A Low Complexity Extrinsic Message Based Decoding Algorithm for Non-Binary LDPC Codes

Nanfan Qiu, Wen Chen, Yang Yu, and Chunshu Li
Department of Electronic Engineering
Shanghai Jiao Tong University, China
Email: {qiunanfan1, wenchen}@sjtu.edu.cn

***Abstract*—In this paper, we propose a low complexity extrinsic message based decoding algorithm for non-binary LDPC codes. This algorithm only requires computations over finite field and integer operations. The novelty of this decoding algorithm lies in that we compute extrinsic message and iteratively update the messages in every iteration. The proposed algorithm provides effective trade-off between computational complexity and performance. Furthermore, complexity issues and decoding performance will be well analyzed in this paper. Simulation results show that we can achieve a better performance than ISRB algorithm with a slight increase in computational complexity.**

***Index Terms*—LDPC; Non-binary LDPC, majority logic decoding, iterative decoding, extrinsic message.**

I. Introduction

Low-Density Parity-Check (LDPC) codes are a class of linear block codes firstly invented in early 1960s by Gallagar [1] and rediscovered by Mackay [2] in 1996. Nowadays LDPC codes have become candidates in many communication protocols, such as WiFi, WiMax, DVB-T2, etc. Recently, their counterpart non-binary LDPC codes constructed over Galois field of size q have shown their potential in improving the coding gain especially at moderate code lengths. Due to their capacity-approaching performance and powerful error-correcting ability, non-binary LDPC codes have been studied extensively in [3] and [4]. So non-binary LDPC code is a key coding technique for providing very high-rate data transmission under high mobility scenarios [5].

The main obstacle for application of non-binary LDPC codes is the huge computational complexity. Mackay [6] devised a fast Fourier transform (FFT) based q-ary sum-product algorithm (QSPA) to reduce the complexity from $O(q^2)$ to $O(q \log q)$. Declercq [7] proposed the extended min-sum (EMS) algorithm where only a subset of the n_m most significant messages in GF(q) is utilized. This decoding technique can reduce the computational complexity because n_m is usually much smaller than q. In addition, the min-max algorithm [8] further reduces the complexity by replacing the sum operation with max operation in check node update. Unfortunately, these algorithms are still too complicated for some real applications.

On the other hand, majority logic based message-passing algorithms have been proposed in recent years, achieving significant reduction in complexity at the cost of extra performance loss [9]. These majority logic based algorithms only require finite field operations, integer additions and integer comparisons, providing efficient trade-off between complexity and performance. Chao Chen proposed a hard-decision based generalized bit-flipping (GBF) in [10]. A serial version symbol-reliability based algorithm is introduced in [11]. This method can provide lower complexity and better performance than algorithms in [10] due to the serial scheduling and a scaling parameter. In [12], an iterative soft reliability-based (ISRB) majority-logic decoding (MLGD) is proposed. This method is developed based on one step majority logic decoding. Comparing with algorithms in [10] and [11], a new insight about check node update process is proposed in [12]. Therefore the reliability measure of the extrinsic information from check node to variable node is more precise and reasonable than previous works with little complexity increasing, which contributes to a better performance. A double-reliability-based MLGD for non-binary LDPC codes is proposed in [13], which utilizes the highest reliability and second highest reliability to improve prediction precision of each check node.

In this paper, we propose a novel low complexity extrinsic message based decoding algorithm for non-binary LDPC codes based on ISRB. Extrinsic message from variable node to check node is utilized to enhance the message-passing process. This method is effective for codes with a large column weight, such as LDPC code constructed based on finite field approach [14].

The rest of this paper is organized as follows. Section II reviews ISRB majority-logic decoding algorithm for non-binary LDPC codes. Section III introduces the low complexity extrinsic message based decoding algorithm in detail. Section IV analyzes the complexity issues of our proposed algorithm. The simulation results which verify the effectiveness of our proposed methods are discussed in Section V. Finally, Section VI draws a conclusion.

