

SOFT DECISION DECODING OF LINEAR BLOCK CODES USING MEMETIC ALGORITHMS

¹ HICHAM BOUZKRAOUI, ² AHMED AZOUAOUI, ³ YOUSSEF HADI, ⁴ LAHCEN NIHARMINE

^{1,3} MISC Laboratory, Faculty of Sciences, Ibn Tofail University, Kenitra, Morocco

² Department of Computer Science, Faculty of Sciences, Chouaib Doukkali University, El Jadida, Morocco

⁴ SIME Lab, ENSIAS, Mohamed V University, Rabat, Morocco

E-mail: ¹hichamm.bouzkraoui@gmail.com, ²azouaoui.a@ucd.ac.ma, ³hadi@uit.ac.ma,
⁴niharminc@gmail.com

ABSTRACT

The general problem of soft-decision decoding a linear code is a NP-complete problem. This article introduces a soft-decision decoding algorithm, the first of its kind, based on memetic algorithm. The new approach is applicable to the more general case of linear codes; binary or nonbinary codes and cyclic and noncyclic codes where the only known structure is given by the generator matrix. The proposed algorithm used in each generation, two individuals selected randomly; the uniform crossing that exploits information specific to the communication system; a mutation that simply involves altering one or more genes in an individual and a local search (LS) that makes a descent by glorifying the created individual. The proposed decoder is simulated in an AWGN channel and enhanced through a parameter tuning process. In other side the simulation results generally show that our decoder is more efficient in terms of bit error rate compared to competitors' decoding algorithms. The analytical complexity of the proposed decoder is also presented and compared to other decoders.

Keywords: Error Correcting Codes, Soft Decision Decoding, Linear Codes, Memetic Algorithms, Metaheuristics

1. INTRODUCTION

Reliable transmission of information from a source to a destination is an open problem in a communication system. In general, the communication system consists of the elements shown in the figure 1. The data source can be analog or digital; source encoding is used to reduce redundancy in information from the source; channel encoder consists of adding redundancy to the transmitted information to protect it against noise and disturbances introduced into the channel. The modulator adapts the coded sequence to the physical channel which represents the link between the transmitter and the receiver. At the reception, the inverse operations are carried out in order to best restore the transmitted signal. The purpose of the channel decoder is to correct errors remaining in the received message. The error correcting codes have been introduced to correct transmission errors or when the data undergo alterations on the storage media. Linear codes can be divided into two main classes: block codes and convolutional codes. Decoding techniques can also be divided in two

categories, namely: hard decision and soft decision. Hard decision processes severely quantized data: the decoder only has symbols with values in F_q . Soft decision takes into account an additional indication of the likelihood or reliability of each of the received symbols [1]. This information is available at the demodulator output. In AWGN channels, the coding gain between Soft-decision decoding and Hard-decision decoding is about 2 dB [2]. Soft-decision decoding is an NP-Complete problem [3] approached by several methods. The first solutions were based on algebraic and probabilistic methods, for example Generalized Minimum Distance Decoding (GMD) [4], the Chase-2 algorithm [5], Hartmann Rudolph's algorithm [6] and the OSD [7] for block codes. In the last few decades, metaheuristics approaches were proposed to solve this problem. These techniques show very interesting performances. For example, the decoding of linear block codes using algorithm A* [8], genetic algorithms (GA) [9], [10], [11] and [12], compact genetic algorithm [13], [14] and [15] and neural networks [16], [17]. In this paper, we introduce a novel decoder based on

memetic algorithms named Memetic Algorithm for Soft Decision Decoding (MADEC). This decoder can be applied to any arbitrary linear code. In order to show the effectiveness of this decoder, we applied it on some binary, non-binary, cyclic and non-cyclic codes. The remainder of the paper is organized as follows. Firstly, Section 2 expresses soft-decision decoding as a combinatorial optimization problem. Secondly, Section 3 introduces the memetic algorithm. Thirdly, in Section 4, the algorithm proposed MADEC is described. The results of the simulation are offered and discussed in Section 5. Finally, Section 6 presents the conclusion and future trends.

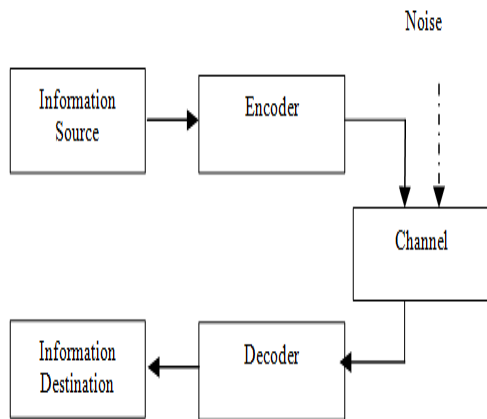


Figure 1: A simplified model communication system

2. SOFT DECISION DECODING AS AN OPTIMISATION PROBLEM

Let F_2 be the binary field, and note $C(n,k,d)$ a linear code of length n , dimension k and minimum distance d , we note also t the error correcting capability of C . This code can be represented by a $k \times n$ matrix G over F_2 called generator matrix, a message m can be then encoded as follows:

$$c = mG$$

In other side, we define a parity check $(n-k) \times n$ matrix noted H which satisfies:

$$HG^T = 0$$

Then we define for every vector $x \in F_2^n$ a syndrome $S(x)$:

$$S(x) = xH^T$$

If the codeword x contains no error then the syndrome $S(x)$ is zero.

