Algebraic decoding for classes of quantum codes

Yannick Saouter, Gilles Burel

Algebraic decoding for classes of quantum codes

Yannick Saouter
CODES team
Institut Mines Télécom Atlantique
Lab-STICC laboratory (CNRS UMR 6285)
Brest, France
https://orcid.org/0000-0001-7980-9168

Gilles Burel
SI3 team
University of Brest
Lab-STICC laboratory (CNRS UMR 6285)
Brest, France
https://orcid.org/0000-0002-1427-4577

***Abstract*—This paper describes a technique to perform the decoding of quantum Calderbank-Steane-Shor codes built from self-orthogonal classical binary codes possessing algebraic decoding procedures. This technique gives a viable alternative to syndrome decoding for codes with large minimum distance. The cases of Reed-Muller and BCH codes are examined. The new method is compared with syndrome decoding on illustrative examples. The asymptotic cost of both methods is also given.**

***Index Terms*—quantum code, algebraic decoding, CSS quantum codes.**

I. Introduction

Quantum technology is an active and promising research area. Possible applications cover many domains of science [1]–[6]. In the domain of quantum communication, qubit teleportation over 1 kilometer was recently announced [7]. Decoherence of qubits is one of the main problems in the domain of quantum technology. As for classical telecommunications, quantum error correcting codes have been proposed to combat this phenomenon [8]. This work has led to numerous constructions of codes. Large codes with sparse parity check matrices, known as quantum LDPC, can be decoded by the quantum belief propagation [9]. However, it is known that belief propagation algorithms have poor behavior with short codes and codes with dense parity check matrices. The most common alternative is syndrome decoding [10, §10.5.8]. The complexity of this technique grows exponentially with the correction power of the code. Recently, two other techniques have been proposed for the decoding of arbitrary quantum codes. In [11], [12], linear programming techniques are used. The decoding problem is then encoded as a $\{0,1\}$ integer linear programming optimization system. This system is then relaxed to a rational linear programming optimization instance, which can be solved by the simplex algorithm or in polynomial time by the Karmarkar algorithm. However, with the rational relaxation, the equivalence with the initial problem is lost. Therefore, there is no guarantee that the global procedure is able to correct any error pattern up to half the minimum distance. This problem can be solved by using branch and bound techniques or by the addition of cutting planes. The resolution of the optimization problem is then iterative and is able to correct any error configuration up to half the minimum distance. The drawback is that $\{0,1\}$ integer linear programming optimization is known to be a NP-complete problem. Therefore, the number of iterations required for success has an exponential upper bound in worst cases. In [13], decoding is performed by adapting the guessing random additive noise decoding (GRAND) procedure [14] to the context of quantum codes. The decoder hardware complexity is proven to be low and there is an exponential gain of time complexity for the Pauli depolarization channel with respect to the maximum likelihood decoder. However, the expected time for success remains still exponential with the length of the quantum error code. In this article, we propose a new alternative applicable for quantum CSS codes [15] built with classical codes having algebraic decoding procedures. This procedure is then compared with syndrome decoding for quantum Reed-Muller codes and quantum BCH codes. The paper is organized as follows. In section II, we summarize the theory of quantum coding. Then in section III, we focus on two fundamental families of quantum codes: stabilizer codes and CSS codes. Section IV presents the classical Reed-Muller and BCH codes. Our approach for algebraic decoding of quantum codes is developed in section V. Finally, in section VI, examples are provided and discussed.

II. Quantum transmission channel

We first introduce the basic notions and properties of quantum objects.

Definition 1 (Qubit)**.** *A qubit is a vector* $(\alpha, \beta) \in \mathbb{C}^2$ *such that* $|\alpha|^2 + |\beta|^2 = 1$.

