Gulf Journal of Mathematics
Vol 4, Issue 4 (2016) 206-216

NP-COMPLETENESS OF THE RANDOM BINARY QUASI-DYADIC COSET WEIGHT PROBLEM AND THE RANDOM BINARY QUASI-DYADIC SUBSPACE WEIGHT PROBLEM

P-L. CAYREL[2], M.K. DIAGNE[1*] AND C.T. GUEYE[3]

Abstract. In 1978, the Syndrome Decoding Problem (SDP) was proven to be NP-complete for random binary codes. Since then, the security of several cryptographic applications relies on its hardness. In 2009, Finiasz extended this result by demonstrating the NP-completeness of certain sub-classes of the SDP (see [9]). In this paper, we prove the NP-completeness of the SDP for a specific family of codes : the random binary quasi-dyadic codes. We use a reduction to the Four Dimensional Matching Problem (proven NP-complete).

1. Introduction

In 1978, the Coset Weight Problem (CWP) and the Subspace Weight Problem (SWP), usually known by the name of Syndrome Decoding Problem (SDP), have been proven to be NP-complete for random binary codes by Berlekamp, McEliece and van Tilborg [4]. The hardness of those two problems is central in code-based cryptography. Indeed, the security of certain cryptographic applications like the public key cryptosystems of McEliece and Niederreiter directly relies on the difficulty of solving an instance of the SDP. In 1994, Shor showed [14] that cryptography based on the factorization or the discrete logarithm problems will not resist to quantum computer attacks. The code-based cryptosystems do not suffer (so far) of quantum attacks. Therefore, in 2009, Finiasz [9] proved the NP-completeness of certain sub-classes of the SDP especially for random binary Goppa codes and proposed to generalize this result to some other sub-classes of the SDP. This leads us to explore other sub-classes of the SDP especially for random binary quasi-dyadic codes. We prove in this paper that the Coset Weight Problem (CWP) and the Subspace Weight Problem (SWP), namely the Syndrome Decoding Problem (SDP), are NP-complete for random binary quasi-dyadic codes. Contrary to Bareto and Misoczki in [12], for our proof, we have done a constructive polynomial reduction and we prove that both the CWP and the SWP are NP-complete for random binary quasi- dyadic codes.

Date: Accepted: Oct 24, 2016.

* Corresponding author.

2010 *Mathematics Subject Classification.* 94B05, 94B60.

Key words and phrases. NP-complete, quasi-dyadic codes, Syndrome Decoding Problem, Coset Weight Problem, Subspace Weight Problem, Four Dimensional Matching problem.

The codes we study are random and then do not suffer of the recent structural attacks. The SDP can be used for signature, identification, hash function.

In this paper, we prove the NP-completeness of the CWP and the SWP for an other class of codes, namely the random binary quasi-dyadic codes, by using a reduction to the Four Dimensional Matching Problem (FDMP). We will give general definitions in section 2, in section 3 we will give the main results and the proofs of the NP-completeness of the CWP and the SWP for the random binary quasi-dyadic codes.

2. General definitions

Definition 2.1. A (n, k)-linear code on $\mathbb{F}_2$ is a subspace of $\mathbb{F}_2^n$ of dimension k. A codeword is an element of the code.

Definition 2.2. The Hamming weight $wt(y)$ of a word $y \in \mathbb{F}_2^n$ is the number of non-zero coordinates of y.

Definition 2.3. The parity check matrix H of a (n, k)-linear code C is a $n \times (n-k)$ matrix such that:

$$\forall c \in \mathbb{F}_2^n, \{c \in C \Leftrightarrow cH = 0\}$$

The Syndrome of a vector $y \in \mathbb{F}_2^n$ is $S(y) = yH$.

2.1. Syndrome Decoding Problem.

Let C be a binary linear code of length n and dimension k and H its parity check matrix of size $n \times z$ where $z = n - k$. A codeword $c \in C$ satisfies $cH = 0$. We define the Coset Weight Problem (CWP) and the Subspace Weight Problem (SWP) as follows:

Coset Weight Problem (CWP)
Input: a binary matrix H, a binary vector S and a non negative integer w.
Property: Does it exist a vector y of weight $\leq w$ such that $yH = S$?

