International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

A New Efficient Technique Based on Majority Logic Decoding to Decode Linear Block Codes

Issam Abderrahman Joundan, Moulay Seddiq El Kasmi Alaoui, Karim Rkizat, Said Nouh, Abdelwahed Namir

Abstract*: *One-Step Majority logic decoding (OSMLD) codes preset a very powerful error correcting schemes due to the simplicity of their decoder. However, families of these codes are limited to a few numbers. In this paper, we present a new adaptation which generalizes the majority-logic decoding for non OSMLD codes. This technique uses MIM method to select codewords from the dual of the code with last digit equal to one and then estimates the best threshold from which we obtain the best performance in term of the bit error rate (BER). The comparison between performances of the proposed technique and other coder/decoder schemes on AWGN (Additive White Gaussian Noise) channel proves its capacity in correcting more errors.

Keywords: ***Error correcting codes, HSDec, Hash table, MIM, syndrome decoding, QR code, BCH Code, OSMLD codes, Majority logic decoding;***

I. INTRODUCTION

The majority-logic decoding is an efficient decoder for decoding certain classes of cyclic codes due to its good performances with a very low complexity when used fortransmission over AWGN channels. The first majority-logic decoding algorithm was devised in 1954 by Reed [1] for a class of multiple-error-correcting codes discovered by Muller [2]. Reed's algorithm was later extended and generalized by many coding investigators. The first unified formulation of majority-logic decoding algorithms was due to Massey [3].

Consider an (n,k) cyclic code C with parity-check matrix H. The row space of H is an (n, n-k) cyclic code, denoted by $C^{\perp}$, which is the dual code of C, or the null space of C. For any vector v in C and any vector w in $C^{\perp}$, the inner product of v and w is zero, that is, $w \bullet v = w_0 v_0 + w_1 v_1 + \cdots + w_{n-1} v_{n-1} = 0$ (1.1). In fact, an n-tuple v is a code vector in C if and only if, for any vector w in $C^{\perp}$, $w \bullet v = 0$. The equality of (1.1) is called a parity-check equation. Clearly, there are 2^{n-k}such parity-check equations.

Now suppose that a code vector v in C is transmitted. Let $e = (e_0, e_1, \cdots, e_{n-1})$ and $r = (r_0, r_1, \cdots, r_{n-1})$ be the error vector and the received vector respectively. Then $r = v + e$ (1.2). For any vector w in the dual code $C^{\perp}$, we can form the following linear sum of the received digitscalled a parity-check sum or simply check sum: $A = w \bullet r = w_0 r_0 + w_1 r_1 + \cdots + w_{n-1} r_{n-1}$ (1.3). Combining(1.2) and (1.3)and using the fact that $w \bullet v = 0$, we obtain the following relationship between the check sum A and error digits in e : $A = w_0 e_0 + w_1 e_1 + \cdots + w_{n-1} e_{n-1}$ (1.4). An error digit e_l is said to be checked by the check sum A if the coefficient $w_l = 1$.

Suppose that there exist J vectors in the dual code $C^{\perp}$: $w_1 = (w_{1,0}, w_{1,1}, \cdots, w_{1,n-1})$, $w_2 = (w_{2,0}, w_{2,1}, \cdots, w_{2,n-1})$, ….., $w_J = (w_{J,0}, w_{J,1}, \cdots, w_{J,n-1})$. Which have the following properties:

The $(n-1)^{th}$ component of each vector is a "1", $w_{1,n-1} = w_{2,n-1} = \cdots = w_{J,n-1} = 1$.

For $i \neq n-1$, there is at most one vector whose i^{th} component is a "1";for example, if $w_{1,1} = 1$ then $w_{2,1} = w_{3,1} = \cdots = w_{J,1} = 0$.

Since $w_{1,n-1} = w_{2,n-1} = \cdots = w_{J,n-1} = 1$, these J check sums are related to the error digits in the following manner:

$$A_1 = w_{1,0} e_0 + w_{1,1} e_1 + \cdots + w_{1,n-2} e_{n-2} + e_{n-1}$$
$$A_2 = w_{2,0} e_0 + w_{2,1} e_1 + \cdots + w_{2,n-2} e_{n-2} + e_{n-1}$$
$$\vdots$$
$$A_J = w_{J,0} e_0 + w_{J,1} e_1 + \cdots + w_{J,n-2} e_{n-2} + e_{n-1}$$

These Jcheck sums are said to be orthogonal on the error digit e_{n-1}. Based on the facts above, an algorithm for decoding e_{n-1} can be formulated as follows:

The error digit $e_{n-1}$is decoded as 1 if a clear majority of the parity-check sums orthogonal on e_{n-1} is 1; otherwise, e_{n-1} is decoded as 0.

