Optimal Rate for Irregular LDPC Codes in Binary Erasure Channel

H. Tavakoli  
Electrical Engineering Department  
K.N. Toosi University of Technology, Tehran, Iran  
tavakoli@ee.kntu.ac.ir

M. Ahmadian Attari  
Electrical Engineering Department  
K.N. Toosi University of Technology, Tehran, Iran  
m_ahmadian@kntu.ac.ir

M. Reza Peyghami  
Department of Mathematics  
K.N. Toosi University of Technology, Tehran, Iran  
peyghami@kntu.ac.ir

Abstract—In this paper, we introduce a new practical and general method for solving the main problem of designing the capacity approaching, optimal rate, irregular low-density parity-check (LDPC) code ensemble over binary erasure channel (BEC). Compared to some new researches, which are based on application of asymptotic analysis tools out of optimization process, the proposed method is much simpler, faster, accurate and practical. Because of not using any relaxation or any approximate solution like previous works, the found answer with this method is optimal. We can construct optimal variable node degree distribution for any given binary erasure rate, e, and any check node degree distribution. The presented method is implemented and works well in practice. The time complexity of this method is of polynomial order. As a result, we obtain some degree distribution which their rates are close to the capacity.

Keywords-component:LDPC code, Infinite analysis method, Density evolution, LP, SDP

I. INTRODUCTION

One of the powerful error-correcting codes, Low-Density Parity-Check (LDPC) codes introduced originally by Gallager in the early sixties [1]. After introduction of Turbo Codes [2], the MacKay’s rediscovery cause some excitedness to the LDPC codes [3]. One important property of long irregular LDPC code is achieving and approaching the capacity of the channel [4]. Binary Erasure Channel (BEC), one of the basic channels, has been studied for achieving and approaching the channel capacity [5]. BEC is usually used as a test problem for the capacity approaching problem, because its constraint, which comes from Density Evolution (DE), is simpler than other type of channel. DE, which was first introduced by Richardson and Urbanke in [6] and extended in [4] and [7], is a numerical tool to show how the iterative message passing decoder, the main LDPC decoder, and works with infinite number of iterations. Both asymptotical consideration of infinite number of iteration, and finite length LDPC codes over BEC has been studied in [8-10].

Nowadays, well known methods for constructing these codes are introduced that approach the channel capacity [11], [12] and [7].

However, a method for achieving the capacity in basic channels has still remained as an open problem. Even more, there is no efficient method to generate practical capacity approaching degree distribution for the BEC. Although some experiences for achieving the channel capacity in infinite node degree distribution were done [13-15].

In [16], a family of optimization problems for finding some LP bounds on the degree distributions over memoryless binary-input output-symmetric (MBIOS) channels was introduced. Instead of solving the non-linear constraint, the main problem of capacity approaching presented in Section II of this paper, using other way such as information-theoretic bounds or a method based on error probability and gap to the capacity, for finding LP constraints was replaced. But finding good degree distribution still remains as a hard problem. However, linear programming tool is mostly used to find an optimum solution for the combinatorial optimization problems. One of the most effective usages is LP decoder introduced by Feldman [17].

Optimization models for finding good degree distribution can be classified in three categories. In the first category, algorithm is based on an evolutionary optimization method such as; hill climbing, genetic algorithm and so on [4, Section IV.]. It is known that the Evolutionary Optimization Solvers (EOS) suffer from some disadvantages such as: 1) EOS cannot guarantee the feasible answer. 2) EOS, most of the time, do not converge. 3) Performance of EOS is sensitive to their subroutine and starting point. These disadvantages restrict EOS to be used in wider classes of problems.

In the second category, algorithm is based on an optimization method, such as Differential Evolution, to search a direct way towards the answer [4, Section IV.]. These types of algorithms are based on infinite number of iterations which may have a loop without consideration of convergence or certification for the optimal answer.