Subspace Weight Problem (SWP)
Input: a binary matrix H and a non negative integer w.
Property: Does it exist a codeword c of weight w such that $cH = 0$?

2.2. $\mathcal{NP}$-completeness.

2.2.1. *Non deterministic Polynomial time ($\mathcal{NP}$).*

Definition 2.4. NP means Non deterministic polynomial time.

Definition 2.5. $\mathcal{NP}$-class
The $\mathcal{NP}$-class is the set of all problems that can be solved by Non deterministic Polynomial time algorithms.

Definition 2.6. $\mathcal{NP}$-problem
A problem in the $\mathcal{NP}$-class is called a $\mathcal{NP}$-problem.
To show that a problem is in the $\mathcal{NP}$-class, it is sufficient to find an algorithm which verifies if a given solution is valid in polynomial time.

Definition 2.7. $\mathcal{NP}$-complete
An $\mathcal{NP}$-problem is said to be $\mathcal{NP}$-complete if the existence of a polynomial time solution for that problem implies that all $\mathcal{NP}$-problems have a polynomial time solution.
A problem is called $\mathcal{NP}$-complete problem if all problem of the $\mathcal{NP}$-class is polynomially reducible to it.

2.2.2. *Polynomial Reduction.* To prove that a problem A is $\mathcal{NP}$-complete, we must do a polynomial reduction of the problem A to an $\mathcal{NP}$-complete problem B. For that it is necessary :

- To assume an algorithm γ is able to solve any instance of A
- To start from an instance U of B
- To convert this instance U to an instance V of A
- To solve A with input V using γ to obtain a solution S
- To convert this solution S to a solution T of B
- The conversions (transformations) must be done in polynomial time.
- Therefore if one day, it exists a polynomial time algorithm to solve A it implies the existence of an algorithm (polynomial) to solve B. That proves that A is $\mathcal{NP}$-complete.

2.3. **Four Dimensional Matching Problem (FDMP).** To show that the SDP is $\mathcal{NP}$-complete Berlekamp, McEliece and van Tilborg built reductions from the Three Dimensional Matching Problem (TDMP) which is $\mathcal{NP}$-complete (it is problem 17 on Karp's list in [10]). In this part, we will do reductions from the Four Dimensional Matching Problem (FDMP) which is also $\mathcal{NP}$-complete [16], to prove that the SDP is $\mathcal{NP}$-complete.

Four Dimensional Matching Problem (FDMP)
Input: a subset $U \subseteq T \times T \times T \times T$ where T is a finite set.
Property: Does it exist a set $W \subseteq U$ such that $\mid W \mid = \mid T \mid$ and every two vectors of W have different i^{th} coordinate, $i \in \{1, 2, 3, 4\}$?

Theorem 2.8. [16] *The Four Dimensional Matching Problem is $\mathcal{NP}$-complete*

Proof. (1) Four Dimensional Matching Problem is in $\mathcal{NP}$:
As certificate, use a given matching. Then, to verify, just check that each element of W, X, Y, and Z are touched exactly once, and that all the quadruples used are valid. This is easily done in polynomial time.
(2) Four Dimensional Matching Problem is complete:
Proof by reduction from the Three Dimensional Matching Problem.
For a given Three Dimensional Matching Problem over disjoint sets X, Y, and Z, $|X| = |Y| = |Z|$ with a set of valid triples T, construct a Four Dimensional Matching problem by creating a set $W, |W| = n$. Create a 1-to-1 correspondence between elements of W and X, so that w_i is paired with x_i. Then create a set of quadruples $Q = \{(w_j, x_j, y_k, z_l) | (x_j, y_k, z_l) \in T\}$.