Correct decoding of $e_{n-1}$is guaranteed, if there is [J/2] or fewer errors in the error vector e. If it is possible to form J parity-check sums orthogonal on e_{n-1}, it is possible to form J parity-check sums orthogonal on any error digit because of the cyclic symmetry of the code.

Manuscript published on November 30, 2019.
*CorrespondenceAuthor
Issam Abderrahman JOUNDAN*, TIM Lab, Faculty of Sciences Ben M'sik, Hassan II University, Casablanca, Morocco Email: joundan.fsb@gmail.com
Moulay Seddiq EL KASMI ALAOUI,TIM Lab, Faculty of Sciences Ben M'sik, Hassan II University, Casablanca, Morocco Email: sadikkasmi@gmail.com
Karim Rkizat, ENSIAS, Mohammed V University in Rabat, Morocco Email: karim.rkizat@um5s.net.ma
Said NOUH, TIM Lab, Faculty of Sciences Ben M'sik, Hassan II University,Casablanca,Morocco Email: Said.nouh@univh2m.ma
Adelwahed NAMIR, TIM Lab, Faculty of Sciences Ben M'sik, Hassan II University,Casablanca, Morocco Email: a.namir@yahoo.fr

The decoding of other error digits is identical to the decoding of e_{n-1}. The decoding algorithm described above is called one-step majority-logic decoding.

Let d_{min} be the minimum distance of the code. Clearly, the one-step majority-logic decoding is effective for this code only if [J/2] is equal to or close to the error-correcting capability of the code; in other words, J should be equal to or close to dmin-1,we say that the code is completely orthogonalisable.However, families of cyclic codes having this property are limited to a few numbers [4] and some constructionof OSMLD codes which are Quasi-Cyclic are presented in [5].

The remainder of this paper is structured as follows. In section 2 we present some decoding algorithms as related works. In section 3 we present the proposed technique, in the section 4, we present the simulation of results of the proposed decoders and we make a comparison with other decoders. Finally, a conclusion and a possible future direction of this research are outlined in section 5.

II. RELATED WORKS

The quadratic residue (QR) codes were first defined in 1964 by Andrew Gleason who demonstrated many of their important properties in a brief letter.Quadratic Residue codes are a powerful cyclic codes, contain the famous Hamming and Golay codes, they offer also the best known minimum distance codes for lengths 191, 199 and 223.Unfortunately, there is no known specific decoder for this family of codes. The Bose, Chaudhuri, and Hocquenghem (BCH) codes form a large class of powerful random error-correcting cyclic codes. This class of codes is a remarkable generalization of the Hamming codes for multiple-error correction. Binary BCH codes were discovered by Hocquenghem in 1959 and independently by Bose and Chaudhuri in 1960. The cyclic structure of these codes was proved by Peterson in 1960. The well known specific decoder for this family of codes is the Berlekamp-Massey (BM) decoder.

In [6], an approach based on the link between syndromes and correctable errors pattern is developed by using hash techniques. In [7], the authors have presented a method called NESWDA to decode up to five errors in a binary systematic quadratic residue QR(47,24,11) code, this method is based on the weight of syndrome difference and proprieties of cyclic codes. The disadvantage of these two methods is that it's just applicable for Quadratic Residue code.

In [8], a deep learning method to improve belief propagation algorithm was proposed, by attribution of weights to the edges of the Tanner graph the authors generalized the standard belief propagation algorithm.

In [9], the authors have developed a Cyclic Weight (CW) algorithm decoding to decode the binary systematic QR(47,24,11) code. In addition to the properties of the cyclic codes, they based on the weights of syndromes; the same authors and in a previous paper [10] they have presented an algebraic decoding algorithm to correct all patterns of four or fewer errors in the binary QR (41, 21, 9) code. In order to decode up to five possible errors in a binary systematic QR(47,24,11) code, the authors of [11] have presented a table lookup decoding algorithm.

By using the Lagrange interpolation formula, the authors of [12] have calculated the needed primary unknown syndrome for the binary QR code and proposed hardware architecture to implement it, also by using the developed Berlekamp-Massey (BM) algorithm and Chien search they decoded the binary QR code. In [13] the authors have proposed a decoding of quadratic residue codes by using hashing search to determine error patterns.

In [14, 15] several hard decoder based on genetic algorithms (GA) are developed, the first one is the HDGA (Hard decision Decoder based on Genetic Algorithms) [14], it used information sets to decode linear block codes. In [15], an efficient decoder called ARDecGA (Artificial reliabilities based decoding algorithm) is presented. It uses a generalized parity check matrix to compute a vector of artificial reliabilities of the binary received word h and it exploited a genetic algorithm to find the maximum likelihood binary word to this vector. The algebraic hard decision decoder [16, 17] of Berlekamp-Massey is based on compute of syndromes and it has an efficient mechanism to localize all corrigible errors, it is applicable on BCH codes. Another version of this last decoder is adapted for Quadratic residue codes [18].

