Paper

Low Density Parity Check Codes Constructed from Hankel Matrices

Mohammed Amine Tehami and Ali Djebbari

Faculty of Electrical Engineering, Djillali Liabes University of Sidi Bel Abbes, Sidi Bel Abbès, Algeria

https://doi.org/10.26636/jtit.2018.121717

Abstract—In this paper, a new technique for constructing low density parity check codes based on the Hankel matrix and circulant permutation matrices is proposed. The new codes are exempt of any cycle of length 4. To ensure that parity check bits can be recursively calculated with linear computational complexity, a dual-diagonal structure is applied to the parity check matrices of those codes. The proposed codes provide a very low encoding complexity and reduce the stored memory of the matrix H in which this matrix can be easily implemented comparing to others codes used in channel coding. The new LDPC codes are compared, by simulation, with uncoded bi-phase shift keying (BPSK). The result shows that the proposed codes perform very well over additive white Gaussian noise (AWGN) channels.

Keywords—dual diagonal matrix, error correcting codes, girth, Hankel matrix, low density parity check codes.

1. Introduction

The field of error correcting codes was developed by introducing them into iterative decoding [1]. Nowadays, low density parity check (LDPC) codes are considered to the best solution, thanks to their considerable importance in error correcting performance and possibility to be represented by a specific parity check binary matrix $M \times N$ [2], [3]. The Tanner graph is a bipartite graph with two sets, i.e. the columns and the rows are depicted as follows: columns represent variable nodes, and rows represent check nodes. The edge is a connection between these two sets [4]. A cycle in the Tanner graph is defined as the path which starts and ends at the same node. If a cycle of this graph is considered, the minimum length of such a cycle is called girth [4]. LDPC codes are classified into two classes: regular, if the number of 1s in each row and column is constant, and irregular, if it varies [5], [6].

In this context, we present a special class of LDPC codes which benefit from low-complexity of decoding implementations due to the absence of cycle of length 4. Such a proposed construction has the following advantages:

- the proposed method guarantees that the constructing matrix avoids any cycles of length 4, which is essential for decoding simplicity,
- this method uses the permutation matrix, which makes the implementation easier, i.e. reduces the number of logical gates required and uses simple shift registers,
- a dual diagonal structure is applied to the parity check matrix of those codes, which ensures that parity check bits can be recursively implemented with linear computational complexity [7], [8].

The remainder of this paper is organized as follows. In Section 2, a description of the Hankel matrix and several conditions required to avoid a girth of length 4 is given. Section 3 presents the encoding concept and shows the advantages of the proposed construction of LDPC codes. Section 4 discusses the simulation results and, finally, Section 5 is devoted to conclusions.

2. Proposed Construction of Matrix

Girth is one of the most important keys that affect the performance of LDPC codes [1], [9]. Recent research indicates that small cycles affect the decoding complexity of these codes. Therefore, research on the construction of LDPC codes with a comparatively large girth, e.g. greater than 4, is still valuable for practical applications [6].

Let **H** be the parity check matrix $M \times N$ size, where M is the number of rows and N is the number of columns. It can be represented in the following form:

$$\mathbf{H} = [\mathbf{H}_1\ \mathbf{H}_2]. \tag{1}$$

$\mathbf{H}_2$ is a dual diagonal matrix of size $M \times M$, which ensures that parity check bits can be recursively calculated with linear computational complexity [7], [8]. The proposed matrix $\mathbf{H}_1$ is of the square type, with $M \times M$ size and can be constructed as follows.

First, we use the Hankel matrix [10] where its elements (indexes) are:

$$a_{i,j} = i + j - 1, \tag{2}$$

where i, j are the numbers of rows and columns respectively.