In the third category, for solving the capacity approaching problem, using LP method is the main approach. In this manner, a heuristic approach, which is not efficient to find good degree distribution has been used in [8, Section V.]. In this method, for maximizing the rate, minimizing the $\sum p_i/j$ is considered. So the necessary condition is $\rho(1 - \varepsilon A(x)) > 1 - x$ on $[0,1]$, where $\rho$ and $\lambda$ are check and variable nodes degree
distributions, respectively. In this approach for designing good codes, finding \( p_i \)'s is the main problem provided that \( \lambda_i \)'s are given. So the optimization problem is:

\[
\begin{aligned}
\text{Min} \sum_{j=1}^{N} p_j \\
\text{Subject to:} \sum_{j=1}^{N} p_j (1 - \varepsilon \lambda (x_i)) > 1 - x_i
\end{aligned}
\]

where \( x_i, 1 < i < N \), are a set of some fractional values in \([0,1]\). So an LP problem for finding \( p_j \)'s can be defined.

Other methods for designing good degree distribution are presented in [18] and [19]. The basic idea of this way is reformulation of the inequality \( \rho (1 - \varepsilon \lambda (x_i)) > 1 - x \) based on Taylor’s series of \( \rho^{-1}(1 - x) \) which gives an infinite series. The variable degree sequences gives by this series.

In contrast to these methods, which have been studied, our method is based on the exact constraint with no relaxation. By relaxation the optimization problem the answer would be sub-optimal. So, by this consideration it is certified that the answer of our SDP problem would be optimal.

The organization of the paper is as follows. In Section II, we provide a brief background on problem definition the main problem for optimizing degree distribution. In Section III, we describe SDP reformulation for optimal rate problem. In Section IV, we introduce how we can optimize a code. At last in Section V, we illustrate our contribution with simulation result.

II. PROBLEM DEFINITION

In this section, we focus on irregular LDPC code ensemble over BEC channel. Let \( \mathcal{G} \) be a bipartite graph with \( k \) message bits that is chosen at random with edge degrees specified by two polynomials:

\[
\rho(x) = \sum_{i=2}^{D_c} \rho_i x^{i-1} \quad \lambda(x) = \sum_{i=2}^{D_v} \lambda_i x^{i-1} \quad (1)
\]

Where \( D_c \) and \( D_v \) are maximum check and variable node degrees, respectively, and the coefficients of both polynomials are probabilistic, i.e.,

\[
\sum_{i=2}^{D_c} \rho_i = 1 \quad \sum_{i=2}^{D_v} \lambda_i = 1 \quad \lambda_i \geq 0, \rho_i \geq 0 \quad (2)
\]

Let \( \overline{d}_c = 1 / \left( \sum_{i=2}^{D_c} \rho_i / i \right) \) and \( \overline{d}_v = 1 / \left( \sum_{i=2}^{D_v} \lambda_i / i \right) \) denote the average check and average variable nodes, respectively. It is well known that the code rate is defined as [7]:

\[
R = 1 - \frac{\overline{d}_v}{\overline{d}_c} \quad (3)
\]

For given erasure probability \( \varepsilon \) \( > 0 \) in BEC, the related channel capacity will be \( C = 1 - \varepsilon \). In BEC with given degree distribution on codes, the necessary and sufficient condition for achieving the zero error probability for erased bits, which comes from DE, is

\[
\lambda(1 - \rho(1 - x)) \leq \frac{x}{\varepsilon} \quad \forall x \varepsilon [0, \varepsilon] \quad (4)
\]

Now, suppose that the check node degree is fixed. Then, in order to maximize the rate of the code, while achieving zero error probability, it is sufficient to solve the following optimization problem:

\[
\begin{aligned}
\text{Max} \sum_{i=1}^{N} \lambda_i \\
\text{Subject to:} \lambda_i \geq 0 \\
\sum_{i=1}^{N} \lambda_i = 1 \\
\sum_{i=1}^{N} \lambda_i (1 - \rho(1 - x))^{i-1} \leq \frac{x}{\varepsilon} \quad \forall x \varepsilon [0, \varepsilon]
\end{aligned}
\]

This problem is a semi-infinite optimization problem, i.e., it includes infinite number of constraints. It is notable that the rate of the code is not constrained while general formulation mentioned. One way for solving this problem is to discretize the problem by partitioning the continuous interval \([0, \varepsilon]\) for \( x \) to discreet set \( \{x_0, x_1, ..., x_N\} \subseteq [0, \varepsilon] \) [8, Section V.]. In this case the problem is converted to an optimization problem with finite number of constraints, but the cost that has been paid for this discretization is that a sub-optimal solution is achieved. It is worth mentioning that this optimization problem is linear with respect to the unknown values \( (\lambda_1, \lambda_2, ..., \lambda_{D_v}) \).