In our study, the source generates a message

m which is encoded to a codeword $c = (c_1, c_2, \dots, c_n)$ using the generator matrix encoding, then BPSK-modulated to a signal $u = (u_1, u_2, \dots, u_n)$ where:

$$u_i = 2c_i - 1$$

This signal is sent over a Gaussian channel, perturbed by an AWG noise which is modeled by a random n -vector $n = (n_1, n_2, \dots, n_n)$, with iid components given by $n_i \sim N(0, N_0/2)$. In the receiver side the received signal is $r = (r_1, r_2, \dots, r_n)$ such that $r = u + n$. The likelihood probability is given by:

$$f_{r/u} = \frac{1}{(\pi N_0)^{n/2}} \exp \left(-\sum_{i=1}^n \frac{(r_i - u_i)^2}{N_0} \right)$$

Clearly MLD can be formally expressed as an optimization problem as follows:

Given a received word r , what is the codeword $c \in C$ which maximizes the likelihood probability $f_{r/u}$?

$$\max\{f_{r/u} / c \in C\} \Leftrightarrow \min\left\{\sum_{i=1}^n (r_i - u_i)^2 / c \in C\right\}$$

Consequently, this problem is reduced to finding the minimum euclidean distance to the received word r overall codewords $c \in C$, this optimization has n variables out of which only k form a generator base, hence we could restrict search space to k variables, in preference we select the most k independent reliable bits, this will initialize the search closer to the global optimum.

3. MEMETIC ALGORITHMS

The concept of memetic algorithms is credited to Moscato [18]. Memetic algorithms are part of the family of evolutionary algorithms. Their goal is to obtain an approximate solution to an optimization problem, when there is no resolution method to solve the problem accurately in a reasonable time. Memetic algorithms are born from hybridization between genetic algorithms (GA) and local search algorithms (LS). They use the same resolution process as genetic algorithms but use a local search operator after the mutation one. The interest of this class of algorithm is the contribution of the diversification of the genetic part accompanied by the intensification of local research. The local search method used in a memetic algorithm is not unique; one can use a simple local search method such as descent methods. All these methods revolve around a simple principle. From an existing solution, search a solution in the neighborhood and accept this solution if it improves the current solution.

4. MADEC ALGORITHM

Let C denote a (n,k,d) binary linear block code of generator matrix G , and let $(r_i)_{1 \leq i \leq n}$ be the received sequence over a communication channel with noise $\sigma^2 = \frac{N_0}{2}$ where N_0 is noise power spectral density.

Let N_i , N_e , N_g and LN_i denote respectively the population size, the number of elite members, the number of generations and the number of generations of local search. Let p_c and p_m be the crossover and the mutation rates.

4.1 Decoding Algorithm

The proposed decoding is depicted on figure 2. The steps of the decoder are as follows:

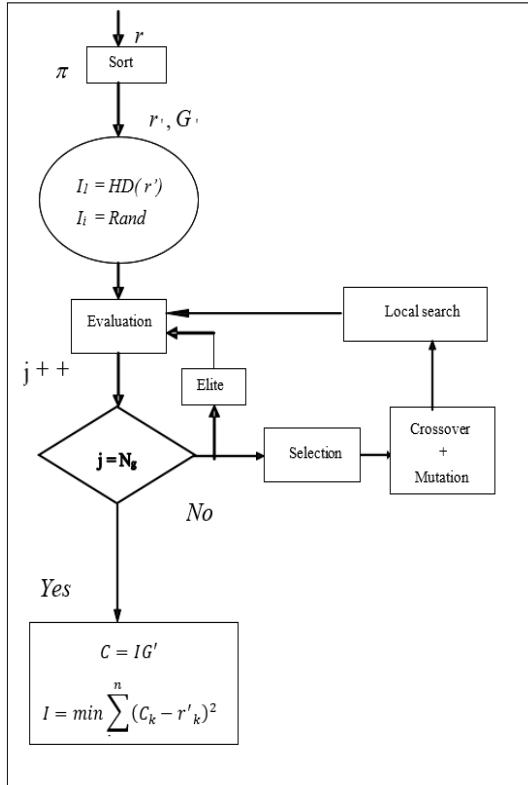


Figure 2: Basic structure of MADEC

The steps of the decoder are as follows:

- Step 1. Sorting the sequence r in descending order ($r' = \pi(r)$), such that the first k columns of the generator matrix $G' = \pi(G)$ are linearly independent.
- Step 2. Generate an initial population of N_i binary vectors of k bits:

- Substep 2.1. The first member, I_1 , of this population is a hard decision of r' .
- Substep 2.2. The other $N_i - 1$ members, $(I_j)_{1 \leq j \leq N_i}$ are uniformly random generated.
- Step 3. For i from 1 to N_g
- Substep 3.1 Compute the fitness of each individual in the population.

