Indonesian Journal of Electrical Engineering and Computer Science
Vol. 25, No. 1, January 2022, pp. 375~381
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v25.i1.pp375-381

A weighted group shuffled decoding for low-density parity-check codes

Fatima Zahrae Zenkouar[1,2], Mustapha El Alaoui[2], Said Najah[1,2]
[1]SIA Laboratory, Faculty of Sciences and Technologies, Sidi Mohammed Ben Abdellah University, Fez, Morocco
[2]Laboratory of Computer Science, Department of Physics, Signals, Automation and Cognitivism (LISAC), Faculty of Sciences Dhar El Mahraz, Sidi Mohamed Ben Abdellah University, Fez, Morocco

Article Info

Article history:

Received Mar 12, 2021
Revised Nov 16, 2021
Accepted Nov 20, 2021

Keywords:

Belief propagation
EFAP-GSBP
Girht
GSBP
LDPC codes
Low latency

ABSTRACT

In this paper, we have developed several concepts such as the tree concept, the short cycle concept and the group shuffling concept of a propagation cycle to decrypt low-density parity-check (LDPC) codes. Thus, we proposed an algorithm based on group shuffling propagation where the probability of occurrence takes exponential form exponential factor appearance probability belief propagation-group shuffled belief propagation (EFAP-GSBP). This algorithm is used for wireless communication applications by providing improved decryption performance with low latency. To demonstrate the effectiveness of our suggested technique EFAP-GSBP, we ran numerous simulations that demonstrated that our algorithm is superior to the traditional BP/GSBP algorithm for decrypting LPDC codes in both regular and non-regular forms.

Corresponding Author:

Fatima Zahrae Zenkouar
SIA Laboratory, Faculty of Sciences and Technologies, Sidi Mohammed Ben Abdellah University
Fez, B.P. 2202–Route Imouzzer, Fez, Morocco
Email: fatimazahrae.zenkouar@usmba.ac.ma

1. INTRODUCTION

In the literature, authors have often used the concept of belief propagation (BP) and the concept of sum and product (SPA) method to control the parity of low-density parity-check codes (LDPC) with good performance. But the concept of sum and product (SPA) decoder has several limitations such as fast divergence and the great difficulty to implement this code. In the literature some authors have proposed solutions to solve these problems. Thus, the authors of the paper [1] have proposed a method based on serial BP decoding. Their algorithm focuses on the variable nodes of the bipartite graph by dividing them into several groups. In the paper [2] the authors focused on the control nodes (CN) of the bipartite graph by dividing them into several groups.

Other authors [3]-[6] have used the concept of serial and parallel decoding through sequential groups of messages to achieve reliable decryption of extrinsic messages within an iteration. Moreover, the authors of the article [7], [8] have shown that the decryption method based on the horizontal group shuffling principle (HGSBP) is the easiest algorithm to implement. Thus we will also use this algorithm as a development of our proposed decoding method. Indeed, we will associate each control node to a group. In this case, each decryption operation will consist of more sub-operations. These sub-operations will initialize the log-likelihood measures generated at the virtual node (VN) variable nodes that are linked to the CNs of the same group in parallel in each group.

Moreover, in this proposed form, the messages will flow within the two-part sub graph consisting of the group's CNs and all the VNs that are connected to its CNs. Thus, considering the CNs and VNs as belonging to the same set unlike conventional group shuffling (GS) scheduling [9]-[18] has improved the efficiency of our proposed algorithm. Then we have considered the short length of the cycle to parameterize again a part of the factorized graph. This allowed us to propose a new algorithm noted weight factor group shuffled belief propagation (WFGSBP) based on the previous idea and a cycle counting algorithm developed in our laboratory. This proposed algorithm allows us to decipher LPDC codes in their regular and non-regular form more efficiently.

In summary, we presented in this work a knowledge-assisted binary phase shift keyin (GSBP) algorithm [19] that uses a simple criterion to select the weighting factors (WFs). In addition, the suggested technique works on both symmetric and asymmetric graphs. We compare the proposed method to the standard BP and GSBP algorithms in terms of convergent behavior and decoding performance in a study of the most recent reweighted GSBP algorithm [20]-[27]. The rest of the paper is organized is being as: in section 2 we present the basic principles of the GSBP decoding concept. Our proposed algorithm is presented in section 3 while the evaluations of its performance are presented in section 4.

