A new efficient way based on special stabilizer multiplier permutations to attack the hardness of the minimum weight search problem for large BCH codes

Issam Abderrahman Joundan, Said Nouh, Mohamed Azouazi, Abdelwahed Namir
TIM Lab, Faculty of Sciences Ben M'sik, Hassan II University, Casablanca, Morocco

Article Info

Article history:

Received Jan 7, 2018
Revised Nov 8, 2018
Accepted Nov 30, 2018

Keywords:

BCH codes
Canteaut-chabaud algorithm
Minimum distance
Multiplier
Zimmermann algorithm

ABSTRACT

BCH codes represent an important class of cyclic error-correcting codes; their minimum distances are known only for some cases and remains an open NP-Hard problem in coding theory especially for large lengths. This paper presents an efficient scheme ZSSMP (Zimmermann Special Stabilizer Multiplier Permutation) to find the true value of the minimum distance for many large BCH codes. The proposed method consists in searching a codeword having the minimum weight by Zimmermann algorithm in the sub codes fixed by special stabilizer multiplier permutations. These few sub codes had very small dimensions compared to the dimension of the considered code itself and therefore the search of a codeword of global minimum weight is simplified in terms of run time complexity. ZSSMP is validated on all BCH codes of length 255 for which it gives the exact value of the minimum distance. For BCH codes of length 511, the proposed technique passes considerably the famous known powerful scheme of Canteaut and Chabaud used to attack the public-key cryptosystems based on codes. ZSSMP is very rapid and allows catching the smallest weight codewords in few seconds. By exploiting the efficiency and the quickness of ZSSMP, the true minimum distances and consequently the error correcting capability of all the set of 165 BCH codes of length up to 1023 are determined except the two cases of the BCH(511,148) and BCH(511,259) codes. The comparison of ZSSMP with other powerful methods proves its quality for attacking the hardness of minimum weight search problem at least for the codes studied in this paper.

Corresponding Author:

Issam Abderrahman Joundan,
TIM Lab, Faculty of Sciences Ben M'sik,
Hassan II University,
Casablanca, Morocco.
Email: joundan.fsb@gmail.com

1. INTRODUCTION

Reproducing at one point either exactly or approximately a message selected at another point is the fundamental problem of communication, as pointed out by Claude Shannon [1]. The Error-correcting codes are used to improve the reliability of such communication.

The error-correcting capability of a code C is directly related to its minimum distance. For Linear codes, the minimum distance is equal to its lowest non-zero weight codeword. The knowledge of the weights enumerator of a code is important and it permits to compute their analytical performances. Double weight codes are used to elevate the performance and cardinality of spectral amplitude coding (SAC) OCDMA (Optical Code-Division Multiple-Access) systems [2]. The problem of searching codewords of lowest weight in linear codes is NP-hard problem and it is equivalent to the problem of the minimum distance research [3].

BCH codes are used in many applications and many algorithms are developed for decoding them like in [4]. In [5], the employment of BCH codes in SC-FDM-IDMA scheme had yield to good improvement of the BER performance (Bit Error Rate). In [6], the authors propose to concatenate BCH and turbo codes with OSTBC system. This concatenation, called BCH-TURBO-OSTBC, had yield to good result in term of BER performance.

For BCH codes, only a lower bound is known and the minimum distance is known only for some lengths, special cases [7]-[10] and remains an open problem in coding theory. In this paper, our work will focuses on finding the minimum distance of large BCH codes.

The remainder of this paper is organized as follows: The next Section presents the main related works. The Section 3 presents the proposed scheme ZSSMP for BCH codes. The Section 4 presents the main results. The conclusion and the possible future directions of this research are outlined in Section 5.

2. RELATED WORKS

The determination of the minimum distance for primitive BCH codes is hard as pointed out by charpin in [11]. For this reason, many researchers have investigated several methods for finding this metric. This Section summarizes the most important ones.

In [12], Augot, Charpin, and Sendrier presented an algebraic system of Newton's identities. The existence of a solution for this system, prove the existence of words of a given weight in a code. The use of this method for both remaining unknown minimum distance BCH codes of length 255 prove that BCH(255,63,61) has minimum distance 63, and BCH(255,71,59), has minimum distance 61. The use of this method had yield also to new results for some BCH codes of length 511.

