Journal of Theoretical and Applied Information Technology
15th September 2022. Vol.100. No 17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# HIGH SPEED DECODING BY COLLABORATION BETWEEN THE HARTMANN RUDOLPH AND INFORMATION SET DECODING ALGORITHMS

**HAMZA FAHAM[1], MY SEDDIQ EL KASMI ALAOUI[2], SAÏD NOUH[3], MOHAMED AZZOUAZI[4], ISSAM ABDERRAHMANE JOUNDAN[5]**

[1,3,4,5]LTIM Lab, Ben M'sick Sciences Faculty, Hassan II University of Casablanca, Morocco

[2]LIS Lab, Aïn Chock Sciences Faculty, Hassan II University of Casablanca, Morocco

E-mail: [1]faham.hamza@gmail.com, [2]sadikkasmi@gmail.com, [3]nouh_ensias@yahoo.fr, [4]azouazii@gmail.com, [5]joundan.fsb@gmail.com

**ABSTRACT**

Decoders are implemented to retrieve data after its transmission over a noisy communication channel. Soft decision decoders are highly efficient in concatenation schemes exploiting more than one decoding level. In our case, we concatenated the symbol-by-symbol Hartmann Rudolph (HR) decoding algorithm and the Information Set Decoding (ISD) technique that is a word-to-word decoding. In this work, we will suggest to concatenate HR partially exploited (PHR) and the ISD technique in order to decode linear block codes. We will use firstly the HR decoder with a reduced number of dual codewords then the ISD, which uses the output of PHR. We noticed that the suggested serial concatenation guarantees very high performances with less dual codewords number. For instance for the QR(31, 16, 7) code, the satisfying obtained results are based only on 2,74% of the dual codewords. For the same code, we have minimized the runtime by 95% compared to the use of HR alone. This proves the power and the speed of the suggested concatenation.

**Keywords:** *Information Theory, Error Correcting Codes, Hartmann Rudolph (HR), Information Set Decoding, PHR*

## 1.INTRODUCTION

The information theory has introduced the essential components of any digital communication system, in which information is produced by a discrete source of information. In this model, the transmitter envisages a communication with the receiver via a transmission medium. This modeling is schematized through Figure1.

By analyzing this model, we can distinguish the following parts: source encoder/decoder, channel encoder/decoder, modulator/demodulator and the transmission medium. In this work, we are interested by the channel encoder/decoder part.

In fact, a significant interest for standards organizations that conceive protocols for cellular networks is error checking so that authentic reproduction of information is performed. Consequently, error-correcting codes have been introduced. These codes join redundant bits to the transmitted message to conserve the useful information. Error correcting codes are used in many equipment like smartphones, CDs, DVDs, hard disks or packets transmitted over the Internet and cellular telephony.

Error detection and correction works are various, such as decoding algorithms [1] and the linear codes weights enumeration [2].

Concerning the decoders used in telecommunications, we distinguish between two types: soft and hard decision decoders. Soft decision decoders use directly entering symbols and exploit mainly the Euclidian distance as a metric to reduce the distance. While hard decision decoders handle binary inputs resulting from thresholding communication channel output. These decoders use in general Hamming distance as a measure.

In order to judge the efficiency of a given decoder and its ability to be deployed in a reliable telecommunication system, we must determine its BER (Bit Error Rate) results in terms of SNR (Signal-to-Noise Ratio) values.

In this work, we will introduce a decoder generated by means of a serial concatenation between HR decoding algorithm and Information Set

Decoding technique to decode linear block codes. Moreover, we will present the BER results of our proposed decoder and we will give some comparisons with competitors. The rest of this paper is organized in this way: In the second section, we will show different decoders as related works. In the third section, we will introduce the suggested serial concatenation between PHR and ISD. In the fourth section, we will expose experiments and results of our suggested decoding algorithm and we will show some comparisons. Finally, a conclusion is given in the fifth section.