The structure of the Hankel matrix of size $m \times m$ [2] is:

$$\mathbf{H}_a = \begin{bmatrix} 1 & 2 & \dots & m \\ 2 & 3 & \dots & m+1 \\ \vdots & \vdots & \ddots & \vdots \\ m & m+1 & \dots & 2m-1 \end{bmatrix}, \tag{3}$$

with $M = m \times (m-1)$ and m restricted to an even number, greater than 2.

Next, by applying the process of symmetry in relation to an ascending diagonal m of matrix $\mathbf{H}_a$ a new $\mathbf{H}_b$ matrix is obtained:

$$\mathbf{H}_b = \begin{bmatrix} 1 & 2 & \ldots & m \\ 2 & 3 & \ldots & m-1 \\ \vdots & \vdots & \ddots & \vdots \\ m & m-1 & \ldots & 1 \end{bmatrix}. \tag{4}$$

We also construct matrix $\mathbf{H}_b$ having the elements of $a_{i,j}, 1 \leq i \leq m$ and $1 \leq j \leq m$, and defined by:

$$a_{i,j} = \begin{cases} a_{i,j} \text{ of } \mathbf{H}_a & \text{if } i+j \leq m+1 \\ a_{(m+1)-i,(m+1)-j} & \text{otherwise} \end{cases}. \tag{5}$$

An example is given to clarify the analysis, with $m = 4$, $\mathbf{H}_b$ is:

$$\mathbf{H}_b = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 3 \\ 3 & 4 & 3 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}.$$

Each index of matrix $\mathbf{H}_b$ is assigned by sub-permutation matrices of size $(m-1) \times (m-1)$, and all indexes with a value equal to m are replaced by a zero matrix of size $(m-1) \times (m-1)$.

For $m = 4$, the sub-permutation matrices are given as follows. The sub-matrix of index '1' is an identity matrix.

$$\text{'1'} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The sub-matrix of index '2' is a sub-identity matrix permuted once to the right.

$$\text{'2'} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

The sub-matrix of index '3' is a sub-identity matrix permuted twice to the right.

$$\text{'3'} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

The sub-matrix of index '4' is a zero matrix.

$$\text{'4'} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

To avoid repeating the sub-matrices in matrix $\mathbf{H}_b$, a choice of their size was performed.

A new matrix noted $\mathbf{H}_c$ is obtained as:

$$\mathbf{H}_c = \begin{bmatrix} 1&0&0&0&1&0&0&0&1&0&0&0 \\ 0&1&0&0&0&1&1&0&0&0&0&0 \\ 0&0&1&1&0&0&0&1&0&0&0&0 \\ 0&1&0&0&0&1&0&0&0&0&0&1 \\ 0&0&1&1&0&0&0&0&0&1&0&0 \\ 1&0&0&0&1&0&0&0&0&0&1&0 \\ 0&0&1&0&0&0&0&0&1&0&1&0 \\ 1&0&0&0&0&0&1&0&0&0&0&1 \\ 0&1&0&0&0&0&0&1&0&1&0&0 \\ 0&0&0&0&0&1&0&1&0&1&0&0 \\ 0&0&0&1&0&0&0&0&1&0&1&0 \\ 0&0&0&0&1&0&1&0&0&0&0&1 \end{bmatrix}$$

Many cycles of length 4 are included in $\mathbf{H}_c$ as depicted in the Tanner graph and shown in Fig. 1: Now, we can easily

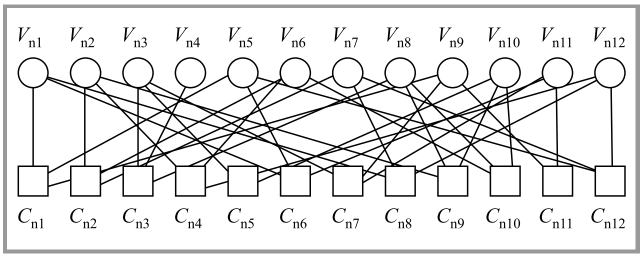

Fig. 1. The Tanner graph of $\mathbf{H}_c(12,3,3)$.

construct matrix $\mathbf{H}_1$ from $\mathbf{H}_c$ by applying the principle of activation on matrix $\mathbf{H}_b$ and using only two indexes (x and y) of matrix $\mathbf{H}_c$.