In [13], Chabaud made a comparison of the both probabilistic algorithms for finding minimum-weight words in a linear code Leon's [14] and Stern's [15]. After that, Chabaud with Canteaut in [16], have developed a new probabilistic algorithm based on the best one. The application of this algorithm on narrow-sense BCH Codes of length 511 had yield to some new results, however the minimum distance is still unknown for other codes.

Zimmermann algorithm [17] is a general algorithm for computing the minimum distance of a linear code. It is implemented in GAP (package Guava) [18] over fields F_2 and F_3. It is also implemented, in Magma over any finite field.Zimmermann's algorithm is explained in detail in [19].

Wallis and Houghten in [20] have implemented the genetic algorithm for computing the minimum distance for BCH codes. Simulations results show that the genetic algorithm outperforms other artificial intelligence techniques like the Tabu Search presented in [21] and hill-climbing. In [22], the authors have optimized the parameters of the genetic algorithmand consequently they obtained more accurate results.

By formulating ant colony optimization (ACO) to incorporate Tabu Search (TS), Blandin [23], continues to improve his tabu search technique presented in [21]. This hybrid technique, called ACOTS, had yield to more accurate results.

The artificial intelligence Simulated Annealing presented in [24] was shown to be useful in finding the minimum distance for linear codes. In [25], Ajitha has used the metropolis algorithm to attack the minimum weight code word problem. This close algorithm to the Simulated Annealing gives more accurate results in comparison to previous works presented in [20]-[24]. In [25], Aylaj and Belkasmi continue to improvethe Simulated Annealing presented in [24]. The proposed Simulated Annealing (PSA) had yield to a fast convergence by reducing the number of iterations of the classical Simulated Annealing approachas well as obtaining good results in comparison to the previous works presented in [20], [22], [22], [25].

In [27], Berrou has presented an efficient approach based on the notion of Error Impulse response of a Soft-In decoder. The proposed idea make a relation between the minimum distance and the level of noise added to all-zero codeword by considering the minimum distance as the smallest level of noise from which the decoder fails in correction. In [22], the authors have improved this idea and presented the Multiple Impulse Method (MIM). In [28], the authors presented an efficient local search technique called MIM-RSC, which consist in applying the MIM method on some Random Sub Codes of reduced dimensions. The proposed method had yield to good results compared to the previous works presented in [20], [22], [23], [25], [26] as well as finding the true minimum distance of some BCH codes of length 1023 and 2047.

3. THE PROPOSED SCHEME

Instead of searching in some random sub codes like in [28], our proposed scheme consists in searching in few determined sub codes fixed by special permutations from the automorphism group of BCH codes. It is well known that for BCH($n=2^m-1,\delta$) codes, the multiplier permutations defined on $\{0,1,...,n-1\}$ by $\mu_{2^k}: i \rightarrow 2^k i \pmod{n}$ with $1 \le k \le m-1$ are stabilizers. From these stabilizers, we take only stabilizers with different cycle structure because they fix different sub code and apply Zimmermann algorithm on these sub codes.

For finding the minimum distance of BCH codes. The proposed scheme works as follows:

```
Inputs:
-A generator matrix G of BCH(n=2^m-1,k,δ)
-The permutations $\mu_{2^{j_i}}$  1≤i≤N with different cycle structure
Step 1:
For k=1 to N do
    Find the sub code fixed by $\mu_{2^{j_k}}$
End for
Step 2:
For k=1 to N do
    Find the estimated minimum distance d of the sub code fixed by $\mu_{2^{j_k}}$ by using the Zimmermann algorithm.
End for
Output:
-d as estimated minimum distance of BCH(n,k,δ)
```

Examples: Let’s take theBCH(15,5,7) code. A systematic generator matrix of BCH(15,5,7) code is:

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

By using a mathematical tool, we obtain the generator matrix GS1 of the sub code fixed by μ_2=(0)(1,2,4,8)(3,6,12,9)(5,10)(7,14,13,11) and the generator matrix GS2 of the sub code fixed by μ_4=(0)(1,4)(2,8)(3,12)(6,9)(5)(10)(7,13)(14,11):

$$GS1=\begin{pmatrix} 1\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1 \end{pmatrix} GS2=\begin{pmatrix} 1\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0\,0\,0\,0 \\ 0\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0 \\ 0\,1\,1\,1\,1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,1 \end{pmatrix}$$

In the second step, by applying the Zimmermann algorithm on the first sub code, the minimum distance obtained is equal to 7, which is the designed distance for the considered BCH code, and therefore the minimum distance is 7.

