Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol.6, No.2, December 2018, pp.365-372
Available online at:*http://pen.ius.edu.ba*

An efficient combination between Berlekamp-Massey and Hartmann Rudolph algorithms to decode BCH codes

Hamza Faham[1], My Seddiq El Kasmi Alaoui[1], Saïd Nouh[1], Mohamed Azzouazi[1]
[1]Departement of Mathematics and Computer Science,Faculty of Sciences Ben M'sik, Hassan II University

Article Info

Received Jun 29, 2018

Keyword:

Error correcting codes
Hartmann Rudolph
Berlekamp Massey
PHR-BM
BCH codes

ABSTRACT

In digital communication and storage systems, the exchange of data is achieved using a communication channel which is not completely reliable. Therefore, detection and correction of possible errors are required by adding redundant bits to information data. Several algebraic and heuristic decoders were designed to detect and correct errors. The Hartmann Rudolph (HR) algorithm enables to decode a sequence symbol by symbol. The HR algorithm has a high complexity, that's why we suggest using it partially with the algebraic hard decision decoder Berlekamp-Massey (BM).

In this work, we propose a concatenation of Partial Hartmann Rudolph (PHR) algorithm and Berlekamp-Massey decoder to decode BCH (Bose-Chaudhuri-Hocquenghem) codes. Very satisfying results are obtained. For example, we have used only 0.54% of the dual space size for the BCH code (63,39,9) while maintaining very good decoding quality. To judge our results, we compare them with other decoders.

Corresponding Author:

Hamza FAHAM,
Departement of Mathematics and Computer Science,
Faculty of Sciences Ben M'sik, Hassan II University,
Av Driss El Harti, SidiOthmane, Casablanca7955, Morocco.
Email: faham.hamza@gmail.com

1. Introduction

Communication is the origin of social and economic development [1]. However, all the means of communication are subject to disturbances. In particular with digital communications [2], interferences can alter the transmitted message, whether it transfers voice, videos, or any other data.
The correction of these errors will be a necessity. Between two people, communication is facilitated by the brain. In fact, this last compensates for disturbances due to external noise because it has background on the used language and the context of the conversation. For digital communications, the handled values are 0 and 1. Therefore, when a received value is false, then there is an error that must be corrected.
To solve this problem, error correcting codes have been introduced [3]. These latter add redundancy bits to the transmitted message to protect the useful information. Various error correcting codes are used in different devices such as smartphones, CDs, DVDs, hard disks or packets transmitted over Internet or over mobile networks. In this paper, we propose a serial concatenation between symbol by symbol and word by word decoders to decode BCH codes.
The remainder of this paper is structured as follows. In section 2 we present some related works. In section 3 we present the proposed approach, in the section 4, we present the simulation results of the proposed decoder and we make a comparison with other decoders. Finally, a conclusion and a possible future direction of this research are outlined in section 5.

2. Relatedworks

In [4] Huang et al. have presented a method based on the link between syndromes and correctable errors pattern by employing hash techniques; in [5] an approach called New Efficient Syndrome-Weight Decoding Algorithm was developed to decode up to five errors in a binary systematic Quadratic Residue QR(47,24,11) code, this technique is founded on the weight of syndrome difference and proprieties of cyclic codes. These two methods have a major disadvantage. They are just applicable for Quadratic Residue (QR) codes. By exploiting the Bit Error Rate Term, El ghayyaty et al. [6] have published a performances study of BCH error correcting codes and they gave a comparative study between the BCH(15, 7, 2) and BCH(255, 231, 3) codes. In [7], quadratic residue codes were discussed over a defined ring.

In [8] a very interesting result was proved; the extended quadratic residue binary codes are the only nontrivial extended binary cyclic codes that are invariant under the projective special linear group. In [9] El idrissi et al. proposed a comparative study of performance between the Bose-Chaudhuri-Hocquenghem codes BCH (15, 7, 2) and BCH (255, 231, 3) using the bit error rate term (BER). In [10,11] a deep learning method to enhance belief propagation algorithm was introduced. By attribution of weights to the edges of the Tanner graph, the standard belief propagation algorithm was generalized. In [12] an iterative hard decision decoding algorithm for binary linear block codes was introduced using a Binary Symmetric Channel (BSC).

