A REVIEW OF CONSTRUCTION METHODS FOR REGULAR LDPC CODES

Rutuja Shedsale
Department of Electrical Engineering,
Veermata Jijabai Technological Institute (V.J.T.I.)Mumbai, India.

E-mail: rutuja_shedsale@yahoo.co.in

Nisha Sarwade

Department of Electrical Engineering,
Veermata Jijabai Technological Institute (V.J.T.I.)Mumbai, India.

E-mail: nishasarvade@vjti.org.in

Abstract

Low-Density parity-check (LDPC) codes are one of the most powerful error correcting codes available today. Their Shannon capacity approaching performance and lower decoding complexity have made them the best choice for many wired and wireless applications. This paper gives an overview about LDPC codes and compares the Gallager's method, Reed-Solomon based algebraic method and the Progressive edge growth (PEG) combinatorial method for the construction of regular LDPC codes.

Keywords Low-Density parity-check (LDPC) codes, Reed-Solomon (RS) Codes, SPA, Tanner graph, Progressive Edge Growth(PEG).

1. Introduction

Low-Density parity-check (LDPC) codes were discovered by Gallager in early 1960s [1]. After being overlooked for almost 35 years, this class of codes were recently rediscovered by Mackay and Neal and Wiberg [8] and shown to form a class of Shannon limit approaching codes [2], [6-8]. This class of codes decoded with iterative decoding, such as the sum-product algorithm (SPA) [1, 9], performs amazingly well for a lot of different channels. Since their rediscovery, LDPC codes have become a focal point of research for a variety of applications such as distributed source coding [10] and Forward error correction (FEC) [5].

The paper is organized as follows: Section 2 introduces the necessary concepts about LDPC codes and their representation. Section 3 describes the pseudorandom construction method proposed by Gallager [1,2] .We summarize the construction methods based on the Reed-Solomon (RS) Codes [4] and the Progressive Edge Growth(PEG) Algorithm in Section 4 and Section 5 respectively. Finally, Section 6 concludes this paper.

2. Overview

The LDPC codes are a class of linear block codes. The name comes from the characteristic of their parity-check matrix which contains only a few 1's in comparison to the amount of 0's. Such a structure guarantees both: a lower decoding complexity and good distance properties [2].

We define two numbers describing these matrices: ρ for the number of 1's in each row and γ for the columns. For an $m \times n$ matrix to be called low-density the two conditions $\gamma \ll m$ and $\rho \ll n$ must be satisfied [3].

A parity-check matrix is said to be regular when γ is same for all the columns and ρ is constant for all the rows. If an LDPC code is described by a regular parity-check matrix, it is called a (γ, ρ)-regular LDPC code otherwise it is an irregular LDPC code.

Generally there are two different methods to represent LDPC codes. Like all linear block codes they can be described via matrices. The second method is a graphical representation.

2.1 *Matrix Representation*

Let's look at an example for a regular LDPC code. The matrix defined in (1) is a 4×8 parity check matrix for the (2, 4) regular code. This matrix can't really be called low-density, since the size of H should be large enough for the condition given above to be satisfied.

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

2.2 *Graphical Representation*

Tanner considered LDPC codes and showed how they may be represented effectively by a so-called bipartite graph, also known as Tanner graph [2].It provides a complete representation of the code and it aids in the description of the decoding algorithm [9].The Tanner graph for (1) is given in Figure 1.

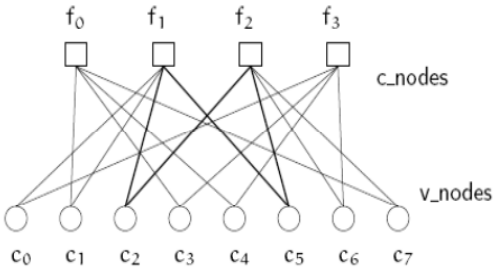

Figure 1. Tanner graph corresponding to the parity check matrix in matrix (1).The marked path c2- f1-c5- f2- c2 is an example for a short cycle of length 4.