2. GROUP SHUFFLED BELIEF PROPAGATION DECODING

As we explained in the previous paragraph, the GSBP algorithm uses a mixture of parallel and sequential coding at the same time which improves its convergence [28], [29] unlike the classical BP algorithm which uses only parallel coding at each iteration where all the variable nodes perform the message passing in parallel. Assume we have an LDPC code of codeword lenght N, there will be N variable nodes v1, v2, …, vN), eah Gk is defined as:

$$Gk = \{vn : n \in \{1, 2 \dots N\} \; and \; k = [\frac{n}{Ng}]\} \quad (1)$$

2.1. System model and decoding schedule

Assume a codeword $C = (c1, c2, \dots, cN)$ is binary phase shift keyin-modulated (BPSK) and transmitted over and additive white Gaussien noise (AWGN) channel with noise variance σ^2. If we note by Y=(y1,y2,…,yN) the vector received by the channel and Ln the log-likelihood ratio (LLR) relative to the variable node n given by:

$$Ln = \frac{2}{\sigma^2} * yN \quad (2)$$

Let Gg be the gth CN group, $1 < g < G$ and U be a set of CNs, iteration counter is I, and maximum number of iterations is Imax. The GSBP algorithm may therefore be described is being as shown in Figure 1.

- Step 0 : initialisation

Set I=1, U={x|1≤ $x \leq M$}, and Gg=∅ for 1≤ $g \leq G$

- Step 1 : Grouping check node

Collect NG elements randomly from the set U to form G1, let U=U\G1.
Collect NG-NG*r element randomly from the set U and NG*r elements from G1 to create G2. For 3≤ $g \leq G$, collect
NG-NG*r element randomly from the set U and NG*r elements from
Gg-1\Gg-2 to create Gg and let U= U\Gg

- Step 2 : message passing

For 1≤ $g \leq G$

a) CN update : ∀ m ∈ G_g, n ∈ N (m)

$Lm \to n = 2tanh^{-1} (\prod_{n' \in N(m)} \tanh (\frac{1}{2} Ln' \to m))$

b) VN update: $\forall n \in U$m′ $\in Gg$ N(m′), m∈M(m)

$Ln \to m$ = Ln + $\sum_{m' \epsilon M(n) \backslash m} Lm' \to n$

- Step 3 : total LLR computation

$\forall n, 1 \leq n \geq N$

$L_n^{total,(l)} = L_n + \sum_{m' \in N(m)} L m' \to n$

- Step 4: hard decision and stopping criterion test

a) Create $D^{(l)}$= $[d1^{(l)}, d2^{(l)}, \dots., dn^{(l)}]$ such that

$dn^{(l)} = 0$ if $L_n^{total,(l)} \geq 0$ and $dn^{(l)}$=1 if $L_n^{total,(l)} < 0$

If $D^{(l)}.H^T$=0 or Imax is reached, stop decoding and output $D^{(l)}$ as the decoded codeword. Otherwise, set l=l+1 and U= {x|1≤ $x \geq M$}, go to step 1.

Figure 1. GSBP decoding clustering

The previous algorithm shows that three factors influence the random variables that are the messages from Ln to m and Lm to n. These factors are the codes received from the channel, their structures and the algorithm used for decoding. We have thus adopted approaches already published in the literature using Gaussian random variables where the code C= (0, 0, ...,0) is modulated through the BPSK norm by the vector X= (1, 1, ...,1). We presented in Figure 2 the block diagram of our algorithm where we used a horizontal processing according to the GSBP concept. Moreover, we considered two types of (CN) nodes according to whether they are updated or not.

Then we use a new division of the non-empty intersections to analyze their influence on the convergence of the proposed algorithm. Thus, for each sub iteration of each iteration we divide it into four classes. If g indicates the number of the sub iteration, class a) will be constituted by the nodes of type (CN) updated at the hth sub iteration such that h is greater than g. Class b) is constituted by the nodes of the (g-1) the group. Class c) contains nodes of type (CN) that are not in class b), whereas class d) contains nodes of type (CN) that are not in either class a) or class b).