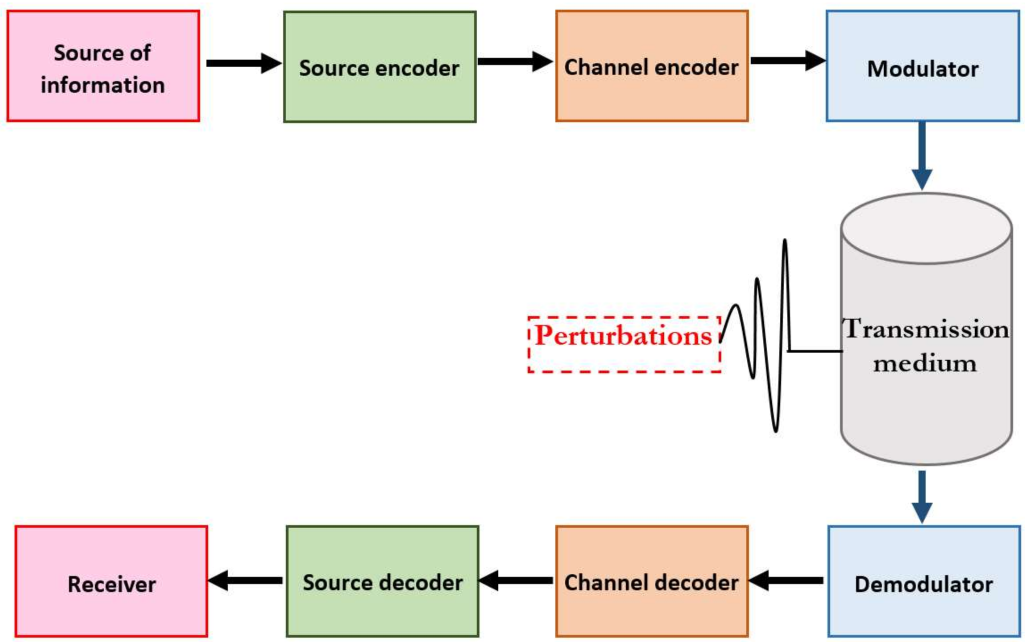


*Figure 1: Basic Modeling Of A Digital Communication System*

## 2. RELATED WORKS

In [3], the original Ordered-Statistics Decoding (OSD) [4] was modified by considering disjoint segments of the Most Reliable Independent Positions (MRIPs). In [5] a non-iterative soft decision BCH decoding algorithm is presented. In [6] the authors have presented an improved soft BCH decoding algorithm. In [7] a modification to the MacWilliams's Permutation Decoding Algorithm (PDA) is performed. The authors of [8] have suggested an iterative decoder at the base of a soft PDA. In [9] two dual domain soft decoding algorithms based on a compact genetic algorithm with larger tournament size are proposed. In [10], the authors have presented a soft-decision decoding algorithm at the base of syndrome decoding and hash techniques. They have also presented in [11] two fast decoders called HSDec and HWDec and the Chase-HSDec decoder in [12]. The well-known Hartmann-Rudolph decoder (HR) [13] is a soft-decision decoding algorithm that employs a symbol-by-symbol decoder. The author of [14] has considered a class of decoding algorithms for error-correcting code spaces. He has examined an operationally simple algorithm of this kind for cyclic code spaces.

The Berlekamp-Massey (BM) algebraic hard decoder [15, 16] exploits computing of syndromes to decode BCH codes. Another version of the BM algorithm was designed for QR codes by authors of [17]. In [18] the originators have investigated the Lagrange interpolation formula, the well-developed BM algorithm and Chien search to decode up QR codes. In [19] the authors have introduced a functional decoding of quadratic residue codes exploiting hashing search to determine error patterns.

In [20, 21] Recurrent Neural Network (RNN) architecture is introduced to decode linear block codes. Authors of [22] have presented an original two extra column trellis min-max decoder. They have also introduced in [23] a forward-backward four-way merger min-max algorithm in addition to a decoding architecture for NB-LDPC codes. Originators of [24] have presented a hybrid decoder for Reed–Muller codes. The authors of [25] have presented an algorithm which enables to decode a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

BCH code $C_n$ of length $n$, by means of decoding a cyclic code $C_{(n+1)n}$ of length $(n + 1)n$. In [26] the authors have introduced an improved Courtois-Finiasz-Sendrier (CFS) algorithm through code based hash function. The originators of [27] have presented two powerful algorithms named the direct method and the lookup table decoding in order to decode systematic quadratic residue codes.

