Identification Of Quantum Encoder Matrix From A Collection Of Pauli Errors

Gilles Burel[(1)], Hugo Pillin[(1)], El-Houssaïn Baghious[(1)], Paul Baird[(2)], Roland Gautier[(1)]
[(1)] *University of Brest, Lab-STICC, CNRS, UMR 6285*, F-29200 Brest, France
[(2)] *University of Brest, LMBA, CNRS, UMR 6205*, F-29200 Brest, France
Contact: Gilles.Burel@univ-brest.fr

***Abstract*—Quantum information processing is a rapidly evolving field, due to promising applications in communications, cryptography, and computing. In this framework, there is a need to protect quantum information against errors, using quantum error-correcting codes. Efficient quantum codes, based on the stabilizer formalism (that exploits elements of the Pauli group), have been proposed. The stabilizer formalism allows one to simulate quantum codes and quantum errors using operations inside the Pauli group only, leading to huge gains in simulation time. However, to deeply study and simulate unconventional quantum errors and devices, there is a need to know the true quantum operator (represented by a unitary matrix). In this paper, we propose an algorithm, based on linear algebra, to identify the quantum encoder matrix from a collection of Pauli errors. The approach is two-steps. First, from a collection a Pauli errors whose matrix representation is diagonal, a search of common eigenvectors identifies the encoder matrix up to phase indeterminates. Second, additional Pauli errors with nondiagonal matrix representations are used to eliminate the remaining indeterminations. Simulation results are also provided to illustrate and validate the approach.**

***Index Terms*—quantum information, quantum error correction, Pauli errors, physical layer integrity**

I. Introduction

Protection of quantum information is a fundamental problem in the context of quantum communications and quantum computing. Experiments using optical fibers [1] and terrestrial free-space channels [2] have proved that transmission of quantum information can be achieved over distances as high as about 100 kilometers. Two years ago, transmission of quantum information between a ground observatory and a low-Earth-orbit satellite, over distances of up to 1,400 kilometers, was reported [3] [4]. These experiments constitute milestones on the path to a metropolitan - and even a global - quantum Internet. Quantum communications can also be integrated to a conventional IoT security infrastructure with an extra layer which is based on quantum state (as shown in [5] this quantum state prevents any sort of harmful actions from the eavesdroppers in the communication channel).

Quantum communication channels open new challenges in physical layer security and integrity [6]. As in the classical domain, quantum information can be protected through the use of redundancy and error correction codes. However, the quantum bits (qubits) which carry the information have significant differences with the conventional bits. These differences originate from the fundamental postulates of quantum physics (seen section II).

Efficient quantum codes, based on the stabilizer formalism (that exploits elements of the Pauli group) [7], have been proposed. In section III we show how quantum coding is carried out, and take the simplest efficient quantum code (a 5-qubit code) to illustrate this.

The stabilizer formalism, based on Pauli errors and operations in the Pauli group, allows efficient simulation of quantum codes. This formalism is built on the background results which show that, under some hypotheses, the quantum errors can be discretized [8]. While we will not go into details here, let just say that is has to do with the facts that (i) a measurement is carried out on the decoder side and (ii) every linear combination of correctable errors is also a correctable error. However, to be able to study and simulate unconventional quantum errors and devices, there is a need to know the true quantum encoder matrix. In this paper, we propose an algorithm, based on linear algebra, to identify the quantum encoder matrix from a collection of given Pauli errors. In section IV we present the proposed approach, which was designed to use only basic linear algebra tools, available in any scientific software. Then, simulation results are provided in section V to illustrate and validate the algorithm: we check that the method is able to identify the encoding matrix of a known code (a 5-qubit code) from a collection of Pauli errors.

II. Quantum bits and quantum coding

A. Quantum bits (qubits) and qubit registers

There are two main differences between bits and qubits, which take their origin in quantum state superposition and quantum entanglement.

First, due to the superposition principle, a qubit is not restricted to either 0 or 1, but can be any superposition of these two basic states. Mathematically, using Dirac notation, this is written:

$$|\varphi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle \tag{1}$$

where α_0 and α_1 are arbitrary complex coefficients subject to $|\alpha_0|^2 + |\alpha_1|^2 = 1$. Physically any 2D quantum system can carry a quantum bit. For instance, the spin of an electron is a 2D quantum system, and the spin up and down can be associated to the basic states $|0\rangle$ and $|1\rangle$. Therefore, once the

basis vectors $|0\rangle$ and $|1\rangle$ are chosen, a qubit can be seen as a unit vector in $\mathbb{C}^2$.