An individual is a set of k bits. The fitness function is the squared euclidean distance between the permuted received word and the encoded individual such that:

$$f(I) = \sum_{i=1}^n (c_i - r'_i)^2 \quad \text{where } c = IG'$$

- Substep 3.2. The best (elite) N_e members of this generation are inserted in the next one.
- Substep 3.3. The other $N_i - N_e$ members of the next generation are generated as follows:
- Sub-substep 3.3.1. Selection operation: a selection operation that uses the random method is applied in order to identify the parents $(I'^{(1)}, I'^{(2)})$ on which the reproduction operators are applied.
- Sub-substep 3.3.2. Crossover operator: Create a new vector I'_j "child" of k bits. Let Rand_1 be a uniformly random value between 0 and 1 generated at each occurrence. The crossover operator is defined as follows:

If $\text{Rand}_1 < P_c$, then the i^{th} bit of child $(I'_j)_{N_e+1 \leq j \leq N_i}$ $1 \leq i \leq k$ is given by:

$$I'_{ji} = \begin{cases} I_i^{(1)} & \text{if } I_i^{(1)} = I_i^{(2)} \\ \text{otherwise} & \begin{cases} I_i^{(1)} & \text{if } \text{Rand}_2^{(i)} < p \\ I_i^{(2)} & \text{otherwise} \end{cases} \end{cases}$$

Where

$$p = \begin{cases} \frac{1}{1 + e^{\frac{4r'_i}{N_0}}} & \text{if } I^{(1)} = 1 \text{ and } I^{(2)} = 0 \\ \frac{e^{\frac{4r'_i}{N_0}}}{1 + e^{\frac{4r'_i}{N_0}}} & \text{if } I^{(1)} = 0 \text{ and } I^{(2)} = 1 \end{cases}$$

Note that if $\text{Rand}_1 > p_c$

$$I'_j = \begin{cases} I^{(1)} & \text{if } \text{Rand} < 0.5 \\ I^{(2)} & \text{otherwise} \end{cases}$$

- Sub-substep 3.3.4. Mutation operator:

If the crossover operation realized, the bits I'_{ji} are muted with the mutation rate p_m :

$$I'_{ji} \leftarrow 1 - I'_{ji} \text{ if } Rand_3^{(i)} < p_m$$

- Sub-substep 3.3.5 Local search :

Repeat

Choose $I' \in V(I)$ such that $f(I')$ is minimal

$$I \leftarrow I'$$

until (counter > LN_g)

$V(I)$: set of binary strings at a distance 1 of x “we only change 1 bit”

- Step 4. The decoder decision is $I^* = \pi^{-1}(I_{best})$, where I_{best} is the best member from the last generation.

Remark:

In step 1 of the MADEC, in order to have a light algorithm we apply the Gaussian eliminations on the k independent columns corresponding to the most reliable positions, without the permutation π . This optimization is not used in other similar works [7], [9] and [13].

4.2 Complexity Analysis

Table 1: Complexity of Chase-2, OSD-m, GADEC, AutDAG, CGAD, SDGA, Chana, DDGA and MADEC algorithms

Algorithm	Complexity
Chase-2	$O(2^t n^2 \log n)$
OSD-m	$O(n^{m+1})$
GADEC	$O(N_i N_g [kn + \log(N_i)])$
DDGA	$O(N_i N_g [k(n-k) + \log(N_i)])$
AutDAG	$O(N_i N_g kn)$
SDGA	$O(2^t (N_i N_g [kn^2 + kn + \log(N_i)]))$
CGAD	$O(T_c k(n-k))$
Chana dec	$O(2^{p+1} (k \log n [n + \log(n-k)]))$
MADEC	$O(N_i N_g [LN_g kn + \log(N_i)])$

Let n be the code length, k be the code dimension, t be the error correction capability of a linear block code c, N_i be the population size which must be equal to the total number of individuals in the population, N_g be the number of generation and let

LN_g be the number of generation of local search. The Table 1 shows the complexity of the nine algorithms. The Chase-2 and SDGA [11] algorithms increase exponentially with t, while OSD and Chana [19] increase with m and p respectively where m is the order of OSD and p is the number of tests sequence. For DDGA [12], GADEC [9] and AutDAG [20] algorithms, the complexity is polynomial in k, n, N_i and N_g . For MADEC algorithm, the complexity is polynomial in k, n, N_i , N_g and LN_g , making it less complex compared to other algorithms. For CGAD algorithm [15], the complexity is also polynomial in k, n and T_c where T_c presents the average number of generations.