In [13] a Cyclic Weight (CW) algorithm decoding was developed to decode the binary systematic (47,24,11) quadratic residue (QR) code; in addition to the weights of syndromes, they exploited properties of the cyclic codes; the same authors and in a previous paper [14], have presented an algebraic decoding algorithm to correct all patterns of four or fewer errors in the binary QR(41,21,9) code. To decode up to five possible errors in a binary systematic QR(47,24,11) code, a table lookup decoding algorithm was presented [15].

The authors of [16] have calculated the needed primary unknown syndrome for the binary QR code using the Lagrange interpolation formula. In [17] the authors have presented a decoding of quadratic residue codes by using hashing search to determine error patterns.

Several hard decoder based on genetic algorithms (GA) were introduced. We begin by the HDGA (Hard decision Decoder based on Genetic Algorithms) [18], it exploits information sets to decode linear block codes; the second one is the Bit Flipping decoding algorithm (BF) [19, 20] developed initially for LDPC codes and generalized after on linear block codes, it is based on the verification of many orthogonal equations. In [21], authors presented an efficient decoder called ARDecGA (Artificial Reliabilities based Decoding Genetic Algorithm); it is based on a generalized parity check matrix that computes a vector of artificial reliabilities of the binary received word and it uses a genetic algorithm to determine the maximum likelihood binary word to this vector. Recently, the authors of [22] have developed a new decoder called HSDec(hard decision decoder based on Hash and Syndrome Decoding) based on syndrome computing and hash techniques, this decoder is used to decode various linear codes and has a reduced temporal complexity.

3. The proposed combination scheme

The famous Hartmann-Rudolph decoder (HR) [25] is a soft decision decoder that uses a symbol by symbol decoding algorithm.Hartman and Rudolph have showed that the probability that a bit corresponding to a symbol r_j, of the sequence r to decode, is equal to 1 or 0, depends on all the codewords of the dual code $C^{\perp}$ generated by the control matrix H.
From the received sequence r and by using the formula (1), the HR algorithm decides if the m^{th} bit of the decoded word $c^{'}$ is equal to 1 or 0.

$$\begin{cases} c'_m = 0 \quad if \quad \sum_{j=1}^{2^{n-k}} \prod_{l=1}^{n} \left(\frac{1-\Phi_l}{1+\Phi_l} \right)^{c_{jl}^{\perp} \oplus \delta_{ml}} > 0 \\ c'_m = 1 \qquad\qquad\qquad\qquad otherwise \end{cases} \tag{1}$$

where:

- ✓ $\delta_{ij} = \begin{cases} 1 & if\ i = j \\ 0 & else \end{cases}$
- ✓ $\phi_m = \frac{\Pr(r_m|1)}{\Pr(r_m|0)}$
- ✓ $The\ bit\ c_{jl}^{\perp}\ denotes\ the\ l^{th}\ of\ the\ j^{th}\ codewords\ of\ the\ code\ C^{\perp}$

The formula (1) uses 2^{n-k} dual codewords which increases the HR temporal complexity, so this algorithm will be applicable only for small length codes.To remedy this problem, Nouh *et al.* [26] have proposed to use just a part, M<2^{n-k} dual codewords, of dual space. In this case the used decoder is called Partial Hartmann and Rudolph decoder (PHR). The formula (1) becomes.

$$\begin{cases} c_m^{'} = 0 \quad if \quad Q = \sum_{j=1}^{M} \prod_{l=1}^{n} \left(\frac{1-\Phi_l}{1+\Phi_l} \right)^{c_{jl}^{\perp} \oplus \delta_{ml}} > 0 \\ c_m^{'} = 1 \qquad \text{otherwise} \end{cases} \tag{2}$$