II. Review of Iterative Soft-Reliability-Based MLGD Algorithm

In this section, we will briefly review the ISRB decoding algorithm. For details about one step majority logic decoding and ISRB for non-binary LDPC codes, one can refer to [12]. Important notation and definitions used throughout this paper will also be given in this section.

This work is supported by the National 973 Project #2012CB316106, by NSF China #61161130529, and by the National 973 Project #2009CB824904.

978-1-4673-6380-8/13/$31.00©2013 IEEE

A. Notation and Definitions

Let $\mathcal{C}$ be a (d_v,d_c)-regular non-binary LDPC code of block length N and dimension K, which has a $M \times N$ parity-check matrix $\mathbf{H}$ with column weight d_v and row weight d_c. Then code rate is given by $R_c = \frac{K}{N}$. Let GF(q) denote a Galois field with q elements $(0, 1, 2 \ldots, q-1)$, where q is a power of prime number. Elements in GF(q) are called symbols. Each entry of $\mathbf{H}$ are taken from GF(q). In general, an LDPC code has a Tanner graph representation of the matrix $\mathbf{H}$, which consists of N variable nodes and M check nodes corresponding to each column and each row. Let $M(n)$ denote the set of check nodes neighboring to variable node n and $N(m)$ denote the set of variable nodes neighboring to check node m. Then a single check equation is of the form:

$$\sum_{n \in N(m)} h_{m,n} c_n = 0 \tag{1}$$

For a transmitted codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, we expand each code symbol into r-tuple over GF(2), where $r = \log_2(q)$. Then a sequence of nr bits are transmitted over a binary-input Additive White Gaussian Noise (AWGN) channel with two-sided power spectral density $\frac{N_0}{2}$. The Binary Phase Shift Keying (BPSK) modulation is adopted, with modulation mapping $x \mapsto 1 - 2x$. At the receiver, we have $\mathbf{y} = (\mathbf{y_0}, \mathbf{y_1}, \ldots, \mathbf{y_{n-1}})$ denote the received sequence, where each $\mathbf{y_j} = (y_{j,0}, y_{j,1}, \ldots, y_{j,r-1})$.

B. Algorithm Description

For $0 \leq t < r$, we quantize each received bit $y_{j,t}$ into $2^\omega - 1$ intervals, where $u_{j,t}$ is the quantized value represented by ω bits with range in $[-(2^\omega - 1), +(2^\omega - 1)]$. Let a_l denote the element l in GF(q) where $0 \leq l < q$, and $(a_{l,0}, a_{l,1}, \ldots, a_{l,r-1})$ denote the binary representation of a_l. For $0 \leq j < n$, the initialized reliability measure can be computed by

$$\varphi_{j,l} = \sum_{t=0}^{r-1} (1 - 2a_{l,t}) u_{j,t}, \tag{2}$$

where $a_{l,t}$ is the t-th bit of binary representation of a_l. $\varphi_{j,l}$ denotes the reliability measure that the j-th symbol $(y_{j,0}, y_{j,1}, \ldots, y_{j,r-1})$ should be decoded into a_l. Then $\boldsymbol{\varphi}_j = (\varphi_{j,0}, \varphi_{j,1}, \ldots, \varphi_{j,q-1})$ is called the decision vector of the jth received symbol y_j. For $0 \leq i < m$, we define

$$\phi_{i,j} = \min_{j' \in N(i) \backslash j} \max_{l} \varphi_{j',l}. \tag{3}$$

which can be regarded as a reliability measure of the extrinsic information contributed to variable node j. This value is determined by the minimal reliability of received symbols in $N(i) \backslash j$.