The quantum state of a collection of n independent qubits is the tensor product $\otimes$ of the individual quantum states. For instance, for a collection of 2 independent qubits, we have:

$$|\varphi\rangle = (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle) \quad (2)$$

This state can be developed as:

$$|\varphi\rangle = \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle \quad (3)$$

where $|ab\rangle = |a\rangle \otimes |b\rangle$.

Second, due to quantum entanglement, a collection of n qubits (let us call it an n-qubit register) is not always separable into individual qubits. That is, we cannot consider a qubit independently of the qubits with which it is entangled. This is a pure quantum phenomena which has no equivalent in the classical world. To illustrate this, consider a 3-qubit register. The basic states of this register are $\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$. Therefore, the quantum state of the register is:

$$|\varphi\rangle = \sum_{(a,b,c)\in\{0,1\}^3} \alpha_{abc} |abc\rangle \quad (4)$$

where α_{abc} are arbitrary complex coefficients subject to

$$\sum_{(a,b,c)\in\{0,1\}^3} |\alpha_{abc}|^2 = 1 \quad (5)$$

Here, $|\varphi\rangle$ can be seen as a unit vector in $\mathbb{C}^8$.

It is easy to see that, except in some special cases, the quantum state of the register is not separable, i.e. usually we cannot factorize (4) into:

$$|\varphi\rangle = (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle) \otimes (\gamma_0 |0\rangle + \gamma_1 |1\rangle) \quad (6)$$

It is quantum entanglement, much more than superposition, that makes quantum communications and quantum computation so promising. Indeed, due to quantum entanglement, the quantum state of an n-qubit register lives in a 2^n-dimensional space, and cannot be decomposed into a collection of n states living in 2-dimensional spaces. So, the quantum state is described by 2^n (instead of $2n$) complex coefficients.

Therefore, in the following, we will consider the quantum state of an n-qubit register as a vector living in a Hilbert space $\mathcal{H}$ of dimension 2^n, which will be associated to $\mathbb{C}^{2^n}$.

B. Operations on qubit registers

Due to the Schrödinger equation, the evolution of a quantum system is always described by a unitary matrix (with complex entries) that operates in the state space. Hence, any evolution of an n-qubit register is described by a $2^n \times 2^n$unitary matrix. It follows that any quantum operation is reversible.

Usually, for practical realization, the desired evolution operator is decomposed into basic operators which operate on 1 or 2 qubits only, and which are called "quantum gates". This is similar to digital electronics in which complex circuits are built on basic gates (such as NAND, NOT, etc.) which operate on 1 or 2 bits only. A quantum gate which operates on 1 qubit is described by a 2×2 unitary matrix, and a quantum gate which operates on 2 qubits is described by a 4×4 unitary matrix.

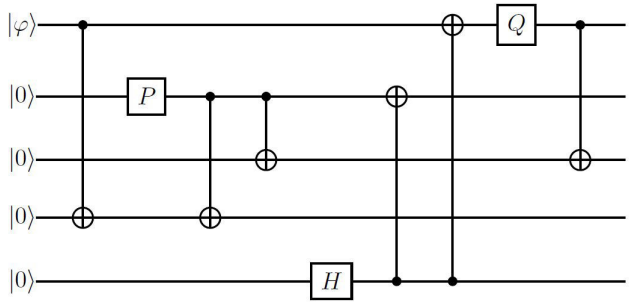

Fig. 1. 5-qubit encoder.

A quantum error itself is described by a unitary operator. The Pauli errors, which are a foundation of quantum coding theory, are described by the matrices below:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (7)$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (8)$$

$$Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \quad (9)$$

Together with the identity matrix I, and the multiplicative factors $\{-1, +1, -i, +i\}$ they form a group known as the Pauli group.

An example of quantum circuit is the 5-qubit quantum encoder (Fig. 1) described in [9]. It encodes $k = 1$ qubit into $n = 5$ entangled qubits and protects against an arbitrary single-qubit error.