Definition 2 (Quantum state)**.** *A quantum state of length n is a vector $(\alpha_1, \alpha_2, ..., \alpha_{2^n}) \in \mathbb{C}^{2^n}$ such that $\sum_{i=1}^{2^n} |\alpha_i|^2 = 1$.*

Therefore a qubit is a quantum state of length 1. Some particular quantum states need to be introduced. We will use the notations $|0\rangle = (1, 0)$ and $|1\rangle = (0, 1)$. Therefore we have $(\alpha, \beta) = \alpha |0\rangle + \beta |1\rangle$ and an arbitrary qubit is a weighted sum of $|0\rangle$ and $|1\rangle$ with norm equal to 1. Moreover, the quantum state of length n denoted $|a_1 a_2 ... a_n\rangle$ with $a_i \in \{0, 1\}$ will be the tensor product $|a_1\rangle \otimes |a_2\rangle \otimes ... \otimes |a_n\rangle$. Thus, an arbitrary quantum state of length n is also a weighted sum of the 2^n preceding quantum states and with a norm equal to 1.

Definition 3 (Pauli group)**.** *The following four matrices of $\mathbb{C}^{2\times 2}$ are called Pauli matrices:*

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The Pauli group of size n is then defined as:

$$\mathcal{E}_n = \{1, -1, i, -i\} \times \{I, X, Y, Z\}^{\otimes n}.$$

Therefore, for $E \in \mathcal{E}_n$, we may write:

$$E = \lambda \bigotimes_{i=1}^{n} E(i)$$

with $\lambda \in \{1, -1, i, -i\}$ and $E(i) \in \{I, X, Y, Z\}$. We will also write $E = \lambda[E(1)E(2)...E(n)]$.

It can be checked that $XZ = -ZX = -iY$, $XY = -YX = iZ$, $YZ = -ZY = iX$ and $X^2 = Y^2 = Z^2 = I$. Therefore, two Pauli matrices E_1 and E_2 either commute if $E_1 E_2 = E_2 E_1$ or anticommute if $E_1 E_2 = -E_2 E_1$. More precisely, a Pauli matrix commutes with itself and matrix I and anticommutes with the two other Pauli matrices. Therefore similarly two elements of the Pauli group of size n either commute or anticommute.

Definition 4. *Let $E = [E(1)E(2)...E(n)]$ and $F = [F(1)F(2)...F(n)]$, we will note $E \bigstar F = 0$ (resp. 1) if $EF = FE$ (resp. $EF = -FE$) and we have $E \bigstar F = \sum_{i=1}^{n} E(i) \bigstar F(i) \pmod 2$.*

Quantum communication channels may affect transmitted quantum states in various ways. In order to evaluate quantum error correcting codes two basic channels are defined.

Definition 5 (Pauli communication channel)**.** *Let $|\phi\rangle$ be a quantum state of size n. A Pauli communication channel, defined by four positive parameters p_I, p_X, p_Y and p_Z such that $p_I + p_X + p_Y + p_Z = 1$, outputs the quantum state $E|\phi\rangle$ with $E = [E(1)E(2)...E(n)]$ where for all $1 \leq i \leq n$, $E(i) = I$ (resp, X, Y, Z) with probability p_I (resp. p_X, p_Y, p_Z).*

Definition 6 (Depolarizing channel)**.** *A depolarizing channel, defined by a parameter p with $0 \leq p \leq 1$, is a Pauli communication channel with $p_I = 1 - p$ and $p_X = p_Y = p_Z = p/3$.*

III. Stabilizer and CSS codes

In classical communications, error correcting codes are used to combat transmission errors due to the communication channel. In the framework of quantum communications, quantum error correcting codes are also used to deal with the effects of quantum channels. An important family of quantum error correcting codes is the class of stabilizer codes [8].

Definition 7 (Stabilizer code)**.** *Let $\mathcal{S}$ be a commutative subgroup of $\mathcal{E}_n$ not containing $-I^{\otimes n}$, then the quantum error correcting code $\mathcal{C}$ stabilized by $\mathcal{S}$ is defined as:*

$$\mathcal{C} = \{|\phi\rangle \in \mathbb{C}^{2^n} \text{ such that } S|\phi\rangle = |\phi\rangle \text{ for all } S \in \mathcal{S}\}.$$

Classical notions for error correcting codes can then be defined in the quantum communication framework.