Considering the above argument, one can realize that the main problem in Eq. (5) is the last constraint. Due to this fact, in this paper, we are going to reformulate this constraint as a Linear Matrix Inequality (LMI) and therefore we get a semidefinite reformulation for Eq. (5). By doing this reformulation, we are able to solve it by using polynomial time interior-point methods. It is notable that this reformulation leads to an exact solution for solving the problem instead of suboptimal solutions. Numerical results confirm our claim in comparison with the existence method.

III. SDP FORMULATION FOR THE OPTIMAL RATE PROBLEM

A. Problem Formulation

Our aim in this section is to reformulate the infinitely many constrained optimization problem Eq.(5) as an equivalent semidefinite programming problem in order to apply the well known polynomial time interior-point methods to solve this problem.

Let us briefly describe our reformulation. We first restrict ourselves to discuss about the main constraint of the problem, i.e.,

\[
\lambda(1 - \rho(1 - x)) \leq \frac{x}{\varepsilon} \quad \forall x \varepsilon [0, \varepsilon] \quad (6)
\]

or about its equivalent reformulation as

\[
\lambda(1 - \rho(1 - \varepsilon x)) \leq x \quad \forall x \varepsilon [0, 1] \quad (7)
\]

In other words, the feasible region of the problem (5) contains all the vectors \( \lambda \) that satisfy in the following relation:

\[
P(x) = x - \lambda(1 - \rho(1 - \varepsilon x)) \geq 0, \quad \forall x \varepsilon [0, 1] \quad (8)
\]
Since \( \lambda(x) \) and \( \rho(x) \) are polynomials, so the function \( P(x) \) a polynomial function with degree at most \( D_cD_v \). Let \( q = D_cD_v \) and
\[
P(x) = \sum_{j=1}^{q} P_j x^j
\] (9)
where \( P_j = \rho_j x_1 + \cdots + \rho_k x_k \). Using Binomial Theorem and some simple calculations, one can verify that for \( \rho(x) = x^n \), the coefficients \( P_j \) are computed as follows:
\[
P_j = \left\{ \begin{array}{ll}
1 - \sum_{i=0}^{j} \lambda_i \varphi_{k-i} & j = 1 \\
n \sum_{j=1}^{k} \lambda_j \varphi_{k-j-1} x^k & j \neq 1
\end{array} \right.
\] (10)
where the coefficients \( \varphi_{k-i} \) are defined as:
\[
\varphi_{k,i} = (-1)^{k+i} \sum_{n_i \geq 0} \prod_{i=1}^{k} \pi_i \n \] In order to express Eq. (8) as an LMI, we first focus on the reformulation of its general form, i.e.,
\[
P(x) \geq 0, \quad \forall x \in \mathbb{R}
\] (11)
and assume that \( q = 2k \) is an even number. It has been proved in [20] that the infinitely many constraints (11) is semi-definite representable and its semi-definite representation is:
\[
\{ \lambda | P(x) \geq 0, \quad \forall x \in \mathbb{R} \}
\] (12)
where \( \lambda \) denotes the Lowner order of the matrices that stands for positive semi-definiteness of the matrices.

**Proof**: We have:
\[
\Pi(x) = \sum_{j=0}^{q} P_j x^{2j} (x^2 + 1)^{q-j}
\] (14)
Using Newton’s expansion, we obtain:
\[
x^2 (x^2 + 1)^{q-j} = x^{2j} \sum_{j=0}^{q} \left( \frac{q-j}{j} \right) x^{2r} = \sum_{j=0}^{q} \left( \frac{q-j}{j} \right) x^{2r+j}
\]
Therefore,
\[
\Pi(x) = \sum_{j=1}^{q} \left( \begin{array}{c}
p_j (q-j) x^{2j} + p_j (q-1) x^{2j+2} + \cdots + p_j x^{2q} \end{array} \right)
\] This easily shows that
\[
\Pi_t = \left\{ \begin{array}{ll}
\sum_{j=1}^{q} \left( \begin{array}{c}
p_j (q-j) x^{2j} + p_j (q-1) x^{2j+2} + \cdots + p_j x^{2q} \end{array} \right) & t = 2j \\
0 & t = 2j + 1
\end{array} \right.
\]
which completes the proof of the lemma. \( \square \)