## 3.THE SUGGESTED SERIAL CONCATENATION

### 3.1. HR decoding algorithm

HR is a symbol-by-symbol decoding algorithm at the base of a probabilistic study. HR uses the whole $2^{n-k}$ dual codewords. It has an extremely raised complexity because of using this huge number of dual codewords. Formula (1) presents the HR approach [13] to determine if the mth bit of the decoded word c' is equal to 1 or 0 from the received sequence r.

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

Where $\delta_{ij} = \begin{cases} 1 \; if \; i = j \\ 0 \; otherwise \end{cases} \; and \; \phi_m = \frac{\Pr(r_m|1)}{\Pr(r_m|0)}$

The bit $c_{jl}^{\perp}$ is the $l^{th}$ bit of the $j^{th}$ codeword of the code $C^{\perp}$

### 3.2. Information Set Decoding

In a C(n, k) error correction code, we define an information set [28, 29] as a set of k symbols of a codeword that are independently identified. The other (n-k) symbols represent redundant parity-check part. Therefore, if we can get an error-free information set, in order that the totality of the wrong bits are parity check ones, then it is possible to decode easily the transmitted vector. We represent an information set via an n-dimensional vector that contains k bits equal to 1 and remaining bits are equal to 0.

### 3.3. The proposed concatenation principle

In their algorithm, Hartmann and Rudolph have suggested to use all the dual codewords. The authors of [30] have proposed to exploit just M dual codewords. Consequently, the Hartmann and Rudolph algorithm is applied just on few symbols of the received sequence. Then Hartmann and Rudolph algorithm is named partial HR (PHR). Formula (1) becomes (2).

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

When the formula (2) is employed, the temporal complexity of HR decoder changes from $O(n^2 2^{n-k})$ to $O(n^2 M)$ which makes it suitable even for codes whose parity bit number is very high. Minimizing the number of the employed dual codewords affects remarkably the decoding efficiency. Wherefore, we suggest reprocessing the sequence resulted from the PHR decoder using the ISD decoding (word-by-word decoding).

## 4.EXPERIMENTS AND RESULTS

In order to prove our suggested scheme power and speed, we show our decoder simulation results concerning certain BCH and Quadratic Residue codes and we compare these results to some other decoders. Table 1 summarizes the simulation parameters used.

*Table 1: Simulation Parameters*

| Simulation parameter | Value |
|---|---|
| Communication channel | AWGN |
| Digital modulation scheme | BPSK |
| Minimum residual errors | 200 |
| Minimum transferred blocks | 1000 |

We represent error correction performances by plotting the Bit Error Rate (BER) in terms of Signal to Noise Ratio (SNR). Knowing that when communication is carried out without encoding and decoding steps, the bit error rate achieves $10^{-5}$ for signal to noise ratio equal to 9.6 decibels (dB).

Figure 2 presents the simulation results of our decoder for three BCH codes of length 63. This figure indicates a coding gain about 4,6 decibels for BCH(63, 39, 9) code.

Figure 3 presents our decoder performances for QR codes of length from 23 to 79. This figure shows that QR (47, 24, 11) code realized a coding gain about 4,6 decibels.

Journal of Theoretical and Applied Information Technology
15th September 2022. Vol.100. No 17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

