New efficient techniques to catch lowest weights in large Quadratic Residue codes

Issam Abderrahman JOUNDAN, Said NOUH and Abdelwahed NAMIR

Abstract—For a large Quadratic Residue (QR) code C, the problem of finding the minimum weight d is NP-hard and many research techniques have been developed to attack its hardness such as simulated annealing, Multiple Impulse Method, Ant Colony Optimization, Zimmermann algorithms and MIM-FSI method. The true value of the minimum weight in QR codes is known for only lengths less than or equal to 223. In this work, we propose new efficient schemes to catch lowest weights codewords in QR codes. The first proposed scheme Zimmermann-FSI uses the Zimmermann algorithm for searching lowest weights in the sub code SubEQR fixed by a self invertible element of the projective special linear group. The code SubEQR has a small dimension comparing to C itself. This reduction of the dimension permits to reduce considerably the research space size and it is behind the success of the Zimmermann-FSI scheme. This good result has encourages us to continue on reducing again the dimension of SubEQR and to propose the second scheme Zimmermann-FSI-RSC which uses the Zimmermann algorithm to catch lowest weights in a list of sub codes of small dimensions randomly extracted from the sub code SubEQR. The two proposed schemes are validated on all QR codes of known minimum weight. The comparison between MIM-FSI, Zimmermann-FSI and Zimmermann-FSI-RSC on many large QR codes proves the efficiency of the two latest ones in terms of run time reduction and the results quality. The proposed methods performed very well in comparison to previously known results and they yield to some new ones for lengths up to 601.

Keywords—Automorphism group, projective special linear group, Quadratic Residue codes, minimum distance, minimum weight, Multiple Impulse Method, Zimmermann’s algorithm, MIM-FSI method.

I. Introduction

The channel coding technique permits to detect and correct errors by adding redundancy in original data before transmission. In reception, the selected decoder uses the added information in correction. Each linear error correcting code C(n,k,d) can be generated by a binary generator matrix of k rows and n columns. k is called the dimension and n is the length of C.

The weight of a word is the number of ones it contains. The error-correcting capability of a linear code is equal to its lowest non-zero weight.

For each prime n of the form: \( n = \pm 1 (mod \ 8) \), the Quadratic Residue code \( QR(n) = QR(n,(n+1)/2,d) \) of length n is generated by the polynomial \( g(x) = \prod_{x=Q} (x - \beta^j) \) where Q is the collection of all nonzero quadratic residue integers modulo n: \( Q = \{ j^2 \mod n : 1 \leq j \leq n-1 \} \) and \( \beta \) is a primitive \( n^e \) root of unity in GF(2^n), where m is the smallest positive integer such that \( n \) divides \( 2^m - 1 \). Each QR code can be extended to a EQR(n+1,(n+1)/2,d+1) code whose codewords are obtained by adjoining a parity-check bit to a fixed position \( \infty \) of every codeword of the QR(n) code.

QR codes are a family of powerful error correcting codes, they have potential applications in modern communication systems and digital signal processing systems and they are recently decoded by fast and efficient methods [1-5]. They are used to construct quantum synchronizable codes [6]. In [7], authors have generalized QR codes over Galois rings using the Galois Theory. In [8], a self-dual code and a formally self-dual code are obtained from extended QR codes.

In this paper our work will focused on finding the minimum distance of large Quadratic Residue codes which is a NP-complete problem as proved in [9].

The Pless identity [10] permits to write the following equality:

\[
\text{for } j \leq (n-1)/2 : 2jA_{2j} = (n-(2j-1))A_{2j-1} \quad (2)
\]

With \( A_i \) denotes the number of codewords of weight i in \( QR(n) \) code and \( E_i \) denotes the number of codewords of weight i in \( EQR(n) \).

