Good Quasi-Cyclic Codes from Circulant Matrices Concatenation using a Heuristic Method

Bouchaib AYLAJ
LIMA Lab, Faculty of Sciences
Chouaib Doukkali University
El jadida, Morocco

Mostafa BELKASMI
SIME Labo, ENSIAS
Mohammed V University
Rabat, Morocco

Said NOUH
TIM Lab, Faculty of Sciences Ben M'sik
Hassan II University
Casablanca, Morocco

Hamid ZOUAKI
LIMA Lab, Faculty of Sciences
Chouaib Doukkali University
El jadida, Morocco

***Abstract*—In this paper we present a method to search *q* circulant matrices; the concatenation of these circulant matrices with circulant identity matrix generates quasi-cyclic codes with high various code rate *q/(q+1)* (*q* an integer).**

This method searches circulant matrices in order to find the good quasi-cyclic code (QCC) having the largest minimum distance. A modified simulated annealing algorithm is used as an evaluator tool of the minimum distance of the obtained QCC codes. Based on this method we found 16 good quasi-cyclic codes with rates (1/2, 2/3 and 3/4), their estimated minimum distance reaches the lower bounds of codes considered to be the better linear block codes in Brouwer's database.

***Keywords*—Circulant matrix; quasi-cyclic Codes; Minimum Distance; Simulated Annealing; Linear Error Correcting codes**

I. INTRODUCTION

In coding theory, a large side of research has been interested in design and construction of error correcting codes families which are the basis of the channel coding element in the digital communication system. This research is not an easy problem. Moreover, the sphere packing problem is equivalent to finding a linear code with largest minimum Hamming weight in a given space [1]. The term good codes in this work, refers to maximizing the minimum distance for a binary linear code of a given parameters: length and dimension or various-code rate and/or high-code rate.

The author in [2] used the canonical form based in circulant matrices to found many good codes: quadratic residue codes and high quality group codes, and the author in [3] found the best quadratic residues with the same circulant property over the field *GF(3)*

More generally, the author in [4] proposes a quadratic double circulant codes schemes which are a generalization over any field *GF(q)* and for any length code, on the contrary, of the construction methods cited in [1] [2].

The design of good error correcting codes is a difficult problem, which remains open in coding theory. Recently this problem is attacked with meta-heuristic methods. Some of these works, A. El Gamal et al. [5] used simulated annealing to build good source codes, good channel codes and spherical codes. in [6] Chatonnay et al. introduced genetic algorithms for finding good linear codes. In [7] [8] the authors found good double and triple circulant codes, using the multiple pulse method and genetic algorithms. Comellas et al. [9] used genetic algorithms to design constant weight codes. Walice et al. [10] have presented a comparative study of meta-heuristic techniques applied to estimate the minimum distance of BCH Codes.

The determination of the minimum distance of linear block codes (minimum Hamming weight) by classical methods is hardly feasible; in general, this is an NP-hard problem [11]. The combinatorial nature of the problem requires an enumeration of the codewords for a linear code in order to find one with the minimum weight. Unfortunately, exhaustive exploration of the search space, is not possible, especially when the length n increases [12][13], which means that the size of the search space that is 2^k codewords, becomes prohibitively high, where *k* is the dimension of code. Hence, the need of a met-heuristic technique to estimate the minimum Hamming weight value or in some cases, to find its true value.

We present in this paper, a method to search a good quasi-cyclic codes with rate *q/(q+1)* (where *q* is an integer) based in extensive random search for circulant matrices, and we chose the heuristic simulated annealing method (SA) to find the value of the minimum distance of quasi-cyclic codes that we have constructed.

The remainder of this paper is presented in six sections. On the next section, we give an introduction on quasi-circulant codes, the minimum distance of linear block codes, encoding operations and simulated annealing method. In section III we present the method for searching the good quasi-cyclic codes. The modified Simulated Annealing method is presented in section IV. The obtained codes and experiment results are presented in section V. Finally, concluding remarks and perspectives of this work are given in section VI.

II. Error Correcting Codes and Simulated Annealing Method

A. Quasi-Circulant Codes

Let *(n, k, d)* denote the linear block code over a field *GF(q)* with *q* elements of length *n*, dimension *k*, minimum distance *d* and the code rate *k/n*.

Let *r=n-k* be the code redundancy.