Let’s now take another example of the BCH(511,358,37) code. The permutations μ_2, μ_4, μ_{16}, μ_{32}, μ_{128}, and μ_{256} have the same cycle structure and fix the same sub code. On the other hand, the permutations μ_8 and μ_{64} fix also the same sub code. By using a mathematical tool, we obtain the generators matrix of the sub code fixed by μ_2 and $\mu_{8.}$

In the second step, by applying the Zimmermann algorithm on the sub code fixed by $\mu_{2,}$ the minimum distance obtained is equal to 39, which is greater than the designed distance for the considered BCH code. Then we pass to the sub code fixed by the second permutation with different cycle structure, which is here $\mu_{8,}$ by applying the Zimmermann algorithm on this sub code, the minimum distance obtained is equal to 37, which is equal to the designed distance for the considered BCH code, and therefore the minimum distance is 37.

4. RESULTS AND DISCUSSIONS

This Section presents a validation of the proposed method on BCH codes of known minimum distance and its application for finding the minimum distance of BCH codes of unknown minimum distance. This Section presents also a comparison between the proposed scheme and previous work on minimum distance for BCH codes.

All results have been done using a simple configuration machine: Intel(R) Core(TM) i3-4005U CPU @1.70GHz RAM 4GO. These results are made by running the cited algorithm in 1day for each code.

4.1. Validation of the proposed scheme

In order to validate the proposed method, it is applied on all BCH codes of known minimum distance presented in Table 1 All the narrow-sense primitive binary BCH codes of length 255 have their minimum distance equal to their designed distance except BCH(255,63,61), which has minimum distance 63, and BCH(255,71,59), which has minimum distance 61. The both last result have been proved in [12], by using the Newton's identities.

Table 1 summarizes the obtained results. It shows that the minimum weight found by the proposed method is equal to the true value of the minimum distance of all BCH codes of length 255. Therefore, the proposed method is validated for length 255.

Table 1. Validation of the proposed scheme

BCH(n,k,δ)	True value of minimum distance	d(ZSSMP)	BCH(n,k,δ)	True value of minimum distance	d(ZSSMP)
BCH(255,247,3)	3	3	BCH(255,115,43)	43	43
BCH(255,239,5)	5	5	BCH(255,107,45)	45	45
BCH(255,231,7)	7	7	BCH(255,99,47)	47	47
BCH(255,223,9)	9	9	BCH(255,91,51)	51	51
BCH(255,215,11)	11	11	BCH(255,87,53)	53	53
BCH(255,207,13)	13	14	BCH(255,79,55)	55	55
BCH(255,199,15)	15	15	BCH(255,71,59)*	61	61
BCH(255,191,17)	17	17	BCH(255,63,61)*	63	63
BCH(255,187,19)	19	19	BCH(255,55,63)	63	63
BCH(255,179,21)	21	21	BCH(255,47,85)	85	85
BCH(255,171,23)	23	23	BCH(255,45,87)	87	87
BCH(255,163,25)	25	25	BCH(255,37,91)	91	91
BCH(255,155,27)	27	27	BCH(255,29,95)	95	95
BCH(255,147,29)	29	29	BCH(255,21,111)	111	111
BCH(255,139,31)	31	31	BCH(255,13,119)	119	119
BCH(255,131,37)	37	37	BCH(255,9,127)	127	127
BCH(255,123,39)	39	39			

4.2. Comparison of the proposed scheme with Zimmermann algorithm

In order to compare the proposed scheme with Zimmermann algorithm, their applications on some BCH codes are made. Table 2 summarizes the obtained results. These results demonstrate that the proposed scheme made an efficient local search and consequently give accurate results in very short time. The obtained results show also the benefits of restricting the search space to sub codes with some properties related to the specified code.