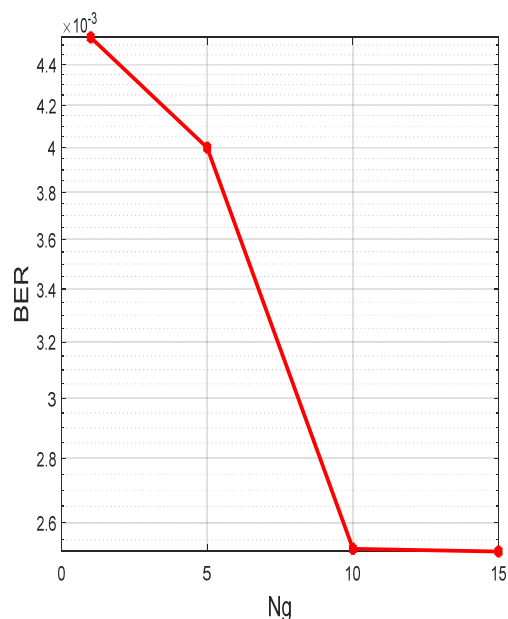
5. SIMULATION RESULTS AND DISCUSSIONS

5.1 Parameter Tuning

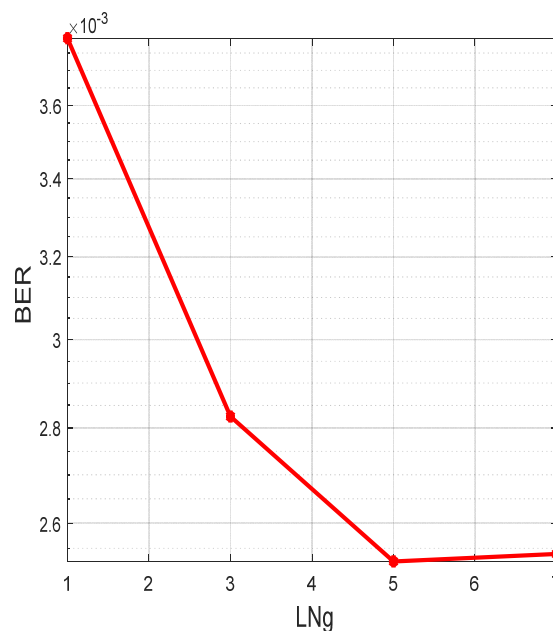
In order to tune the proposed algorithm, MADEC, we do intensive simulations. The simulations were made with default parameters outlined in Table 2. The performances are given in terms of BER (bit error rate) as a function of the concerned parameter.

Table2: Default parameters

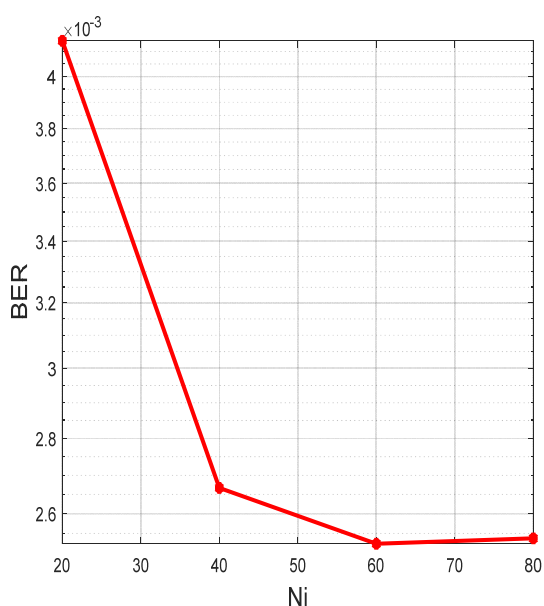
Parameter	Value
p_c (crossover rate)	0.97
p_m (mutation rate)	0.03
N_g (generation number)	10
N_i (population size)	60
LN_g (generation Number of LS)	5
Channel	AWGN
Modulation	BPSK
Minimum number of bit errors	200
Minimum number of blocks	1000
Code	BCH(63,45,7)
SNR	3dB

Figure 2: Evolution of BER with the parameter N_g

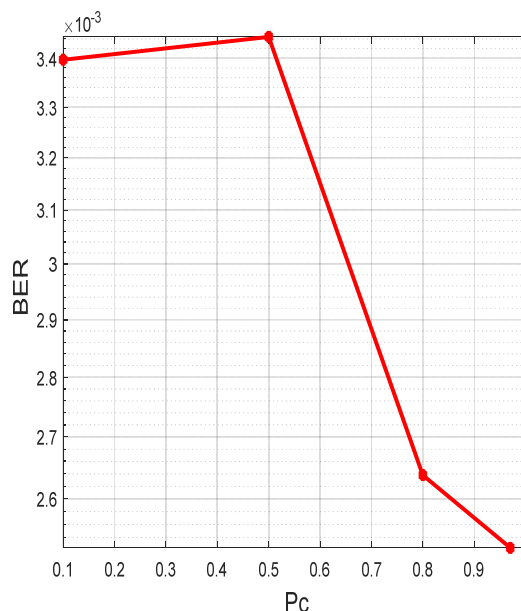
We observe from the above figure, that the best performance is achieved when $N_g=10$, which is set later in our simulations.

Figure 4: Evolution of BER with the parameter LN_g

The figure 4, the BER is decreasing, beyond $LN_g=5$ there is no improvement.

Figure 3: Evolution of BER with the parameter N_i

From the figure 3, the BER is decreasing and reach the optimal value when $N_i=60$, then the performance degrade, hence it is useless to use big populations in order to increase efficiency.

Figure 5: Evolution of BER with the parameter p_c

In the above figure, the BER function increases starting from $p_c=0.1$, arriving at $p_c=0.5$ it regresses, we estimate $p_c=0.97$ as the most suitable value for this parameter.