Recently, several decoders based on hash techniques have been developed[19, 20, 21]; for example in[19], the authors have developed two hard decoders HSDec and HWDec applicable to linear block codes and based on syndrome and hash techniques.

III. THE PROPOSED DECODER

The proposed technique GOSMLD works as follows:

Inputs: - A generator matrix G of the linear code C (n, k).
Step 1: by using the MIM Method, Find a list of vectors $w_i = (w_{i,0}, w_{i,1}, \cdots, w_{i,n-1})$ from the dual code $C^{\perp}$ with $w_{i,n-1} = 1$.
Step 2: Estimate the best threshold from which, we obtain the best performance in term of the bit error rate (BER).

IV. SIMULATION RESULTS AND COMPARISON

To show the efficiency of the proposed technique, we give in this section its error correcting performances for some non OSMLD cyclic codes. A comparison with other decoding algorithms over the Additive White Gaussian Noise (AWGN) channelwith a BPSK (Binary Phase Shift Keying) modulation is done. All simulations are obtained by using the parameters given in Table 1. The error correcting performances will be represented in terms of Bit Error Rate (BER) in each Signal to Noise Ratio (SNR=Eb/N0).

TABLE I. DEFAULT SIMULATION PARAMETERS.

Simulation parameters	Value
Channel	AWGN
Modulation	BPSK
Minimum number of residual bit in errors	200
Minimum number of transmitted blocks	1000

In order to show the efficiency of the proposed decoders we made several simulations for plotting their error correcting performances for many QR codes and BCH codes. The figure 1represents the performances of the GOSMLD for some QR codes of length up to 73. Knowing that if the data are transmitted without coding in the sending step and without correction in the receiving step over AWGN channel then the BER reaches the value 10^{-5} at the SNR=9.6 therefore the proposed scheme permits to obtain a gain of coding about 2.2 dB for QR(23,12,7), 2 dB for QR(31,16,7),3dB for QR(47,24,11), 2.8dB for QR(71,36,11)and about 2.9dB for QR(73,37,13). The figures 2 and 3 represent the performances of the GOSMLD for some BCH codes of lengths31 and 63 respectively. These figures show that our scheme permits to obtain a gain of coding go to 2.1dB for length 31 and go to 2.8dB for length 63.

In order to study the impact of the threshold at the Bit Error Rate (BER), a number of simulations are done. The figure 4 summarizes the obtained results for the same number M of codewords of the dual code find by the MIM Method [22]. The obtained results show that the value of the threshold has a great impact on Bit Error Rate. The best value of the threshold for QR(31,16,7) is 0.57. That is, if the sum of parity-check sum exceeds 68 then flips the last digit. For the other digit, view the cyclic structure of the code, we use the same way on the shift vector.

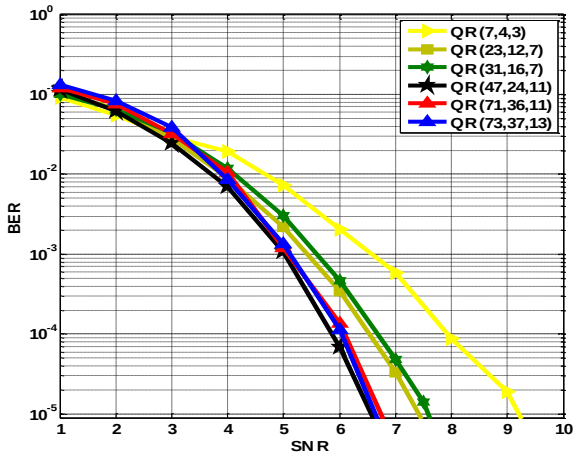

Fig. 1.Performances of GOSMLD for some QR codes of length up to 73.

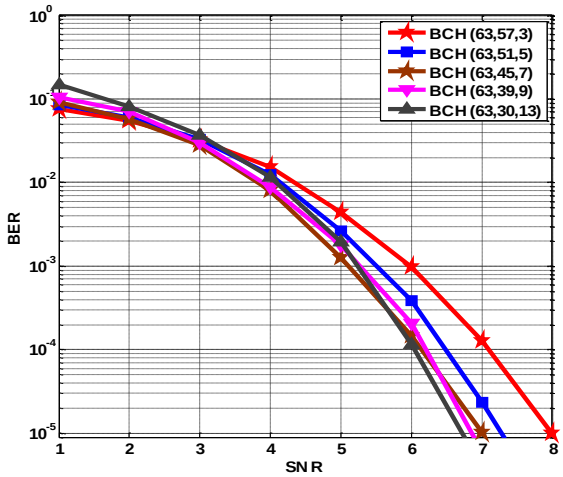

Fig. 2.Performances of GOSMLD for some BCH codes of length 63.