Table 2. Comparison between the Proposed Scheme and Zimmermann Algorithm for Some BCH Codes

BCH(n,k,δ)	d(Zimmermann)	Run Time of Zimmermann (s)	d(ZSSMP)	Run Time of Step1 (s)	Run Time of Step2 (s)	Total Run Time of ZSSMP (s)
BCH(511,277,57)	71	46270.380	57	55	0.031	55.031
BCH(511,268,59)	77	6536.488	59	52	1.996	53.996
BCH(511,250,63)	83	64283.238	63	48	0.046	48.046
BCH(1023,573,101)	159	62005.171	101	313	0.264	313.264
BCH(1023,553,105)	167	39973.040	105	373	1.170	374.170

4.3. Comparison of the proposed scheme with canteaut-chabaud algorithm

Table 3 presents a comparison between the proposed scheme and Canteaut-Chabaud algorithm. The obtained results show that the proposed scheme give more accurate results than Canteaut-Chabaud algorithm as well as finding the true minimum distance for the 4 unknown minimum distance of BCH codes of designed distance 59, 75, 77 and 85. Therefore, the remaining codes of length 511 for which the minimum distance is still unknown are BCH(511,148,107) and BCH(511,259,61).

Table 3. Comparison between the Proposed Scheme and Canteaut-Chabaud Algorithm for BCH Codes of Length 511

BCH(n,k,δ)	Canteaut	d(ZSSMP)	BCH(n,k,δ)	Canteaut	d(ZSSMP)
BCH(511,502,3)	3	3	BCH(511,241,73)	73	73
BCH(511,493,5)	5	5	BCH(511,238,75)	>=75	75
BCH(511,484,7)	7	7	BCH(511,229,77)	>=77	77
BCH(511,475,9)	9	9	BCH(511,220,79)	79	79
BCH(511,466,11)	11	11	BCH(511,211,83)	83	84
BCH(511,457,13)	13	13	BCH(511,202,85)	>=85	85
BCH(511,448,15)	15	15	BCH(511,193,87)	87	87
BCH(511,439,17)	17	18	BCH(511,184,91)	91	91
BCH(511,430,19)	19	19	BCH(511,175,93)	95	95
BCH(511,421,21)	21	21	BCH(511,166,95)	95	95
BCH(511,412,23)	23	23	BCH(511,157,103)	103	103
BCH(511,403,25)	25	25	BCH(511,148,107)	>=107	>=107
BCH(511,394,27)	27	27	BCH(511,139,109)	111	111
BCH(511,385,29)	29	29	BCH(511,130,111)	111	111
BCH(511,376,31)	31	31	BCH(511,121,117)	119	119
BCH(511,367,35)	35	36	BCH(511,112,119)	119	119
BCH(511,358,37)	37	37	BCH(511,103,123)	127	127
BCH(511,349,39)	39	39	BCH(511,94,125)	127	127
BCH(511,340,41)	41	41	BCH(511,85,127)	127	127
BCH(511,331,43)	43	43	BCH(511,76,171)	171	171
BCH(511,322,45)	45	45	BCH(511,67,175)	175	175
BCH(511,313,47)	47	48	BCH(511,58,183)	183	183
BCH(511,304,51)	51	51	BCH(511,49,187)	187	187
BCH(511,295,53)	53	53	BCH(511,40,191)	191	191
BCH(511,286,55)	55	55	BCH(511,31,219)	219	219
BCH(511,277,57)	57	57	BCH(511,28,223)	223	223
BCH(511,268,59)	>=59	59	BCH(511,19,239)	239	239
BCH(511,259,61)	>=61	>=61	BCH(511,10,255)	255	255
BCH(511,250,63)	63	63			

4.4. Comparison of the proposed scheme with Aylaj's SA algorithm

In order to compare the proposed scheme with Aylaj's SA algorithm presented in [26], their applications on some BCH codes are made. The Table 4 summarizes the obtained results. These results demonstrate that the proposed scheme outperforms Aylaj's SA algorithm in both time and result quality.

Table 4. Comparison between the PRoposed Scheme and Aylaj's SA Algorithm for Some BCH Codes of Length 511

BCH(n,k,δ)	d(SA)	Run Time of SA (s)	d(ZSSMP)	Run Time of Step1 (s)	Run Time of Step2 (s)	Total Run Time of ZSSMP (s)
BCH(511,304,51)	68	21052	51	45	1.809	46.809
BCH(511,286,55)	73	40220	55	46	0.031	46.031
BCH(511,250,63)	91	29321	63	48	0.046	48.046

4.5. Comparison of the proposed scheme with MIM-RSC method

The Table 5 presents a comparison between the proposed scheme and MIM-RSC method presented in [26]. The obtained results show the efficiency of our scheme in giving accurate results in very short time.