**Theorem**: Let \( \Pi(x) \) be defined as in Lemma 1. Then, the problem (5) is equivalent to the following semi-definite programming problem:
\[
\text{Max } \sum_{i=1}^{n} \lambda_i
\]
Subject to:
\[
\Pi_t = \sum_{j=1}^{q} \left( \begin{array}{c}
p_j (q-j) x^{2j} + p_j (q-1) x^{2j+2} + \cdots + p_j x^{2q} \end{array} \right) & t = 2j \\
0 & t = 2j + 1
\]
where \( \geq \) denotes the component-wise order on the vectors and \( \blockdiag \) denotes the Lowner partial order on symmetric matrices that stands for positive semi-definiteness of the matrices.

**Proof**: According to the discussions of pervious section, the vector \( \lambda \) satisfies Eq. (7) if and only if its image by affine mapping \( P(x) \) to \( \Pi(x) = (1 + x^2)^{q} \) from \( \mathbb{R} \) to \([0, 1]\) satisfies \( \Pi(x) \geq 0 \) for all \( x \in \mathbb{R} \). Using (12), this equality happens if and only if there exists a symmetric positive semi-definite matrix \( B = (B_{ij})_{(q+1) \times (q+1)} \) so that it satisfies the following equations:
\[
\Pi_t = \sum_{i+j=1}^{q+1} B_{ij}, \quad 0 \leq l \leq 2q
\]
The proof is completed by replacing this system of linear equations and LMIs in the problem (5). \( \square \)

In order to illustrate these results, we provide a simple structure example to show how these results can be handled in the real problems and computer programming.

**Example**: Suppose that we are looking for the maximum value of the parameter \( b \) so that the polynomial function \( f(x) = ax^2 + bx + c \) be nonnegative on the interval \([0, 1]\) under the condition \( a = c = 1 \). We apply the above mentioned
results and we first obtain the coefficients of the function $\Pi(x)$ using Lemma 1 as follows:

$$\Pi(x) = (1 + x^2)^2 \left( \frac{x^2}{1 + x^2} \right)$$

$$= (a + b + c)x^4 + (b + 2c)x^2 + c$$

$$= (2 + b)x^4 + (b + 2)x^2 + 1$$

Using Theorem 1, the equivalent semi-definite programming reformulation of the problem is defined as follows:

Max $b$

Subject to: $y_2 = 1$

$y_3 + y_5 = 0$

$-y_1 + y_4 + y_6 + y_8 = 2$

$y_7 + y_9 = 0$

$-y_1 + y_{10} = 2$

$y_1 = b$

$[y_2 \ y_3 \ y_4 \ y_5 \ y_6 \ y_7 \ y_8 \ y_9 \ y_{10}] \succeq 0$

Using SDP softwares, such as SeDuMi and CVX, lead us to optimal solution $b = 1$, which can be verified also by using classical solution ways such as interior point method [20].

V. SIMULATION RESULTS

In this part of paper, we present some numerical results obtained by computer simulations. In this simulation, regular parity check node degree distributions are considered, although an example of using irregular parity check node degree distributions is also presented.

| $\rho(x) = x^5$ | $\rho(x) = x^4$ | $\rho(x) = x^3$ | $\rho(x) = x^2$ | $\rho(x) = x^1$ |
|------------------|------------------|------------------|------------------|------------------|
| $\lambda_2$      | 0.4735           | 0.4393           | 0.4021           | 0.4385           | 0.4329           |
| $\lambda_3$      | 0.2244           | 0.2097           | 0.2137           | 0.1456           | 0.1583           |
| $\lambda_4$      | 0.0536           | 0.0000           | 0.0000           | 0.0000           | 0.0000           |
| $\lambda_5$      | 0.2974           | 0.2974           | 0.2974           | 0.2974           | 0.2974           |
| $\lambda_6$      | 0.0000           | 0.0000           | 0.0000           | 0.0000           | 0.0000           |
| $\epsilon$       | 0.69             | 0.56             | 0.49             | 0.38             | 0.33             |
| $\epsilon^{th}$  | 0.69             | 0.56             | 0.49             | 0.38             | 0.33             |
| $R$              | 0.2959           | 0.421            | 0.4922           | 0.593            | 0.6439           |
| $C$              | 0.31             | 0.44             | 0.51             | 0.62             | 0.67             |
| $\delta$         | 0.0478           | 0.0432           | 0.0349           | 0.0435           | 0.0359           |