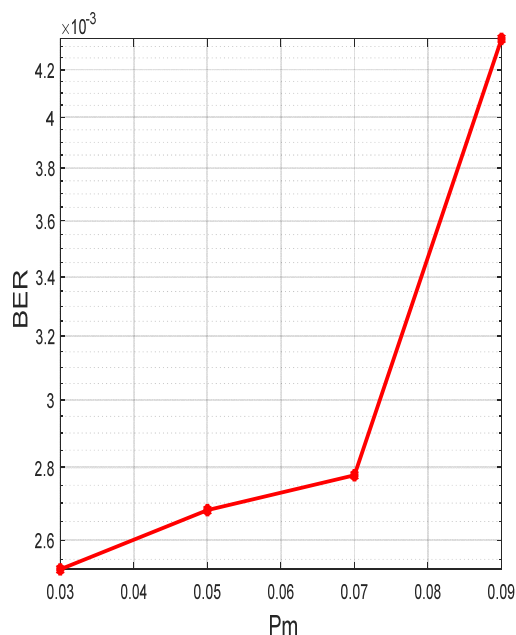


Figure 6: Evolution of BER with the parameter p_m

The figure 6, shows that the MADEC performance go down as the mutation probability grows, this degradation becomes severe when $p_m=0.07$. In any case we may take $p_m=0.03$ as the best choice for this parameter.

5.2 Comparison Of The Proposed Algorithm Versus Other Decoders

In order to compare our proposed algorithm, MADEC, with its competitor, we do intensive simulations. The simulations were made with default parameters outlined in Table 2. The performances are given in terms of BER (bit error rate) as a function of SNR (Signal to Noise Ratio E_b/N_0).

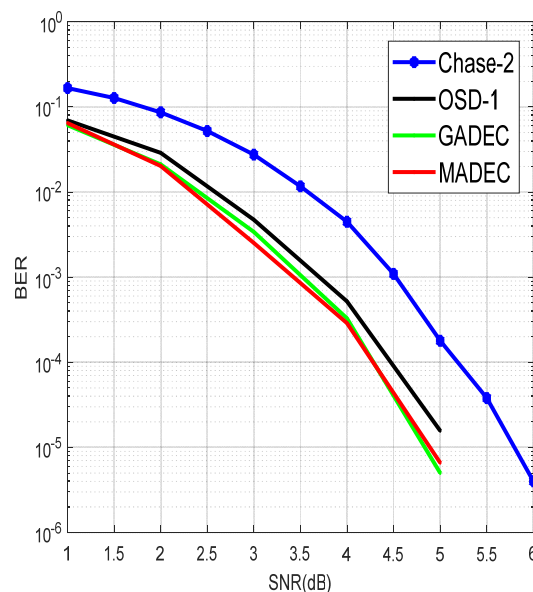


Figure 7: Performances of Chase-2, OSD-1, GADEC and MADEC algorithms for BCH(63,51,5) code

The figure 7 compares the performances of Chase-2, OSD-1, GADEC and MADEC decoders for BCH (63,51,5) code. We notice the superiority of MADEC over Chase-2 and OSD-1 algorithms and comparable with GADEC algorithm for this code. In fact at 10^{-5} we gain about 1dB over Chase-2. Moreover MADEC reaches 6.0×10^{-6} at SNR=5dB.

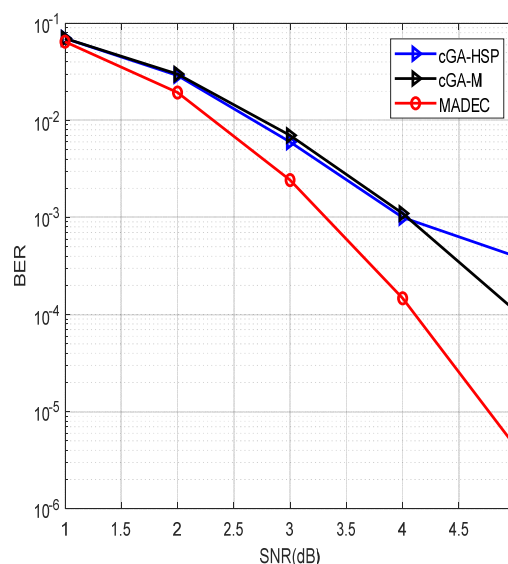


Figure 8: Performances of cGA-HSP, cGA-M and MADEC algorithms for BCH(63,45,7) code

The figure 8 compares the performances of MADEC with the most up to date cGA-HSP and cGA-M decoders. We notice that our decoder exceeds widely its competitors in performance. This gap grows for low noise level. In fact at over the classical algorithm. In fact at 10^{-3} , we gain about 0.75dB and at 10^{-4} , we gain about 1dB over cGA-M.