The quantum gates that operate on one qubit are:

$$H = \frac{1}{\sqrt{2}}(X + Z) \quad (10)$$

$$Q = \frac{1}{\sqrt{2}}(Y + Z) \quad (11)$$

$$P = HQ \quad (12)$$

The quantum gate that operates on 2 qubits is known as Controlled-NOT (CNOT, Fig. 2). In the standard basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ its matrix representation is:

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (13)$$

That is, if the CNOT input state is

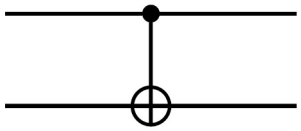

Fig. 2. CNOT quantum gate

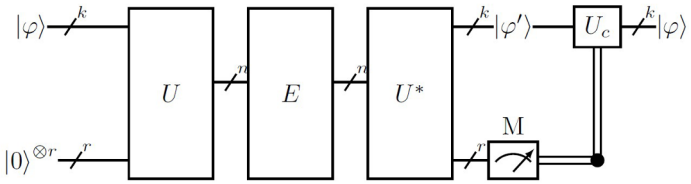

Fig. 3. Principle of quantum coding.

$$|\varphi\rangle = \sum_{(a,b)\in\{0,1\}^2} \alpha_{ab} |ab\rangle \tag{14}$$

Then, the output state is obtained from

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{11} \\ \alpha_{10} \end{pmatrix} \tag{15}$$

That is

$$|\psi\rangle = \sum_{(c,d)\in\{0,1\}^2} \alpha_{c,c+d} |cd\rangle \tag{16}$$

where $c+d$ is the addition modulo 2.

From this description it is easy to obtain the coding matrix U, which, in this case, is a $2^5 \times 2^5$matrix.

C. Measurement

Another fundamental operation is measurement. It transforms a quantum state into a classical state. According to the postulates of quantum physics, the result of measurement is probabilistic. For instance, measurement of the qubit described by (1) will produce classical state 0 with probability $|\alpha_0|^2$ and classical state 1 with probability $|\alpha_1|^2$. Since the quantum state is a unit vector, the sum of probabilities is always 1.

Any measurement requires first to decompose the state space into a direct sum of subspaces. For simple systems, such as a qubit, this is usually implicit. When we just say that a qubit is measured, it is implicit that the subspaces are the 1-D subspaces generated by the basic states $|0\rangle$ and $|1\rangle$.

Measurement of a more complex system, such as an n-qubit register, requires being more precise about what we measure. For instance, consider a 3-qubit register in which we want to measure the second and third qubits. Expressed in the language of linear algebra, this means that we decompose the 8-dimensional state space into a direct sum of four 2D subspaces:

$$\mathcal{H} = \mathcal{H}_{00} \oplus \mathcal{H}_{01} \oplus \mathcal{H}_{10} \oplus \mathcal{H}_{11} \tag{17}$$

where a basis of $\mathcal{H}_{bc}$ is $\{|0bc\rangle, |1bc\rangle\}$

The measurement will produce classical state bc with probability $|\alpha_{0bc}|^2 + |\alpha_{1bc}|^2$

After measurement, the quantum state of the first qubit becomes:

$$|\varphi\rangle = \frac{\alpha_{0bc}}{|\alpha_{0bc}|^2 + |\alpha_{1bc}|^2} |0\rangle + \frac{\alpha_{1bc}}{|\alpha_{0bc}|^2 + |\alpha_{1bc}|^2} |1\rangle \tag{18}$$

That is, the quantum state is projected onto $\mathcal{H}_{bc}$ and renormalized (to keep a unit norm).

III. Principle of quantum coding

The principle of quantum coding is shown in Fig. 3. We append $r = n - k$ ancillary qubits to the k-qubit register that we want to protect. A quantum circuit, modelized by a unitary matrix U (encoder), produces a highly entangled state. Errors are modelized by unitary matrix E and the decoder is another quantum circuit modelized by the Hermitian transpose of U. On the decoder side, we measure the r last qubits, to obtain an r-bit classical register called the syndrome. According to the syndrome, the proper quantum correction circuit U_c is selected.

IV. Description of the method

A. Specification of the problem

The problem we address in this paper can be stated as follows: given a list of Pauli errors E_i with their equivalent errors F_i, determine the unitary operator U such that:

$$U^* E_i U = F_i \tag{19}$$

Or, equivalently:

$$U F_i U^* = E_i \tag{20}$$

where U^* stands for the Hermitian transpose of U.