Let $\mathbf{z} = (z_0, z_1, \cdots, z_{n-1})$ represent the hard decision result of the received sequence. $\mathbf{s} = (s_0, s_1, \cdots, s_{m-1})$ stands for check-sum vector where $\mathbf{s} = \mathbf{z} \cdot \mathbf{H}^T$. For $0 \leq i < m$, we can normalize each check-sum s_i to be orthogonal on z_j as:

$$\widetilde{s}_i = h_{i,j}^{-1} \cdot s_i = z_j + h_{i,j}^{-1} \sum_{k \in N(i), k \neq j} h_{i,k} z_k. \tag{4}$$

Suppose that z_j is erroneous and all the other symbols in $N(i)$ are error free. According to the parity check equation, we have:

$$z_j^{'} + h_{i,j}^{-1} \sum_{k \in N(i), k \neq j} h_{i,k} z_k = 0. \tag{5}$$

Here $z_j^{'}$ is the correct decoding result of symbol z_j. Base on the analysis above, we can easily get:

$$z_j^{'} = h_{i,j}^{-1} \cdot s_i - z_j. \tag{6}$$

Notice that this equation is not always satisfied because not all the other symbols in $N(i)$ are error free. Then we define $\sigma_{i,j} = h_{i,j}^{-1} \sum_{k \in N(i), k \neq j} h_{i,k} z_k$ which indicates that check node i votes variable node j being decoded into the element $\sigma_{i,j}$. In the next step, we will add all the votes from neighboring check nodes of variable j to the indicated element of variable node j. For $0 \leq j < n$, define $\boldsymbol{\psi}_j = (\psi_{j,0}, \psi_{j,1}, \ldots, \psi_{j,q-1})$ as the reliability measure of the voting. For $0 \leq l < q$, $\psi_{j,l}$ can be obtained by

$$\psi_{j,l} = \sum_{\sigma_{i,j} = l, i \in M(j)} \phi_{i,j}. \tag{7}$$

Let $\mathbf{R}_j = (R_{j,0}, R_{j,1}, \ldots, R_{j,q-1})$ denote the reliability measure vector of symbol z_j and I_{max} denote the maximum iteration number. With these definitions, the ISRB algorithm can be formulated as follows:

- Initialize Compute $\boldsymbol{\varphi}$ using (2). Compute $\boldsymbol{\phi}$ using (3). Set $\mathbf{R} = \lambda \boldsymbol{\varphi}$, here λ is the scaling factor.
- Step 1 Calculate $\mathbf{s} = \mathbf{z} \cdot \mathbf{H}$. If $\mathbf{s} = \mathbf{0}$ or reach the maximum iteration number I_{max}, stop decoding and output the decoded result; otherwise, go to the next step.
- Step 2 Calculate the set of normalized check sums according to (4). Then compute the prediction $\sigma_{i,j}$ from each check node i.
- Step 3 Calculate $\boldsymbol{\psi}_j$ using (7). Update reliability measure $\mathbf{R}_j = \mathbf{R}_j + \boldsymbol{\psi}_j$.
- Step 4 Make the hard decision $z_j = \arg \max_{l \in GF(q)} R_{j,l}$ for all variable nodes. Go to Step 1.

III. Proposed Extrinsic Message Based Decoding Algorithm

In this section, we will introduce the extrinsic message based decoding algorithm specifically designed for non-binary LDPC codes. Firstly we will summarize the differences between ISRB MLGD algorithm and our proposed algorithm. Then after fixing these problems in ISRB, our proposed algorithm can be derived. As stated above, ISRB can significantly reduce the computational complexity for the reasons that check node update process is simple and no complicated operations exist in this algorithm. Comparing with ISRB MLGD algorithm, two steps can be distinguished in our proposed algorithm. Firstly, our method updates not only the decoding prediction from check node to variable node but also the reliability measure of this prediction during each iteration. While in ISRB MLGD only the decoding prediction is updated and reliability measure of this prediction which calculated in the initialization step will stay constant. In the second place,

we propagate the extrinsic information of each variable node for message update, the messages passed from a variable node j to any neighboring check node i contain information from all the neighboring check nodes except for i itself.