Table 5. Comparison between the proposed Scheme and MIM-RSC method for some BCH codes of lengths 511 and 1023

BCH(n,k,δ)	d(MIM-RSC)	Run Time of MIM-RSC (s)	d(ZSSMP)	Run Time of Step1 (s)	Run Time of Step2 (s)	Total Run Time of ZSSMP (s)
BCH(511,277,57)	77	3288	57	55	0.031	55.031
BCH(511,268,59)	81	10667	59	52	1.996	53.996
BCH(1023,573,101)	165	18295	101	313	0.264	313.264
BCH(1023,553,105)	177	51756	105	373	1.170	374.170

4.6. Results of the proposed scheme for some large BCH codes

In order to find the minimum distance of some large BCH codes, the proposed schemeis applied by using a simple machine of the configuration given above. The obtained results are given in the Table 6 so that

d_f represent the minimum distance found by our scheme. This table shows the height capacity of the proposed technique to find a minimum weight codeword in very short time.

Table 6. True Minimum Weights of Some BCH Codes of Length 1023 Found by the Proposed Scheme

BCH(n,k,δ)	df	Run time of Step1 (s)	Run time of Step2 (s)	Total Run Time (s)	BCH(n,k,δ)	df	Run time of Step1 (s)	Run time of Step2 (s)	Total Run Time (s)
BCH(1023,1013,3)	3	185	0.078	185.078	BCH(1023,638,85)	85	368	0.733	368.733
BCH(1023,1003,5)	5	192	0.093	192.093	BCH(1023,628,87)	87	353	0.436	353.436
BCH(1023,993,7)	7	190	0.078	190.078	BCH(1023,608,91)	91	340	0.249	340.249
BCH(1023,983,9)	9	193	0.093	193.093	BCH(1023,598,93)	93	358	0.218	358.218
BCH(1023,973,11)	11	197	0.109	197.109	BCH(1023,588,95)	95	372	0.546	372.546
BCH(1023,963,13)	13	200	0.124	200.124	BCH(1023,573,101)	101	313	0.264	313.264
BCH(1023,953,15)	15	201	0.124	201.124	BCH(1023,563,103)	103	372	0.218	372.218
BCH(1023,943,17)	17	208	0.124	208.124	BCH(1023,553,105)	105	373	1.170	374.170
BCH(1023,933,19)	19	210	0.140	210.140	BCH(1023,493,119)	119	353	0.218	353.218
BCH(1023,923,21)	21	219	0.140	219.140	BCH(1023,483,121)	121	397	0.202	397.202
BCH(1023,913,23)	23	212	0.139	212.139	BCH(1023,473,123)	123	390	0.187	390.187
BCH(1023,903,25)	25	212	0.155	212.155	BCH(1023,453,127)	127	406	0.358	406.358
BCH(1023,893,27)	27	217	0.140	217.140	BCH(1023,443,147)	147	358	14.039	372.039
BCH(1023,883,29)	29	222	0.186	222.186	BCH(1023,423,151)	151	356	0.217	356.217
BCH(1023,873,31)	31	226	0.171	226.171	BCH(1023,403,157)	157	338	0.186	338.186
BCH(1023,863,33)	33	229	0.171	229.171	BCH(1023,393,159)	159	340	1.466	341.466
BCH(1023,858,35)	35	232	0.156	232.156	BCH(1023,383,165)	165	401	0.904	401.904
BCH(1023,848,37)	37	243	0.171	243.171	BCH(1023,368,171)	171	401	0.420	401.420
BCH(1023,838,39)	39	238	0.156	238.156	BCH(1023,318,183)	183	413	0.436	413.436
BCH(1023,828,41)	41	232	0.171	232.171	BCH(1023,288,191)	191	405	0.186	405.186
BCH(1023,808,45)	45	238	0.186	238.186	BCH(1023,258,213)	213	395	0.186	395.186
BCH(1023,798,47)	47	255	0.171	255.171	BCH(1023,208,231)	231	409	0.109	409.109
BCH(1023,788,49)	49	252	0.171	252.171	BCH(1023,183,239)	239	418	0.124	418.124
BCH(1023,778,51)	51	264	0.187	264.187	BCH(1023,143,253)	253	401	0.108	401.108
BCH(1023,768,53)	53	254	0.217	254.217	BCH(1023,133,255)	255	395	0.093	395.093
BCH(1023,758,55)	55	258	0.202	258.202	BCH(1023,123,341)	341	407	0.108	407.108
BCH(1023,748,57)	57	263	0.187	263.187	BCH(1023,121,343)	343	385	0.108	385.108
BCH(1023,738,59)	59	265	0.186	265.186	BCH(1023,111,347)	347	397	0.093	397.093
BCH(1023,728,61)	61	280	0.218	280.218	BCH(1023,101,351)	351	417	0.078	417.078
BCH(1023,718,63)	63	270	0.217	270.217	BCH(1023,91,363)	363	339	0.077	339.077
BCH(1023,708,69)	69	270	0.421	270.421	BCH(1023,76,375)	375	355	0.078	355.078
BCH(1023,698,71)	71	282	0.187	282.187	BCH(1023,56,383)	383	373	0.077	373.077
BCH(1023,688,73)	73	282	0.186	282.186	BCH(1023,36,447)	447	378	0.046	378.046
BCH(1023,678,75)	75	279	0.249	279.249	BCH(1023,26,479)	479	371	0.046	371.046
BCH(1023,668,77)	77	282	0.249	282.249	BCH(1023,16,495)	495	372	0.031	372.031
BCH(1023,658,79)	79	279	0.264	279.264	BCH(1023,11,511)	511	348	0.030	348.030
BCH(1023,648,83)	83	352	0.342	352.342					