The definition of \( EQR \) and (2) permit to write the following equality:

\[
\text{for } j \leq n-1 \quad E_{4j} = \frac{n+1}{n+1-2j}A_{n+1-2j} = \frac{n+1}{2j}A_{2j-1} \quad (3)
\]

The formula (2) proves that:

\[
d(QR(n)) = d(EQR(n)) - 1 \quad (4)
\]

PSL_2 is a part of the automorphism group of Quadratic Residue codes. It is the set of permutations over \{0,1,2,...,n-1,\infty\}, of the form \( y \rightarrow (ay+b)/cy+d \) where a, b, c and d are elements of GF(n) verifying : ad-bc=1. For all values of n, the binary EQR(n) code is invariant under PSL_2 [11].

For a prime \( n = -1 (mod \ 8) \), the minimum distance \( d \) of a QR(n) code is related to its length by the following Krasikov inequality [12]:

\[
d + 1 \leq 0.166315 n \quad (5)
\]
In [13], the likelihood weight enumerators of some quadratic residue codes are found.

The remainder of this paper is organized as follows. The next section presents some background on Quadratic Residue codes, the projective special linear group $\text{PSL}_2$ and the main related works. The section 3 presents the proposed schemes: Zimmermann-FSI and Zimmermann-FSI-RSC. The section 4 presents the main results. The conclusion and the possible future directions of this research are outlined in section 5.

II. Related works

The determination of the minimum weight $d$ in a linear block code $C(n,k,d)$ permits to know its capability in detecting and in correcting errors or erasures. When the dimension $k$ increases, the size of the search space becomes prohibitively large and exhaustive search becomes not feasible. In [14-21] authors have used many techniques to find the true value of the minimum distances of QR codes for all lengths less than or equal to 223. For more lengths, this metric is still unknown. This section summarizes the most important previous works.

Wallis and Houghten [22] have applied many heuristic search techniques for BCH codes. They concluded that genetic algorithms with a large population size significantly outperformed hill-climbing, tabu search and hybrid techniques (GA – Hill climbing and GA - Tabu Search). In [23] the authors had improve some parameter of GA and get best result for BCH code compared to wallis and simulated Annealing [24] and applied this GA to QR codes of length up to 223.

Instead the turbo decoder used in [25], the MIM method (Multiple Impulse Method) [23] uses the OSD decoder of order 3 and injects errors in many positions. This method has permits to find good results in terms of time and precision.

Leon [26] has proposed an efficient probabilistic method based on information sets and the automorphism group and applied this method to QR codes of length up to 521.

Aylaj and Belkasmi [27] have proposed a new simulated annealing by using new mechanism of moving the search in different regions of solution space by degeneration of energy. They obtained new lower bounds for some linear codes.

Zimmerman algorithm [28] is a general algorithm for computing the minimum distance of a linear code. It is implemented in GAP (package Guava) [29] over fields $F_2$ and $F_3$. It is also implemented in Magma over any finite field. The method by Zimmerman is outlined in Algorithm 1. It is based on the so called information sets. Given a linear code $C$ with parameters $[n, k, d]$ and a generator matrix $G$, an information set $S = \{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ is a subset of $k$ indices such that the corresponding columns of $G$ are linearly independet. Therefore, after permutation of columns and elementary row operations we get a systematic matrix $\Gamma_i = (I_k | A_i)$. Assume that we are able to find $m-1$ disjoint information sets $(S_1 \cap \cdots \cap S_{m-1} = \emptyset)$, then we get $m-1$ different matrices $\Gamma_i = (I_k | A_i)$. Notice that there still may be left $n - k(m - 1)$ positions, so that the corresponding columns of $G$ do not have rank $k$ but $k_m < k$, then after applying column permutations and row operations, one gets $\Gamma_{m} = \begin{pmatrix} I_k & A \\ 0 & B \end{pmatrix}$. In overall, the number of $\Gamma$ matrices is $m$: The first $m-1$ will have full rank $k$, and the last one will have a rank strictly smaller than $k$.

The idea is to consider an upper bound $U$, initialized to $n-k+1$, and a lower bound $L$, initialized to 1. Then, both bounds are updated after enumerating codewords, and it is checked whether $L \leq U$; if so, the minimum weight is $U$.