Note that when F_i is diagonal, the columns of U are the eigenvectors of E_i.

B. First step

In this step, we use n independent equations in which each F_i is a tensor product of I and Z only (including at least one Z). Therefore, matrices F_i are diagonal, and their diagonal elements are $+1$ and -1 only. Since the F_i commute, the E_i commute also. This is a direct consequence of (20):

$$\begin{aligned} E_j E_i &= (U F_j U^*)(U F_i U^*) \\ &= U F_j F_i U^* \\ &= U F_i F_j U^* \\ &= (U F_i U^*)(U F_j U^*) \\ &= E_i E_j \end{aligned} \tag{21}$$

The approach below takes profit of the fact that commuting operators possess a set of common eigenvectors.

As an illustration, let us consider $n = 3$ and the matrices below. For economy of notation, $+$ and $-$ stand for $+1$ and

-1 respectively, and "diag" returns a square diagonal matrix with the elements of the specified vector on the main diagonal.

$$\begin{aligned} F_1 &= Z \otimes I \otimes I \\ &= \text{diag}(\begin{bmatrix} + & + & + & + & - & - & - & - \end{bmatrix}) \end{aligned} \tag{22}$$

$$\begin{aligned} F_2 &= I \otimes Z \otimes I \\ &= \text{diag}(\begin{bmatrix} + & + & - & - & + & + & - & - \end{bmatrix}) \end{aligned} \tag{23}$$

$$\begin{aligned} F_3 &= I \otimes I \otimes Z \\ &= \text{diag}(\begin{bmatrix} + & - & + & - & + & - & + & - \end{bmatrix}) \end{aligned} \tag{24}$$

Since matrix U doesn't depend on i in (20) its columns are common eigenvectors of the E_i. For instance, in the example above, the second column of U is a common eigenvector of E_1, E_2 and E_3 associated to eigenvalues $+1$, $+1$ and -1.

Let us note $\Upsilon_i^+$and Υ_i^- the eigenspaces corresponding to eigenvalues $+1$ and -1 of E_i. The dimension of these eigenspaces is exactly 2^{n-1} .

Since U is unitary, these eigenspaces are orthogonal. Furthermore, since the eigenvalues are $+1$ and -1 only, their direct sum is the whole space:

$$\Upsilon_i^+ \oplus \Upsilon_i^- = \mathcal{H} \tag{25}$$

As an example to explain the method, let us set u to be the second column of U. We have:

$$u \in \Upsilon_1^+ \cap \Upsilon_2^+ \cap \Upsilon_3^- \tag{26}$$

Which, on account of the discussion above, is equivalent to:

$$u \notin \Upsilon_1^- \cup \Upsilon_2^- \cup \Upsilon_3^+ \tag{27}$$

The dimension of $\Upsilon_1^+ \cap \Upsilon_2^+ \cap \Upsilon_3^-$ is 1 (see (22) to (24)), so u is determined up to a multiplicative factor.

From the eigendecomposition of E_i, we obtain orthogonal bases of Υ_i^+ and Υ_i^-. Let us note $M_i^\pm$ the matrices whose columns are the vectors of these bases. The sizes of these matrices are $(2^n \times 2^{n-1})$.

We create a $(2^n \times n2^{n-1})$ matrix M such that

$$M = \begin{bmatrix} M_1^- & M_2^- & M_3^+ \end{bmatrix} \tag{28}$$

The columns of M generate $\Upsilon_1^- \cup \Upsilon_2^- \cup \Upsilon_3^+$. The dimension of this subspace is $2^n - 1$ because the dimension of its complement is 1, as can be seen from the choice of the F_i. Hence, the rank of M is $2^n - 1$ and the dimension of its nullspace is 1.

Then, we compute a *unitary* vector u such that

$$u^* M = 0 \tag{29}$$

This vector u is in the nullspace of M. Therefore, it is a solution of (27).

To compute u, we can use the Singular Value Decomposition (SVD) of M

$$M = QSV^* \tag{30}$$

and take u as the last column of Q. Indeed, the last column of Q is a unit vector (because Q is unitary) and it is in the nullspace of M (because M is not full-rank).