Algorithm 1 Proposed Extrinsic Message Based Decoding Algorithm

1: **Initialization**: Compute φ using (3); Initialize $\mathbf{z}$ by making hard decision; Set $\mathbf{R} = \boldsymbol{\varphi}$.
2: **for** $k = 1$ to $Imax$ **do**
3: **for** $i = 0$ to m-1 **do**
4: $s_i = \sum_{j \in N(i)} h_{i,j} z_j$.
5: **end for**
6: Stopping criterion test.
7: **for** $i = 0$ to m-1 **do**
8: **for** $j \in N(i)$ **do**
9: $p_{i,j} = (h_{i,j})^{-1} \cdot s_i - z_j$.
10: **end for**
11: **end for**
12: **for** $j = 0$ to n-1 **do**
13: **for** $i \in M(j)$ **do**
14: $\tau_{i,j} = \lambda \left(\max_{l \in GF(q)} R_{i,j,l} \right)$.
15: **end for**
16: **end for**
17: **for** $i = 0$ to m-1 **do**
18: **for** $j \in N(i)$ **do**
19: $\psi_{i,j} = \min_{j' \in N(i) \backslash j} \tau_{i,j'}$.
20: **end for**
21: **end for**
22: **for** $i = 0$ to m-1 **do**
23: **for** $j \in N(i)$ **do**
24: **for** $x \in M(j) \backslash i$ **do**
25: $R_{i,j,p_{x,j}} = R_{i,j,p_{x,j}} + \psi_{x,j}$.
26: **end for**
27: **end for**
28: **end for**
29: **Tentative Decoding** :
30: **for** $j = 0$ to n-1 **do**
31: $z_j = \arg\max_l (R_{j,l})$.
32: **end for**
33: **end for**

The details of our proposed algorithm are described in algorithm 1. Firstly we compute the syndrome in line 4. Then stopping criterion is tested in line 6. If all the parity check equations are satisfied or algorithm reaches the maximum iteration number, we will stop the decoding iteration and output the result. In line 9 $p_{i,j}$ is the prediction from check node i that variable node j should be decoded into $p_{i,j}$. In line 14 $\tau_{i,j}$ denotes the reliability measure of extrinsic information passed from variable node j to check node i. In line 19 $\psi_{i,j}$ denotes the reliability measure of extrinsic information passed from check node i to variable node j. The parameter λ in line 14 is the scaling factor which should be selected carefully to optimize the decoding performance. The optimal value of λ depends on signal-to-noise ratio (SNR) and code structure. Here λ is selected through experiments and we keep it constant for simplicity. Line 25 is the key step in our algorithm. The reliability messages passed from variable node j to check node i are calculated by accumulating all the reliability measures from check node x where $x \in M(j) \backslash i$, as Figure.1 shows. While in ISRB, this extrinsic information is not considered and it adds all the messages from check node to the indicated element of variable node. Line 31 represents the tentative decoding. In algorithm 1 we keep the propagated message remain independent of the original message by utilizing the extrinsic information. Because the correlation of the message with original messages will prevent the resulting probability from being exact.

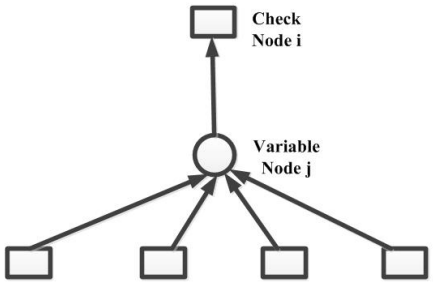

Fig. 1. Extrinsic Information Propagation .