So, if there exists a solution to the Four Dimensional Matching Problem, then the corresponding triples form a solution to the Three Dimensional Matching Problem, and vice versa. □
□

Example 2.9. Now, let us give an illustration in order to show the relation between the SDP and the FDMP. Let $T = \{1, 2, 3, 4\}$ and $U = \{U_1, U_2, U_3, U_4\}$ with $U_1 = (1, 2, 3, 4)$; $U_2 = (2, 1, 4, 3)$; $U_3 = (3, 4, 1, 2)$; $U_4 = (4, 3, 2, 1)$. To relate the FDMP to the SDP, we introduce the incidence matrix A of size $\mid U \mid \times 4 \mid T \mid = 4 \times 16$. We construct this matrix by expressing every coordinates of each vector U_i, $i = \{1, 2, 3, 4\}$ in the basis {1, 2, 3, 4} :

1	2	3	4
1	0	0	0
0	1	0	0
0	0	1	0
0	0	0	1

Then in this basis : $1 = 1000 \quad 2 = 0100 \quad 3 = 0010 \quad 4 = 0001$, we obtain the matrix A (the i^{th} row in A corresponds to U_i in the basis {1, 2, 3, 4} $1 \leq i \leq 4$) :

$$A = \left(\begin{array}{cccc|cccc|cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{array}\right)$$

The matrix A has four 1 per line, one for each coordinate, in the column corresponding to the correct element of T. With this new representation of the set U corresponding to the matrix A, a valid solution to the FDMP is the existence of $\mid T \mid$ rows of A whose mod 2 sum is (1, 1, ... 1, 1). We will now show that the SDP is $\mathcal{NP}$-complete by reducing FDMP to it. Let us define this reduction :
Suppose that we had a polynomial-time algorithm for the SDP (called β). Given an input : $U \subseteq T \times T \times T \times T$ for the FDMP, let A be the $|U| \times 4|T|$ incidence matrix described above. Then running β with inputs $H = A$, $S = (1, 1, 1, \ldots, 1, 1)$, and $w = |T|$, we would see, in polynomial time, whether the matching existed or not. When we find a solution y to SDP, we can find from y the solution of the FDMP. Indeed, each position i of the non zero elements of y is the index of the element U_i of U, obtained from the row i of A and thus the solution of the FDMP is the set W of these U_i. So the solution of the SDP can be transformed into a solution of the FDMP. This proves that the SDP is $\mathcal{NP}$-complete.

2.4. **Quasi-dyadic codes.**

2.4.1. *Dyadic codes.* The dyadic codes are defined only for n a power of 2: $n = 2^r$, $r \in \mathbb{N}$.
For any integer $i \in \{0, 1, 2, \ldots 2^r - 1\}$, let $[i] = (i_{r-1}, i_{r-2}, \ldots i_1, i_0)$ denotes its radix-2 representation, where :

$$i = i_{r-1}2^{r-1} + i_{r-2}2^{r-2} + \ldots + i_1 2^1 + i_0 2^0 \text{ with } i_j = \{0, 1\} \text{ for } j \in \{0, 1, \ldots, r-1\}$$

Radix-2 addition of two numbers i and j denoted by $i \oplus j$ is defined in [15] by:

$$i \oplus j = k \text{ where } k_\ell = (i_\ell + j_\ell) \mod 2 \quad \forall \ell \in \{0, \ldots, r-1\}.$$

Definition 2.10. The *m-dyadic shift*, $m = 0, 1, \ldots, n-1$, of a vector $(a_0, a_1, \ldots, a_{n-1})$ is the vector: $(a_{0\oplus m}, a_{1\oplus m}, \ldots, a_{n-1\oplus m})$

Example 2.11. Let us take the vector of length 4: (a_0, a_1, a_2, a_3).
The 3-dyadic shift applied to this vector gives $(a_{0\oplus 3}, a_{1\oplus 3}, a_{2\oplus 3}, a_{3\oplus 3}) = (a_3, a_2, a_1, a_0)$.
The 3-dyadic shift applied to $(0, 1, 0, 1)$ gives $(1, 0, 1, 0)$.

Definition 2.12. We call a linear code of length $n = 2^r$ on a field $\mathbb{F}$, a *dyadic code* if the m-dyadic shift on each codeword is a codeword $\forall m \in \{0, \ldots, n-1\}$.