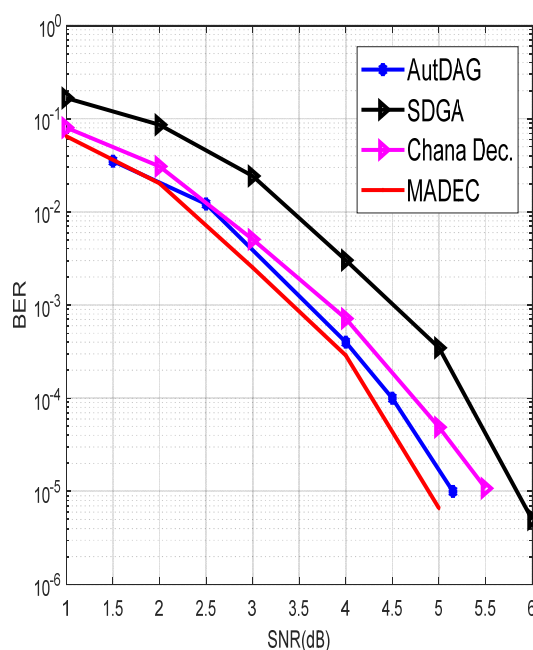


Figure 9: Performances of AutDAG, SDGA, Chana and MADEC

The performance of SDGA, AutDAG, Chana and MADEC algorithms, for BCH(63,45,7) code, is shown in figure 9. From the later, we remark that our algorithm is better the other algorithms. In fact, at 10^{-5} we have a gain of 0.25dB over AutDAG, 0.6dB compared to Chana decoder and 1db against SDGA.

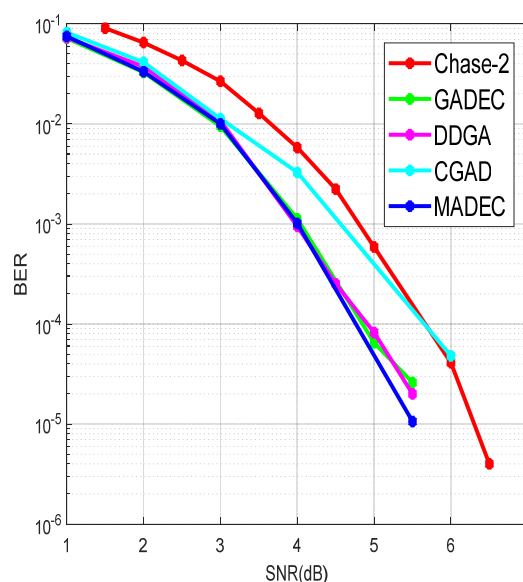


Figure 10: Performances of Chase-2, GADEC, DDGA, CGAD and MADEC algorithms for BCH(63,51,5) code

The performance of MADEC is better than Chase-2 and CGAD algorithms as shown in figure 5. According to this figure, we observed that MADEC is comparable to GADEC and DDGA algorithms. Besides, our decoder reaches 10^{-5} BER at SNR=5.5dB

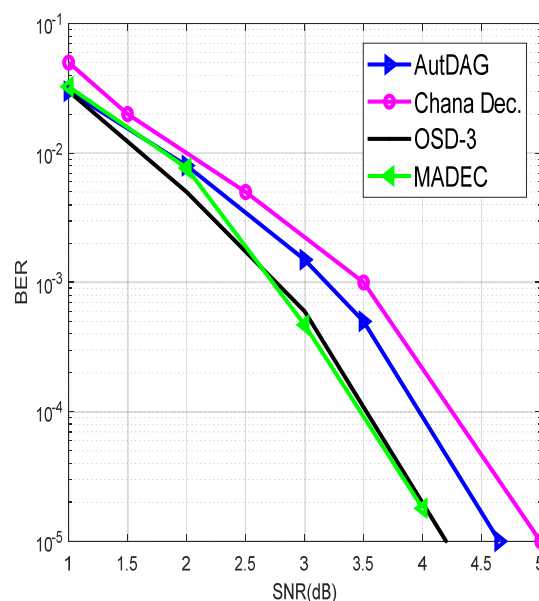


Figure 11: Performances of AutDAG, Chana Dec., OSD-3 and MADEC algorithms for QR(71,36,11) code

The figure 11 compares the performance of MADEC with others decoders for QR(71,36,11) code. From this figure, we remark that MADEC is better than AutDAG, Chana algorithm and comparable to the OSD-3.

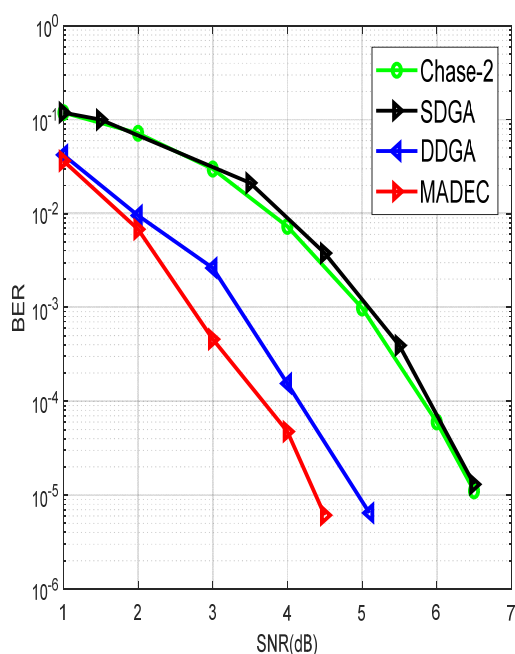


Figure 12: Performances of SDGA, Chase-2, DDGA and MADEC algorithms for RS(15,7,9) code

The performance of MADEC, DDGA, SDGA and Chase-2 algorithms, for RS(15,7,9) code, is shown in figure 12. From the later, we remark that our algorithm outperforms Chase-2 and SDGA by 2dB at 10⁻⁵.MADEC also outperforms DDGA by 0.6dB at 10⁻⁵.