The codewords are enumerated as follows: consider all the linear combinations $i \cdot \Gamma_j$ for $j = 1, \ldots, m$, where $i = (i_1, \ldots, i_k)$ and $wt(i) = 1$. After computing any linear combination, if the new weight is smaller than $U$, then $U$ is updated with the new weight. Moreover, after finishing with all linear combinations $i \cdot \Gamma_j$ for $j = 1, \ldots, m$, the lower bound is increased in $m-1$ units (actually one after each $\Gamma_j$) for the disjoint information sets. Now the same procedure is repeated for linear combinations $i \cdot \Gamma_j$ for $j = 1, \ldots, m$ and $wt(i) = 2$. Then, the same is done for $wt(i) = 3$, and so on until $L \geq U$ is obtained.

Algorithm 1 (Minimum weight for a linear code C)

Input: The generator matrix $G$ of the linear code $C$ with parameters $[n, k, d]$.

Output: $d$ The minimum weight of $C$.

$\begin{array}{l}
L := 1; \\
U := n - k + 1; \\
w := 1;
\end{array}$

while $w \leq k$ and $L < U$ do

$\begin{array}{l}
U := \min\{U, \min\{wt(i \cdot \Gamma_j) : i \in \mathbb{F}_k^2 \mid wt(i) = w\}\} ; \\
end for
\end{array}$

$L := (m - 1)(w + 1) + \max\{0, w + 1 - k + k_m\}$;

$w := w + 1$;

end while

return $U$;

In [30], we have used an efficient scheme to compute the minimum distance for linear codes. This method is based on reduction of the code dimension and the use of the MIM method on a given sub code fixed by a self invertible permutation $\sigma$ of the projective special linear group of Extended Quadratic Residue codes. The dimension of this sub code is very low comparing to the dimension of $C$ itself .In the next section we will apply the Zimmermann algorithm on this sub code.

III. The proposed schemes

This section presents the Zimmermann-FSI method for finding the lowest weight in large QR codes. The first proposed scheme Zimmermann-FSI works as follows:

**Inputs:** - $n$ a prime : $n = \pm (mod 8)$
- A generator matrix $G$ of $EQR(n+1)$

**Step 1:** find an element $\sigma \in \text{PSL}_2(n)$: $\sigma^2 = 1$ (self invertible)

**Step 2:** find the sub code:

$\text{SubEQR}(n+1, \sigma) = \{c \in EQR(n) : \sigma(c) = c\}$ fixed by $\sigma$ by
The second proposed scheme Zimmermann-FSI-RSC (on Random Sub codes) works as follows:

**Inputs:** - n a prime : \( n \equiv \pm 1 \pmod{8} \)
- A generator matrix \( G \) of EQR(n+1)
- \( N \), the number of random sub codes

Step 1: find an element \( c \in \text{PSL}_2(n) \): \( c^2 = 1 \) (self invertible)

Step 2: find the sub code \( SC = \{ c \in \text{EQR}(n) : \sigma(c) = c \} \) fixed by \( \sigma \) by solving the following system (S) of two fundamental equations:

\[
(S) = \begin{cases}
\sigma(c) = c \\
c = (\text{Inf}, \text{Red}) = \text{Inf} * G
\end{cases}
\]

Step 3: find the estimated minimum distance \( d \) of \( \text{SubEQR}(n+1, \sigma) \) by using the Zimmermann method.

Output: \( d - 1 \) as estimated minimum distance of QR(n)

### IV. Results and Discussions

This section presents a validation of the proposed method on all binary quadratic residue codes of known minimum distance and its application for finding the minimum distance of some unknown minimum distance.

In the comparison of Zimmermann-FSI with other method, we define the weight gain \( WG \) as the difference between the lowest weight obtained by the Zimmermann-FSI scheme and that obtained by other method: \( WG = d(\text{Zimmermann-FSI}) - d(\text{Other}) \).

All results have been done using a simple configuration machine: Intel(R) Core(TM) i3-4005U CPU @1.70GHz.

#### A. Validation of Zimmermann-FSI Method:

In order to validate the proposed method, it is applied on all QR codes of known minimum distance presented in [14-21]. The TABLE I summarizes the obtained results, it shows that the minimum weight found by the Zimmermann-FSI method is equal to the true value of the minimum distance of all QR codes of known minimum distance. Then the Zimmermann-FSI method is validated for length less than or equal to 223. This table shows that the proposed scheme gives the lowest weight codeword in a very short time.