2.4.2. *Dyadic matrix.*

Definition 2.13. Given a ring $\mathcal{R}$ and a vector $h = (h_0, \ldots, h_{n-1}) \in \mathcal{R}^n$, the dyadic matrix $\delta(h) \in \mathcal{R}^{n\times n}$ is the symmetric matrix with components $\delta_{ij} = h_{i\oplus j}$. The sequence h is called its signature. A dyadic matrix is symmetric.

Remark 2.14. A dyadic code is a code whose parity check matrix is dyadic.

2.4.3. *Quasi-dyadic codes.* Suppose that each codeword is subdivided in blocks of same length.

Definition 2.15. A code is said *m-quasi-dyadic* if the m-dyadic-shift applied on all blocs of each codeword is a codeword.

2.4.4. *Quasi-dyadic matrix.*

Definition 2.16. A quasi-dyadic matrix is a (possibly non-dyadic) block matrix whose component blocks are dyadic sub-matrices.

Definition 2.17. A quasi-dyadic code is a linear error-correcting code that admits a quasi-dyadic parity-check matrix. A quasi-dyadic code is of length $n = \ell 2^r$, $\ell \in \mathbb{N}^*$ and ℓ is the number of blocs of the codewords.

The parameters of quasi dyadic codes are:

$n = \ell 2^s$ with $\ell \in \mathbb{N}^*, s \in \mathbb{N}$ and $k = (\ell - m)2^s$ with $m \in \mathbb{N}^*$ and $\ell > m$

. For more details on quasi-dyadic codes, the reader is invited to read [2].

2.5. **The Kronecker Product.** Let A be a $k \times \ell$ matrix, and let B be a $m \times n$ matrix.

Definition 2.18. The *Kronecker product* of A and B (denoted $A \otimes B$) is the $km \times \ell n$ matrix:

$$A \otimes B := \begin{pmatrix} a_{1,1}B & a_{1,2}B & \cdots & a_{1,\ell}B \\ a_{2,1}B & a_{2,2}B & \cdots & a_{2,\ell}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{k,1}B & a_{k,2}B & \cdots & a_{k,\ell}B \end{pmatrix},$$

where $a_{h,j}$ denotes the element of A in row h and column j. Note that the Kronecker product of two matrices is another matrix, usually a much larger one (see [11])

3. Results

In this section, we will construct a reduction from the Four Dimensional Matching Problem (FDMP) which is also $\mathcal{NP}$-complete [16], to prove that the random binary quasi-dyadic Coset Weight Problem is $\mathcal{NP}$-complete.

3.1. The random binary Quasi-dyadic Coset Weight Problem (QDCWP).

The CWP for random binary quasi-dyadic codes can be formulated as follows:
Let $l > 1$, $s, m \in \mathbb{N}^*$, $l > m$, $n = l \times 2^s$, $k = (l-m) \times 2^s$, a non negative integer $w \leq n$ and a vector $S \in \mathbb{F}_2^{m2^s}$.

Input: Let H be a random binary quasi-dyadic matrix of length $n \times (n-k)$.

*Property:*Does it exist $y \in \mathbb{F}_2^n$ of weight $wt(y) \leq w$ such that $yH = S$?

Theorem 3.1. *The QDCWP is NP-complete.*

Before the proof of this theorem, we give its different steps:

- First, let $U \subseteq T \times T \times T \times T$ where T is a finite set, be the inputs of FDMP.
- For each vector U_i of U, we express each coordinate in the basis T (see Example. 2.9) which gives us the vector h_i.
- With the vectors h_i, we construct a matrix H whose row i is the vector h_i. From H now, we construct a quasi-dyadic matrix H' by using the Kronecker product. This matrix H' will be the input of the QDCWP.
- We take as inputs of the QDCWP: the quasi-dyadic matrix H' and $S = (1, 1, \ldots, 1, 1)$ and prove that a solution of the QDCWP with these inputs can be transform into a solution of the FDMP.

That will prove the $\mathcal{NP}$-completeness of the random binary quasi-dyadic Coset Weight Problem.