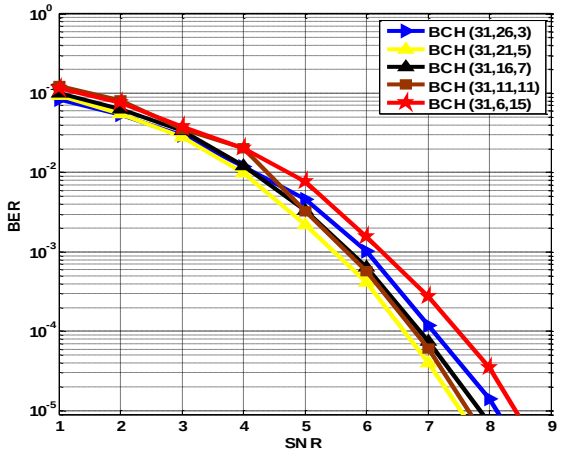

Fig. 3.Performances of GOSMLD for some BCH codes of length 31.

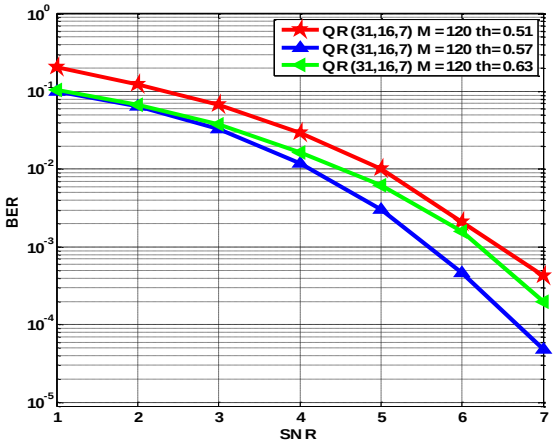

Fig. 4.Impact of the threshold at the BER for QR(31,16,7).

The figures5, 6, 7, and 8, represent a comparison of the performance of GOSMLD and HSDec for some QR code of length up to 47. The obtained results prove that our technique passes relatively the performances of HSDec decoder.

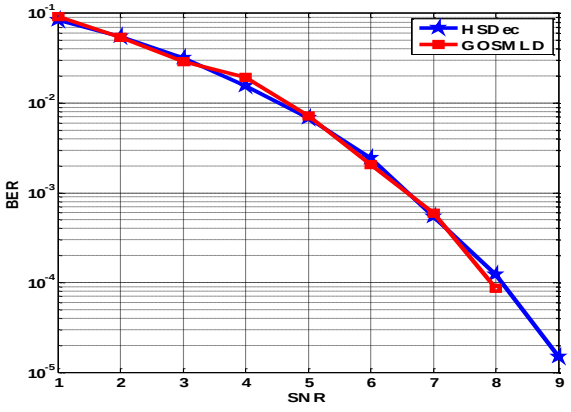

Fig. 5.Comparison of the performances of GOSMLD and HSDec for QR(7,4,3) code.

Retrieval Number: D9425118419/2019©BEIESP
DOI:10.35940/ijrte.D9425.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

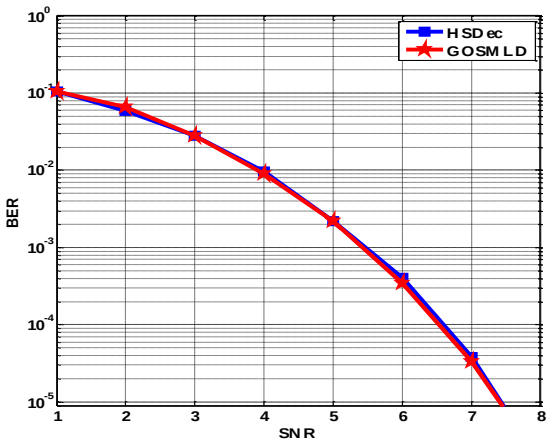

Fig. 6.Comparison of the performances of GOSMLD and HSDec for QR(23,12,7) code.

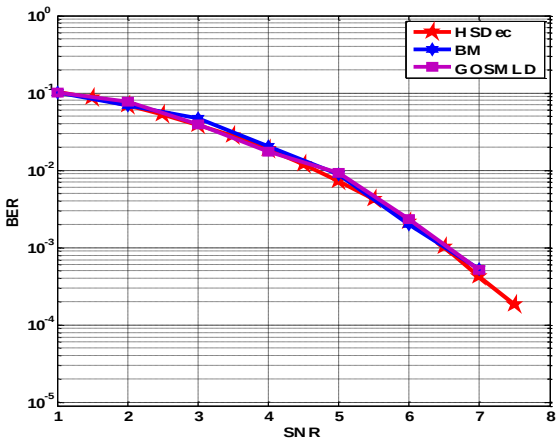

Fig. 9.Comparison of the proposed GOSMLD, HSDec and BM for BCH(15,5,7).