The sum of these two indexes is equal to the index which is situated on the ascending diagonal m, by applying:

$$x + y = m, \tag{6}$$

with x, y and m being the indexes of permutation matrices. For example, when $m = 4$, there are two combinations. This means that we can activate the indexes ($x = 1$ with $y = 3$), which helps obtain matrix $\mathbf{H}_1$.

$$\mathbf{H}_1 = \begin{bmatrix} 1&0&0&0&0&0&0&0&1&0&0&0 \\ 0&1&0&0&0&0&1&0&0&0&0&0 \\ 0&0&1&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0&0&1 \\ 0&0&0&1&0&0&0&0&0&1&0&0 \\ 0&0&0&0&1&0&0&0&0&0&1&0 \\ 0&0&1&0&0&0&0&0&1&0&0&0 \\ 1&0&0&0&0&0&1&0&0&0&0&0 \\ 0&1&0&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&1&0&0 \\ 0&0&0&1&0&0&0&0&0&0&1&0 \\ 0&0&0&0&1&0&0&0&0&0&0&1 \end{bmatrix}$$

Hence, the matrix $\mathbf{H}$ can be represented as:

$$\mathbf{H} = \begin{bmatrix}
1&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&1&0&0&1&1&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0\\
1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0\\
0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0\\
0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&1&0&0\\
0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&1&0\\
0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&1
\end{bmatrix}$$

3. Encoding Concept

Gallager has shown that codes of column-weight-two have a minimum distance increasing logarithmically with code length, compared to a linear increase when the column weight is at least three [1]. Despite the low increase in minimum distance, these codes have shown good potential in some applications, such as partial response channels [11], [12] and also require less computation due to column weight.

Although LDPC code performance is high, the hardware implementation still remains a challenge due to the large size and complex random (unstructured) row-column connections [13]. This complexity has been reduced by using structured codes [13]. However, the girth (smallest cycle) has been reduced by using a constraint over row-column connections [14]. It has been shown that if the girth increases, the decoding performance is higher [15], [16].

LDPC codes are linear codes. Thus, they can be expressed as the null space of a parity check matrix $\mathbf{H}$ [2]. Considered c as a codeword written as $c = [d\ p]$, where d and p are the data and parity bits respectively. The parity relationship can be written as [17]:

$$\mathbf{H}c^T = 0^T . \tag{7}$$

In the proposed method, $\mathbf{H}$ is decomposed into $\mathbf{H} = [\mathbf{H}_1\ \mathbf{H}_2]$, such that:

$$[\mathbf{H}_1\ \mathbf{H}_2][d\ p]^T = 0^T , \tag{8}$$

$$\mathbf{H}_1 d^T = \mathbf{H}_2 p^T , \tag{9}$$

$$p^T = (\mathbf{H}_2^{-1}\mathbf{H}_1)d^T , \tag{10}$$

where $\mathbf{H}_2$ is the dual diagonal matrix and $\mathbf{H}_1$ is built deterministically, as seen above.

Based on the structure of $\mathbf{H}_2$ and Eq. (8), the parity check bits $p = \{p_i\}$ can be easily computed from a given data $d = \{d_i\}$ and matrix $\mathbf{H}_1$ as in [18]:

$$p_1 = \sum_j h^1_{1j} d_j , \tag{11}$$

$$p_i = p_{i-1} + \sum_j h^1_{ij} d_j \bmod 2 , \tag{12}$$

where h^1_{ij} are the elements of $\mathbf{H}_1$.