We have presented on Figure 3 the state of the four classes after three sub-iterations for an overlap ratio r<0.5. We have also presented on Figure 4 the composition of the four classes for an overlapping ratio r between 0.5 and 1. Let us consider the l-th iteration of our proposed algorithm and compute the average values of the updated variables. For this, letμcg, X(l) be the mean of the message sent by a Class-x CN, that is, μ$cg, X(l) = E\{Lg, m(\rightarrow l)n\}$, where m is a member of the class CNs, n is a VN that links to m in the gth subiteration of the lth iteration. We begin with the VN update equation. Suppose the VN of degree-i, n is connected to p CNs of class d, q CNs of class b and i-p-q CNs of class a. For the g-th subiteration of the l-th iteration, we have, for g = 1.

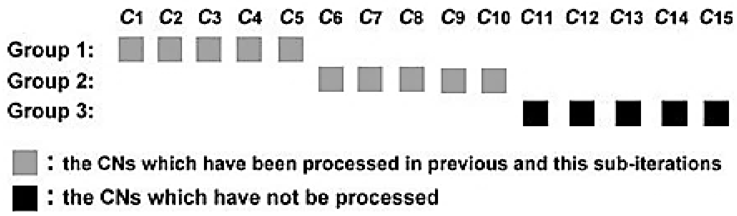

Figure 2. After two sub-iterations, an example of GSBP

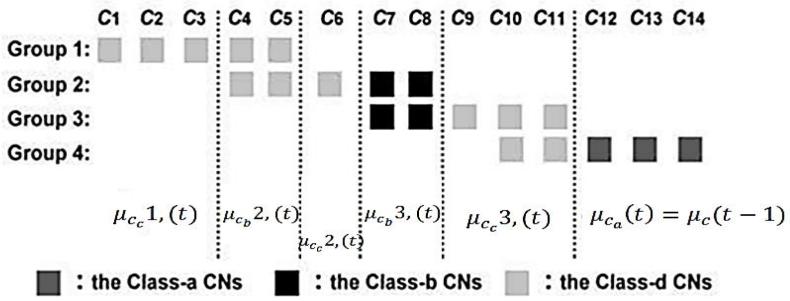

Figure 3. When R < 0.5, an example of NDGSBP after three sub-iterations

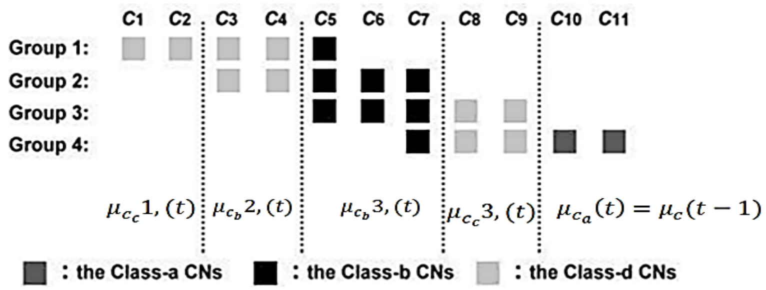

Figure 4. An application for NDGSBP following three sub-iterations when $0.5 \leq R \leq 1$

3. PROPOSED WFGSBP ALGORITHM

The suggested WFGSBP method is described in this part, which determines the reweighting parameters based on simple criteria. Because the technique does not need a symmetrical factor graph, it may be used to generate LDPC codes with both regular and irregular designs. We'll go through the cycle counting method briefly before moving on to our message forwarding rules and the WFGSBP decoding algorithm flow. The GSBP method, while improves decoding results convergence, nonetheless has a lot of flaws, particularly in terms of implementation. We present the WFGSBP method for regular and irregular LDPC codes suggested for the GSBP to minimize complexity as shown in Figure 5.