Definition 8 (Dimension of a stabilizer code)**.** *Let $\mathcal{C}$ be a stabilizer code of n qubits. The dimension of $\mathcal{C}$, denoted $\dim(\mathcal{C})$ is the integer value k such that $\mathcal{C}$ is a subspace of dimension 2^k in $\mathbb{C}^{2^n}$.*

It can then be proven that:

Theorem III.1. *Let $\mathcal{C}$ be a stabilizer code of n qubits stabilized by $\mathcal{S}$. Let r be the number of independent generators of $\mathcal{S}$. We have then:*

$$\dim(\mathcal{C}) = n - r.$$

Definition 9 (Centralizer)**.** *Let $\mathcal{S}$ be the stabilizer of a quantum code $\mathcal{C}$ of length n. The centralizer of $\mathcal{S}$, denoted $C(\mathcal{S})$ is the subgroup generated by all the elements of $\mathcal{E}_n$ commuting with all the elements of $\mathcal{S}$:*

$$C(\mathcal{S}) = \{E \in \mathcal{E}_n \text{ such that } E \bigstar S = 0 \text{ for all } S \in \mathcal{S}\}.$$

Definition 10 (Syndrome)**.** *Let $\mathcal{S} = \{S_1, S_2, ..., S_r\}$ be the stabilizer of a quantum code $\mathcal{C}$. Let E be a Pauli error. The syndrome of E is then the vector $s(E) = (E \bigstar S_1, E \bigstar S_2, ..., E \bigstar S_r)$.*

As in the classical case, syndrome values are used to detect and eventually correct transmission errors. Suppose that $E \bigstar S_i = 1$ for some $1 \leq i \leq r$. We have then, for any $|\phi\rangle \in \mathcal{C}$, $E(|\phi\rangle) = ES_i(|\phi\rangle) = -S_i E(|\phi\rangle)$, therefore $E(|\phi\rangle)$ is not stabilized by S_i and thus is not a codeword of $\mathcal{C}$. Therefore an error is detected. Suppose now that $E \in \mathcal{S}$. Then by definition, $E(|\phi\rangle) = |\phi\rangle$ for all $|\phi\rangle \in \mathcal{C}$. We have then a benign error since it does not affect the

codewords of $\mathcal{C}$. In this case, we have also $s(E) = 0$ and, in fact, this error is not detected. In the third case, we have $E \in C(\mathcal{S}) \setminus \mathcal{S}$. We have then $s(E) = 0$ and this error is not detected. However, by definition of $\mathcal{C}$ and since $E \notin \mathcal{S}$, there is a codeword $|\phi\rangle \in \mathcal{C}$ such that $E(|\phi\rangle) \neq |\phi\rangle$. The code $\mathcal{C}$ is then not invariant on the action of E. As a consequence, the received quantum state $E(|\phi\rangle)$ is potentially erroneous and undetected. It is said that a serious error has occurred. A consequence of this particularity is that for a quantum code $\mathcal{C}$, two kinds of minimum distance are defined.

Definition 11 (Minimum distance)**.** *Let $\mathcal{C}$ be a quantum code stabilized by $\mathcal{S}$. The minimum distance of $\mathcal{C}$ is then defined by:*

$$d_{min}(\mathcal{C}) = \min\{w(E) \text{ such that } E \in C(S) \setminus S\}$$

where $w(E) = \sum_{i=1}^{n} \mathbb{1}(E(i) \neq I)$.

Definition 12 (Non degenerate minimum distance)**.** *Let $\mathcal{C}$ be a quantum code stabilized by $\mathcal{S}$. The non-degenerate minimum distance of $\mathcal{C}$ is then defined by:*

$$d'_{min}(\mathcal{C}) = \min\{w(E) \text{ such that } E \in C(S) \text{ and } E \neq I^{\otimes n}\}.$$

We are now in position to introduce the Calderbank-Shor-Steane construction of quantum error correcting codes [15], [16].