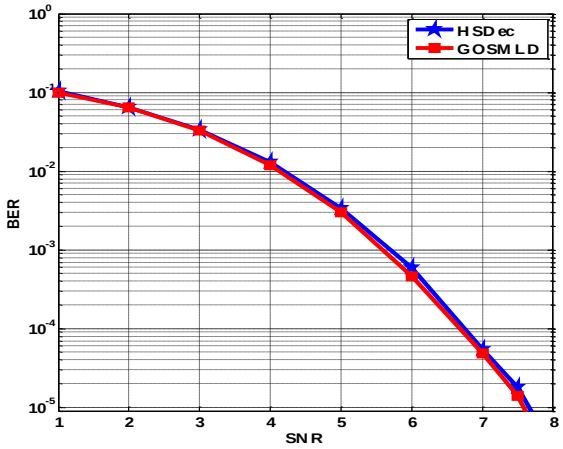

Fig. 7.Comparison of the performances of GOSMLD and HSDec for QR(31,16,7) code.

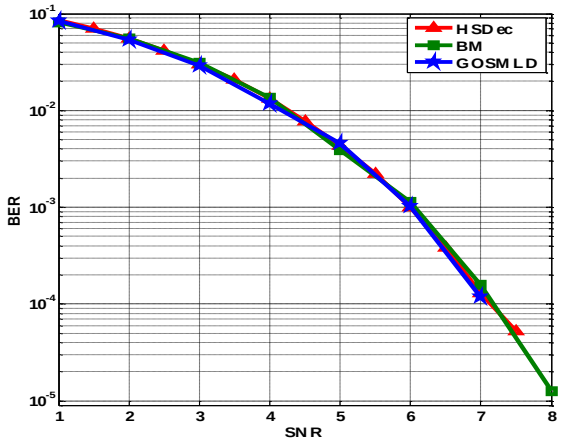

Fig. 10. Comparison of the proposed GOSMLD, HSDec and BM for BCH(31,26,3).

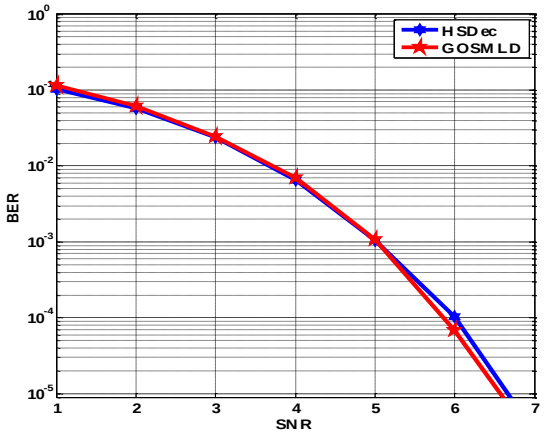

Fig. 8.Comparison of the performances of GOSMLD and HSDec for QR(47,24,11) code.

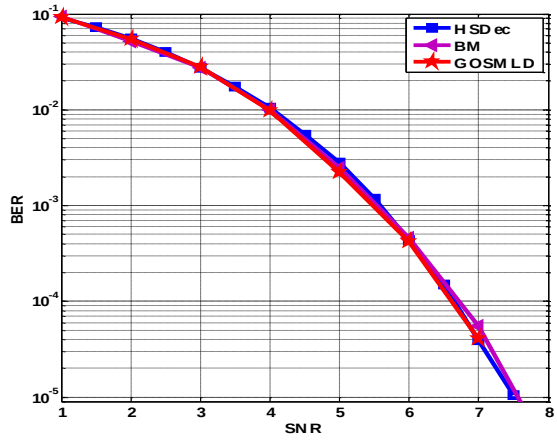

Fig. 11. Comparison of the proposed GOSMLD, HSDec and BM for BCH(31,21,5).

The figures9, 10, 11, 12, 13, 14, 15 and 16 represent a comparison of the performance of GOSMLD, HSDec and BM for some BCH codes. The obtained results prove that our technique reach the same performance of these decoders.