- Step 0 : initialisation

This step consist of calculating short cycles ρi=exp(-(Si/(k*Ug)))
Then we compute the LLR value of the received symbol:
λi=log [P (Xi=0|Yi)/P (Xi=1|Yi]

- Step 1 : Grouping check node

Collect NG elements randomly from the set U to form G1, let U=U\G1.
Collect NG-NG*r element randomly from the set U and NG*r elements from G1 to create G2. For $3\leq g \leq G$, collect
NG-NG*r element randomly from the set U and NG*r elements from
Gg-1\Gg-2 to create Gg and let U= U\Gg

- Step 2 : message passing

For $1\leq g \leq G$
CN update : ∀ m ∈ G_g, n ∈ N (m)
$Lm \rightarrow n = 2tanh^{-1}\left(\prod_{n' \in N(m)} \tanh\left(\frac{1}{2}Ln' \rightarrow m\right)\right)$
VN update: $\forall n \in U m' \in Gg$ N(m′), m∈M(m)
$Ln \rightarrow m = Ln + \sum_{m' \epsilon M(n)\backslash m} Lm' \rightarrow n$

- Step 3 : total LLR computation

$\forall n, 1 \leq n \geq N$
$L_n^{total,(l)} = L_n + \sum_{m' \epsilon N(m)} L\,m' \rightarrow n$

- Step 4: hard decision and stopping criterion test

Create $D^{(l)} = [d1^{(l)}, d2^{(l)}, \ldots, dn^{(l)}]$ such that
$dn^{(l)} = 0$ if $L_n^{total,(l)} \geq 0$ and $dn^{(l)}=1$ if $L_n^{total,(l)} < 0$
If $D^{(l)}.H^T=0$ or Imax is reached, stop decoding and output $D^{(l)}$ as the decoded codeword. Otherwise, set l=l+1 and U= $\{x|1\leq x \geq M\}$, go to step 1.

Figure 5. Weighted factor shuffled grouped belief propagation algorithm

4. SIMULATION AND RESULTS

We have chosen the three codes C1, C2, and C3.
C1: LDPC code of codeword size N = 1296 and code ratio 1/2 for the IEEE 802.11 standard [30], [31].
C2: LDPC code of N = 1056 and code ratio 1/2 for the IEEE 802.16 standard [10].
C3: An independent replicate accumulate (IRA) code of N = 1024 and code ratio 1/2, where the distribution polynomials λ(x) and ρ(x) for the variant versus control links, respectively, are defined as:

$$\lambda(x) = 0.3330x + 0.3851x\,2 + 0.0002x\,3 + 0.1392x\,6 + 0.1425x\,7 \qquad (3)$$

$$\rho(x) = 0.9849x\,5 + 0.0151x\,6 \qquad (4)$$

Johnson and Weller in [32], Tatsukawa *et al.* [33], the IRA code is presented and proven to be appropriate for the AWGN channel. We create such an IRA code at random using an approach described in [33], which does not use any technique to increase local girths. It's because we want to investigate if the suggested grouping's performance is influenced by Tanner graph topologies.

We run the simulations on an AWGN canal after BPSK modulating from 1 dB to 5 dB at 0.5 dB intervals until the number of bit errors in the evaluated code words reaches 10^5 or the number of trials reaches $10^7 (Imax = 5)$. We simulate the WFGSBP decoding for r 4,8 and 16, along with the BP run (grouping r=1). The average number of iterations is shown in Figures 6-8. At virtually all observation locations, the mean value for the original GSBP decoding is higher or equal to that for WFGSBP decoding.

In conclusion, even if the maximum number of iterations is modest, the suggested method can enhance the performance of the GSBP decoding. When signal-to-noise ratio (SNR) reaches 4.5 [dB], the impact is very noticeable (when the canal noise has a deep impact).

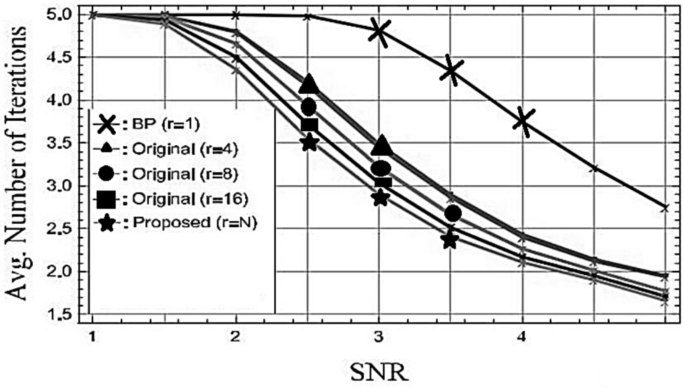

Figure 6. BER performance comparison of LDPC codes using the decoding algorithm: WGSBP, GSBP, and BP for C1