Definition1:

A matrix *M* square of order *r* over *GF(q)* is called circulant if each successive row a cyclic shift of the previous one, it has the following form:

$$M = \begin{pmatrix} m_0 & m_1 & m_2 & \cdots & m_{r-1} \\ m_{r-1} & m_0 & m_1 & \cdots & m_{r-2} \\ m_{r-2} & m_{r-1} & m_0 & \cdots & m_{r-3} \\ & & \cdots\cdots\cdots & & \\ m_1 & m_2 & m_3 & \cdots & m_0 \end{pmatrix}$$

The vector of the first row $(m_0, m_1 \ldots, m_{r-1})$ is called the header of the circulant matrix *M*

Definition2:

A Quasi-Cyclic Code *QCC(n, k)*, is a linear block code of length n and the rate *T* which satisfies the following properties:

- Any cyclic shift of a code word by *s* symbols gives another code word of QCC.
- The smallest integer *s* check this, is called the index of the code.

Quasi-cyclic codes are the general case of cyclic codes. When the integer *s=1* the QCC are cyclic codes

The quasi-cyclic codes can be generated by parallel or serially concatenated schemes of the circulant matrices.

The case of Double Circulant Codes (DCC)

A code linear of length *n=2r* and dimension *k=r*, with generator matrix of the form *G=[I M]* is called a double circulant code, where *M* is an *r x r* circulant matrix and *I* is an *r x r* identity matrix over *GF(2)*.More properties of DCC codes are given in [14].

Example of DCC: The QCC(24, 12, 8) code is a double circulant code of header vector *[1,1,0,1,1,1,1,0,1,0,0,0]*, with generator matrix *G*:

$$G = \begin{pmatrix} 1 & & & & & & & & & & 1&1&0&1&1&1&1&0&1&0&0&0 \\ & 1 & & & & & & & & & 0&1&1&0&1&1&1&1&0&1&0&0 \\ & & 1 & & & & & & & & 0&0&1&1&0&1&1&1&1&0&1&0 \\ & & & 1 & & & & & & & 0&0&0&1&1&0&1&1&1&1&0&1 \\ & & & & 1 & & & & & & 1&0&0&0&1&1&0&1&1&1&1&0 \\ & & & & & 1 & & & & & 0&1&0&0&0&1&1&0&1&1&1&1 \\ & & & & & & 1 & & & & 1&0&1&0&0&0&1&1&0&1&1&1 \\ & & & & & & & 1 & & & 1&1&0&1&0&0&0&1&1&0&1&1 \\ & & & & & & & & 1 & & 1&1&1&0&1&0&0&0&1&1&0&1 \\ & & & & & & & & & 1 & 1&1&1&1&0&1&0&0&0&1&1&0 \\ & & & & & & & & & & 0&1&1&1&1&0&1&0&0&0&1&1 \\ & & & & & & & & & & 1&0&1&1&1&1&0&1&0&0&0&1 \end{pmatrix}$$

The case of Triple circulant codes (TCC)

A code linear of length *n= n=3r* and dimension *k=r*, with generator matrix of the form *G=[I | M | N]* is called a triple circulant code, where *M* and *N* are two *r x r* circulant matrix and *I* is an *r x r* identity matrix over *GF(2)*.

We can define the generator matrix of Triple Circulant Code TCC by two vectors headers $[m_0, m_1, \ldots, m_{r-1}]$ and $[n_0, n_1, \ldots, n_{r-1}]$ which are respectively associated with the matrices *M* and *N* as the follow

$$M = \begin{pmatrix} m_0 & m_1 & m_2 & \cdots & m_{r-2} & m_{r-1} \\ m_{r-1} & m_0 & m_1 & \cdots & m_{r-3} & m_{r-2} \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ m_1 & m_2 & m_3 & \cdots & m_{r-1} & m_0 \end{pmatrix}$$

$$N = \begin{pmatrix} n_0 & n_1 & n_2 & \cdots & n_{r-2} & n_{r-1} \\ n_{r-1} & n_0 & n_1 & \cdots & n_{r-3} & n_{r-2} \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ n_1 & n_2 & n_3 & \cdots & n_{r-1} & n_0 \end{pmatrix}$$

Example of TCC: The *QCC (27, 9, 6)* code is a Triple circulant code, of the two vectors headers *[0,1,1,1,0,1,0,0,1]* and *[1,1,0,1,1,0,1,1,0]*, with generator matrix *G* :

$$G = \begin{pmatrix} 1 & & & & & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ & 1 & & & & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ & & 1 & & & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ & & & 1 & & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ & & & & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ & & & & & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ & & & & & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ & & & & & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ & & & & & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

B. Minimum distance of a linear code

Let C be an (n, k, d) linear block code over a field $GF(2)$ with 2 elements. The code C has 2^k codeword which is a k-dimensional subspace of the $GF(2)^n$.