A bipartite or Tanner graph consists of two types of nodes which may be connected by edges. The two types of nodes are 'variable' nodes and 'check' nodes. The Tanner graph of a code is drawn according to the following rule: check node j is connected to variable node i whenever element hji in H is '1'.There are m = (n – k) check nodes, one for each check equation and n variable nodes, one for each code bit ci, where n is the block length and k denotes the number of information bits. The m rows of H specify the m c-node connections and the n columns of H specify n v-nodes.

A cycle in a Tanner graph is a sequence of connected vertices which start and end at the same vertex in the graph, and which contains other vertices no more than once. The length of a cycle is the number of edges it contains, and the girth of a graph is the size of its smallest cycle. For optimum decoding performance the Tanner graph should free of short cycles of length 4 [2].

3. Gallager's Construction Technique

For a given choice of ρ and γ, Gallager[1-2] gave the following construction method for a class of linear codes specified by their parity-check matrices. Form a $k\gamma \times k\rho$ matrix H that consists of γ ($k\gamma \times k\rho$) submatrices,H_1, H_2,… H_γ.Each row of a submatrix has ρ 1's and each column of a submatrix contains a single 1.Thus,each submatrix has a total of $k\rho$ 1's.For $1 \leq i \leq k$, the ith row of H_1 contains all its ρ 1's in columns (i-1) ρ+1 to $i\rho$.The other submatrices are merely column permutations of H_1.

$$H = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_\gamma \end{bmatrix}$$

Random permutations of columns of H_1 to form the other submatrices result in a class of LDPC codes with the properties given in section II. There is no known method for finding these permutations to guarantee that no short cycles (especially of length 4) exist in the resultant code. Computer searches[2] are required to find good permutations and hence good LDPC codes.From this construction, it is clear that(1)no two rows in a submatrix of H have any 1-component in common; and (2)no two columns of submatrix of H have more than one 1 in common.The density of H is 1/k. For H to be sparse, k is chosen much greater than 1.

For Example, given the regular (Gallager) LDPC code parameters n=20, k=5, ρ=4 and γ=3,the resultant H is given by the following[3],

H=

1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0
0	1	0	0	0	1	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	0	1	0	0	0	1	0	0
0	0	0	1	0	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0
0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1
1	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0
0	1	0	0	0	0	1	0	0	0	1	0	0	0	0	1	0	0	0	0
0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	1	0
0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	1	0	0	0
0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1

The feature of LDPC codes to perform near the Shannon limit of a channel exists mostly for large block lengths. For example there have been simulations that perform within 0.0045 dB of the Shannon limit at a bit error rate of 10^{-6} with a block length of 10^{7}[7].The large block length results in large parity-check and generator matrices. The complexity of multiplying a code-word with a matrix depends on the amount of 1's in the matrix. If we put the sparse matrix H in the systematic form [P^T I] then the generator matrix G can be calculated the Gauss Elimination method [3] as G= [I P]. The sub-matrix P is generally not sparse so the encoding complexity will be quite high. Since the complexity grows in O(n^2) even sparse matrices don't result in a good performance if the block length gets very high.

4. RS-based Regular-LDPC codes

In [4], Ivana Djurdjevic et.al. proposed an algebraic method for constructing regular LDPC codes is presented. This construction method is based on the simple structure of Reed–Solomon (RS) codes with *two* information symbols. It guarantees that the Tanner graphs [4] of constructed LDPC codes are free of cycles of length 4 and hence have girth at least 6. The construction results in a class of LDPC codes in Gallager's original form [1]. These codes are simple in structure and have good minimum distances. They perform well with iterative decoding or SPA. Such parity check matrices can be masked to generate new and better LDPC codes [2].