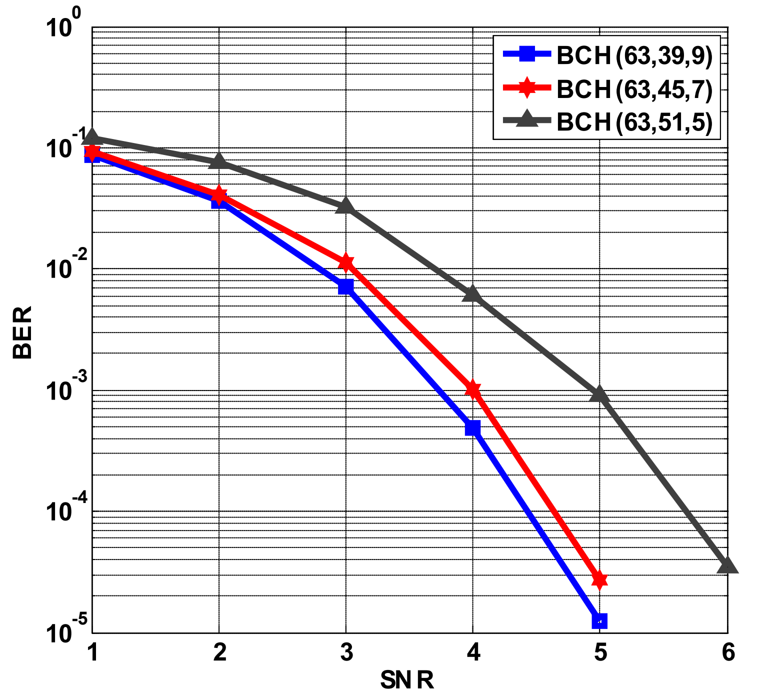


*Figure 2: Our decoder performances for three BCH codes of length 63*

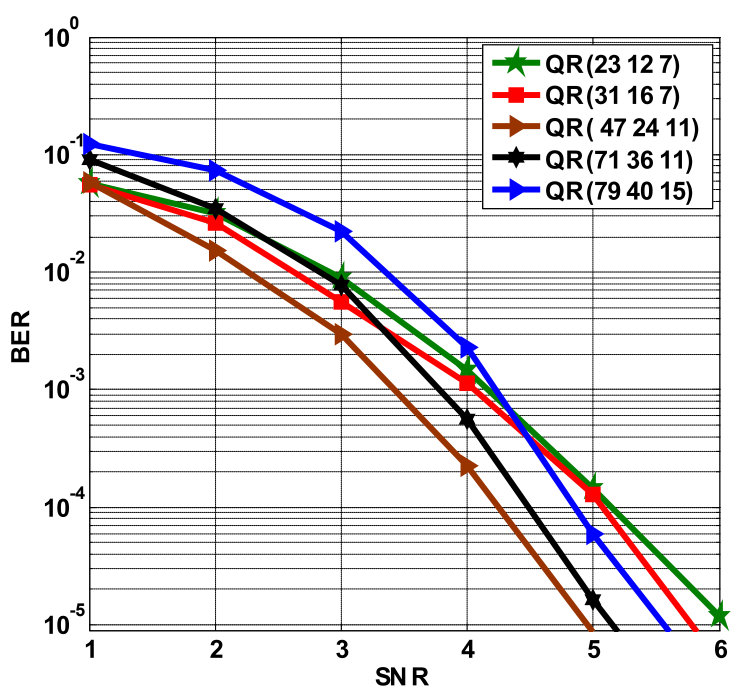


*Figure 3: Our Decoder Performances For QR Codes Of Length From 23 To 79*

Fig.4 compares the decoding results of PHR-ISD and Chase-HSDec [12] for QR (31, 16, 7) and QR (47, 24, 11) codes. We deduce that the two decoding algorithms have almost identical performances for QR (31, 16, 7), but PHR-ISD exceeds Chase-HSDec for QR (47, 24, 11).

Journal of Theoretical and Applied Information Technology
15th September 2022. Vol.100. No 17


ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In Figure 5, we compare decoding results of PHR-ISD, PHR-SPDA[30] and Chase-HSDec decoding algorithms for BCH(63, 39, 9). We conclude that our proposed decoding algorithm offers a coding gain about 0,5 dB compared with Chase- HSDec and has the same decoding results as PHR-SPDA.