TABLE I. NUMERICAL RESULTS FOR RATE MAXIMIZATION BY REGULAR PARITY CHECK NODE

**Example 2**: If $\rho(x) = 0.48555x^5 + 0.51445x^6$, the best variable degree distribution with 6 degree is $\lambda(x) = 0.4032x + 0.1512x^2 + 0.4454x^6$. Corresponding rate is Rate = 0.5267 with Capacity = 0.55.

In following, some results for comprising with Table I. Presented. Our criteria for comparing are based on 5 criteria which presented in [7]. They are:

1. lower maximum degree
2. high rate
3. high threshold
4. lower fraction of degree-two edges
5. ratio $\delta = R/C$

First of all, in [19] For a Type-A, a code with $\epsilon = 0.48$ and $\rho(x) = x^5$ is introduced, the variable node degree distribution is:

$$\lambda(x) = 0.4167x + 0.1667x^2 + 0.1000x^3 + 0.0700x^4 + 0.0532x^5 + 0.0426x^6 + 0.0353x^7 + 0.0300x^8 + 0.0260x^9 + 0.0229x^{10} + 0.0204x^{11} + 0.0165x^{12}$$

For this code we have $R = 0.4998$ and $\epsilon^{th} = 0.48$. If we use the ratio between rate and capacity we have $R/C = 0.9611$.

In continue, for a Type-MB in [19] a code with $\epsilon = 0.48$ and $\rho(x) = x^5$ is introduced, the variable node degree distribution is:

$$\lambda(x) = 0.205031x + 0.455716x^2 + 0.193248x^3 + 0.146004x^4 + 0.106257x^5 + 0.486659x^6$$

For this code we have $R = 0.4926$. If we use the ratio between rate and capacity we have $R/C = 0.9473$.

Secondly, in [21] a method is represented which used some LP solver after each other, one of the best answer with this method is a code with $\epsilon = 0.5$ and $R = 0.433942$

$$\lambda(x) = 0.205031x + 0.455716x^2 + 0.193248x^3 + 0.146004x^4 + 0.106257x^5 + 0.486659x^6$$

If we use the ratio between rate and capacity we have $R/C = 0.86$. For an example in related database as a code, we have with $\epsilon = 0.948$ and $R = 0.05$

$$\lambda(x) = 0.553245x + 0.154015x^2 + 0.0169892x^3 + 0.11779x^4 + 0.0673477x^5 + 0.0163603x^6 + 0.074253x^7 + 0.010390x^{10} + 0.396949x^{19}$$

$$\rho(x) = 0.1x + 0.99x^2$$

If we use the ratio between rate and capacity we have $R/C = 0.961$.

Thirdly, there is an optimized code in [7, Example 3.63] with $\epsilon = 0.4741$ and $R = 0.5$

$$\lambda(x) = 0.106257x + 0.486659x^2 + 0.101390x^{10} + 0.396949x^{19}$$

$$\rho(x) = 0.5x^7 + 0.5x^8$$
If we use the ratio between rate and capacity we have $R/C = 0.9507$.

In order to show the efficiency and effectiveness of our proposed, we discretize the interval obtained values of $\lambda_i$'s. The results are given in Fig. 1 in which the horizontal axe shows $N$ and the vertical axe is the obtained values of $\lambda_i$'s.

Fig.1 FOUND ANSWER BY USING DISCRETIZING.

Comparing to the best results obtained until now, the found answers are better in rate maximization based on 5 criteria.

VI. CONCLUSION

In this paper, first of all, we showed how rate optimization problem as an NLP, can be modeled as a semidefinite problem without any relaxation or simplification. Simulation results in both regular and irregular parity check node degree distribution were presented. These results in most cases are better than the best reported results.