Proof. We prove the $\mathcal{NP}$-completeness of the QDCWP by reducing the FDMP to it. Here is the reduction.
• Let us assume an algorithm γ is able to solve any instance of the QDCWP.
• Start from an instance U of the FDMP.
Let $U \subseteq T \times T \times T \times T$, where T is a finite set, be the inputs of FDMP.
• Convert this instance U to an instance H' of QDCWP.
For each vector U_i of U ($i \in \{1, 2, \ldots |U|\}$), we express each of its coordinates in the basis T (as in the Example. 2.9) which gives the vector h_i of length $4|T|$. We can construct a matrix H whose row i is the vector h_i, $i \in \{1, 2, \ldots |U|\}$. H is a $|U| \times 4|T|$ matrix (see Fig. 1). From this matrix H we construct the quasi-dyadic matrix H' such that $H' = H \otimes I_2$ (where $\otimes$ represents the Kronecker product and I_2 the identity matrix of size 2×2) with blocks $H'_{ij} = H_{ij}I_2$. H' (see Fig. 2), which will be the input of the QDCWP, is a quasi-dyadic matrix of size $2|U| \times (2 \times 4|T| = 8|T|)$ composed by identity matrices and null matrices, of size 2×2, which are dyadic . • Solve the QDCWP with the inputs H' and $S = (1, 1, \ldots, 1, 1)$ (S with $8|T|$ ones (1)), using γ to obtain a solution y.
Running the algorithm γ with the inputs H' and $S = (1, 1, \ldots, 1, 1)$ (S with $8|T|$ ones (1)), we will find out in polynomial time whether the matching existed or

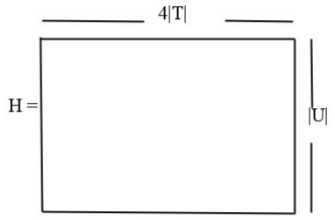

FIGURE 1. Matrix H.

FIGURE 2. Quasi-dyadic matrix H' used to reduce FDMP to QDCWP.

not.
A solution to the QDCWP, with H' and S as inputs, is a vector y of weight $2|T|$ such that $yH' = S$, thus find the solution y is equivalent to find $2|T|$ lines of H' whose sum gives S. The solution y is a vector of length $2|U|$ which contains $2|T|$ non zero elements at the positions corresponding to the positions of the $2|T|$ lines summed.
• Convert this solution y of the QDCWP into a solution W of the FDMP.
From the solution y of the QDCWP, we can find the solution of the FDMP. Indeed first, we construct a vector y' of length $|U|$ such that $y'_i = y_{i\times 2}$, $0 \leq i \leq |U| - 1$. We are interested now in the positions j of the non zero elements of y' (the vector y' has $|T|$ non zero elements), second we search in H the row j to form a vector V_j ($j \in \{0, 1, 2, \ldots, |U| - 1\}$). Thus we will obtain $|T|$ vectors V_j. Now, let us denote W the set composed by these $|T|$ vectors V_j, the set W is the solution of the FDMP.
If one day it exists a polynomial time algorithm able to solve the QDCWP that implies the existence of a polynomial time algorithm to solve the FDMP.
This proves that the random binary quasi-dyadic Coset Weight Problem is $\mathcal{NP}$-complete. □

3.2. **The random binary Quasi-dyadic Subspace Weight Problem (QDSWP).**
The SWP for random binary quasi-dyadic codes can be formulated as follows:
Let $l > 1$, $s, m \in \mathbb{N}^*$, $l > m$, $n = l \times 2^s$, $k = (l - m) \times 2^s$ and a non negative integer $w \leq n$.

*Input:*Let H be a random binary quasi-dyadic matrix of length $n \times (n - k)$.

*Property:*Does it exist a codeword $c \in \mathbb{F}_2^n$ of weight $wt(c) = w$ such that $cH = 0$?

Theorem 3.2. *The QDSWP is NP-complete.*

Proof. We prove the $\mathcal{NP}$-completeness of the QDSWP by reducing the FDMP to it. Here is the reduction.

• Let us assume an algorithm β is able to solve any instance of the QDSWP.

• Start from an instance U of the FDMP.

Let $U \subseteq T \times T \times T \times T$, where T is a finite set, be the inputs of FDMP.

• Convert this instance U to an instance H_1' of QDSWP.