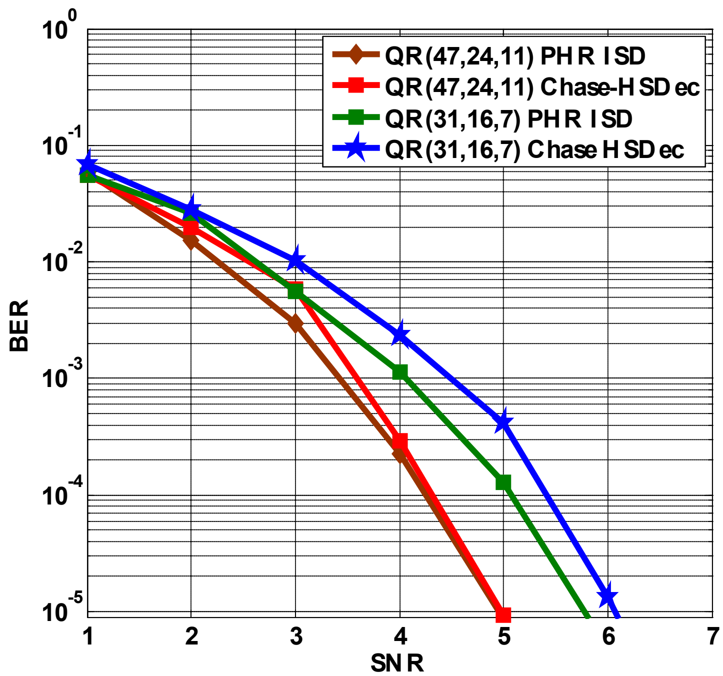


*Figure 4: Performances Of PHR-ISD And Chase-Hsdec For Some QR Codes*

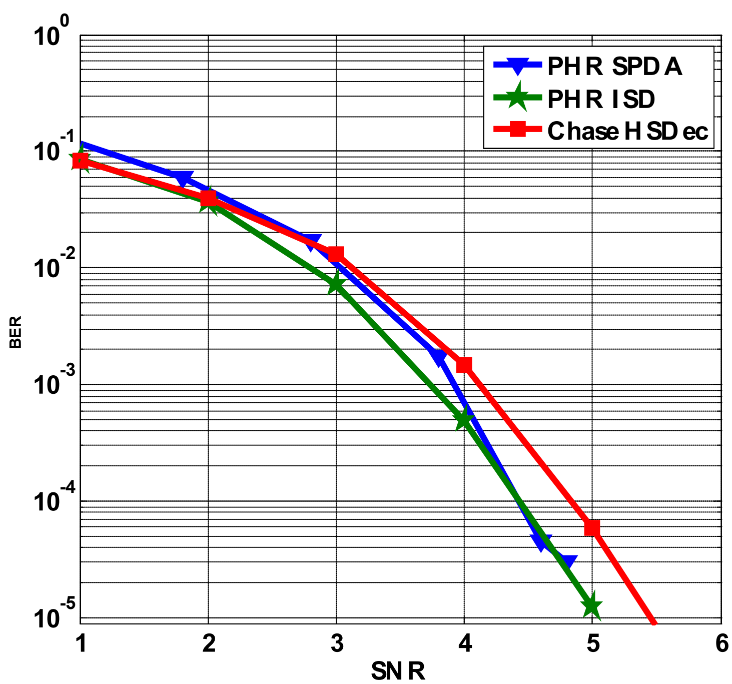


*Figure 5: Performances Of PHR-ISD, PHR-SPDA And Chase-Hsdec For BCH (63, 39, 9)*

In Fig. 6, we compare the decoding results of our decoding algorithm, PHR-BM [31], Chase-HSDec and cGAD [9] decoders for BCH (63, 45, 7). We conclude that our decoder has the same performances as PHR-BM and exceeds other competitors for this code.

To prove the efficiency of our suggested serial concatenation, we show in figures 7 and 8 respectively a comparison of our suggested decoding algorithm PHR-ISD, ISD and HR algorithms for BCH (31, 21, 5) and QR(31, 16, 7) codes. From these figures, we deduce that the proposed serial combination, of HR partially exploited and ISD, guarantees very good performances with a little number of dual codewords. For instance, for QR (31, 16, 7), the good obtained results are at the base of just 900 codewords which means that we have used only 2,74% of the dual code space. Table 2 presents the reduction rate of used codewords for BCH (31, 21, 5) and QR (31, 16, 7) codes.