#### B. Comparison between Ant Colony Optimization (ACO) and Zimmermann-FSI:

The TABLE II compares Ant Colony Optimization (ACO) Method [21] with Zimmermann-FSI . This table shows that Zimmermann-FSI outperforms very well the ACO method in finding the true value of the minimum distance for Quadratic Residue codes of length up to 199.

#### C. Comparison between Aylaj’s SA and Zimmermann-FSI:

The TABLE III compares Aylaj’s SA algorithm [27] with Zimmermann-FSI . This table shows that Zimmermann-FSI outperforms very well the Aylaj’s SA in finding lowest weight codewords in Quadratic Residue codes.

#### D. Comparison between MIM and Zimmermann-FSI:

The TABLE IV compares MIM Method [23] with Zimmermann-FSI . This table shows that Zimmermann-FSI outperforms MIM in finding lowest weight codewords for Quadratic Residue codes.

#### E. Comparison between Zimmermann-FSI scheme and Zimmermann method:

In order to compare the Zimmermann-FSI scheme with the Zimmermann method [28-29], their applications on some QR codes are made. The TABLE V gives the obtained results. It shows that the Zimmermann-FSI scheme greatly outperforms the Zimmermann method on finding lowest weight codewords. The run time of the two methods is 24 hours in the same configuration machine given above.

#### F. Comparison between MIM-FSI and Zimmermann-FSI:

The TABLE VI compares and summarizes the total run time and the result quality of the two methods MIM-FSI and Zimmermann-FSI. This table shows that Zimmermann-FSI outperforms MIM-FSI in both total run time and in the results quality.

#### G. Comparison between Zimmermann-FSI and Zimmermann-FSI-RSC methods:

The TABLE VII compares and summarizes the minimum distance found by the two methods Zimmermann-FSI and Zimmermann-FSI-RSC. This TABLE shows that Zimmermann-FSI-RSC outperforms Zimmermann-FSI especially for large codes.
TABLE I. Validation of Zimmermann-FSI method

\[
\begin{array}{cccc}
\text{QR Codes} & \text{True value of the minimum distance} & d(\text{Zimmermann-FSI}) & d(\text{Zimmermann-FSI-RSC}) \\
n & k & \text{of the minimum distance} & d(\text{Zimmermann-FSI}) & d(\text{Zimmermann-FSI-RSC}) \\
17 & 9 & 5 & 5 & 5 \\
41 & 21 & 9 & 9 & 9 \\
73 & 37 & 13 & 13 & 13 \\
89 & 45 & 17 & 17 & 17 \\
97 & 49 & 15 & 15 & 15 \\
113 & 57 & 15 & 15 & 15 \\
137 & 69 & 21 & 21 & 21 \\
193 & 97 & 27 & 27 & 27 \\
31 & 16 & 7 & 7 & 7 \\
47 & 24 & 11 & 11 & 11 \\
71 & 36 & 11 & 11 & 11 \\
79 & 40 & 15 & 15 & 15 \\
97 & 42 & 31 & 31 & 31 \\
193 & 101 & 63 & 63 & 63 \\
223 & 112 & 31 & 31 & 31 \\
\end{array}
\]

TABLE II. Comparison between Zimmermann-FSI and ant colony optimization (ACO) algorithm of Bland

\[
\begin{array}{cccccc}
\text{Codes QR} & n & k & \text{True value of the minimum distance} & d(\text{Zimmermann-FSI}) & \text{d(ACO) weight gain WG} \\
113 & 57 & 15 & 15 & 16 & 1 \\
137 & 69 & 21 & 21 & 21 & 0 \\
193 & 97 & 27 & 27 & 38 & 11 \\
151 & 76 & 19 & 19 & 19 & 0 \\
199 & 100 & 31 & 31 & 35 & 8 \\
\end{array}
\]