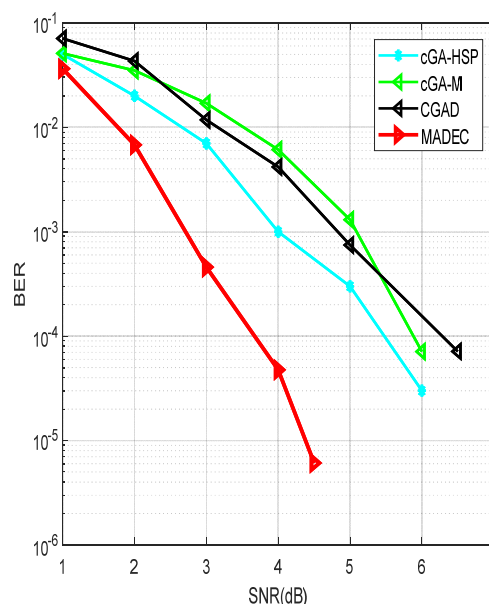


Figure 13: Performances of cGA-HSP, cGA-M, CGAD and MADEC algorithms for RS(15,7,9) code

Simulations of the non-binary RS(15,7,9) , in figure 13, reveal the large decoding power of MADEC over the most recent decoders. In fact at 10⁻⁴ we have a gain of 2dB over cGA-HSP, 2.5dB compared to cGA-M and 3dB against CGAD. In other hand for SNR=4.5 dB MADEC reach the BER 6.0 × 10⁻⁶

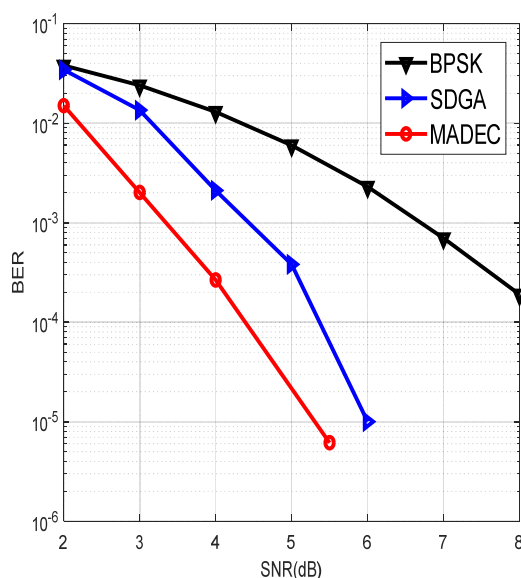


Figure 14: Performances of SDGA and MADEC algorithms for RM(32,16,8) code

The figure 14 presents the performances of MADEC and SDGA algorithms for RM(32,16,8) code. According to this figure, we remark that MADEC outperforms SDGA decoder by 0.65 dB at 10^{-5} .

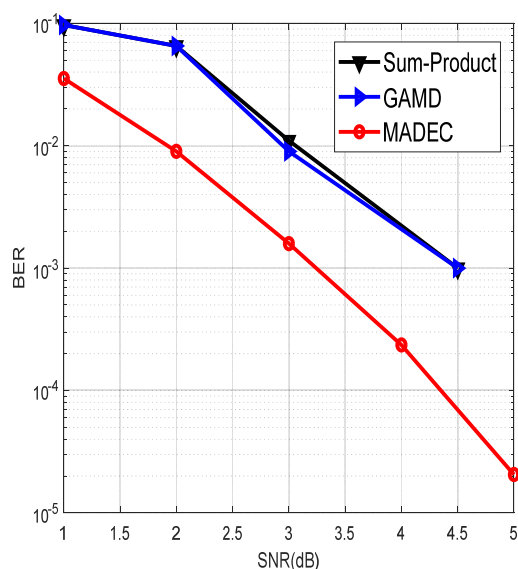


Figure 15: Performances of Sum-Product, GAMD and MADEC algorithms for LDPC(60,30) code

The figure 15 compares the performances of Sum-Product, GAMD [21] and MADEC for LDPC(60,30) code. We notice the superiority of MADEC over the others algorithms. In fact at 10^{-3} we have about 1.25dB gain. Besides, our decoder reaches 2.0×10^{-5} at SNR=5dB.

6. CONCLUSION

In this paper, we have proposed a novel and realistic application on memetic algorithms. We have presented efficient memetic algorithms for soft-decision decoding (MADEC), described this algorithm, simulated on some codes, then we focused on parameter tuning throw several experiments to find the most suitable parameters, later we demonstrated the superiority of this approach over other existing soft decision decoding. For example, the proposed algorithm gives large gains over the Chase-2 decoding algorithm and exceeds the performance of the OSD-3 for QR(71,36,11). In addition our MADEC decoder does not require algebraic decoding as is the case of the Chase-2 algorithm. The computational complexity of the proposed algorithm is also presented, compared with various decoding algorithms, and showed that it has polynomial complexity.