Retrieval Number: D9425118419/2019©BEIESP
DOI:10.35940/ijrte.D9425.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

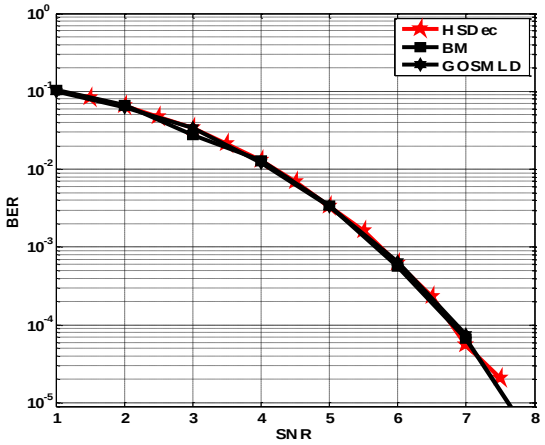

Fig. 12. Comparison of the proposed GOSMLD, HSDec and BM for BCH(31,16,7).

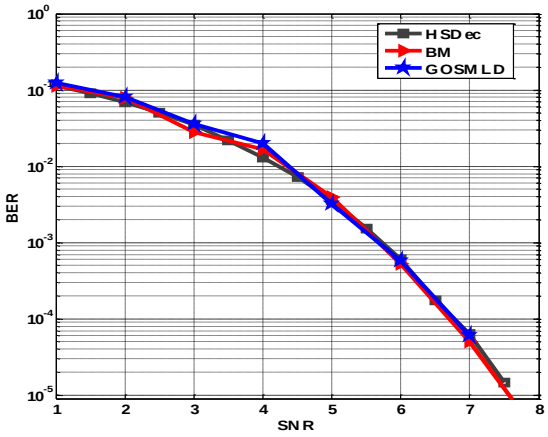

Fig. 13. Comparison of the proposed GOSMLD, HSDec and BM for BCH(31,11,11).

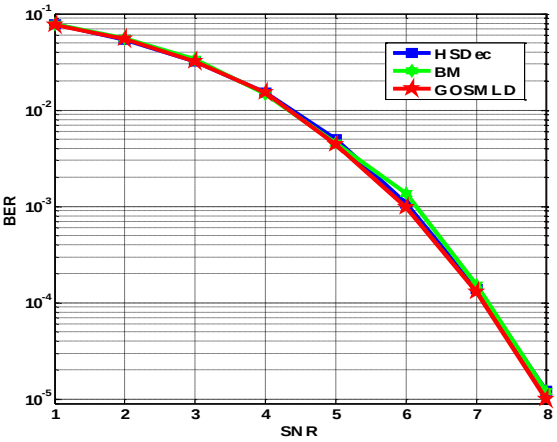

Fig. 14. Comparison of the proposed GOSMLD, HSDec and BM for BCH(63,57,3).

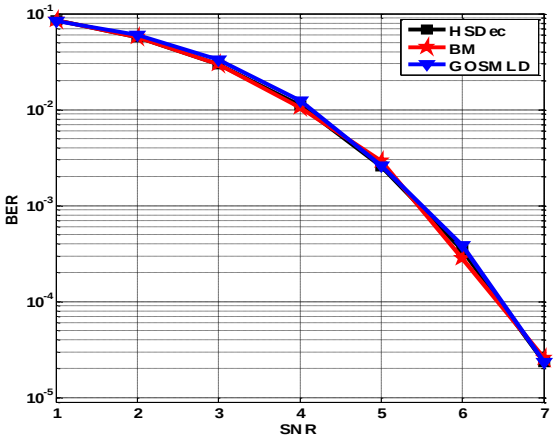

Fig. 15. Comparison of the proposed GOSMLD, HSDec and BM for BCH(63,51,5).

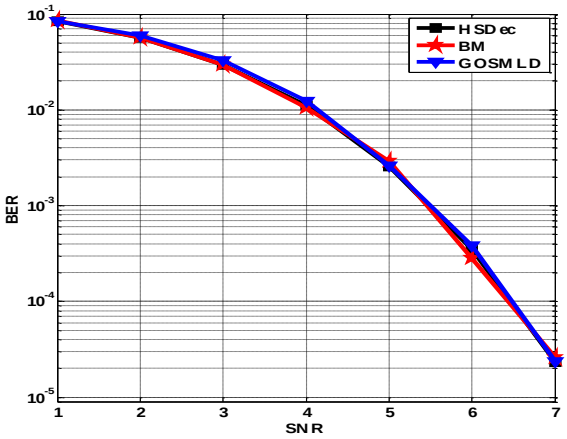

Fig. 16. Comparison of the proposed GOSMLD, HSDec and BM for BCH(127,113,5).

The figure 17, represent a comparison of the performance of GOSMLD, HSDec, ARDecGA and BM for BCH(15,7,5). The obtained results prove that our technique passes relatively the performance of these decoders.