Let a be an element of $GF(2)$, the Hamming weight W_H is defined as follows

$$W_H(a) = \begin{cases} 1 & if \quad a \neq 0 \\ 0 & if \quad a = 0 \end{cases} \qquad (0)$$

For a vector $A=(a_1, \ldots, a_n) \in GF(2)^n$, the Hamming weight W_H is

$$W_H(A) = \sum_{i=1}^{n} W_H(a_i) = \sum_{i=1}^{n} a_i \qquad (1)$$

We call minimum Hamming weight of the code C over $GF(2)$ the positive integer:

$$min\{ W_H(A) : A \in C, A \neq 0\}$$

The minimum distance d_{min} (or the minimum Hamming distance) of the linear code C is the minimum Hamming weight of any nonzero codeword.

$$d_{\min} = \min_{\substack{A \in C \\ A \neq 0}} W_H(A) \qquad (2)$$

C. Encoding linear codes

The encoder transforms each input information vector D into n-tuple codeword A: multiplying D by G the generator matrix of the code C with $n > k$, (see Figure 1)

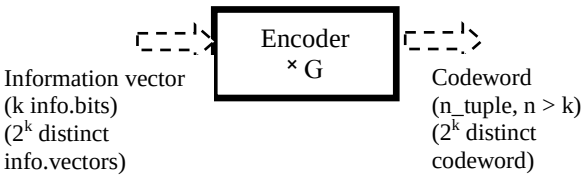

Fig. 1. A simplified Encoder representation

D. Simulated Annealing Method

We can say that simulated annealing is a neighbor search technique where the principle search is deeply inspired on the Metropolis [15] algorithm and the behavior of atoms in metals annealing process. The main idea is to use iteratively the Metropolis algorithm with reduction of the temperature. The annealing concepts in combinatorial optimization problems were introduced in 1980 by Kirkpatrick [16]. These concepts are equivalence to find an optimal energy of solidification in physical process by applying the Metropolis algorithm and search the feasible solutions of the cost function which converge to an optimal solution for a combinatorial optimization problem.

III. The Proposed Method for Search the Good Quasi-Cyclic Codes

In this section we give a method to search good quasi-cyclic codes with different rate $q/(q+1)$ (where q is an integer), this method is based on the search of a header called Total Header TH of length $q*(n-k)$; after we generate q circulant matrices over F, each matrix is defined by the header of length $(n-k)$, the serial concatenation of these headers give the Total Header TH.

The quasi-cyclic code of the code rate $q/(q+1)$ is generated by parallel concatenation of q circulant matrices, that will be serially concatenated with circulant identity matrix. The generator matrix G of the generated quasi-cyclic code is as the following:

$$G = \begin{pmatrix} & & A_1 \\ & & A_2 \\ & I & . \\ & & . \\ & & . \\ & & Aq \end{pmatrix}$$

Where I is a circulant identity matrix over F of size $(q*(n-k))(q*(n-k))$ and A_i , $1 \leq i \leq q$ is a circulant matrices over F of size $(n-k)(n-k)$

The matrix G is of size $(q*(n-k))((q+1)*(n-k))$, and of code rate is $q/(q+1)$.

Once the generator matrix G of the quasi-cyclic code is constructed, we move to determine the value of the minimum distance of this code. This is made by developing the function $F(A)$ named Cost Function as follow:

Let G be the generator matrix of the quasi-code $QCC(n,k)$,with elements g_{ij} over $GF(2)$, whose lines form a basis of QCC.

If the information vector $D= (d_1, d_{2,\ldots,} d_k) \in \{0,1\}^k$ Then the corresponding codeword $A=(a_1, a_{2,\ldots,} a_n)$ can be uniquely written as follows.

$$\forall \ 1 \leq j \leq n \qquad a_j = \bigoplus_{i=1}^{k} d_i g_{ij} \qquad (3)$$

$\oplus$: denote modulo-2-additions

From the equations (1), (2) and (3) we get

$$d_{\min} = \min_{\substack{D \in \{0,1\}^k \\ D \neq 0}} \sum_{j=1}^{n} \left(\bigoplus_{i=1}^{k} d_i g_{ij} \right) \qquad (4)$$

Then we have

$$F(A) = \sum_{j=1}^{n} \left(\bigoplus_{i=1}^{k} d_i g_{ij} \right) \quad \forall D \in \{0,1\}^k - \{0\} \qquad (5)$$

The minimum value of the function *F(A)* presents the value of minimum distance of the Q*CC, i*n other words we want to find a vector information *D* over $\{0,1\}^k$-{0} which minimizes *F(A)*. To determine the minimal solutions (minimum distance) of the *F(A)* function we use a modified simulated annealing algorithm (see section IV) .