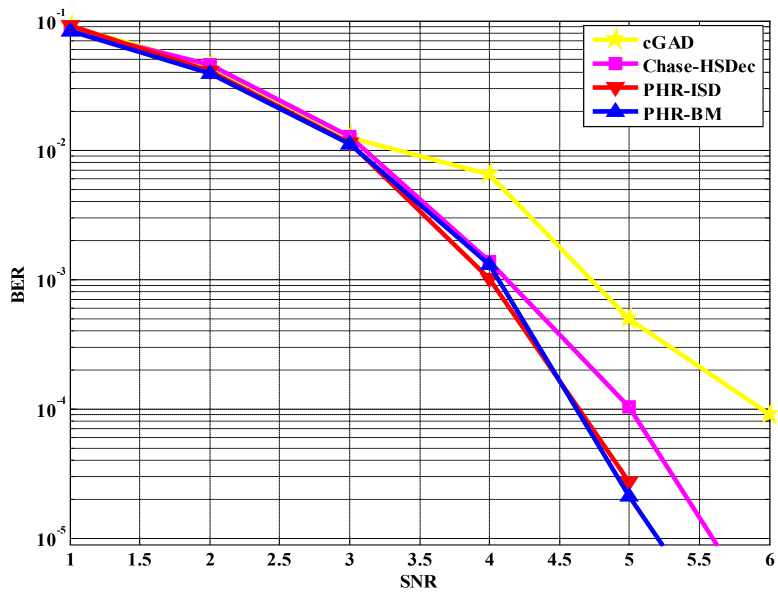


*Figure 6: Performances Of PHR-ISD, PHR-BM, Cgad, And Chase-Hsdec For BCH(63, 45, 7)*

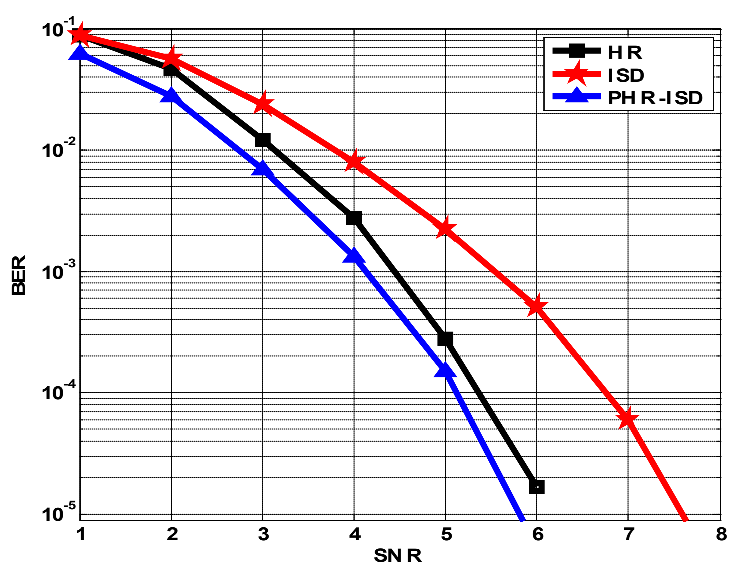


*Figure 7: Comparison of the performances of HR, ISD and PHR-ISD for BCH (31, 21, 5)*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

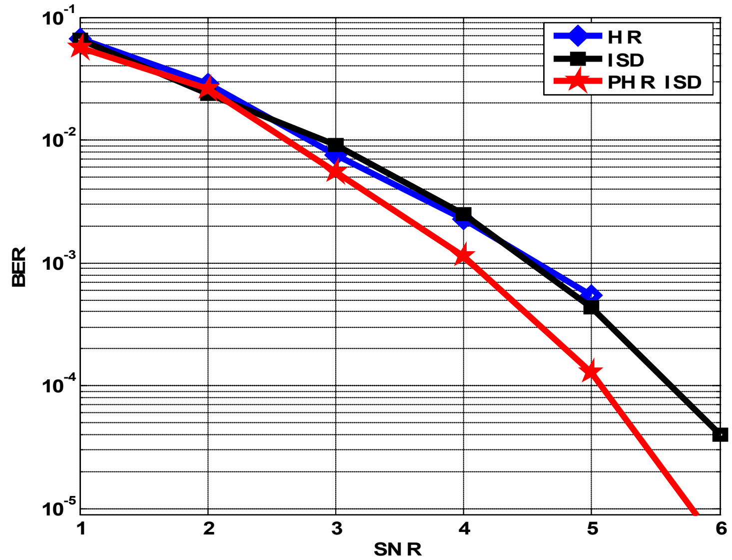


*Figure 8: Comparison of the performances of HR, ISD and PHR-ISD for QR (31, 16, 7)*

*Table 2: Reduction rate of used codewords*

| Code | Number of used codewords of the dual code | | Reduction rate of used codewords |
|---|---|---|---|
| | Hartmann Rudolph | PHR-ISD | |
| BCH(31, 21, 5) | $2^{31-21}=2^{10}=1024$ | 205 | 79,99% |
| QR(31, 16, 7) | $2^{31-16}=2^{15}=32768$ | 900 | 97,25% |

To be sure of the temporal efficiency of our suggested concatenation scheme, we have plotted in Figure 9 the ratio between the required run times of PHR-ISD and HR decoders for QR(31, 16, 7) code; for this code, the reduction in run time is between 82 and 95%.