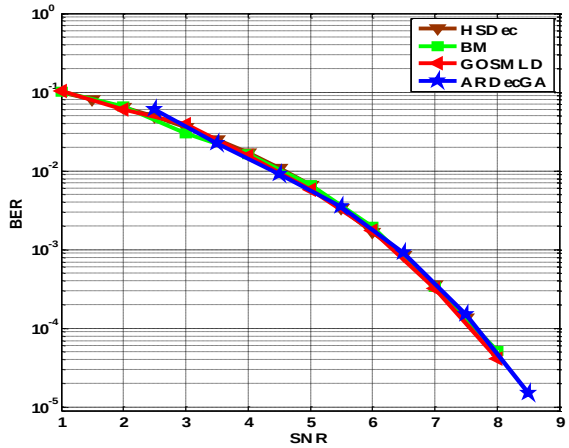

Fig. 17. Comparison of the proposed GOSMLD, HSDec, ARDecGA and BM for BCH(15,7,5).

The figure 18, represent a comparison of the performance of GOSMLD and DND, HDGA, and BM for BCH(63,45,7). The obtained results prove that our technique greatly exceeds HDGA, DND and have relatively the same performance as BM for this code.

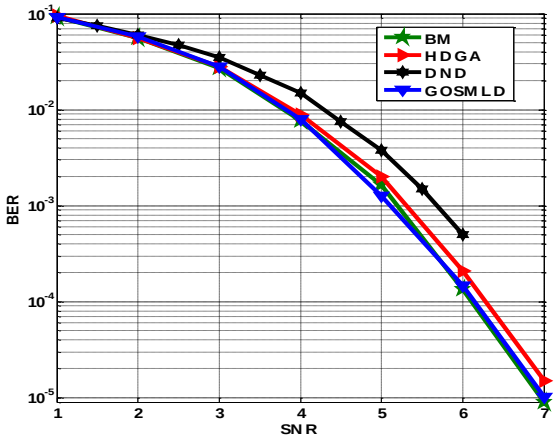

Fig. 18. Comparison of the proposed GOSMLD, DND, HDGA, and BM for BCH(63,45,7)

The figure 19, represent a comparison of the performance of GOSMLD, HDGA and BM for BCH(63,30,13). The obtained results prove that our method greatly exceeds HDGA and BM for this code.

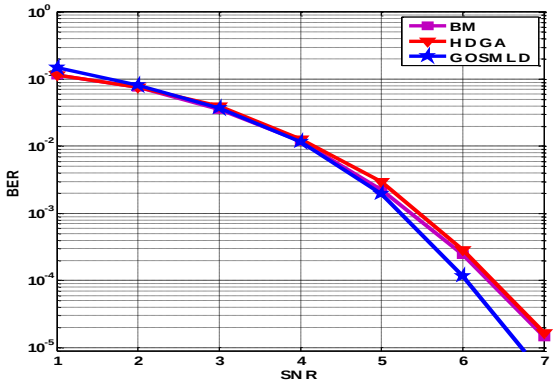

Fig. 19. Comparison of the proposed GOSMLD and HDGA, BM for BCH(63,30,13)

V. CONCLUSION AND PERSPECTIVES

In this paper, we have presented a new efficient hard decision decoding algorithm which generalizes the one step majority-logic decoding for non OSMLD codes.This technique uses a codeword from the dual of the code with last digit equal à one found by MIM method and then estimates the best threshold from which we obtain the best performance in term of the bit error rate (BER). The comparison between performances of the proposed technique and other coder/decoder schemes on AWGN (Additive White Gaussian Noise) channel proves its capacity in correcting more errors.The success of this technique will encourage us to continue to generalize it for other families of error correcting codes.