A. The proposed search method algorithm

We implement an algorithm which uses the features of the aforementioned method. This method searches the good Total Header, so as to find a largest value of the minimum distance of the quasi-cyclic code.

The algorithm is given in **Algorithm 1**

Algorithm 1: Algorithm of the proposed search method

Inputs: *q, n-k, nbr-test, L_B: lower bound of d_{min}*

Outputs: list of good quasi-cyclic codes

For i=*1* to *nbr-test* **do:**

Step1: Generate randomly the Total Header TH of length *q*(n-k)*
Step2: Generate *q* circulant matrices A_i related to TH
Step3: Generate the Generator matrix G of the quasi-cyclic code related to A_i matrices
Step4: Calculate the minimum distance d_{min} of the generated quasi-cyclic code using simulated annealing (In **Algorithm 2**)
Step5: If (d_{min} >= L_B) then take the Total Header TH

End If

End For

Example : Let *q*=3, *r=n-k=6*, if the Total Header is TH=[0 1 1 0 0 1 1 0 1 1 1 1 1 1 0 1 0 0 1]

Then we generate 3 circulant matrices A_1, A_2 and A_3 of sizes 6*6

Where the header of A_1 is h_1=[0 1 1 0 0 1], the header of A_2 is h_2=[1 0 1 1 1 1], the header of A_3 is h_3=[1 0 1 0 0 1] and TH=[h_1 h_2 h_3]

The quasi-cyclic code generated has the following characteristics:

- Length *n=24*
- Dimension *k=18*
- Distance minimal *d=4* by algorithm 2
- Noted QCC(24, 18, 4)
- Code rate T=3/4
- The matrix *G of QCC* is as follow:

$$G = \begin{pmatrix} & A_1 \\ I & A_2 \\ & A_3 \end{pmatrix}$$

$$I = \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & \ddots & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix}_{18\times 18} \quad A_1 = \begin{pmatrix} 011001 \\ 110010 \\ 100101 \\ 001011 \\ 010110 \\ 101100 \end{pmatrix}_{6\times 6}$$

$$A_2 = \begin{pmatrix} 101111 \\ 011111 \\ 111110 \\ 111101 \\ 111011 \\ 110111 \end{pmatrix}_{6\times 6} \quad A_3 = \begin{pmatrix} 101001 \\ 010011 \\ 100110 \\ 001101 \\ 011010 \\ 110100 \end{pmatrix}_{6\times 6}$$

IV. THE MODIEFED SIMULATED ANNEALING ALGORITHM

The use of SA method gives rise to a new SA algorithm. This algorithm is an efficient evaluator of the minimum distance for linear block codes, already has been tested on several family of linear codes in our previous work [17].

The Modiefed Simulated Annealing algorithm which is used to calculate the minimal distance of a QCC codes is given in Algorithm2:

Algorithm 2: The basic algorithm of the modified simulated annealing.

Input(s):
N: number of iterations in each T_i where $10 \leq N \leq 10000$
T_i*=1.2,* T_f*=0.001,* α*=0.9:*cooling factor
Initial Task= *Task_1*
Output(s): minimum distance of the QC code

Generate randomly D_i a starting information vector
Repeat:

Repeat:

If (*Task== Task_1***) then** determine a neighbor information vector (D_{i+1}) from task_1;

Else determine a neighbor information vector (D_{i+1}) from task_ 2;

End if

Evaluate $\Delta F = F(D_{i+1}) - F(D_i)$;

If $\Delta F \leq 0$ **then** $D_i \leftarrow D_{i+1}$;

Generate q= *random [0, 1[;*

Else if ($q \leq Exp(-\Delta F/T)$)

Then $D_i \leftarrow D_{i+1}$;

End if

End if

Until (iterations number < N)

If (Transition *criterion is satisfied==yes* **) Then** switch between *Task_1* and *Task_2*;

End if

$T \leftarrow \alpha.T$;

