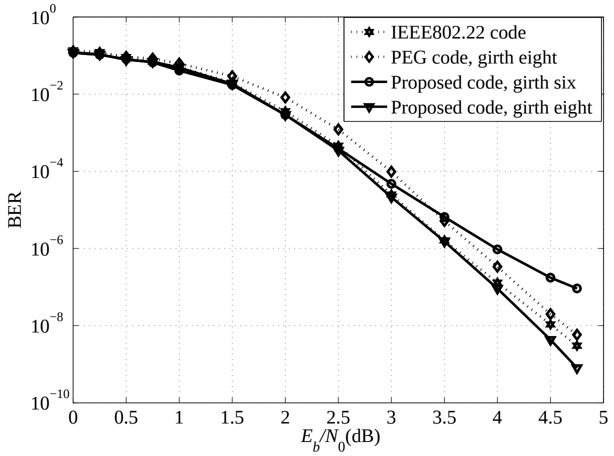

Fig. 2. Performance of the HM-QC-LDPC codes of length 378 bits.

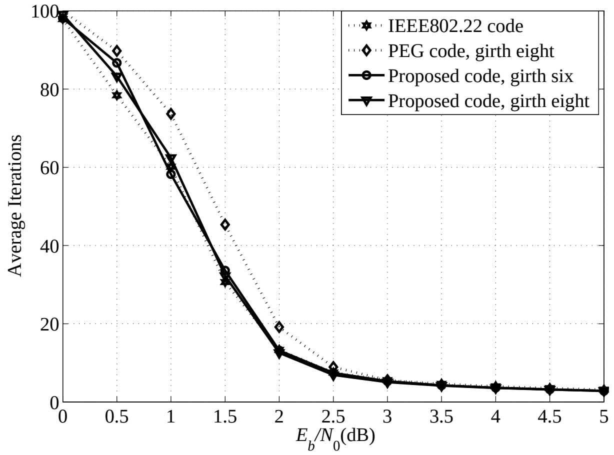

Fig. 3. Average number iterations of the HM-QC-LDPC codes of length 378 bits with the maximum iteration number of 100.

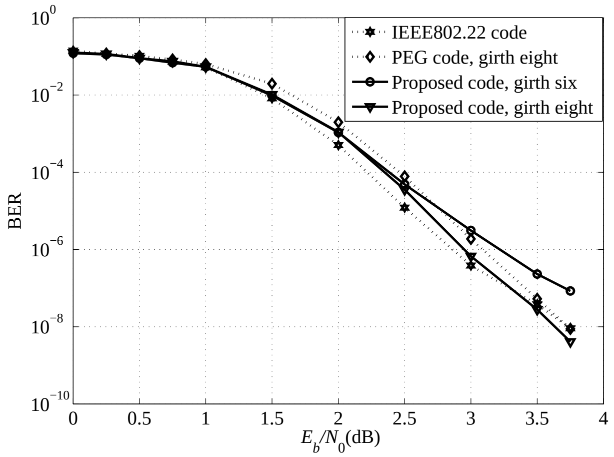

Fig. 4. Performance of the HM-QC-LDPC codes of length 762 bits.

PEG constructed code by about 0.1 dB at the BER of 10^{-8}. It also tempts to produce a better asymptotic performance than the standard code that has a slightly larger length and smaller code rate. The above simulation results also have demonstrated the proposal does construct competent QC-LDPC codes in the range of hundreds of bits long, offering fresh choice for communication systems that impose a strict signal recovery latency tolerance.

V. Conclusion

In this paper, we have proposed a new approach to construct QC-LDPC codes utilizing the Hamming codewords of weight three, namely the HM-QC-LDPC codes. We have constructed HM-QC-LDPC codes of girth six and eight, with a flexible design of codeword length and code rate. Our numerical results have shown the proposal can yield QC-LDPC codes that have a better cycle profile than the PEG constructed codes. In the range of hundreds of bits, they outperform the PEG constructed codes and the IEEE802.22 standard codes. Our future endeavor will investigate nonbinary HM-QC-LDPC codes and other design optimization aspects.

Acknowledgment

This research is supported by the National Basic Research Program of China (973 Program) with project ID 2012CB316100 and the National Natural Science Foundation of China (NSFC) with project ID 61372079. The first author would like to thank Dr. Chulong Liang and Dr. Kechao Huang for their helpful discussions.

References

[1] R. G. Gallager, "Low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 8 (1), pp. 21-28, Jan. 1962.

[2] D. J. C. Mackay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45 (2), pp. 399-431, Mar. 1999.

[3] T. Richardson, A. Shokrollahi and R. Urbanke, "Design of capacity approaching low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47 (2), pp. 619-637, Feb. 2001.

[4] Y. Kou, S. Lin and M. Fossorier, "Low-density parity-check codes based on finite geometries: a rediscovery and new results," *IEEE Trans. Inform. Theory*, vol. 47 (11), pp. 2711-2736, Nov. 2001.

[5] Q. Huang, L. Tang, S. He, Z. Xiong and Z. Wang, "Low-complexity encoding of quasi-cyclic codes based on Galois Fourier transform," *IEEE Trans. Commun.*, vol. 62 (6), pp. 1757-1767, Jun. 2014.

[6] X. Y. Hu and D. M. Arnold, "Regular and irregular progressive-edge-growth Tannar graphs," *IEEE Trans. Inform. Theory*, vol. 51 (1), pp. 386-398, Jan. 2005.

[7] X. Jiang, H. Guan, M. Lee and S. Kim, "Length-compatible PEG-CRT algorithm," *Int. Conf. Wirel. Commun. & Signal Processing (WCSP)*, pp. 1-5, Hangzhou, China, Oct. 2013.

[8] M. Diouf, D. Declercq, M. Fossorier, S. Quya and B. Vasic, "Improved PEG construction of large girth QC-LDPC codes," *Int. Symp. on Turbo Codes & Iterative Infor. Processing (ISTC)*, pp. 146-150, Paris, France, Sept. 2016.

[9] M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. 27 (5), pp. 533-547, Sept. 1981.

[10] S. Lin and D. Costello, *Error Control Coding*, *2nd Edition*, Prentice-Hall, 2004.

[11] F. J. MacWilliams, "A theorem on the distribution of weights in a systematic codes," *Bell Syst. Tech. J.*, vol. 42 (1), pp. 79-94, Jan. 1963.

[12] F. R. Kschischang, B. J. Frey and H. A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inform. Theory*, vol. 47 (2), pp. 498-519, Feb. 2001.