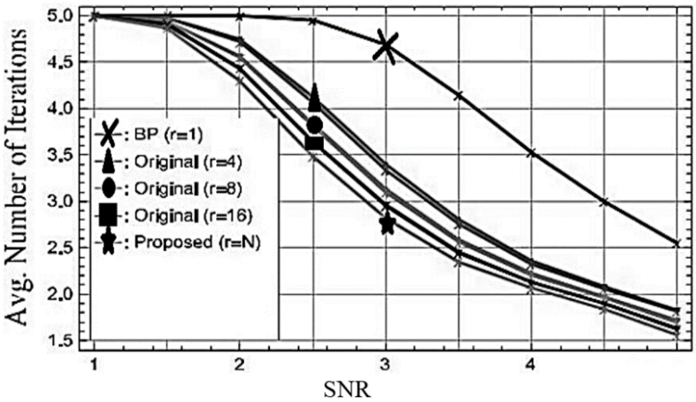

Figure 7. BER performance comparison of LDPC codes using the decoding algorithm: WGSBP, GSBP, and BP for C2

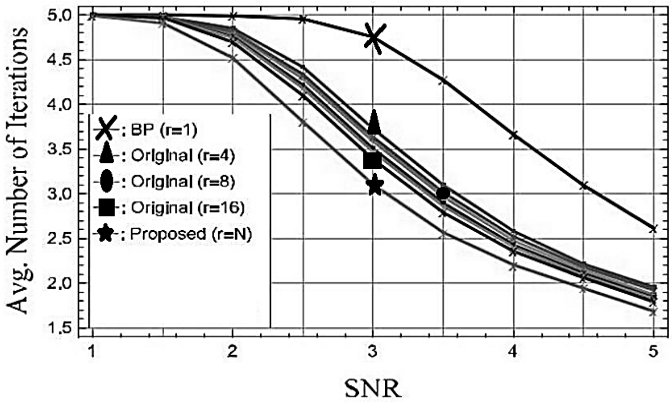

Figure 8. BER performance comparison of LDPC codes using the decoding algorithm: WGSBP, GSBP, and BP for C3

5. CONCLUSION

For the GSBP decoding method, we suggested a grouping based on the weighted parameter strategy in this article. We also found that the suggested approach may improve error correction performance and speed of convergence. Indeed, simulation findings demonstrate that the proposed WFGSBP decoding algorithm may deliver good results while needing fewer decoding rounds than the GSBP method.

REFERENCES

[1] R. Gallager, "Low-density parity-check codes," in *IRE Transactions on Information Theory*, vol. 8, no. 1, pp. 21-28, January 1962, doi: 10.1109/TIT.1962.1057683.

[2] D. J. C. Mackay and R. M. Neal, "Near Shannon limit perform ance of low density parity check codes," *Electron. Lett.*, vol. 33, no. 6, pp. 457-458, Mar. 1997, doi: 10.1049/el:19970362.

[3] N. El Maammar, S. Bri, and J. Foshi, "A comparative simulation study of different decoding schemes in LDPC coded OFDM systems for NB-PLC channel approach," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 15, no. 1, pp. 306-313, july 2019, doi: 10.11591/ijeecs.v15.i1.pp306-313.

[4] T. K. Moon, "Error Correction Coding: Mathematical Meth ods and Algorithms," *Wiley-Blackwell*, July 1, 2005, doi: 10.1002/0471739219.

[5] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes. 1," *Proceedings of ICC '93-IEEE International Conference on Communications*, vol. 2, 1993, pp. 1064-1070, doi: 10.1109/ICC.1993.397441.

[6] N. El Maammar, S. Bri, and J. Foshi, "Performances Concatenated LDPC based STBC-OFDM System and MRC Receivers," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 8, no. 1, pp. 622-630, February 2018, doi: 10.11591/ijece.v8i1.pp622-630.

[7] F. R. Kschischang, B. J. Frey, and H.-Loeliger, "Factor graphs and the sum-product algorithm," in *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 498-519, Feb. 2001, doi: 10.1109/18.910572.