TABLE III. Comparison between Zimmermann-FSI and Aylaj’s SA algorithm

\[
\begin{array}{ccccc}
\text{Codes QR} & n & k & d(\text{SA}) & d(\text{Zimmermann-FSI}) & \text{weight gain WG} \\
383 & 192 & 63 & 47 & 16 \\
431 & 216 & 75 & 47 & 28 \\
463 & 232 & 79 & 59 & 20 \\
479 & 240 & 83 & 55 & 28 \\
409 & 205 & 68 & 47 & 21 \\
433 & 217 & 76 & 37 & 39 \\
449 & 225 & 76 & 55 & 21 \\
439 & 220 & 72 & 47 & 25 \\
\end{array}
\]

TABLE IV. Comparison between ZIMMERMANN-FSI and MIM methods

\[
\begin{array}{cccc}
\text{Codes QR} & \text{d(Zimmermann-FSI)} & \text{d(MIM)} & \text{weight gain WG} \\
n & k & \text{of the minimum distance} & d(\text{MIM}) & \text{weight gain WG} \\
313 & 157 & 39 & 39 & 0 \\
337 & 169 & 39 & 39 & 0 \\
353 & 177 & 41 & 41 & 0 \\
401 & 201 & 41 & 61 & 20 \\
409 & 205 & 47 & 63 & 16 \\
433 & 217 & 37 & 67 & 30 \\
449 & 225 & 55 & 67 & 12 \\
311 & 156 & 35 & 35 & 0 \\
359 & 180 & 39 & 55 & 16 \\
367 & 184 & 47 & 59 & 12 \\
\end{array}
\]

TABLE V. Comparison between Zimmermann-FSI and Zimmermann methods

\[
\begin{array}{cccccc}
\text{Codes QR} & n & k & d(\text{Zimmermann-FSI}) & d(\text{Zimmermann-FSI-RSC}) & \text{Total Run Time of Zimmermann-FSI} & \text{Total Run Time of Zimmermann-FSI-RSC} \\
439 & 220 & 47 & 67 & 332 & 2853 & 20 \\
569 & 285 & 59 & 91 & 54268 & 12422 & 32 \\
631 & 316 & 75 & 103 & 19944 & 48447 & 28 \\
\end{array}
\]

TABLE VI. Comparison between Zimmermann-FSI and MIM-FSI methods

\[
\begin{array}{cccccc}
\text{Codes QR} & n & k & d(\text{Zimmermann-FSI}) & d(\text{MIM-FSI}) & \text{Total Run Time of MIM-FSI} & \text{Total Run Time of MIM-FSI} \\
439 & 220 & 47 & 47 & 438 & 332 \\
487 & 244 & 55 & 55 & 86672 & 553 \\
503 & 252 & 55 & 55 & 42084 & 9084 \\
521 & 261 & 53 & 53 & 226045 & 709 \\
569 & 285 & 59 & 75 & 88518 & 54268 \\
607 & 304 & 83 & 83 & 129550 & 1384 \\
631 & 316 & 75 & 87 & 73283 & 19944 \\
\end{array}
\]

TABLE VII. Comparison between Zimmermann-FSI and Zimmermann-FSI-RSC methods

\[
\begin{array}{cccccc}
\text{Codes QR} & n & k & d(\text{Zimmermann-FSI}) & d(\text{Zimmermann-FSI-RSC}) & \text{Total Run Time of Zimmermann-FSI} & \text{Total Run Time of Zimmermann-FSI-RSC} \\
463 & 232 & 55 & 55 & 55 \\
487 & 244 & 55 & 55 & 55 \\
503 & 252 & 55 & 55 & 55 \\
521 & 261 & 53 & 53 & 53 \\
569 & 290 & 59 & 59 & 59 \\
601 & 301 & 79 & 79 & 79 \\
\end{array}
\]

V. Conclusion and perspectives

In this paper we have proposed new efficient schemes to find the minimum weight in large Quadratic Residue codes. These schemes permits to catch codewords of very smallest weight comparing to other known powerful methods. In the perspectives we have to adapt and use these methods to find the minimum weight in other linear codes like BCH codes, Low Density Parity Check codes (LDPC) and convolutional codes.

References


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 are telecommunications, Information and Coding Theory.

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