For each vector U_i of U ($i \in \{1, 2, \dots |U|\}$), we express each of its coordinates in the basis T (as in the Example. 2.9) which gives the vector h_i of length $4|T|$. We can construct a matrix H (like in the previous proof) whose row i is the vector h_i, $i \in \{1, 2, \dots |U|\}$. H is a $|U| \times 4|T|$ matrix (see Fig. 3).

From this matrix H, we will construct the matrix H_1 below (see Fig. 4).

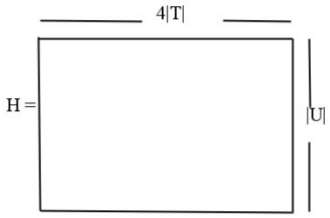

FIGURE 3. Matrix H.

The matrix H_1 is constructed as follows:

H_1 is a $(4|T|(U|+1)+|U|)\times(4|T|(|U|+1))$ matrix with the $|U|$ top rows consisting of H followed by $4|T|$ copies of identity matrices of size $|U|$ and the $4|T|(|U|+1)$ low rows forming an identity matrix of size $4|T|(|U|+1)$.

From the matrix H, we construct like in the previous proof, the $2|U| \times 8|T|$ matrix H' such that $H' = H \otimes I_2$ (where $\otimes$ represents the Kronecker product and I_2 the identity matrix of size 2×2) with blocks $H'_{ij} = H_{ij}I_2$ (see Fig. 5).

Now from H', we construct the quasi-dyadic matrix H" (see Fig. 6) which will be the input of the QDSWP. H" is a $(8|T|(U| + 1) + 2|U|) \times (8|T|(|U| + 1))$ quasi-dyadic matrix just constructed by replacing H by H' in H_1.

• Solve the QDSWP with the inputs H" and $w = 2|T| + 8|T|(|U| + 1)$, using β to obtain a solution c.

Running the algorithm β with the inputs H" and and $w = 2|T| + 8|T|(|U| + 1)$, we will find out in polynomial time whether the matching existed or not.

A solution to the QDSWP, with H" and w as inputs, is a vector c of weight w such that $cH = 0$, thus find the solution c is equivalent to find $2|T|+8|T|(|U|+1)$ lines of H" whose sum gives 0. We will choose among the $2|U|$ first lines of H", $2|T|$ lines whose sum give $S_1 = (1, 1, \dots, 1, 1)$ (S_1 with $8|T|(|U|+1)$ ones (1)). So to make this sum null we will add the $8|T|(|U| + 1)$ last lines of H" (all the lines of the lower identity matrix) that will give us the null sum we search. Therefore to find a null sum of H" lines we will add $2|T|$ lines (among the $2|U|$ first lines of H") whose sum will give S_1 and the $8|T|(|U| + 1)$ last lines of H" which gives a total of $2|T| + 8|T|(|U| + 1)$ lines of H" added. The solution c is a vector of length $2|U| + 8|T|(|U| + 1)$ which contains $2|T| + 8|T|(|U| + 1)$ non zero elements at the positions corresponding to the positions of the $2|T| + 8|T|(|U| + 1)$ lines

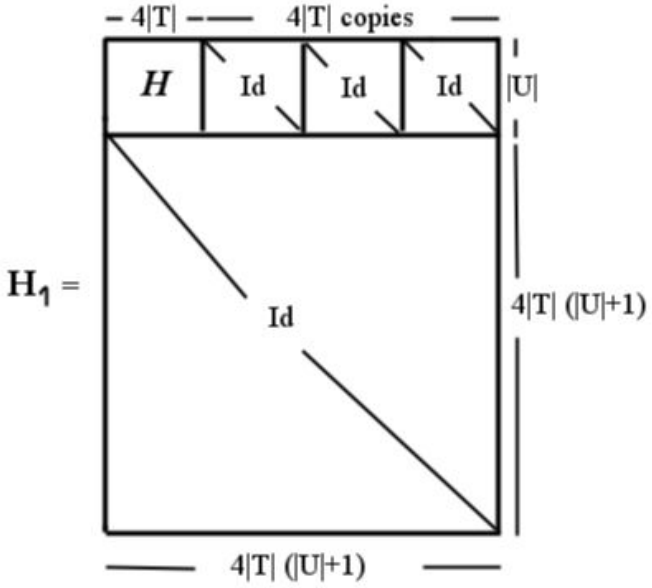

FIGURE 4. Matrix H_1.