The obtained results will open new horizons for the metaheuristics methods in the information theory.

REFERENCES:

- [1] G. C. Clark, J.B. Cain, Error-Correction Coding for Digital Communication, New York Plenum, 1981.
- [2] J. G. Proakis, Digital Communications, 3rd ed. McGrawHill, 1995.
- [3] Berlecamp, E.R.; McEliece, R.J.; Van, H.C.A.V. On the inherent intractability of certain coding problems. IEEE Trans. on Information Theory, pp. 384-386, May 1978.
- [4] Forney, G.D. Generalized minimum distance decoding. IEEE Trans. on Information Theory, vol. 12, pp. 125-131, 1966.
- [5] Chase, D. A class of algorithms for decoding block codes with channel measurement information. IEEE Trans. on Information Theory, vol. 18, pp. 170-182, January 1972.

- [6] Hartmann, C.R.P.; Rudolph, L.D. An optimum symbol-by-symbol decoding rule for linear codes. *IEEE Trans. Information Theory*, pp. 514-517, 1976.
- [7] Fossorier, M.P.C.; Lin, S. Soft-decision decoding of linear block codes based on ordered statistics. *IEEE Trans. on Information Theory*, vol. 41, pp. 1379-1396, September 1995.
- [8] Han, Y. S.; Hartmann, C.R.P.; Chen, C.C. Efficient maximum likelihood soft-decision decoding of linear block codes using algorithm A*, Technical Report SU-CIS-91-42, School of Computer and Information Science, Syracuse University, Syracuse, NY 13244, December 1991.
- [9] Maini, H.; Mehrotra, K.; Mohan, C. Soft-decision decoding of linear block codes using genetic algorithms. In *Proceedings of the IEEE International Symposium on Information Theory*, Trondheim, Norway, 1994, p. 397.
- [10] Cardoso, F.A.; Arantes, D.S. Genetic decoding of linear block codes. In *Proceedings of International Conference on Telecommunications Congress on Evolutionary Computation*; Washington, DC, USA, 1999, pp. 2302-2309.
- [11] Azouaoui, A.; Chana, I.; Belkasmi, M. Efficient Information Set Decoding Based on Genetic Algorithms. *Int. J. of Comm., Netw. and Sys. Sci.*, 2012, Volume 5, No 7, pp 423-429.
- [12] Azouaoui, A.; Belkasmi, M.; Farchane, A. Efficient Dual Domain Decoding of Linear Block Codes Using Genetic Algorithms. *J. of Elec. and Comput. Eng.* 2012, Volume 2012, Article ID 503834.
- [13] Shakeel, I. GA-based Soft-decision decoding of linear block codes. In *Proceedings of the International Conference on Telecommunications Congress on Evolutionary Computation*. Doha, Qatar, 4-7 April 2010, pp. 13 - 17.
- [14] Berkani, A.; Azouaoui, A.; Belkasmi, M.; Aylaj, B. Improved Decoding of linear Block Codes using compact Genetic Algorithms with larger tournament size. *Int. J. of Comput. Sci. Issu.*, January 2017, Volume 14, Issue 1, pp 15-24
- [15] Azouaoui, A.; Berkani, A.; Belkasmi, M. An Efficient Soft Decoder of Block Codes Based on Compact Genetic Algorithm. *Int. J of Comput. Sci. Issu.*, September 2012, Volume 9, Issue 5, No 2, pp 431-438.
- [16] Berbia, H.; Elbouanani, F.; Belkasmi, M.; Romadi, R. An Enhanced Genetic Algorithm Based Decoder for Linear Codes. In *Proceedings of the 3rd International Conference on Information and Communication Technologies: From Theory to Applications*; Damascus, Syria, 2008, pp. 1-5.
- [17] Wu, J.L.; Tseng, Y.H.; Huang, Y.M. Neural Networks Decoders for Linear Block Codes. *Int. J. Comput. Eng. Sci.* 2002, volume 3, No.3, pp.235-255.
- [18] Moscato, P. *On Evolution, Search, Optimization, Genetic Algorithms and Martial Arts: Towards Memetic Algorithms*, California Institute of Technology, 1989.
- [19] Chana, I.; Allouch, H.; Belkasmi, M. An efficient new soft-decision decoding algorithm for binary cyclic codes. In *Proceedings of the International Conference On Multimedia Computing and Systems (ICMCS)*, Ouarzazate, Morocco, April 2011, pp 823-828
- [20] Nouh, S.; Chana, I.; Belkasmi, M. Decoding of Block Codes by using Genetic Algorithms and Permutations Set. *Int. J. of Comm. Netw. and Info. Secu.* 2013, Volume 5, No 3, pp 201-209.
- [21] Scandurra, A.G.; Dai Pra, A.L.; Arnone, L.; Passoni, L.; Castineira Moreira, J. A Genetic-Algorithm Based Decoder for Low Density Parity Check Codes, *Lat. Am. Appl. Res.* 2006; Volume 36, No 3, pp 169-172.