Definition 13 (CSS quantum code)**.** *Let C be a classical binary linear code of length n and dimension k such that $\mathsf{C} \subset \mathsf{C}^{\perp}$ and $d_{min}(\mathsf{C}^{\perp}) = d$. Let G be a $k \times n$ generating matrix of C. Let $\mathcal{S}_X = \{S_{X,1}, S_{X,2}, ..., S_{X,k}\}$ (resp. $\mathcal{S}_Z$) such that $S_{X,i} = \bigotimes_{j=1}^{n} X^{G_{ij}}$ (resp. $S_{Z,i} = \bigotimes_{j=1}^{n} Z^{G_{ij}}$). Then the code $\mathcal{C}$ stabilized by $\mathcal{S} = \mathcal{S}_X \cup \mathcal{S}_Z$ is a $[[n, n-2k, d]]$ quantum code i.e. of length n, dimension $n-2k$ and minimum distance d.*

A classical code C such that $\mathsf{C} \subset \mathsf{C}^{\perp}$ is said to be self-orthogonal or weakly self-dual. For instance, if C is a subcode of a self-dual code, then it is a self-orthogonal code. For example, the 7-qubit Steane code can be defined in the stabilizer formalism as the CSS quantum code defined from the self-orthogonal $[7, 3, 4]$ code whose dual is the Hamming $[7, 4, 3]$ code.

IV. Self-orthogonal classical codes

In this section, we recall the definitions of two classical families of error correcting codes and discuss of self-orthogonality.

A. Reed-Muller codes

Reed-Muller codes were invented by I.S. Reed in 1953 [17] [18, ch. 13, §3]. They were used, for instance by the space probe Mariner 9, launched in 1971, during its trip to Mars.

Definition 14 (Reed-Muller code)**.** *Let r and m integers such that $0 \leq r < m$ and $m \geq 2$. Then the Reed-Muller code of order r in m, denoted $RM(r, m)$ is a binary error-correcting code of length $n = 2^m$, dimension $\sum_{i=0}^{r} \binom{m}{i}$ and minimum distance 2^{m-r}. If $r = 0$, it is the repetition code of length n. If $r = m - 1$, it is the parity code of length n. If $1 \leq r < m - 1$, we have:*

$$RM(r, m) = \{(u, u + v) \text{ such that } u \in RM(r, m-1) \text{ and } v \in RM(r-1, m-1)\}.$$

This family of codes has two important properties gathered in the next theorem.

Theorem IV.1. *If $0 \leq r < m$, we have $RM(r, m)^{\perp} = RM(m - r - 1, m)$. Moreover, if $0 \leq r_1 < r_2 < m$, we have $RM(r_1, m) \subset RM(r_2, m)$.*

As a consequence, we have:

Theorem IV.2. *If $r \leq \frac{m-1}{2}$, the code $RM(r, m)$ is self -orthogonal. Moreover, if m is odd and $r = \frac{m-1}{2}$, it is self-dual.*

These codes can then be used in the CSS construction to obtain quantum codes. Moreover this family possesses an algebraic decoding procedure based on majority votes [17] [18, p. 385] which enables the decoding of these codes up to half the minimum distance. The time complexity of this procedure is $O(n \log^r n)$ for the code $RM(r, m)$ [19].

B. BCH codes

Another classical family of codes is the class of BCH codes [18, ch. 9]. They were invented in 1960 by R.C. Bose and D.K. Ray-Chaudury, and also independently by A. Hocquenghem. They have numerous applications in past and recent telecommunications standards.

Definition 15 (BCH codes)**.** *Let n be an odd integer and α be a primitive n-th root of the unity. Let b and δ be integers such that $b \geq 0$ and $\delta \geq 2$ and let g be the binary polynomial of least degree such that:*

$$g(\alpha^b) = g(\alpha^{b+1}) = ... = g(\alpha^{b+\delta-2}) = 0.$$

Then if $\deg(g) < n$, the cyclic code of length n generated by g is as binary BCH code of dimension $n - \deg(g)$ and its minimum distance is larger than δ.

These codes can be decoded by the Peterson-Gorenstein-Zierler procedure. For large values of δ, the Berlekamp-Massey procedure [20] or the Euclidean remainder procedures [21] are, however, more practical [18, ch. 9, §6]. The time complexity of these two latter algorithms is comparable and quadratic with the minimum distance. However, the computation of syndromes and the Chien search increase the global cost by $O(n\delta)$. In [22], the following result is proved.