In [18], a comparative study with an LDPC code defined from a randomly generated parity check matrix [6] has shown that if $\mathbf{H}$ is brought into $[\mathbf{H}_2, \mathbf{H}_1]$, and $\mathbf{H}_2$ has a dual diagonal structure, several advantages are obtained:

- there is no need of Gaussian elimination for the encoding process,
- $\mathbf{H}_2$ is always non-singular i.e. $\mathbf{H}_2$ is always invertible,
- if $\mathbf{H}_1$ is sparse, it requires very little memory to store $\mathbf{H}$ in the encoder.

Besides the advantages cited above, there are two other advantages offered by the proposed construction:

- $\mathbf{H}_1$ is effectively sparse, comprising largely 0s $\left(\frac{M-w}{M}\right)$ and has a low density of 1s $\left(\frac{w}{M}\right)$ where w is the weight (number of ones in each column or row) of $\mathbf{H}_1$, which ensures a very low encoding complexity [19];
- The particularity structure of the obtained matrix $\mathbf{H}_1$ (can be built from identity sub-matrix only, with some permutations) considerably reduces memory usage.

4. Simulation Results

Monte Carlo simulations were used to estimate the bit error rate (BER) of an LDPC code. Iterative belief propagation and additive white Gaussian Noise (AWGN) were applied as the decoding algorithm and channel, respectively. For simulation purposes, we used the rate $R = \frac{1}{2}$ and block length $N = 4324$. This simulation is running for at least 1000 code words and the maximum iteration is 80.

The performance of uncoded BPSK is presented with the aim of comparing it with coded BPSK, using the new LDPC code and other LDPC codes. The signal to noise ratios (SNR) for the coded BPSK and the uncoded BPSK are defined, as in [20], with the first one being:

$$SNR_1 = 10\log\frac{E_b}{2\sigma^2 R} \tag{13}$$

and the other one defined as:

$$SNR_2 = 10\log\frac{E_b}{2\sigma^2}\,. \tag{14}$$

Figure 2 represents BER performance of the proposed LDPC codes and of uncoded BPSK with $N = 4324$, $j = 2$ (j represents the weight of columns) and $R = \frac{1}{2}$.

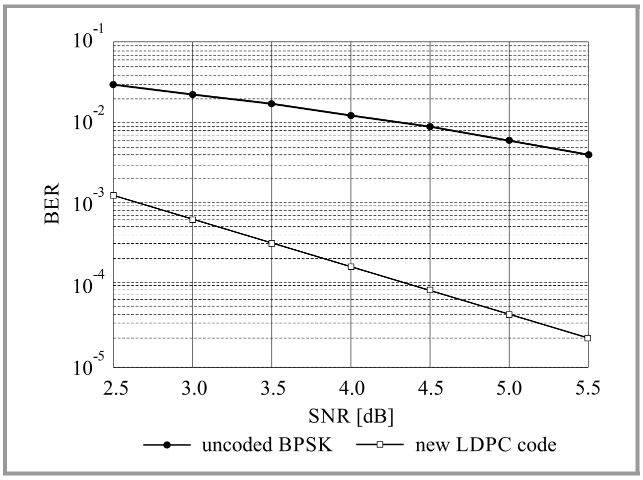

Fig. 2. BER of the proposed LDPC codes and uncoded BPSK with $N = 4324$, $j = 2$ and $R = \frac{1}{2}$.

From Fig. 2, we can observe that the new LDPC code offers better performances compared to the uncoded BPSK transmission. At BER$= 10^{-3}$, the obtained gain is about 1.9 dB.

Table 1 shows the comparison of BER performance of the proposed LDPC codes, with $N = 4324$, $j = 2$ with three others codes: Random codes, GB-(Geometry Based) LDPC and TS-(Turbo-Structured) LDPC codes [20].

Table 1
BER performance of the proposed LDPC codes with Random codes, GB-LDPC codes and TS-LDPC codes.