The Berlekamp-Massey (BM) algorithm [23-24] is an efficient method to decode BCH codes. We note by $c(x) = \sum_{j=0}^{n-1} c_j x^j$, $r(x) = \sum_{j=0}^{n-1} r_j x^j$ and $e(x) = \sum_{j=0}^{n-1} e_j x^j$ respectively the transmitted codeword polynomial, the received word polynomial and the added error polynomial. If the received word contains $\gamma \leq t$ errors in the positions$(i_j)_{1 \leq j \leq \gamma} (0 \leq i_j \leq n-1)$, so:$e(x) = \sum_{j=0}^{n-1} (r_j + c_j) x^j = \sum_{j=1}^{\gamma} e_{i_j} x^{i_j}$.

In this paper, we propose a serial concatenation between the Hartmann Rudolph algorithm partially exploited (PHR) and the Berlekamp-Massey (BM) decoder in order to decode a received sequence, it is first partially processed with the PHR decoder and then with BM decoder. We call PHR-BM the resulting decoder of this combination.

4. Simulation results

To show the efficiency of the proposed scheme, we present in this section the simulation results of PHR-BM for some BCH codes and we compare its BER performances with some concurrent decoders. We note that we use a PBSK(Binary Phase Shift Keying) modulation over an AWGN (Additive white Gaussian noise) channel with a minimal residual errors equal to 200 and a minimum transmitted blocks equal to 1000.

If the transmission is carried out without coding on the transmitter side and without decoding on the receiver side, the BER reaches 10-5 at SNR (Signal-to-Noise Ratio) equal to 9.6 dB.

Figure1. presents the obtained performances of the proposed decoder for some BCH codes of length 127. From this figure, we deduce that the gain of coding is about 4.5 dB for the BCH(127,99,9) code, about 4.4 dB for the BCH(127,106,7) code and 3.9 dB for the BCH(127,113,5) code.

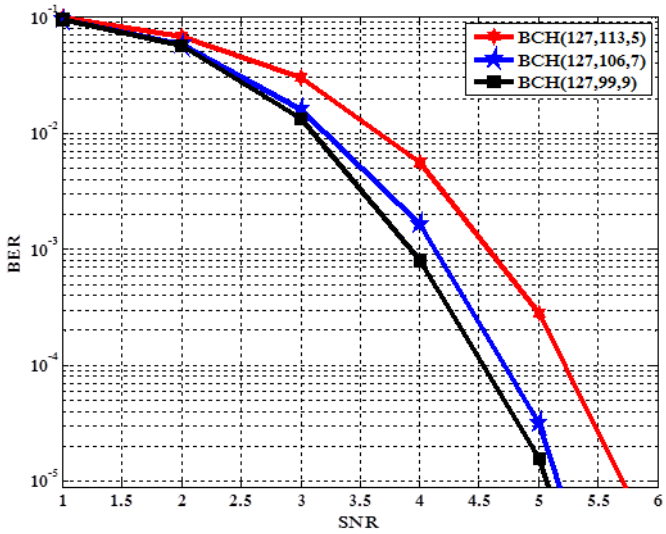

Figure 1.PHR-BM performances for some BCH codes of length 127

In Figure 2. we present the performances of PHR-BM for the BCH codes of length 63, this figure shows that the obtained gain of coding is about 4.8 dB for BCH(63,39,9) code, about 4.4 dB for BCH(63,45,7) code and about 4 dB for BCH(63,51,5) code.