Theorem IV.3. *Let* C *be a cyclic code of length* n *whose generating polynomial is* g*. Let* $I_{\mathsf{C}} = \{i \text{ such that } 0 \leq i \leq n-1 \text{ and } g(\alpha^i) = 0\}$*. Then we have* $I_{\mathsf{C}^\perp} = \{i \text{ such that } n - i \notin I_{\mathsf{C}}\}$.

Therefore we have:

Theorem IV.4. *Let* C *be a cyclic code of length* n *with generating polynomial* g*. Then* C *is self-orthogonal if and only if the property:*

$$g(\alpha^{n-i}) \neq 0 \Rightarrow g(\alpha^i) = 0$$

holds for all $0 \leq i \leq n-1$.

The search of convenient codes can then be made using the two latter theorems. However, as we will see in the next section, in our procedure an algebraic decoder will be required for $\mathsf{C}^\perp$. Therefore $\mathsf{C}^\perp$ is chosen to be a BCH code, and thus C is generally not a BCH code. For a given length n, we select all possible values for b and δ and $I_{\mathsf{C}^\perp}$ is defined by the union of all cyclotomic classes containing $\alpha^b, ..., \alpha^{b+\delta-2}$. Using theorem IV.3, we have then $I_{\mathsf{C}} = \{i \text{ such that } n - i \notin I_{\mathsf{C}^\perp}\}$. Finally, if the criterion of theorem IV.4, is verified for the code C, our decoding procedure can be applied to the CSS code obtained from C.

V. Decoding of CSS codes

The purpose of this section is to describe our decoding procedure. Let then $\mathcal{C}$ be a quantum error correcting defined accordingly to definition (13). Let then $\mathfrak{c}$ be a quantum codeword of $\mathcal{C}$. We have $\mathfrak{c} = \bigotimes_{i=1}^n \mathfrak{c}_i$. Let c_Z be the length n binary word such that $c_Z = (c_{Z,1}, c_{Z,2}, ..., c_{Z,n})$ and $c_{Z,i} = 0$ if $\mathfrak{c}_i = I$ or Z and $c_{Z,i} = 1$ otherwise. Since $\mathfrak{c} \in \mathcal{C}$, we have $\mathfrak{c} \bigstar S_{Z_j} = 0$, for all $1 \leq j \leq k$. However, $\mathfrak{c} \bigstar S_{Z_j} = \sum_{i=1}^n \mathfrak{c}_i \bigstar S_{Z_j,i}$. Moreover $S_{Z_j,i} = Z$ if $G_{ji} = 1$ and $S_{Z_j,i} = I$ if $G_{ji} = 0$. Therefore we have $\mathfrak{c}_i \bigstar S_{Z_j,i} = c_{Z,i} G_{ji}$, so that $\mathfrak{c} \bigstar S_{Z_j} = (c_Z, G_j)$. Thus we have $(c_Z, G_j) = 0$ for $1 \leq j \leq k$ and c_Z is a codeword of $\mathsf{C}^\perp$. Similarly, we define the length n binary word c_X for the Pauli operator X and considering the commutation of $\mathfrak{c}$ with the stabilizer subset S_X, we also obtain that $c_X \in \mathsf{C}^\perp$. Reciprocally, if $c_Z \in \mathsf{C}^\perp$ and $c_X \in \mathsf{C}^\perp$ there a is unique corresponding Pauli operator $\mathfrak{c}$ which is defined as $\mathfrak{c} = \bigotimes_{i=1}^n \mathfrak{c}_i$ with:

$$\mathfrak{c}_i = \begin{cases} I \text{ if } c_{X,i} = 0 \text{ and } c_{Z,i} = 0, \\ X \text{ if } c_{X,i} = 0 \text{ and } c_{Z,i} = 1, \\ Y \text{ if } c_{X,i} = 1 \text{ and } c_{Z,i} = 1, \\ Z \text{ if } c_{X,i} = 1 \text{ and } c_{Z,i} = 0. \end{cases}$$

As previously, we have $c \bigstar S_{X,j} = (c_X, G_j) = 0$ and $c \bigstar S_{Z,j} = (c_Z, G_j) = 0$ for all j and $\mathfrak{c}$ is a codeword of $\mathcal{C}$.