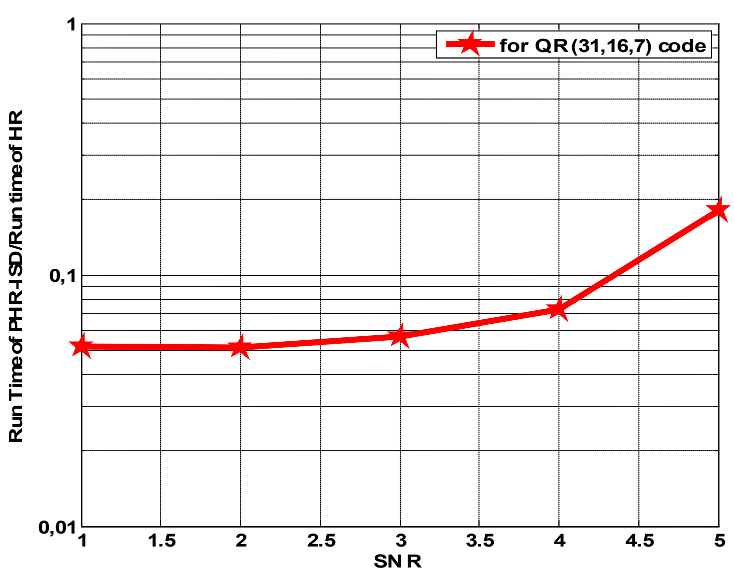


*Figure 9: Ratio between the required run times of PHR-ISD and HR algorithms for QR (31, 16, 7)*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

We conclude that with PHR-ISD we have been able to reduce remarkably the run time of the Hartmann Rudolph decoder, which shows the efficiency and the speed of the concatenation idea.

## 5. CONCLUSION

We have introduced a fast and efficient decoding algorithm thanks to a serial concatenation of the Hartmann and Rudolph decoder and Information Set Decoding technique. We have applied it on BCH and QR codes. The comparison results show that the suggested PHR-ISD guarantees better performances comparing with some competitors. The number of used codewords is very low, which has enabled us to minimize remarkably the temporal complexity. For instance, for QR (31, 16, 7), we have reached good decoding performances at the base of only 900 dual codewords. In other words, just 2,74% of the dual code space has been used. The great results of PHR-ISD will open a new way for the use of artificial intelligence algorithms in the coding theory domain.

## REFERENCES:

[1] Faham, H., El Kasmi Alaoui, M.S., Nouh, S., Azzouazi, M., "High Performance Decoding by Combination of the Hartmann Rudolph Decoder and Soft Decision Decoding by Hash Techniques", *Lecture Notes in Networks and Systems*, 2021, 211 LNNS, pp. 781–790. https://doi.org/10.1007/978-3-030-73882-2_71

[2] Faham, H., Nouh, S., Alaoui, M.S.E.K., Sadiq, M., Azzouazi, M., "New Way to Enumerate Large Quadratic Residue Codes Based on Hash and Automorphism Group", *Lecture Notes in Networks and Systems*, 2022, 357 LNNS, pp. 545–556. https://doi.org/10.1007/978-3-030-91738-8_50

[3] Alnawayseh, S.E.A and Loskot, P.: Ordered statistics-based list decoding techniques for linear binary block codes. EURASIP Journal on Wireless Communications and Networking 2012:314 (2012).

[4] M. Fossorier, S. Lin, Soft-decision decoding of linear block codes based on ordered statistics. IEEE Trans. Inf. Theory. 41, 1379–1396 (1995).

[5] Jung, B., Kim, T., Lee, H.: Low-Complexity Non-Iterative Soft-Decision BCH Decoder Architecture for WBAN Applications. Journal of Semiconductor Technology and Science, Vol.16, No.4 (2016).

[6] Lin, Y.M., Chang, H.C., Lee, C.Y.: Improved High Code-Rate Soft BCH Decoder Architectures With One Extra Error Compensation. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 21, No. 11 (2013).