FIGURE 5. Quasi-dyadic matrix H'.

summed.

• Convert this solution c of the QDSWP into a solution W' of the FDMP.

From the solution c of the QDSWP, we can find the solution of the FDMP. Indeed first, we construct a vector c' of length $|U| + 4|T|(|U| + 1)$ such that $c'_i = c_{i\times 2}$, $0 \leq i \leq (|U|+4|T|(|U|+1))-1$. We are interested in the positions k of the non zero elements of the $|U|$ first coordinates of c' (the $|U|$ first coordinates of the solution c' has $|T|$ non zero elements). Second we search in H_1 the line k and a vector W_k is formed from the $4|T|$ first elements of this line k ($k \in \{0; |U|-1\}$). Thus we will obtain $|T|$ vectors W_k. Now, let us denote W' the set composed by these $|T|$ vectors W_k, the set W' is the solution of the FDMP.

If one day it exists a polynomial time algorithm able to solve the QDSWP that implies the existence of a polynomial time algorithm to solve the FDMP.

This proves that the random binary quasi-dyadic Subspace Weight Problem is $\mathcal{NP}$-complete. □

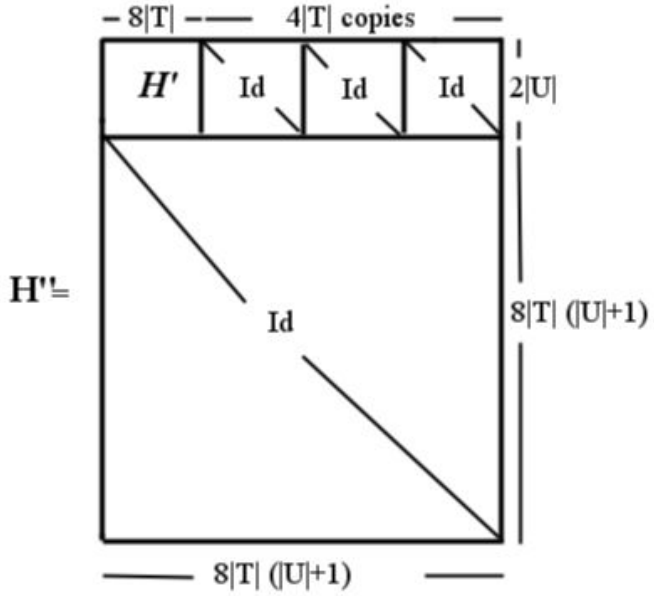

FIGURE 6. Quasi-dyadic matrix H" used to reduce FDMP to QDSWP.

As we have proven that the QDCWP and the QDSWP are NP-complete for random binary quasi-dyadic codes we can thus conclude that the Syndrome Decoding Problem is NP-complete for random binary quasi-dyadic codes.

4. Conclusion

We have extended Finiasz's results which prove the NP-completeness of certain sub-classes of the Syndrome Decoding Problem (SDP). Indeed, in this paper, we have proven the NP-completeness of the SDP for another class of codes: the random binary quasi-dyadic codes. We have, firstly, proven the NP-completeness of the random binary quasi-dyadic Coset Weight Problem (CWP) and secondly the NP-completeness of the random binary quasi-dyadic Subspace Weight Problem (SWP) by doing a constructive polynomial reduction of those problems to a NP-complete one: the Four Dimensional Matching Problem (FDMP). In the future, it will be interesting to study if the Syndrome Decoding Problem (both Coset Weight Problem and Subspace Weight Problem) is still NP-complete for other family of structured codes.

5. ACKNOWLEDGMENT

This work was carried out with financial support from the government of Canada's International Development Research Centre (IDRC), and within the framework of the AIMS Research for Africa Project and with financial support of the CEA-MITIC for CBC project. The authors are very very grateful to Professor A. Chillali and would like to thank Sidi Mohamed Ben Abdellah Univercity (USMBA), LSI and FP of Taza in MOROCCO for their valued supports.