Here, for sake of simplicity, we have explained how to obtain the second column of U in the 3-qubit case. It is straightforward to generalize the approach to other columns and other values of n. Basically, one just has to adapt (28) and select the correct upper signs in the $M_i^\pm$ according to the number of the column:

$$M = \begin{bmatrix} M_1^\pm & M_2^\pm & \cdots & M_n^\pm \end{bmatrix} \tag{31}$$

It is not necessary that the F_i contains one Z only. For instance, the example below would also produce a result

$$\begin{aligned} F_1 &= Z \otimes Z \otimes I \\ &= \text{diag}(\begin{bmatrix} + & + & - & - & - & - & + & + \end{bmatrix}) \end{aligned} \tag{32}$$

$$\begin{aligned} F_2 &= I \otimes Z \otimes Z \\ &= \text{diag}(\begin{bmatrix} + & - & - & + & + & - & - & + \end{bmatrix}) \end{aligned} \tag{33}$$

$$\begin{aligned} F_3 &= I \otimes I \otimes Z \\ &= \text{diag}(\begin{bmatrix} + & - & + & - & + & - & + & - \end{bmatrix}) \end{aligned} \tag{34}$$

The only condition is that the equations be independent, i.e. the matrix D formed by stacking the diagonals of the F_i do not contain identical columns:

$$D = \begin{pmatrix} + & + & - & - & - & - & + & + \\ + & - & - & + & + & - & - & + \\ + & - & + & - & + & - & + & - \end{pmatrix} \tag{35}$$

C. Second step

After step 1, there remains an indetermination. Indeed, let us note Λ a unitary diagonal matrix and $\widetilde{U}$ the matrix U found in step 1. Because the F_i used in step 1 are diagonal, they commute with Λ. Then, it is easy to prove that, in that case, any $U = \widetilde{U}\Lambda$ is also a solution of (20):

$$\begin{aligned} UF_iU^* &= \widetilde{U}\Lambda F_i \Lambda^* \widetilde{U}^* \\ &= \widetilde{U}\Lambda\Lambda^* F_i \widetilde{U}^* \\ &= \widetilde{U}F_i\widetilde{U}^* \\ &= E_i \end{aligned}$$

To suppress this indetermination, let us use n equations in which each F_i is a tensor product of I and X only. As an illustration, let us consider $n = 3$ again and the matrices below (only nonzero elements are displayed):

$$\begin{aligned} F_4 &= X \otimes I \otimes I \\ &= \begin{pmatrix} & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \end{pmatrix} \end{aligned} \tag{36}$$

$$F_5 = I \otimes X \otimes I$$
$$= \begin{pmatrix} & & 1 & & & & & \\ & & & 1 & & & & \\ 1 & & & & & & & \\ & 1 & & & & & & \\ & & & & & & 1 & \\ & & & & & & & 1 \\ & & & & 1 & & & \\ & & & & & 1 & & \end{pmatrix} \quad (37)$$

$$F_6 = I \otimes I \otimes X$$
$$= \begin{pmatrix} & 1 & & & & & & \\ 1 & & & & & & & \\ & & & 1 & & & & \\ & & 1 & & & & & \\ & & & & & 1 & & \\ & & & & 1 & & & \\ & & & & & & & 1 \\ & & & & & & 1 & \end{pmatrix} \quad (38)$$

Let us note $\widetilde{F}_i = \widetilde{U}^* E_i \widetilde{U}$. Then, (19) is equivalent to

$$\Lambda^* \widetilde{F}_i \Lambda = F_i \quad (39)$$

Set a and b to be the row and column indices. We have:

$$e^{-j\theta_a} \widetilde{F}_i(a,b) e^{j\theta_b} = F_i(a,b) \quad (40)$$

Then, when $F_i(a,b) \neq 0$ we can compute θ_a from θ_b:

$$e^{j\theta_a} = \frac{\widetilde{F}_i(a,b)}{F_i(a,b)} e^{j\theta_b} \quad (41)$$

The strategy is as follows:

1) Choose θ_1 (arbitrary)
2) Select i such that $F_i = I \otimes \cdots \otimes I \otimes I \otimes X$ (i.e. $i = 6$ in the example above). We have $F_i(2,1) = 1$ then we can compute θ_2 from θ_1
3) Select i such that $F_i = I \otimes \cdots \otimes I \otimes X \otimes I$ (i.e. $i = 5$ in the example above). We have $F_i(3,1) = 1$ and $F_i(4,2) = 1$ then we can compute θ_3 from θ_1 and θ_4 from θ_2
4) and so on, until the whole diagonal of Λ is determined.