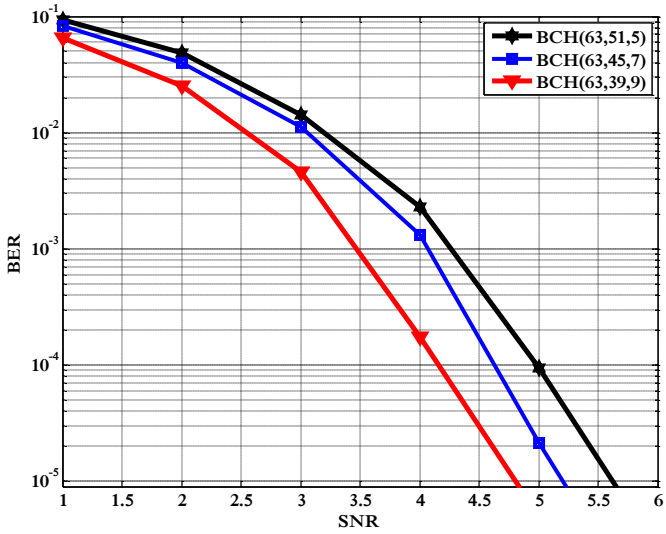

Figure 2. PHR-BM performances for some BCH codes of length 63

Figure 3. presents the PHR-BM performances of the BCH codes of length 31, this figure shows that the obtained gain of coding is about 4.1 dB for BCH(31,11,11) code, about 4 dB for BCH(31,16,7) and about 3.8 dB for BCH(31,21,5) code.

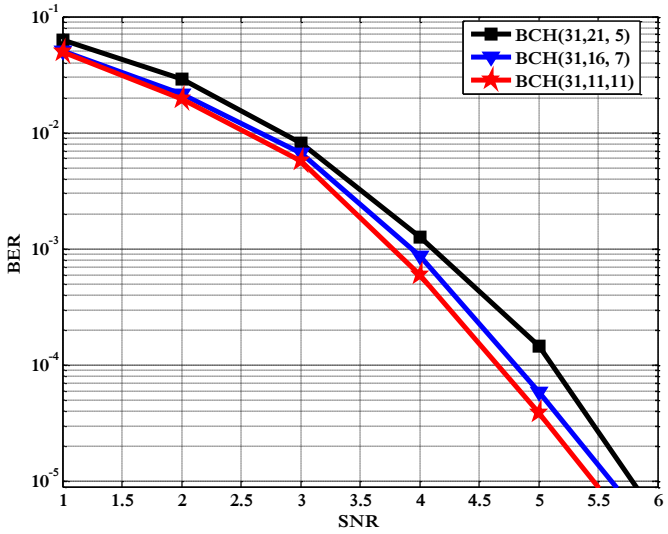

Figure 3. PHR-BM performances for some BCH codes of length 31

The previous figures show the high decoding quality of the proposed PHR-BM decoder. In the next figures we make comparison between our proposed decoder and some concurrent decoders.

Figure 4.shows the comparison of BER performances between PHR-BM and Berlekamp-Massey[23-24] decoders. The concatenation between the Hartmann Rudolph partially exploited and the Berlekamp-Massey decoder allows us to gain about 1.6 dB comparing to the use of the Berlekamp-Massey alone for the BCH(63,51,5) code. This result confirms the power of the proposed idea.

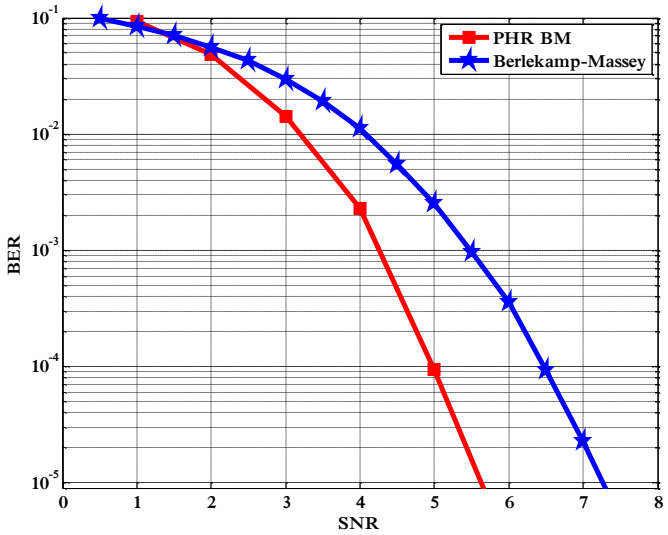

Figure 4. Comparison of BER performances of PHR-BM and Berlekamp-Massey decoders for BCH(63,51,5) code.