5. CONCLUSIONAND PERSPECTIVES

In this paper, we have proposed a new efficient scheme to find the minimum distance for large BCH codes. The experimental results show that the proposed scheme outperforms several known powerful techniques. The true value of the minimum distances and consequently the error correcting capability of all the 165 BCH codes of length up to 1023 are determined except the two cases of the BCH(511,148) and BCH(511,259) codes. In the perspectives of this work, we will apply this powerful scheme to construct good large cyclic codes, and adapt this scheme to compute the minimum distance for other linear codes.

REFERENCES

[1] C. Shannon. "A Mathematical Theory of Communication," *Bell Syst. Tech. J.*, 27 :623–659, juillet et octobre 1948.

[2] Waqas A. Imtiaz and N. Ahmad "Cardinality Enhancement of SAC-OCDMA Systems Using new Diagonal Double Weight Code, " *International Journal of Communication Networks and Information Security*, Vol 6, No. 3, 2014.

[3] A. Vardy, "The intractability of Computing the Minimum distance of a Code, IEEE Transaction on Information Theory," vol. 43, No. 6, pp.1757–1766, 1997.

[4] Saïd Nouh, Idriss Chana and Mostafa Belkasmi, "Decoding of Block Codes by using Genetic Algorithms and Permutations Set," *International Journal of Communication Networks and Information Security*, Vol 5, No. 3, 2013.

[5] Roopali Agarwal, Manoj K. Shukla, "SC-FDM-IDMA Scheme Employing BCH Coding," *International Journal of Electrical and Computer Engineering (IJECE),* Vol. 7, No. 2, pp. 992-998, April 2017.

[6] Sofi Naima, Debbat Fatima, Bendimerad Fethi. Tarik "Performance Improvement of MIMO-OSTBC System with BCH-TURBO Code In Rayleigh Fading Channel", *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 11, No. 3, pp. 898-907, September 2018.

[7] C. Ding, X. Du, Z. Zhou, "The Bose and Minimum Distance of a Class Of BCH Codes," *IEEE Trans. Inf. Theory*, Vol. 61, Issue 5, pp. 2351–2356, May 2015.

[8] C. Ding, "Parameters of Several Classes of BCH Codes," *IEEE Trans. Inf. Theory*, Vol. 61, No. 10, pp. 5322–5330, October 2015.

[9] CunshengDing, Cuiling Fan, Zhengchun Zhou "The Dimension and Minimum Distance of Two Classes of Primitive BCH Codes," *Finite Fields and Their Applications*, Vol. 45, pp. 237-263, May 2017.

[10] Hao Liu, Cunsheng Ding, Chengju Li "Dimensions of Three Types of BCH Codes Over GF(q)," *Discrete Mathematics*, Vol. 340, Issue 8, pp. 1910-1927, August 2017.

[11] P. Charpin "Open problems on cyclic codes", in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Vol. I, North-Holland, pp.963–1063 (Chapter11), 1998.