IV. Complexity Analysis

In this section, we will analyze the computational complexity of our proposed algorithm. The computational complexity of ISRB algorithm is fully described in [12]. As our algorithm is based on ISRB, the main emphasis is placed on the extra complexity comparing with ISRB. Let d_c be the check node degree and d_v be the variable node degree. In ISRB, the complexity for calculating the reliability measure of each voting in equation (3) is $N(q-1)+Md_c(d_c-1)$ real comparisons. While in our algorithm, we need $I_{max}(Nd_v(q-1)+Md_c(d_c-1))$ real comparisons as line 14 and 19 indicate. The extra complexity comes from two parts. Firstly we update the reliability measure of messages from check nodes in each iteration, so the maximum iteration number should be considered. Secondly the size of messages propagated from variable node to check node is enlarged because extrinsic information is considered. Considering variable node reliability update step in line 25, ISRB needs Md_c real additions to calculate the reliability. While in our algorithm, the complexity is $Md_c(d_v - 1)$ for calculating extrinsic messages propagated from variable node to check node. For other parts in decoding algorithm, the complexity of our algorithm stays the same as ISRB. Through these analysis, we can conclude that our algorithm increases the decoding complexity a little. However, compared with other belief propagation based decoding algorithms like FFT based min-sum [6] or min-max [8], the complexity of our proposed algorithm is still in a lower level. In the following, we will prove that the extra complexity is deserved because this algorithm will improve the decoding performance.

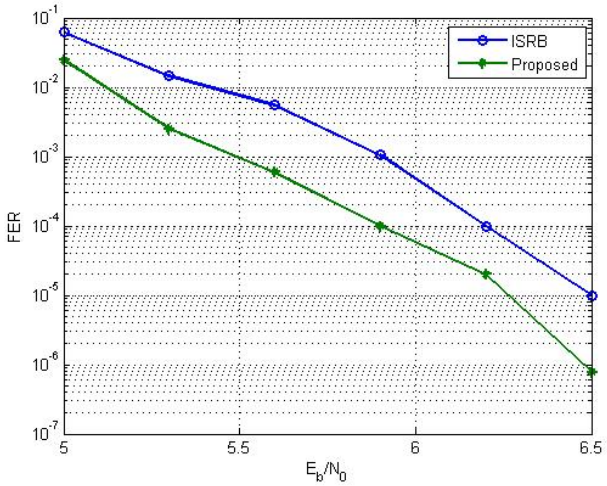

Fig. 2. FER performance of ISRB and proposed extrinsic message based decoding algorithm for at most 25 iterations with non-binary LDPC code over GF(16) of blocklength-135 rate-$1/3$.

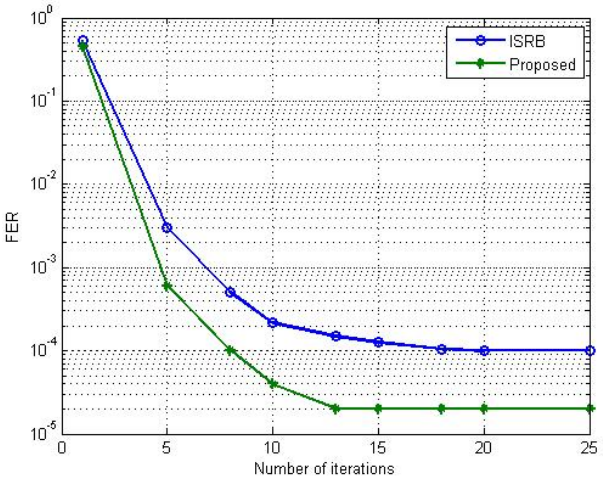

Fig. 3. FER performance vs the number of iterations for non-binary LDPC codes over GF(16) with blocklength-135 rate-$1/3$ over AWGN channel using ISRB decoding and proposed algorithm at a fixed $E_b/N_0 = 6.2dB$.

V. Simulation Results

In this section we will analyze the error correcting performance of different decoding algorithms over AWGN channel. In the simulations we use the same rate-$1/3$ non-binary LDPC code with block length 135 over GF(16). This non-binary LDPC code is constructed using matrix dispersion method-I in [14].

The Frame Error Rate (FER) of different algorithms for 25 iterations is presented in Fig. 2. We can see that the proposed method outperforms ISRB for about 0.3dB at the SNR of 5.9dB. The reason is that the proposed algorithm updates reliability measure iteratively and propagate the extrinsic messages. The excellent performance justifies the effectiveness of our proposed message propagation scheme.

Fig. 3 shows the frame error rate (FER) performance of different algorithms as the number of iterations increase. It is shown that our proposed method can converge faster than ISRB decoding algorithm. ISRB needs nearly 20 iterations for convergence while our proposed method needs only 13 iterations for convergence.