In Figure 5.we make a comparison of BER performances between the proposed PHR-BM, the Deep Neural Decoder (DND) [13] and the HSDec decoder[22]. From this figure we deduce that the BER performances of PHR-BM far exceed the HSDec and DND decoders.

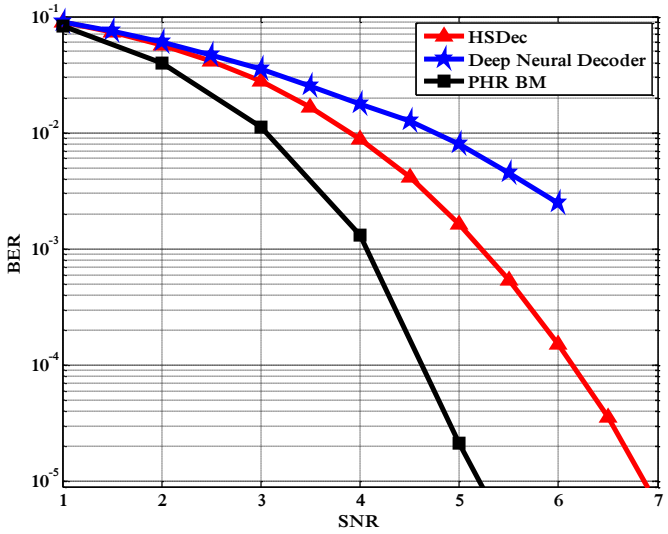

Figure 5. Comparison of BER performances of PHR-BM, HSDec and Deep Neural Decoder for BCH(63,45,7) code.

Figure 6.shows a comparison of BER performances between the proposed PHR-BM and another symbol by symbol and word by word decoder, S2W2DEC [26] that combine the Hartmann Rudolph partially exploited and the SPDA algorithm. This figure shows that PHR-BM passes remarkably the BER performances of the S2W2DEC for BCH(63,39,9) code.

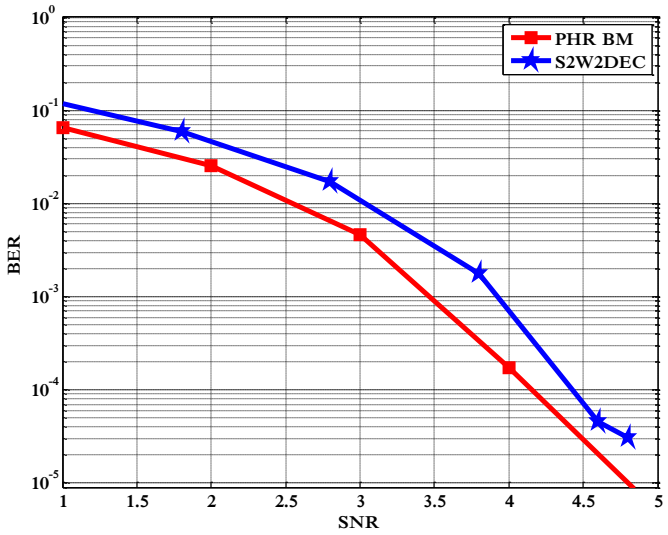

Figure 6.Comparison of BER performances of PHR-BM and S2W2Dec for BCH(63,39,9) code.

In the Figure 7.we present a comparison between HSDec [22], ARDecGA[21], BERT[6] and the proposed combination PHR-BM for the BCH(15,7,5) code. From this figure, we can deduce that our decoder PHR-BM passes remarkably the HSDec, ARDecGA and BERT decoders for this code.