BER	Proposed LDPC codes	Random codes [20]	GB-LDPC codes [20]	TS-LDPC codes [20]
	E_b/N_0			
10^{-3}	2.5	3	3	3
10^{-4}	4	4	4	3.8

From Table 1, it can be observed that the proposed codes exhibit a performance gain of about 0.5 dB compared to Random, GB-LDPC and TS-LDPC codes at BER of 10^{-3}. At BER of 10^{-4}, the proposed LDPC codes provide the same performance when compared to the unstructured Random codes, GB-LDPC codes and offer a loss in gain of about 0.2 dB when compared to the TS-LDPC codes. From this, we can say that the proposed LDPC codes can reach the error floor region, for long length. The results demonstrate that the proposed LDPC codes, having a uniform structure and low complexity when it comes to hardware implementation (reduced logic gates and the use of simple shift registers), offer an error rate performance that is slightly better than that of more complex unstructured LDPC codes.

5. Conclusion

In this paper, we have presented a method of constructing a parity check matrix of an LDPC code. The main advantage of such a method is its ability to demonstrate how to avoid girth of length 4 by using the Hankel matrix. Also, a dual diagonal structure is applied to parity check matrices, which ensures that parity check bits can be recursively calculated with linear computational complexity

References

[1] R. G. Gallager, "Low-density parity-check codes", *IRE Transact. Inform. Theory*, vol. 8, no. 1, pp. 21–28, 1962 (doi: 10.1109/TIT.1962.1057683).

[2] W. Sulek, "Seed Graph Expansion for Construction of Structured LDPC Codes", in *Proc. 6th Int. Sym. on Wireless Commun. Sys. ISWCS*, Siena, Italy, 2009, pp. 216–220 (doi: 10.1109/ISWCS.2009.5285248).

[3] D. Xia, H. He, Y. Xu, and Y. Cai, "A novel construction scheme with linear encoding complexity for LDPC codes", in *Proc. 4th Int. Conf. on Wireless Commun. Network. and Mob. Comput.*, Dalian, Liaoning, China, 2008, pp. 1–4 (doi: 10.1109/WiCom.2008.358).

[4] R. Tanner, "A recursive approach to low complexity codes", *IEEE Transact. Inform. Theory*, vol. 27, no. 5, pp. 533–547, 1981 (doi: 10.1109/TIT.1981.1056404).

[5] Y. Abid, O. Sidek, M. F. M. Salleh, and F. Ghani, "A new quasi-cyclic low density parity check codes", in *Proc. 2009 IEEE Sym. on Indust. Electron. & Applic.*, Kuala Lumpur, Malaysia, 2009, pp. 239–242 (doi: 10.1109/ISIEA.2009.5356472).

[6] D. J. C. MacKay, "Good codes based on very sparse matrices", *IEEE Transact. Inform. Theory*, vol. 45, no. 2, pp. 399–431, 1999 (doi: 10.1109/18.748992).

[7] Q. Guo-lei and Z. Dong, "Design of structured LDPC codes with quasi-cyclic and rotation architecture", in *Proc. 2010 3rd Int. Conf. on Adv. Comput. Theory and Engineer. ICACTE*, Chengdu, Sichuan, China, 2010, pp. 655–657 (doi: 10.1109/ICACTE.2010.5578934).

[8] M. Yang, W. E. Ryan, and Y. Li, "Design of efficiently encodable moderate length high-rate irregular LDPC codes", *IEEE Trans. Commun.*, vol. 52, no. 4, pp. 564–571, 2004 (doi: 10.1109/TCOMM.2004.826367).

[9] K. Liu, Z. Fei, J. Kuang, and X. Li. "A novel algorithm for removing cycles in quasi-cyclic LDPC codes", in *Proc. 2009 IEEE 20th Int. Sym. on Person. Indoor and Mob. Radio Commun.*, Tokyo, Japan, 2009, pp. 1054–1058 (doi: 10.1109/PIMRC.2009.5450003).