4.1 *RS Codes With Two Information Symbols*

Consider the Galois field GF (q) with q elements, where q is a positive integer power of a prime number. Let ρ be a positive integer such that $2 \leq \rho <$q. The generator polynomial of cyclic (n, k,dmin) RS code C is given by [2]:

$$g(X) = (X-\alpha)(X-\alpha^2).....(X-\alpha^{\rho-2})$$
$$=g_0 + g_1X + ... + X^{\rho-2}$$

Notice that n =q-1, k = q- ρ+1, $g_i \in$ GF (q) and α is a primitive element of a field.The parity check matrix R_H for a Reed-Solomon code has size $(\rho-2)\times$n.The rank of matrix R_H can be utmost $(\rho-2)$.Thus minimum distance is dmin= $(\rho-1)$.
Now consider the (q−1)-tuple vector

$$g^{(0)} = (g_0, g_1, \ldots, g_{\rho-2}, 0, 0, \ldots 0)$$

Note that $g_{\rho-2} = 1$. By cyclically shifting $g^{(0)}$, we get generator matrix G of size k ×n for code *C*.

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & . & . & 1 & 0 & . & . & 0 \\ 0 & g_0 & g_1 & g_2 & . & . & 1 & .0 & . & . \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & . & . & g_0 & g_1 & g_2 & . & . & . & 1 \end{pmatrix}$$

C is shortened by deleting the first *q*-ρ+1 information symbols from each codeword of *C* [2].The generator matrix for shortened RS code C_b is a submatrix of size $2 \times \rho$ and it is shown below:

$$G_b = \begin{pmatrix} g_0 & g_1 & g_2 & . & . & . & 1 & 0 \\ 0 & g_0 & g_1 & g_2 & . & . & . & 1 \end{pmatrix}$$

4.2 *Properties of Shortened Code C_b*

1. Since the length of codewords in C_b is ρ and the minimum distance between two codewords of C_b is $(\rho - 1)$, two codewords in C_b only agree at most at one location.
2. Let *c* be a codeword of weight ρ. If we multiply *c* by $\forall\beta \in$ GF(q), we get set ${C_b}^{(1)}$ of (q-1) codewords of weight ρ. Now, length of every ${C_b}^{(1)}$ is also ρ. So ${C_b}^{(1)}$ is a MDS (Maximum Distance Separable) code.
3. Let us partition C_b into a q cosets ${C_b}^{(1)}$, ${C_b}^{(2)}$,.., ${C_b}^{(q)}$ based on ${C_b}^{(1)}$.Notice that ${C_b}^{(i)}$ is a MDS code. Therefore two codewords in any coset ${C_b}^{(i)}$ must differ in all the locations.

4.3 *Construction of LDPC code check matrix*

Let us now explain the explicit construction procedure for a LDPC code check matrix H.

1. All q elements of GF (q) can be expressed as some power of a primitive element α. Let us define the location vector of α^i as a q-tuple over GF(2) is given by:
   $Z(\alpha^i)$= (0,0,….,1,0,…,0), where *i*th element of $Z(\alpha^i)$ is 1 and all other elements are 0.
   Choose one codeword $b = (b_1, b_2 \ldots b_\rho) \in {C_b}^{(i)}$.If we replace each b_i $(1 \leq i \leq \rho)$ by its location vector $Z(b_i)$, we get
   $Z(b) = (Z(b_1), Z(b_2),\ldots. Z(b_\rho))$, which is a ρq-tuple of weight ρ over GF(2).
2. Arrange all q ρq-tuple of ${C_b}^{(i)}$ as rows of a matrix and call this matrix as *Ai*. The weight of each column of *Ai* is 1.
3. Choose a positive integer γ, such that $1 \leq \gamma \leq$ q. Then the parity check matrix *H* of size γq× ρq is defined as:

$$H \triangleq \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_\gamma \end{bmatrix}$$

Since each column of *Ai* has weight 1, weight of an each column of H is γ.So, H is a (γ, ρ)-regular matrix. Each row in *Ai* is a coset member, so each row in *Ai* is different,
Two rows in *Ai* do not have single common element and two codewords in C_b agree at atmost one symbol location (dmin = $\rho - 1$).Hence it can be said that no two rows from *Ai*, *Aj*, $i \neq j$ agree at more than a single element. This will imply that the Tanner graph corresponding to H is free of length 4 cycles.