ACKNOWLEDGEMENT

This work was partially supported by ITRC.

REFERENCES

[1] R. G. Gallager, "Low-Density Parity-Check Codes", Cambridge, MA: MIT Press, 1963.
[2] C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon limit error correcting coding and decoding", Proceedings 1993 IEEE International Conference on Communications, pp. 1064–1070, Geneva, Switzerland, May 1993.
[3] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity-check codes", IEE Electronic Letters, vol. 32, no. 18, pp. 1545–1546, August 1996.
[4] T. Richardson, A. Shokrollahi and R. Urbanke, "Design of capacity approaching irregular low-density parity-check codes", IEEE Trans. on I.T., vol. 47, no. 2, pp. 619–637, February 2001.
[5] H. D. Pfister, I. Sason and R. Urbanke, "Capacity-achieving ensembles for the binary erasure channel with bounded complexity", IEEE Trans. on I.T., vol. 51, no. 7, pp. 2352–2379, July 2005.
[6] T. Richardson and R. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding", IEEE Trans. on I.T., vol. 47, no. 2, pp. 599–618, February 2001.
[7] T. Richardson and R. Urbanke, "Modern Coding Theory", Cambridge University Press, 2008.
[8] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi and D. A. Spielman, "Efficient erasure-correcting codes", IEEE Trans. on I.T., vol. 47, no. 2, pp. 569–584, February 2001.
[9] C. Di, D. Proietti, I. E. Telatar, T. J. Richardson, and R. L. Urbanke, "Finite length analysis of low-density parity-check codes on the binary erasure channel", IEEE Trans. I.T., vol. 48, no. 6, pp. 1570-1579, June 2002.
[10] T. J. Richardson, A. Shokrollahi, and R. Urbanke, "Finite-length analysis of various low-density parity-check ensembles for the binary erasure channel", in Proc. IEEE I.S. I.T., Switzerland, July 2002, p. 1.
[11] D. J. Costello and G. D. Forney, "Channel coding: The road to channel capacity", Proceedings of the IEEE, vol. 95, no. 6, pp. 1150–1177, June 2007.
[12] "Special issue on Codes on Graphs and Iterative Algorithms", IEEE Trans. on Information Theory, vol. 47, no. 2, February 2001.
[13] A. Shokrollahi, "Capacity-achieving sequences", IMA Volume in Mathematics and its Applications, vol. 123, pp. 153–166, 2000.
[14] P. Oswald and A. Shokrollahi, "Capacity-achieving sequences for the erasure channel", IEEE Trans. on Information Theory, vol. 48, no. 12, pp. 3017–3028, December 2002.
[15] A. Shokrollahi, "New sequences of linear time erasure codes approaching the channel capacity", in Proc. 13th International Symposium on Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (M. Fossorier, H. Imai, S. Lin, and A. Poli), no. 1719 in Lecture Notes in Computer Science, pp. 65-76, 1999.
[16] I. Sason, "On universal properties of capacity-approaching LDPC code ensembles", IEEE Trans. on Communications, vol. 57, pp. 1972–1981, July 2009.
[17] J. Feldman, "Decoding Error-Correcting Codes via Linear Programming", PhD thesis, Massachusetts Institute of Technology, Cambridge, MA.
[18] H. Saeedi and A. H. Banihashemi, "New sequences of capacity achieving LDPC code ensembles over the binary erasure channel", ISIT 2008, Toronto, Canada, July 6 - 11, 2008.
[19] H. Saeedi and A. H. Banihashemi, "Systematic design of Low-Density Parity-Check code ensembles for binary erasure channels", IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 58, NO. 1, JANUARY 2010.
[20] A. Ben-Tal, A. Nemirovski, "Lectures on Modern Convex Optimization", MPS-SIAM Series on Optimization, SIAM, Philadelphia, 2001.
[21] A. Anmaouar A. Montanari R. Urbanke, "How to find good finite-length codes: from art towards science", European Transactions on Telecommunications, Special Issue: Special Issue on Turbo Coding 2006, Volume 18, Issue 5, pages 491–508, August 2007.