REFERENCES

1. .S. Reed, “A Class of Multiple-Error-Correcting Codes and the Decoding Scheme,” IRE Trans., IT-4, PP. 38-49, Septembre 1954.
2. D.E. Muller, “Applications of Boolean Algebra to Switching Circuit Design and to Error Detection,” IRE Trans., EEC-3, pp. 6-12, Septemre 1954.
3. J. L. Massey, Threshold Decoding, MIT Press, Cambridge, Mass. 1963.
4. S. Lin and D.J. Costello, ”Error Control Coding: Fundamentals and Applications”, Prentice-Hall, Englewood Cliffs, NJ, 1983.
5. Karim Rkizat , Mohammed Lahmer , Mostafa Belkasmi and Said Nouh “Construction and Iterative Threshold Decoding for Low Rates Quasi-Cyclic One Step Majority LogicDecodable Codes”,International Conference on Advanced Communication Systems and Information Security (ACOSIS),17-19 Oct. 2016, Marrakesh, Morocco.
6. Huang, C.F., Cheng, W.R., 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).
7. Yani, Z., Xiaomin, B., Zhihua, Y., Xusheng, W.: Decoding of the Five-Error-Correcting Binary Quadratic Residue Codes.American Journal of Mathematical and Computer Modeling 2(1), 6-12 (2017).
8. Nachmani, E., Béery, Y., Burshtein,D.: Learning to Decode Linear Codes Using Deep Learning. In: IEEE2016 Fifty-fourth Annual Allerton Conference (2016).
9. Lin, T., Lee H., Chang H., Truong T.: A cyclic weight algorithm of decoding the (47, 24, 11) quadratic residue code. Information Sciences 197, 215–222(2012).
10. Lin, T., Truong,T., Lee, H., Chang, H.: Algebraic decoding of the (41, 21, 9) Quadratic Residue code. Information Sciences 179, 3451–3459(2009).
11. Lin, T., Lee H., Chang H., Chu, S., Truong, T.: High speed decoding of the binary (47, 24, 11) quadratic residue code. Information Sciences 180,4060–4068 (2010).
12. Jing, M., Chang, Y., Chen, J., Chen, Z., Chang,J.: A new decoder for binary quadratic residue code with irreducible generator polynomial. In IEEE 2008 Asia Pacific Conference onCircuits and Systems APCCAS (2008).
13. Chen,Y., Huang, C., Chang,J.: Decoding of binary quadratic residue codes with hash table. IET Common. 10(1), 122–130 (2016).
14. Azouaoui, A., Chana, I., Belkasmi, M.: Efficient Information Set Decoding Based on Genetic Algorithms. International Journal of Communications Network and System Sciences 5(7) (2012).
15. Nouh, S., El khatabi, A., Belkasmi,M.: Majority voting procedure allowing soft decision decoding of linear block codes on binary channels. International Journal of Communications, Network and System Sciences 5(9) (2012).
16. Berlekamp, E. R.: Algebraic Coding Theory. rev. ed., Aegean Park Press (1984).
17. Massey, J. L.: Shift-register synthesis and BCH decoding. In IEEE 1969 Transaction on Information Theory IT-15 vol.1, 122–127 (1969).
18. Chen, Y.H., Truong,T.K., Chang,Y., Lee,C.D., Chen, S.H.: Algebraic decoding of quadratic residue codes using Berlekamp-Massey algorithm. Journal of Information Science and Engineering 23(1), 127–145 (2007).
19. S. EL KASMI ALAOUI, S. NOUH, A. MARZAK, "Two new fast and efficient hard decision decoders based on Hash techniques for real time communication systems". 2nd International conference on Real Time Intelligent Systems (RTIS 2017) 18-20 October 2017, University Hassan II, Casablanca.
20. S. EL KASMI ALAOUI, S. NOUH, A. MARZAK, "A low complexity soft decision decoder for linear block codes", the 1st International Conference on Intelligent Computing in Data Sciences (ICDS 2017) 18-19 December 2017, EST Meknes.
21. El Kasmi Alaoui M.S., Nouh S., Marzak A.: High Speed Soft Decision Decoding of Linear Codes Based on Hash and Syndrome Decoding. International Journal of Intelligent Engineering and Systems, Vol.12, No.1 (2019).
22. Askali M., Azouaoui A., Nouh S., Belkasmi M. (2012) On the Computing of the Minimum Distance of Linear Block Codes by Heuristic Methods, International Journal of Communications, Network and System Sciences, 5(11), 774-784.

AUTHORS PROFILE

IssamAbderrahman JOUNDAN received his Master in networks and telecommunications in 2011 from University of ChouaibDoukkali, El Jadida, Morocco. Currently he is doing his PhD in Computer Science at TIM Lab, Faculty of sciences Ben M'Sik, Hassan II university, Casablanca, Morocco. His areas of interest are Information and Coding Theory.

Karim Rkizat, received his Master in omputer networks telecommunications and multimedia in 2011 from ENSIAS, Mohammed V UniversityRabat, Morocco. Currently he is doing his PhD in Computer Science at ICES teamENSIAS, Mohammed V UniversityRabat, Morocco. His areas of interest are Information and Coding Theory.

MoulaySeddiq EL KASMI ALAOUI received his Master in Networks and Systems in 2010 from Hassan I University, Faculty of Sciences and Technology Settat, Morocco. Currently he is doing his PhD in Computer Science at TIM Lab, Faculty of Sciences Ben M'Sik, Hassan II University, Casablanca, Morocco.

Said NOUH is Professor at Faculty of sciences Ben M'Sik, Hassan II university, Casablanca, Morocco. He had PhD in computer sciences at ENSIAS (National School of Computer Science and Systems Analysis), Rabat, Morocco in 2014. His current research interests telecommunications, Information and Coding Theory.

Abdelwahed NAMIR is a Professor at Faculty of Sciences Ben M'Sik, Hassan II University of Casablanca, Morocco. He obtained his Doctoral Thesis of State in Digital Methods of the Engineer at EMI (school Engineer's Mohammedia) of Rabat in 1993. His current research interests: Decision-making mathematics, decision-making computing,Telecommunication.