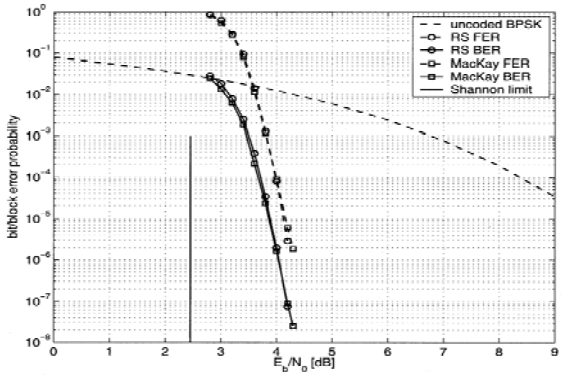

Figure 2. Error performance of the (2048, 1723) RS-based Gallager (6,32)-regular LDPC code with construction field GF(2^6).

For Example: In Figure 2, error performance with iterative decoding of (6, 32)-regular LDPC code over GF(2^6) using the SPA is given. This (6, 32) regular (2048, 1723) RS-LDPC code has been adopted as the FEC in the IEEE 802.3an 10GBase-T standard [5].

4. Progressive Edge Growth Algorithm

A bipartite graph can be described using variable nodes, check nodes and set of edges E. The progressive edge growth (PEG) algorithm proposed by Xiao-Yu Hu et.al.is a general method for the construction of finite length regular and irregular Tanner graphs having large girth by establishing-edges or connections between the variable and check nodes in an edge-by-edge or progressive manner. For given variable node, an edge connects it to one of the check node such that girth is maximum. Thus, PEG algorithm yields large girth when compared

to codes constructed using random methods[8]. Hence, code constructed using PEG algorithm has low error floor in comparison with code constructed using random methods[11].

The PEG algorithm generates good codes for any given block length and rate, provided a density-evolution optimized degree sequence is supplied. Its low complexity makes it suitable for constructing codes of very large lengths and, with a slight modification to avoid the Gauss Elimination step, they can generate linear-time-encoding LDPC codes The Gallager's construction, does not have this degree of flexibility[2,11].

Given the graph parameters,i.e. the number of variable nodes *n*, the number of check nodes *m=n-k*, and the symbol/variable node degree sequence D_v, an edge selection procedure is started such that the placement of a new edge on the graph has very less impact on the girth.
The variable node degree sequence can be described as follow:

$$D_v = \{d_{v1}, d_{v2}, d_{v3}, \ldots, d_{vn}\}$$

Where d_{vi} represents the degree of i^{th} variable node.

Input: sequence D_v
Output: parity check matrix H
Initialize all check nodes with degree 0
for i = 1 to n **do**
  for j = 1 to d_{vi} **do**
    if j = 1 **then**
      1. Find minimum degree check nodes set $C = \{c_1, c_2, c_3, \ldots, c_m\}$ $1 \leq m \leq n\text{-}k$ such that $deg(c_1) \leq deg(c_2) \leq \ldots \leq deg(c_m)$
      2. Choose check node $c_1 \in C$
      3. Put an edge between i^{th} variable node and check node c_1
      4. Increase the degree of c_1 by 1
  else
      1. For i^{th} variable node find check nodes set $C = \{c_1, c_2, c_3, \ldots, c_m\}$ $1 \leq m \leq n\text{-}k$ such that girth is maximum and $deg(c_1) \leq deg(c_2) \leq \ldots \leq deg(c_m)$
      2. Put an edge between i^{th} variable node and check node c_1
      3. Increase the degree of c_1 by 1
    end if
  end for
end for

Check node degree distribution obtained using the above algorithm is almost uniform. Whenever multiple choices are available to pick check node from set C, we can either pick first check node in the set C or randomly pick any check node from set C. In algorithm, we always choose the first member of set C. Figure 3 is an example of symbol/variable node degree D_v = {2,2,2,2,3,3,3,3}[11].The dashed lines represents an edges incident on variable of degree 2 and dark lines represents edges corresponding to variable nodes of degree 3.