[12] Daniel Augot, Pascale Charpin, and Nicolas Sendrier "Studying the Locator Polynomials of Minimum Weight Codewords of BCH Codes," *IEEE Transactions on Information Theory*, Vol. 38, No. 3, May 1992.

[13] Chabaud F. "Asymptotic Analysis of Probabilistic Algorithms for Finding Short Codewords." In: Camion P., Charpin P., Harari S. (eds) *Eurocode '92. International Centre for Mechanical Sciences (Courses and Lectures)*, vol 339. Springer, Vienna, 1993.

[14] J. Leon, "A Probabilistic Algorithm for Computing Minimum Weights of Large Error-Correcting Codes", *IEEE Trans. Inform. Theory*, Vol. 34, pp.1354–1359, 1988.

[15] J. Stern, "A method for finding codewords of small weight," in CodingTheory and Applications, G. Cohen and J. Wolfmann, Eds. New York: Springer-Verlag, pp. 106-113, 1989.

[16] Anne Canteaut and Florent Chabaud, "A New Algorithm for Finding Minimum-Weight Words in a Linear Code: Application to Primitive Narrow-Sense BCH Codes Of Length 511," *IEEE Trans. Inform. Theory*, Vol. 44, No. 1, pp 367-378, January 1998.

[17] Zimmermann K.-H., "Integral Hecke Modules, Integral Generalized Reed-Muller Codes, and Linear Codes Technische Universitat HamburgHarburg," Tech. Rep. 3-96, 1996.

[18] The GAP Group. "GAP–Groups, Algorithms, and Programming, Version 4.7.9". 2015. http://www.gap-system.org.

[19] Grassl, M. "Searching for Linear Codes with Large Minimum Distance," *Discovering mathematics with Magma, Algorithms Comput. Math*., 19, Springer, Berlin, pp. 287–313, 2006.

[20] 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.

[21] J.A. Bland, D.J. Baylis, "A Tabu Search Approach to the Minimumdistance of Error-Correcting Codes," *Int. J. Electron.* 79, pp. 829–837, 1995.

[22] Askali M., Azouaoui A., Nouh S., Belkasmi M. "On the Computing of the Minimum Distance of Linear Block Codes by Heuristic Methods," *International Journal of Communications, Network and System Sciences*, 5(11), 2012, pp. 774-784.

[23] J.A. Bland. "Local Search Optimisation Applied To The Minimum Distance Problem," *Advanced Engineering Informatics*, 21, 2007.

[24] M. Zhang and F. Ma, "Simulated Annealing Approach to the Minimum Distance of Error-Correcting Codes," *International Journal of Electronics*, Vol. 76, No. 3, pp. 377-384, 1994.

[25] Ajitha Shenoy K. B, Somenath Biswas, Piyush P. Kurur, "Performance of Metropolis Algorithm for the Minimum Weight Code Word Problem," *Genetic and Evolutionary Computation Conference*, 2014.

[26] Bouchaib Aylaj and Mostafa Belkasmi, "New Simulated Annealing Algorithm for Computing the Minimum Distance of Linear Block Codes," *Advancesin Computational Research, indexed Google Scholar* ISSN: 0975-3273, E-ISSN: 0975-9085, Vol. 6, Issue 1, pp. 153-158, 2014.

[27] C. Berrou, S. Vaton, M. Jezequel and C. Douillard,"Computing the Minimum Distance of Linear Codes bythe Error Impulse Method," *Proceedings of IEEE Globecom*, Taipei, 17-21, pp. 10-14, November 2002.

[28] S. NOUH, I. A. Joundan, B. Aylaj, M. Belkasmi, A. Namir "New Efficient Scheme Based on Reduction of the Dimension in the Multiple Impulse Method to Find the Minimum Distance of Linear Codes," *International Review on Computers and Software IRECOS*, Vol. 11, No. 9, pp. 742-751, September 2016.

BIOGRAPHIES OF AUTHORS

Issam Abderrahman Joundan received his Master in networks and telecommunications in 2011 from University of Chouaib Doukkali, 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.

Said Nouh is associate 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.

Mohamed Azouazi is a Professor at Faculty of Sciences Ben M'Sik, Hassan II University of Casablanca, Morocco. He obtained his Doctoral Thesis of automatic processing of natural languagesat EMI (school Engineer's Mohammedia) of Rabat in 1997. His current research interests: Constraint of Satisfaction Problem, BIG DATA, Predictive analysis, Deep Learning.

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