[8] H. Xiao and A. H. Banihashemi, "Graph-based message-passing schedules for decoding LDPC codes," in *IEEE Transactions on Communications*, vol. 52, no. 12, pp. 2098-2105, Dec. 2004, doi: 10.1109/TCOMM.2004.838730.

[9] J. S. Yedidia, W. T. Freeman, and Y. Weiss, "Understandin g belief propagation and its generalizations," *Exploring artificial intelligence in the new millennium*, vol. 8, pp. 236-239, 2003.

[10] M. J. Wainwright, T. S. Jaakkola, and A. S. Willsky, "Tree-based reparameterization framework for analysis of sum-product and related algorithms," in *IEEE Transactions on Information Theory*, vol. 49, no. 5, pp. 1120-1146, May 2003, doi: 10.1109/TIT.2003.810642.

[11] M. J. Wainwright, T. S. Jaakkola, and A. S. Willsky, "A new class of upper bounds on the log partition function," in *IEEE Transactions on Information Theory*, vol. 51, no. 7, pp. 2313-2335, July 2005, doi: 10.1109/TIT.2005.850091.

[12] T. R. Halford and K. M. Chugg, "An algorithm for counting short cycles in bipartite graphs," in *IEEE Transactions on Information Theory*, vol. 52, no. 1, pp. 287-292, Jan. 2006, doi: 10.1109/TIT.2005.860472.

[13] J. Liu and R. C. de Lamare, "Novel intentional puncturing schemes for finite-length irregular LDPC codes," *2011 17th International Conference on Digital Signal Processing (DSP)*, 2011, pp. 1-6, doi: 10.1109/ICDSP.2011.6004903.

[14] J. Liu and R. C. de Lamare, "Finite-length rate-compatible LDPC codes based on extension techniques," *2011 8th International Symposium on Wireless Communication Systems*, 2011, pp. 41-45, doi: 10.1109/ISWCS.2011.6125306.

[15] H. Wymeersch, F. Penna, and V. Savić, "Uniformly reweighted belief propagation: A factor graph approach," *2011 IEEE International Symposium on Information Theory Proceedings*, 2011, pp. 2000-2004, doi: 10.1109/ISIT.2011.6033905.

[16] H. Wymeersch, F. Penna, and V. Savic, "Uniformly Reweighted Belief Propagation for Estimation and Detection in Wireless Networks," in *IEEE Transactions on Wireless Communications*, vol. 11, no. 4, pp. 1587-1595, April 2012, doi: 10.1109/TWC.2012.021412.111509.

[17] J. Liu and R. C. de Lamare, "Low-Latency Reweighted Belief Propagation Decoding for LDPC Codes," in *IEEE Communications Letters*, vol. 16, no. 10, pp. 1660-1663, October 2012, doi: 10.1109/LCOMM.2012.080312.121307.

[18] R. Tanner, "A recursive approach to low complexity codes," in *IEEE Transactions on Information Theory*, vol. 27, no. 5, pp. 533-547, September 1981, doi: 10.1109/TIT.1981.1056404.

[19] W. Ryan and S. Lin, "Channel Codes: Classical and Modern," *Cambridge: Cambridge University Press*, 2009, doi: 10.1017/CBO9780511803253.

[20] T. M. Cover and J. A. Thomas, "Elements of Information Theory," *2nd edition. Wiley-Interscience*, 2006.

[21] Xiao-Yu Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth tanner graphs," *in IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 386-398, Jan. 2005, doi: 10.1109/TIT.2004.839541.

[22] D. Vukobratovic and V. Senk, "Generalized ACE Constrained Progressive Edge-Growth LDPC Code Design," in *IEEE Communications Letters*, vol. 12, no. 1, pp. 32-34, January 2008, doi: 10.1109/LCOMM.2008.071457.

[23] A. G. D. Uchôa, C. Healy, R. C. de Lamare, and R. D. Souza, "LDPC codes based on Progressive Edge Growth techniques for block fading channels," *2011 8th International Symposium on Wireless Communication Systems*, 2011, pp. 392-396, doi: 10.1109/ISWCS.2011.6125390.