Until $(T > T_f)$

Task_1: Let $D_i = (D_{i1},..., D_{ik})$ be the current information vector over $GF(2)^k$ and $S_i = (s_{i1},..., s_{ik})$ a switch vector over $GF(2)^k$, randomly generated, where $1 \leq W_H(S_i) \leq k$. The neighborhood information vector D_{i+1} is defined as follows:

Step1. $$D_{i+1} = D_i \oplus S_i \quad \text{mod2} \qquad (6)$$

Step2. $W_H(D_{i+1})$ must be between 1 and minimum distance upper bound of the QC code

Step3. $D_{i+1} \in GF(2)^k - \{0\}$

Task_2: Let Γ_p be the cyclic shift of p places of elements

The neighborhood information vector D_{i+i} is produced by generate a random integer number p over $[1, k-1]$, and we apply the cyclic shift Γ_p on D_i.

$$D_{i+1} = \Gamma_p(D_i) \qquad (7)$$

Criterion of transition between Task_1 and Task_2

The transition between Task-1 and Task-2 is made randomly from an uniform distribution.

V. Computational Experiment Results

We performed the computational experiments with:

- Software: program developed in language C
- Hardware: *CPU CORE 2Duo 2GHz* and *2GB* of RAM

We used the parameters in algorithm 2 for simulated annealing algorithm.

All good quasi-cyclic codes that we found by this method, using the modified simulated annealing method, have been verified and validated independently using the well known computer algebra package, MAGMA [18].

Here, the term good quasi-cyclic code refers to a binary quasi-cyclic code with the largest d_{min} for a given length n and dimension k. In cases where there is more than one good code, only one is chosen.

The Tables I, II and III as following summarize the obtained good quasi-cyclic codes with code rate $q/(q+1)$ where q is an integer between 1 and 3.

Note that *LB* and *UP*, respectively, denote Lower Bound and Upper Bound on the minimum distance of a linear code for a given parameters, these limits are taken from the Brouser's data base[19]. d_{magma} is the minimum distance calculated by the calculator algebraic Magma[18] and d_{found} is the minimum distance of QCC obtained by the modified simulated annealing algorithm. The obtained QCC codes seem to be good codes because their estimated minimum distance is equal to their lower bounds.

TABLE I. Good Quasi-Cyclic Codes Found using Algorithm 1, with Q=1, Code Rate T=1/2

Rate	QCC	Binary Total Header TH	d_{found}	d_{magma}	LB	UB
1/2	C(60,30)	000010111001111001000000110000	**12**	**12**	**12**	14
	C(52,26)	00010111000000010010111110	**10**	**10**	**10**	12
	C(58,29)	01110111110010100111010101010	**12**	**12**	**12**	14
	C(76,38)	11111010011110011011111011011000011	**14**	**14**	**14**	18
	C (94,47)	10001101010110011011010000000111110110001110010	**16**	**16**	**16**	22

TABLE II. Good Quasi-Cyclic Codes Found using Algorithm 1, with *Q=2*, Code Rate *T=2/3*

Rate	Codes	Binary Total Header TH	d_{found}	d_{magma}	LB	UB
2/3	QCC(93,62)	011111011111000110101110111011010111110111001011010010000000100	**10**	**10**	**10**	**14**
	QCC(99,66)	011011111101101111011110000001110010100111100110111111011110010101	**10**	**10**	**10**	**14**
	QCC(105,70)	010110010000010001110000100001100000111000110010001000000111000100 1100	**10**	**10**	**10**	**15**
	QCC(123,82)	110001100010000111110100011010100101001011100001111111111101011011001 1011001001111	**12**	**12**	**12**	**17**
	QCC(150,100)	011111001110110011000110000101100101000100000000101111100011001010100 0111111111001000000011111011111	**14**	**14**	**14**	**20**
	QCC(156,104)	000001011010001001011101100001101101110111001100001100100001110010010 010000110110001100011000010011000 1	**14**	**14**	**14**	**22**

TABLE III. GOOD QUASI-CYCLIC CODES FOUND USING ALGORITHM 1, WITH *Q=3*, CODE RATE *T=3/4*

Rate	Codes	Binary Total Header TH	d_{found}	d_{magma}	LB	UB
3/4	QCC(68,51)	00011011111110101110110100110010010111010001101100 1	**6**	**6**	**6**	**8**
	QCC(72,54)	10100011100000011000001001100110000111111001011001111 1	**6**	**6**	**6**	**8**
	QCC(92,69)	10010101111110001111101110111100100001001010100101001100101011110011 1	**8**	**8**	**8**	**10**
	QCC(96,72)	01001111011010001011000011011000010110000011000000100000010010111000110 1	**8**	**8**	**8**	**10**
	QCC(108,81)	11110011111101011001111010111001101111011110010111111100010111011111110111110011 01	**8**	**8**	**8**	**11**