We can remark that the number of elements being determined is multiplied by 2 each time, then using n equations is sufficient to determine the 2^n diagonal elements of Λ.

Eventually, there remains a global phase indertermination, because θ_1 has been chosen arbitrarily. This is not a problem, because in quantum physics the global phase has no significance.

V. Simulation Results

In order to illustrate and validate the approach, let us consider the collection of Pauli errors shown in Table I. Here, in order to be able to check the results, this collection has been computed using the 5-qubit encoder circuit (Fig. 1), while in a standard application of the method it would be given a priori. Also, still for verification purpose, the true matrix U shown in Fig. 4 and Fig. 5 has been computed using the encoder circuit.

TABLE I
Collection of Pauli errors

E_i	F_i
$Y \otimes I \otimes X \otimes I \otimes Z$	$Z \otimes I \otimes I \otimes I \otimes I$
$-I \otimes Y \otimes X \otimes X \otimes Z$	$I \otimes Z \otimes I \otimes I \otimes I$
$Z \otimes Z \otimes Z \otimes I \otimes Z$	$I \otimes I \otimes Z \otimes I \otimes I$
$Y \otimes Z \otimes X \otimes Z \otimes I$	$I \otimes I \otimes I \otimes Z \otimes I$
$-X \otimes X \otimes X \otimes I \otimes X$	$I \otimes I \otimes I \otimes I \otimes Z$
$-X \otimes I \otimes X \otimes X \otimes I$	$X \otimes I \otimes I \otimes I \otimes I$
$-I \otimes Z \otimes I \otimes I \otimes Z$	$I \otimes X \otimes I \otimes I \otimes I$
$I \otimes I \otimes X \otimes I \otimes I$	$I \otimes I \otimes X \otimes I \otimes I$
$I \otimes I \otimes I \otimes X \otimes I$	$I \otimes I \otimes I \otimes X \otimes I$
$I \otimes I \otimes I \otimes I \otimes Z$	$I \otimes I \otimes I \otimes I \otimes X$

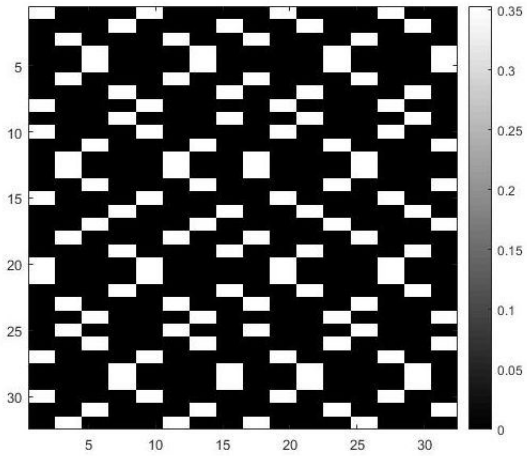

Fig. 4. True Matrix U (elements moduli) for the 5-qubit encoder.

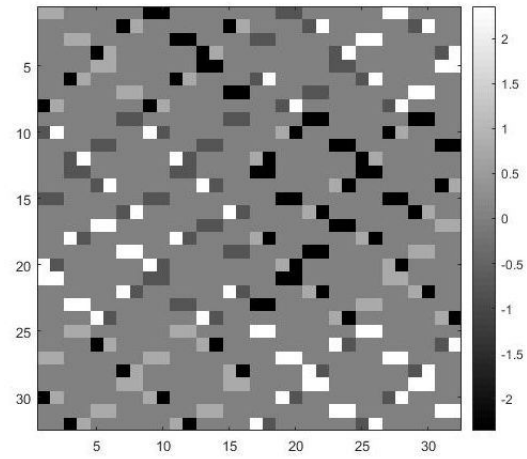

Fig. 5. True Matrix U (elements arguments) for the 5-qubit encoder.