[7] Askali, M., Nouh, S., Belkasmi, M.: A Soft decision version of the Permutation decoding algorithm. NTCCCS 12 workshop, Oujda, Morocco (2012).

[8] Askali, M., Ayoub, F., Chana, I., Belkasmi, M.: Iterative Soft Permutation Decoding of Product Codes. Computer and Information Science, Vol. 9, No. 1 (2016).

[9] Berkani A., Azouaoui A., Belkasmi M., Aylaj B.: Improved Decoding of linear Block Codes using compact Genetic Algorithms with larger tournament size. IJCSI International Journal of Computer Science Issues, Volume 14, Issue 1 (2017).

[10] 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).

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

[12] El Kasmi Alaoui M.S., Nouh S., Marzak A.: A low complexity soft decision decoder for linear block codes. In Proc. of the First International Conference on Intelligent Computing in Data Sciences (2017).

[13] 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.

[14] Prange, E.: The use of information sets in decoding cyclic codes. In IEEE Transactions on Information Theory, 8(5), 5-9 (1962).

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

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

[17] 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). In: Proc. of the First International Conference on Intelligent Computing in Data Sciences, 2017.

[18] Jing M.H., Chang Y., Chen J.H., Chen Z.H., Chang J.H.: A New Decoder for Binary Quadratic Residue Code with Irreducible Generator Polynomial. IEEE Asia Pacific Conference on Circuits and Systems (2008).
[19] Chen Y.H., Huang C.F., Chang J.: Decoding of binary quadratic residue codes with hash table. IET Commun., Vol. 10, Iss. 1, pp. 122–130 (2016).
[20] Nachmani E., Marciano E., Burshtein D., Béery Y.: RNN Decoding of Linear Block Codes. arXiv:1702.07560v1 [cs.IT] (2017)
[21] Nachmani E., Marciano E., Lugosch L., Gross W.J., Burshtein D., Béery Y.: Deep Learning Methods for Improved Decoding of Linear Codes. IEEE Journal of Selected Topics in Signal Processing, Volume: 12, Issue: 1 (2018).
[22] Pham Thi H. and Lee H.: Two-Extra-Column Trellis Min–Max Decoder Architecture for Nonbinary LDPC Codes. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 25, No. 5 (2017).
[23] Pham Thi H., Ajaz S., Lee H.: High-throughput partial-parallel block-layered decoding architecture for nonbinary LDPC codes. INTEGRATION the VLSI journal 59, 52–63 (2017)
[24] Li S., Zhang S., Chen Z., Geun Kang S.: A hybrid decoding of Reed–Muller codes. International Journal of Distributed Sensor Networks, Vol. 13(2) (2017).
[25] Shah T., Khan M., De Andrade A.A.: A decoding method of an n length binary BCH code through (n + 1)n length binary cyclic code. Anais da Academia Brasileira de Ciências 85(3): 863-872 (2013).
[26] Ren F., Zheng D., Wang W.: An Efficient Code Based Digital Signature Algorithm. International Journal of Network Security, Vol.19, No.6, PP.1072-1079 (2017).
[27] Chien C.H.: Developing Efficient Algorithms of Decoding the Systematic Quadratic Residue Code with Lookup Tables. International Journal of Operations Research Vol. 13, No. 4, 165−174 (2016).
[28] A. Azouaoui, I. Chana, M. Belkasmi.: Efficient Information Set Decoding Based on Genetic Algorithms. International Journal Communications, Network and System Sciences, 2012, 5, 423-429
[29] Baldi M, Barenghi A, Chiaraluce F, Pelosi G, Santini P. A Finite Regime Analysis of Information Set Decoding Algorithms. Algorithms. 2019; 12(10):209.
[30] S. NOUH, B. AYLAJ. : Efficient Serial Concatenation of Symbol By Symbol and Word by Word decoders. International Journal of Innovative Computing, Information and Control, volume 14 (2018).
[31] Faham, H., Alaoui, M.S.E.K., Nouh, S., Azzouazi, M., “An efficient combination between Berlekamp-Massey and Hartmann Rudolph algorithms to decode BCH codes”, *Periodicals of Engineering and Natural Sciences*, 2018, 6(2), pp. 365–372. http://dx.doi.org/10.21533/pen.v6i2.540