VI. CONCLUSION

We gave a method to search good quasi-cyclic codes with different rate $q/(q+1)$ (where q is an integer) and we presented 16 new quasi-cyclic codes with minimum distances equal to lower bounds of the good linear codes in Brouwer's database. The fact that we have integrated a modified simulated annealing in the search algorithm speeded up the extensive random search process. In the future work, we will try to search with this efficient technique others better linear block codes, and to test the obtained codes in Encoder/Decoder systems for computational complexity and BER performance.

REFERENCES

[1] Conway J.H. and Sloane N.J.A. Sphere Packings, Lattic-es and Groups, 3rd ed., Springer, New York, 1999.

[2] Karlin M. IEEE Trans. Inform. Theory, 15, 81-92, 1969.

[3] Pless V. J. Combinatorial Theory, 12, 119-142, 1972.

[4] Gaborit P. J. Combin. Theory, A97, 85-107, 2002.

[5] El Gamal A.A., Hemachandra L.A., Shperling I. & Wei V.K.W. *IEEE Transactions on Information Theory*, 33(1),pp 116-123, 1987

[6] Jérôme Lacan, Pascal Chatonnay, "Search of Optimal Error Correcting Codes with Genetic Algorithms," Proceedings of the 6th International Conference on Computational Intelligence, Theory and Applications: Fuzzy Days, Springer-Verlag, 1999.

[7] A. Azouaoui, M.Askali and M. Belkasmi , "A genetic algorithm to search of good double-circulant codes", IEEE International Conference on Multimedia Computing and Systems (ICMCS'11) proceeding ,pp 829- 833, Ouarzazate, Morocco, April 07-09,2011.

[8] Askali M., et al. Discovery of Good Double and Triple Circulant Codes using Multiple Impulse Method. Advances in Computa-tional Research, ISSN: 0975-3273 & E-ISSN: 0975-9085, Volume 5, Issue 1, pp.-141-148, 2013.

[9] Comellas F., Roca R. Using genetic algorithms design constant weight codes. In applications of Neural Networks to Telecommunications, 119-124, Lawrence Erlbaum Associates, Mahwah, NJ, USA, 1993.

[10] J. Wallis and K. Houghten, "A Comparative Study of Search Techniques Applied tothe Minumum Distance of BCH Codes," Conference on Artificial Intelligence and Soft Computing, Banff, 17-19 July 2002.

[11] A. Vardy, "The Intractability of Computing the Minimum Distance of a Code", IEEE Transaction on Information Theory, vol. 43, N.6, 1997.

[12] Pless V.S. and Huffman W.C. Handbook of Coding Theory, Elsevier, Amsterdam, 1998.

[13] Coley D. An Introduction to Genetic Algorithms for Scien-tists and Engineers, World Scientific, 1999.

[14] McWilliams F.J. and Sloane N.J.A. The Theory of Error-Correcting Codes, Amsterdam, The Netherlands: North-Holland Mathematical Library, 1977.

[15] Metropolis, A. Rosenbluth, M. Rosenbluth, A. Teller, and E. Teller. Equation of state calculations by fast computing machines. Journal of Chemical Physics, 21 :1987–1091, 1953.

[16] Kirkpatrick, S , Gelatt, C.D., Vecchi, M.P. Optimization by Simulated Annealing. Science, vol220, No. 4598, pp671-680, 1983.

[17] Aylaj B. and Belkasmi M. New Simulated Annealing Algorithm for Computing the Minimum Distance of Linear Block Codes. Advances in Computational Research, ISSN: 0975-3273 & E-ISSN: 0975-9085, Volume 6, Issue 1, pp.-153-158, 2014.

[18] Bosma, W., Cannon, J.J., and Playoust, C.: 'The Magma algebra system I: the user language', J. Symb. Comput., 24, pp. 235–266, 1997.

[19] Brouwer, A.E.: 'Bounds on the size of linear codes', in Pless, V.S., and Huffman, W.C. (Eds.): 'Handbook of coding theory' (Elsevier, North Holland), http ://www.codetables.de/, 1998.