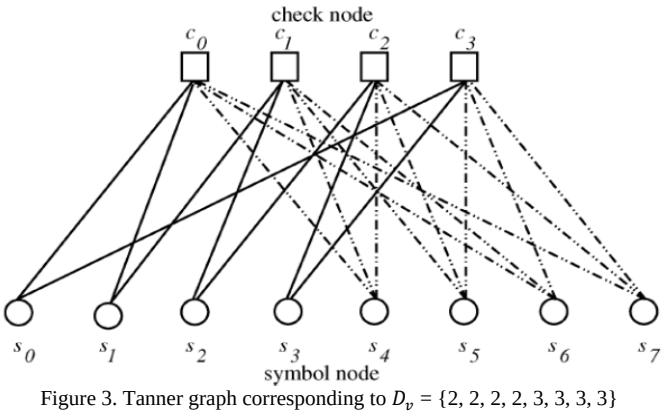

Figure 3. Tanner graph corresponding to D_v = {2, 2, 2, 2, 3, 3, 3, 3}

5. Conclusion

Good regular LDPC codes with large block lengths constructed using Gallager's pseudorandom technique are largely computer generated. This leads to the following limitations:

i. Do not ensure absence of short cycles.
ii. Due to lack structure, the encoding complexity is very high for large column weights and code lengths.

The above drawbacks are overcome using the algebraic method studied in section IV which exploits the structural advantages of the Reed Solomon codes and results in a class of Gallager's LDPC codes having simple structure, good minimum distances and a girth atleast 6.So they work well with the SPA decoding. Furthermore, because of the cyclic nature of the RS-LDPC code their encoding is simple and can be implemented using linear shift registers.

The PEG algorithm also avoids the occurrence of short cycles by providing larger girths even better than RS-based codes. It can be easily tailored to construct LDPC codes having triangular structure which makes them linear-time encodable. Moreover computation and storage requirements in the encoder are also reduced because of sparsity of the parity check matrix.

Thus compared with Gallager's explicit construction, the RS-LDPC and PEG construction in general achieves a better girth and minimum distance properties with much less complexity. However, the PEG algorithm can also be applied to generate irregular graphs whereas the Gallager's and the RS-based construction only apply to regular codes.

References

[1] R. Gallager, "Low-density parity-check codes," IRE Trans. Information Theory, pp. 21-28, January 1962.

[2] Shu Lin and Costello, "Error Control Coding", Pearson-Prentice Hall, 2004.

[3] Othman O. Khalifa, Sheroz khan, Mohamad Zaid, and Muhamad Nawawi, "Performance Evaluation of Low Density Parity Check Codes", International Journal of Computer Science and Engineering, pp. 67-70, Spring 2008.

[4] Ivana Djurdjevic, Jun Xu, Khaled Abdel-Ghaffar and Shu Lin, "A Class of Low-Density Parity-Check Codes Constructed Based on Reed-Solomon Codes With Two Information Symbols",IEEE Communication letters, Vol. 7, No. 7, July 2003.

[5] Amendment: Physical Layer and Management Parameters for 10 Gb/s Operation, Type 10GBASE-T, IEEE *Draft* P802.3an/D2.1.

[6] C.E. Shannon, "A Mathematical Theory of Communication", The Bell System Technical Journal, Vol. 27, pp. 379 - 423; 623 - 656, July, October 1948.

[7] S.-Y. Chung, G. D. Forney Jr ,T. J. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit," *IEEE Communun. Lett.*, vol. 5, pp. 58–60, Feb. 2001.

[8] J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45, pp. 399–432, Mar. 1999.

[9] T. Richardson and R. Urbanke, "Modern Coding Theory", Cambridge 2003.

[10] Angelos D. Liveris, Zixiang Xiong and Costas N. Georghiades, "Compression of Binary Sources With Side Information at the Decoder Using LDPC Codes", IEEE Communications Letters, Vol. 6, NO.10, October 2002.

[11] Xiao-Yu Hu, Member, IEEE, Evangelos Eleftheriou, Fellow, IEEE, and Dieter M.Arnold, Member, IEEE. _Regular and Irregular Progressive Edge-Growth Tanner Graphs_, IEEE Transactions On Information Theory, Vol. 51, No.1, January 2005.