References

1. C.Aguilar Melchor, S. Bettaieb, P. Gaborit, and J. Schrek; *A Code-Based Undeniable Signature Scheme*, IMA, Int. Conf, pp.99-119 (2013)
2. P. S. L. M. Barreto, P.-L. Cayrel, R. Misoczki, and R. Niebuhr; *Quasi-dyadic CFS signatures*, Inscrypt 2010, pp.336-349 (2010)
3. T. P. Berger; *Construction of dyadic MDS matrices for cryptographic applications*, in arxiv.org, (2014)
4. E. R. Berlekamp, R. J. McEliece and H. C. van Tilborg; *On the inherent intractability of certain coding problems*, IEEE IT, Vol. 24, no. 3, pp.384-386 (1978)
5. J-C Faugère, A. Otmani, L. Perret, F. de Portzamparc, J-P Tillich; *Structural weakness of compact variants of the McEliece cryptosystem*, IEEE International Symposium on Information Theory, pp. 1717-1721 (2014)
6. J. C. Faugère, A. Otmani, L. Perret, F. de Portzamparc, J. P. Tillich; *Structural Cryptanalysis of McEliece-Like Schemes with Symmetric Keys*, Designs, Codes and Cryptography, (2015)
7. J. C. Faugère, A. Otmani, L. Perret, J. P. Tillich; *Algebraic Cryptanalysis of McEliece Variants with Compact Keys*, Henri Gilbert, editor, EUROCRYPT, volume 6110 of Lecture Notes in Computer Science, pp. 279-298 (2010)
8. J. C. Faugère, L. Perret, F. de Portzamparc; *Algebraic Attack against Variants of McEliece with Goppa Polynomial of a Special Form*, In Palash Sarkar and Tetsu Iwata, editors, Advances in Cryptology - ASIACRYPT- 20th International Conference on the Theory and Application, (2014)
9. M. Finiasz; *$\mathcal{NP}$-completeness of Certain Sub-classes of the Syndrome Decoding Problem*, in arxiv.org, (2009)
10. R.M. Karp; *Reducibility among combinatorial Problems*, in Complexity of Computer Computations, Plenum, pp.85-103 (1972)
11. A.J. Laub; *Matrix analysis for scientists and engineers*, University of California, Chap 13 (2005)
12. R. Misoczki, P. S. L. M. Barreto; *Compact McEliece Keys from Goppa Codes*, Jacobson Jr., M.J., Rijmen, V., Safavi-Naini, R. (eds) SAC 2009, LNCS,vol 5867, pp. 376-392 (2009)
13. R. Niebuhr; *Critical attacks in code-based cryptography*, in WEWoRC 2011, (2011)
14. P.W.Shor; *Polynomial-Time Algorithm for Prime Factorization and Discrete Logarithms on a quantum computer*, SIAM Journal on Computing, Vol. 26(5), pp.1484-1509 (1997)
15. B. Sundar Rajan and M. H. Lee; *Quasi-Cyclic Dyadic Codes in the Walsh-Hadamard Transform Domain*, IEEE IT, Vol. 48, N. 8, pp.2406-2412 (2002)
16. http://bit.ly/1fpMxhf

[1]Université Cheikh Anta Diop, Faculté des Sciences et Techniques, DMI, LACGAA, Dakar, Senegal.
E-mail address: khady@aims-senegal.org

[2]Laboratoire Hubert Curien, UMR CNRS 5516 Bâtiment F 18 rue du professeur Benoît Lauras, 42000 Saint-Etienne, France.
E-mail address: pierre.louis.cayrel@univ-st-etienne.fr

[3]Université Cheikh Anta Diop, Faculté des Sciences et Techniques, DMI, LACGAA, Dakar, Senegal.
E-mail address: cheikht.gueye@ucad.edu.sn

A. Chillali, Sidi Mohamed Ben Abdellah University, FP, LSI, Taza, Morocco.
E-mail address: abdelhakim.chillali@usmba.ac.ma