[24] Y. Yang, J.-Z. Huang, S. Tong, and X.-M. Wang, "Replica horizontal-hhuffled iterative decoding of low-density parity-check codes," *The Journal of China Universities of Posts and Telecommunications*, vol. 13, no. 6, pp. 32-40, Jun. 2010, doi: 10.1016/S1005-8885(09)60522-7.

[25] T. J. Richardson and R. L. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," in *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 599-618, Feb 2001, doi: 10.1109/18.910577.

[26] S.-Y. Chung, T. J. Richardson, and R. L. Urbanke, "Analysis of sum-product decoding of low-density parity-check codes using a Gaussian approximation," in *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 657-670, Feb 2001, doi: 10.1109/18.910580.

[27] S. Ten Brink, G. Kramer, and A. Ashikhmin, "Design of low-density parity-check codes for modulation and detection," in *IEEE Transactions on Communications*, vol. 52, no. 4, pp. 670-678, April 2004, doi: 10.1109/TCOMM.2004.826370.

[28] E. Sharon, A. Ashikhmin, and S. Litsyn, "Analysis of Low-Density Parity-Check Codes Based on EXIT Functions," in *IEEE Transactions on Communications*, vol. 54, no. 7, pp. 1349-1349, July 2006, doi: 10.1109/TCOMM.2006.877935.

[29] Z. Song, R. Yu, and P. Ma, "Gaussian Approximation for LDPC Codes under Group Shuffled Belief Propagation Decoding," *2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, 2010, pp. 1-4, doi: 10.1109/WICOM.2010.5600988.

[30] IEEE 802 Committee, "Part 11: Wireless LAN MAC and PHY specifications amendment 10: Mesh networking," *IEEE P802. 11s D3.* 0, 2009.

[31] "IEEE Standard for Air Interface for Broadband Wireless Access Systems," in *IEEE Std 802.16-2017 (Revision of IEEE Std 802.16-2012)*, pp. 1-2726, 2 March 2018, doi: 10.1109/IEEESTD.2018.8303870.

[32] S. J. Johnson and S. R. Weller, "Constructions for irregular repeat-accumulate codes," *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, 2005, pp. 179-183, doi: 10.1109/ISIT.2005.1523318.

[33] R. Tatsukawa, A. Manada, and H. Morita, "Irregular repeat accumulate codes based on max-flow algorithm for energy-saving networks," in *Proc. 9th Int. Conf. Body Area Netw.*, 2014, pp. 326-330, doi: 10.4108/icst.bodynets.2014.256920.

BIOGRAPHIES OF AUTHORS

Fatima Zahrae Zenkouar received a state engineering degree in embedded systems and industrial data from the National School of Applied Sciences, University of Sidi Mohammed Ben Abdellah, Fez, Morocco in 2015. He is currently pursuing his Ph.D. degree in Computer Science with the Laboratory of Intelligent Systems and Application at the Faculty of Science and Technology of Fez. His research interests include signal/data processing, Code theory, parallel computing, and LDPC algorithms. She can be contacted at email: fzenkouar@gmail.com.

Mustapha El Alaoui is born in the Old Medina, Fes, Morocco, 1994. He recieved his Master degree since 2017 in Micro-Electronics in Faculty of Sciences Dhar EL Mahraz (FSDM), Sidi Mohammed Ben Abdellah University (USMBA), Fez, Morocco. He received a Ph.D degree in Electrical Engineering in 2021 from Laboratory of Computer Science, Signals, Automation and Cognitivism (LISAC), Department of Physics, FSDM, USMBA, Fez, Morocco. His research interests include Li-Ion battery charger interface (BCI) and BMS, RFID passif and actif tags, CMOS mixed mode integrated circuit design, Integrated Class-D power output stage and renewable energy. He can be contacted at email: Mustapha.elalaoui@usmba.ac.ma.

Said Najah received a Ph.D degree in Computer Science from the Faculty of Science, University Sidi Mohamed Ben Abdellah, Fez, Morocco in 2006. He is currently a professor of the Department of Computer Science, Faculty of Science and Technology Fez Morocco. He is a member in the Laboratory of Intelligent Systems and Application (LSIA Laboratory). His current research interests include parallel computing, code theory, signal processing and artificial intelligence. He can be contacted at eEmail: said.najah@usmba.ac.ma.