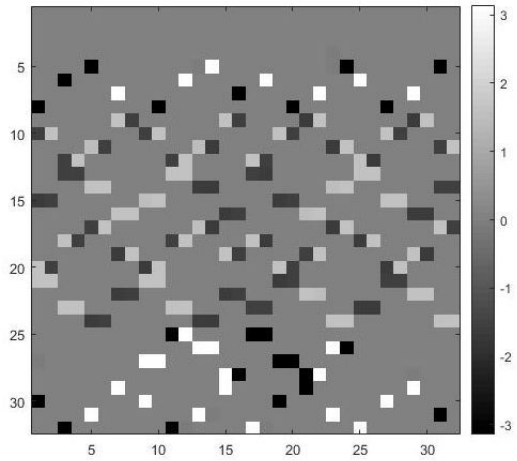

Fig. 6. Estimated Matrix U (elements arguments) after step 1.

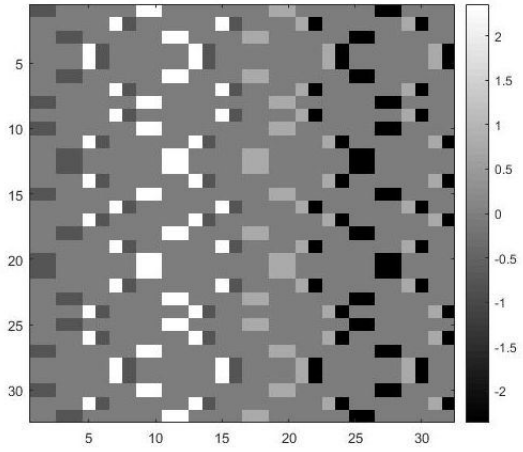

Fig. 7. Phase differences between estimated and true matrix U, after step 1

Using the given collection of errors, step 1 of the method produces a matrix U whose coefficients have moduli exactly the same as those of the true matrix (Fig. 4), but whose arguments (Fig. 6) do not correspond to that of the true matrix (Fig. 5).

If we compute the ratio, element by element, between the estimated matrix and the true matrix, we obtain a matrix whose elements arguments are shown on Fig. 7. By convention, the arguments of the ratios corresponding to null values in the true matrix are set to zero, since they do not matter. We can note that the non-cancelled values may differ from one column to another, but are identical inside a column.

After step 2, these remaining differences have been removed, and we obtain an estimated matrix U which is equal to the true matrix, up to a global phase. However, this remaining indetermination doesn't mater because, as said before, the global phase has no significance in quantum physics.

VI. Conclusion

The physical layer is the lowest layer in any communication protocol: it is concerned with generating, modulating, and transmitting signals. The recent field of quantum communications opens new challenges concerning security and integrity of the physical layer. In this paper we have proposed an approach, based on simple linear algebra tools, to identify the encoding matrix of a quantum code from a collection of Pauli errors. Knowledge of the encoding matrix is useful for simulation of the encoder without being restricted to hypotheses on the errors or on the correction capacity of the code. On a more speculative point of view, which will be part of our future work, it might also be useful in an interception context, helping one to identify the system used by a non-cooperative transmitter.

Acknowledgment

The authors thank the IBNM (Institut Brestois de l'Electronique et du Numérique), CyberIoT Chair of Excellence, for its support.

References

[1] Valivarthi, R. et al. "Quantum teleportation across a metropolitan fibre network", Nat. Photon. 10, 676–680 (2016)
[2] Yin, J. et al., "Quantum teleportation and entanglement distribution over 100-kilometre freespace channels", Nature 488, 185–188 (2012).
[3] Sheng-Kai Liao et al., "Satellite-to-ground quantum key distribution", Nature 549, 43–47 (2017)
[4] Ji-Gang Ren et al., "Ground-to-satellite quantum teleportation", Nature 549, 70–73 (2017)
[5] Md Samin Rahman, Md Hossam-E-Haider, "Quantum IoT: A Quantum Approach in IoT Security Maintenance", 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)
[6] Travis S. Humble, "Quantum Security for the Physical Layer", IEEE Communications Magazine 51 (8), 56-62 (August 2013)
[7] Robert Raussendorf, "Key ideas in quantum error correction". Phil. Trans. R. Soc. A, (2012) 370, 4541–4565
[8] Michael A. Nielsen & Isaac L. Chuang, "Quantum Computation and Quantum Information", Cambridge University Press, 2010
[9] Jin-Yuan Hsieh, Che-Ming Li, Der-San Chuu, "Analytical technique for simplification of the encoder–decoder circuit for a perfect five-qubit error correction", 2006, New J. Phys. 8 80