VI. Conclusions

In this paper we propose an extrinsic message based decoding algorithm for non-binary LDPC codes. The proposed algorithm is a novel MLGD algorithm which requires low decoding complexity. Furthermore, we improve the statistical independence of information by propagating extrinsic messages in each iteration. The computational complexity of this proposed method is also discussed in detail. Clarified by the analysis and simulation results, we show that the proposed decoding method significantly improves the error correcting performance with little complexity increasing. So this method can offer very effective trade-off between complexity and decoding performance.

References

[1] R. G. Gallager, "Low-Density Parity-Check Codes." Cambridge, MA: MIT Press, 1963.

[2] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Information Theory*, vol. 45, no. 2, pp. 399-431, March 1999.

[3] Y. Yu, Wen Chen, and L. Wei, "Design of Convergence-Optimized Non-binary LDPC Codes over Binary Erasure Channel," *IEEE Wireless Communications Letters*, vol. 1, no. 4, pp. 336-339, 2012.

[4] N. Qiu, Wen Chen, Y. Lu, and Y. Yu, "Informed Dynamic Scheduling for Majority-Logic Decoding of Non-Binary LDPC Codes," *IEEE Global communications (GC)*, 2013, to be published.

[5] D. Makrakis, P.T. Mathiopoulos, D.P. Bouras, "Optimal decoding of coded PSK and QAM signals in correlated fast fading channels and AWGN: a combined envelope, multiple differential and coherent detection approach," *IEEE Transactions on Communications*, vol.42, no.1, pp.63-75, Jan 1994.

[6] D. J. C. MacKay and M. C. Davey, "Evaluation of Gallager codes of short block length and high rate applications," *in Proc. IMA International Conf. Mathematics its Applications: Codes, Syst. Graphical Models*, pp. 113-130, 2000.

[7] D. Declercq and M. Fossorier, "Decoding algorithms for nonbinary LDPC codes over GF(q)," *IEEE Trans. Commun.*, vol. 55, no. 4, pp.633 -643, 2007.

[8] Savin. V, "Min-Max decoding for non binary LDPC codes," *IEEE International Symposium on Information Theory*, pp.960-964, July. 2008.

[9] Xiaofu Wu, Cong Ling, Ming Jiang, Enyang Xu, Chunming Zhao, Xiaohu You, "New insights into weighted bit-flipping decoding," *IEEE Trans. Commun.*, vol.57, no.8, pp.2177-2180, Aug. 2009.

[10] Chao Chen, Baoming Bai, Xinmei Wang, Ming Xu, "Nonbinary LDPC codes constructed based on a cyclic MDS code and a low-complexity nonbinary message-passing decoding algorithm," *Communications Letters, IEEE* , vol.14, no.3, pp.239-241, March 2010.

[11] F. Garcia-Herrero, M.J. Canet, J. Valls, M.F. Flanagan, "Serial Symbol-Reliability Based Algorithm for Decoding Non-Binary LDPC Codes," *IEEE Communications Letters*, vol.16, no.6, pp.909-912, June 2012.

[12] C.-Y. Chen , Q. Huang , C.-C. Chao and S. Lin, "Two low-complexity reliability-based message-passing algorithms for decoding non-binary LDPC codes," *IEEE Trans. Commun.*, vol. 58, no. 11, pp.3140 -3147 , Nov. 2010.

[13] Y. Lu, N. Qiu, Z. Chen, S. Goto, "An efficient majority-logic based message-passing algorithm for non-binary LDPC decoding," *IEEE Asia Pacific Conference on Circuits and Systems* , pp. 479- 482 , Dec. 2012.

[14] Lingqi Zeng, Lan Lan, Y. Tai, Shumei Song, Shu Lin, , K. Abdel-Ghaffar, "Transactions Papers - Constructions of Nonbinary Quasi-Cyclic LDPC Codes: A Finite Field Approach," *IEEE Transactions on Communications*, vol.56, no.4, pp.545-554, April 2008.