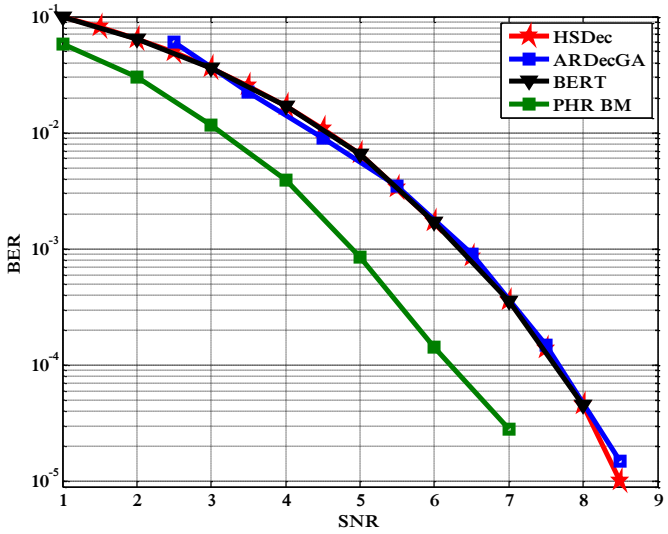

Figure 7. ComparisonComparison of BER performances of PHR-BM, HSDec, ARDecGA and BERT decoders for BCH(15,7,5) code.

5. Conclusion

In this paper we have presented an efficient approach based on a serial concatenation between the Hartmann Rudolph algorithm partially exploited and the Berlekamp-Massey algorithm in order to decode BCH codes. The simulation resultsshow that the proposed scheme gives very good BER performances compared to the seperate use of combined decoders. Moreover, the partial use of the HR decoder considerably reduces its temporal complexity which makes it usable even for small rate codes that are very useful for noisy communications. For example, we have used only 0.54% of the dual space sizefor the BCH code (63,39,9) while maintaining very good decoding quality.
In the perspectives, we will apply the proposed scheme to other error correcting codes and other decoders.

References

[1] Hebah H. O. Nasereddin, MOATH FAQIR, "The impact of internet of things on customer service: A preliminary study", Periodicals of Engineering and Natural Sciences, Vol 7, No 1 (2019)
[2] Enes Akca, "Development of Computer-Aided Industrial Design Technology", Periodicals of Engineering and Natural Sciences, Vol 5, No 2(2017)

[3] G. C. Clarck, J.B Cain, "Error-Correction Coding for Digital Communication", New York Plenum. 1981.
[4] Huang CF., Cheng WR., Yu C. "A Novel Approach to the Quadratic Residue Code". In: Pan JS., Tsai PW., Huang HC. (eds) Advances in Intelligent Information Hiding and Multimedia Signal Processing. Smart Innovation, Systems and Technologies, Vol. 64. Springer, Cham, 2017.
[5] Yani Zhang, Xiaomin Bao, Zhihua Yuan, Xusheng Wu. "Decoding of the Five-Error-Correcting Binary Quadratic Residue Codes". American Journal of Mathematical and Computer Modelling. Vol. 2, No. 1, 2017, pp. 6-12. doi: 10.11648/j.ajmcm.20170201.12, 2017.

[6] Elghayyaty Mohamed et al. "Performance Study of BCH Error Correcting Codes Using the Bit Error Rate Term BER". Int. Journal of Engineering Research and Application. ISSN : 2248-9622, Vol. 7, Issue 2, (Part - 2), pp.52-54, February, 2017.

[7] Raka, M., Kathuria, L. & Goyal, M., "(1−2u3)-constacyclic codes and quadratic residue codes over Fp[u]/<u4 – u>", Cryptogr. Commun. Vol. 9, Issue 4, pp 459–473. doi:10.1007/s12095-016-0184-7, 2017.

[8] Ding, H. Liu and V. Tonchev, "All binary linear codes that are invariant under PSL2(n) ", arXiv:1704.01199v1 [cs.IT] 4 Apr 2017.