[10] A. Ahmed and Y. F. Hu, "3M Relationship Pattern for Detection and Estimation of Unknown Frequencies for Unknown Number of Sinusoids Based on Eigenspace Analysis of Hankel Matrix", in *IET 2nd Intel. Sig. Process. Conf. 2013 ISP 2013*, London, UK, 2013, pp. 1–6 (doi: 10.1049/cp.2013.2058).

[11] H. Song, J. Liu, and B. V. K. V. Kumar, “Low complexity LDPC codes for partial response channels”, in *Proc. IEEE Global Telecommun. Conf. GLOBECOM’02*, Taipei, Taiwan, 2002, vol. 2, pp. 1294–1299 (doi: 10.1109/GLOCOM.2002.1188406).

[12] H. Song, J. Liu, and B. V. K. V. Kumar, “Large girth cycle codes for partial response channels”, *IEEE Transact. on Magnet.*, vol. 40, no. 4, part 2, pp. 3084–3086, 2004 (doi: 10.1109/TMAG.2004.829197).

[13] G. Malema and M. Liebelt, “Quasi-cyclic LDPC codes of column-weight two using a search algorithm”, *EURASIP J. Adv. Sig. Process.*, vol. 2007, no. 4, pp. 1–8, 2007 (doi: 10.1155/2007/45768).

[14] M. P. C. Fossorier, “Quasi-cyclic low-density parity-check codes from circulant permutation matrices”, *IEEE Transact. Inform. Theory*, vol. 50, no. 8, pp. 1788–1793, 2004 (doi: 10.1109/TIT.2004.831841).

[15] M. E. O’Sulivan, “Algebraic construction of sparse matrices with large girth”, *IEEE Transact. Inform. Theory*, vol. 52, no. 2, pp. 718–727, 2006 (doi: 10.1109/TIT.2005.862120).

[16] Y. Mao and A. H. Banihasherni, “A heuristic search for good low-density parity-check codes at short block lengths”, *in Proc. IEEE Int. Conf. on Commun. ICC’01*, Helsinki, Finland, vol. 1, 2001, pp. 41–44 (doi: 10.1109/ICC.2001.936269).

[17] T. J. Richardson and R. L. Urbanke, “Efficient encoding of low-density-parity-check codes”, *IEEE Transact. Inform. Theory*, vol. 47, no. 2, pp. 638–656, 2001 (doi: 10.1109/18.910579).

[18] L. Ping, W. K. Leung, and N. Phamdo, ‘Low density parity check codes with semi-random parity check matrix”, *Electron. Let.*, vol. 35, no. 1, pp. 38–39, 1999 (doi: 10.1049/el:19990065).

[19] Z. Hao and Z. Tong, “Block-LDPC: a partial LDPC coding system design approach”, *IEEE Transact. Circuits Sys. I*, vol. 52, no. 4, pp. 766–775, 2005 (doi: 10.1109/TCSI.2005.844113).

[20] J. M. F. Moura, J. Lu, and H. Zhang, “Structured low-density-parity-check codes”, *IEEE Sig. Process. Mag.*, vol. 21, no. 1, pp. 42–55, 2004 (doi: 10.1109/MSP.2004.1267048).

Mohammed Amine Tehami received his B.Sc. and M.Sc. from the Department of Electronics, University of Djilali Liabes, Sidi Bel Abbès, (Algeria) in 2009 and 2011, respectively. He worked as a Research Scientist specializing in LDPC code construction at (LTTNS) Telecommunication and Digital Signal Processing Laboratory, Sidi Bel Abbès. He is interested in channel coding, as well as construction and analysis of LDPC codes.

E-mail: Chahoub_88@yahoo.com
Faculty of Electrical Engineering
Djillali Liabes University of Sidi Bel Abbes
Sidi Bel Abbès, Algeria

Ali Djebbari – for biography, see this issue, p. 8.