[9] El idrissi, R. El gouri, A. Lichioui and H. Laamari, "Performance study and synthesis of new Error Correcting Codes RS, BCH and LDPC Using the Bit Error Rate (BER) and Field-Programmable Gate Array (FPGA)", International Journal of Computer Science and Network Security, Vol.16 No.5, May 2016.

[10] E. Nachmani, Y. Béery and D. Burshtein, "Learning to Decode Linear Codes Using Deep Learning", 2016 IEEE Fifty-fourth Annual Allerton Conference, September 27 - 30, 2016.

[11] Osman Gursoy, Md. Haidar Sharif, "Parallel Computing for Artificial Neural Network Training", Periodicals of Engineering and Natural Sciences, Vol 6, No 1(2018)

[12] M. Esmaeili, A. Alampour, and T. Gulliver, "Decoding Binary Linear Block Codes Using Local Search", 2013 IEEE Transactions On Communications, Vol. 61, No. 6, June 2013.

[13] T. Lin, H. Lee, H. Chang, T. Truong, "A cyclic weight algorithm of decoding the (47, 24, 11) quadratic residue code", Information Sciences, Vol.197, pp. 215–222, 2012.

[14] T. Lin, T. Truong, H. Lee and H. Chang, "Algebraic decoding of the (41, 21, 9) Quadratic Residue code", Information Sciences, Vol.179, pp.3451–3459, 2009.

[15] T. Lin, H. Lee, H. Chang, S. Chu and T. Truong, "High speed decoding of the binary (47, 24, 11) quadratic residue code", Information Sciences Vol. 180, pp.4060–4068, 2010.

[16] M. Jing, Y. Chang, J. Chen, Z. Chen and J. Chang, "A new decoder for binary quadratic residue code with irreducible generator polynomial", Circuits and Systems, APCCAS 2008. IEEE Asia Pacific Conference on, 2008.

[17] Y. Chen, C. Huang and J. Chang, "Decoding of binary quadratic residue codes with hash table", IET Commun., Vol. 10, Iss. 1, pp. 122–130, 2016

[18] Azouaoui, I. Chana and M. Belkasmi "Efficient Information Set Decoding Based on Genetic Algorithms", International Journal of Communications, Network and System Sciences, Vol.5 No.7, July 2012.

[19] R. G. Gallager, "Low-Density Parity-Check Codes", IRE Trans. Inf. Theory, vol. 8, no. 1, pp. 21–28, Jan. 1962.

[20] Robert H. Morelos-Zaragoza, "The Art of Error Correcting Coding", Second Edition, John Wiley & Sons, 2006

[21] S. Nouh, A. El khatabi and M. Belkasmi, "Majority voting procedure allowing soft decision decoding of linear block codes on binary channels". International Journal of Communications, Network and System Sciences, N° 9, Vol 5. 2012.

[22] El Kasmi Alaoui M.S., Nouh S., Marzak A. (2019) Two New Fast and Efficient Hard Decision Decoders Based on Hash Techniques for Real Time Communication Systems. In: Mizera-Pietraszko J., Pichappan P., Mohamed L. (eds) Lecture Notes in Real-Time Intelligent Systems. RTIS 2017. Advances in Intelligent Systems and Computing, vol 756. Springer, Cham.

[23] Berlekamp, E. R.: Algebraic Coding Theory. rev. ed., Aegean Park Press (1984).

[24] Massey, J. L.: Shift-register synthesis and BCH decoding. In IEEE 1969 Transaction on Information Theory IT-15 vol.1, 122–127 (1969)

[25] C. R. P. Hartmann and L. D. Rudolph, "An Optimum Symbol-by-Symbol Decoding Rule for Linear Codes," IEEE Transactions on Information Theory, Vol. 22, pp. 514-517, Sept. 1976.

[26] Said NOUH, Bouchaib AYLAJ. "Efficient Serial Concatenation Of Symbol By Symbol and Word by Word decoders". International Journal of Innovative Computing, Information and Control, volume 14, N°5 2018.