This codeword is emitted through a quantum communication channel and the quantum state $\mathfrak{r}$ is received as output. We will suppose that $\mathfrak{r}$ is a corrupted version of $\mathfrak{c}$ with at most $t = \lfloor \frac{d-1}{2} \rfloor$ errors. We have $\mathfrak{r} = \bigotimes_{i=1}^n \mathfrak{r}_i$. We define r_X and r_Z the length n binary words from $\mathfrak{r}$ in the same way that c_X and c_Z were defined from $\mathfrak{c}$. Thus r_X (resp. r_Z) is a corrupted version of c_X (resp. c_Z) with at most t errors. Then from r_X and r_Z, we can recover c_X and c_Z by any decoding procedure of $\mathsf{C}^\perp$ able to correct at most t errors. Then we can recover $\mathfrak{c}$ and our decoding procedure is correct. The figure 1 summarizes our decoding technique.

Input: $\mathfrak{r} = (\mathfrak{r}_1, \mathfrak{r}_2, ..., \mathfrak{r}_n)$ noisy quantum codeword of $\mathcal{C}$ with at most t errors.

- Set $r_X = (r_{X,1}, r_{X,2}, ..., r_{X_n})$ such that:

$$r_{X,i} = \begin{cases} 0 \text{ if } \mathfrak{r}_i = I \text{ or } X, \\ 1 \text{ if } \mathfrak{r}_i = Y \text{ or } Z. \end{cases}$$

- Set $r_Z = (r_{Z,1}, r_{Z,2}, ..., r_{Z_n})$ such that:

$$r_{Z,i} = \begin{cases} 0 \text{ if } \mathfrak{r}_i = I \text{ or } Z, \\ 1 \text{ if } \mathfrak{r}_i = X \text{ or } Y. \end{cases}$$

- Decode r_X, output c_X.
- Decode r_Z, output c_Z.
- Set $\mathfrak{c} = (\mathfrak{c}_1, \mathfrak{c}_2, ..., \mathfrak{c}_n)$ such that:

$$\mathfrak{c}_i = \begin{cases} I \text{ if } c_{X,i} = 0 \text{ and } c_{Z,i} = 0, \\ X \text{ if } c_{X,i} = 0 \text{ and } c_{Z,i} = 1, \\ Y \text{ if } c_{X,i} = 1 \text{ and } c_{Z,i} = 1, \\ Z \text{ if } c_{X,i} = 1 \text{ and } c_{Z,i} = 0. \end{cases}$$

Output: $\mathfrak{c}$, decoded codeword of $\mathcal{C}$

Fig. 1. Decoding procedure for CSS quantum codes

VI. Examples and discussion

As seen previously Reed-Muller codes $RM(r, m)$ are self-orthogonal if $r \leq \frac{m-1}{2}$. The minimum distance of the associated quantum CSS code is then 2^{r+1} and its dimension is equal to $\sum_{i=r}^{m-r} \binom{m}{i}$. The quantum codes obtained up to length 128 are the following: $[[16, 6, 4]]$, $[[32, 20, 4]]$, $[[64, 50, 4]]$, $[[64, 20, 8]]$, $[[128, 112, 4]]$ and $[[128, 70, 8]]$. The lengths of these codes are restricted to perfect powers of 2. On the contrary, BCH codes exist for various lengths and are easy to construct. A systematic search for convenient BCH codes has been done up to length 127. It was performed by implementing the search procedure detailed in paragraph IV-B with the Maple symbolic software. The table I gives the best quantum codes that were obtained this way. It can be noted that BCH codes are more numerous than Reed-Muller codes. Moreover if we compare Reed-Muller codes to

Code parameters	Generator polynomial generator of BCH code (hexadecimal value for integer argument 2)
$[[15, 7, 3]]$	0x9AF
$[[21, 9, 3]]$	0xA4CB
$[[21, 3, 5]]$	0x1A8F
$[[31, 1, 7]]$	0x147BF
$[[31, 11, 5]]$	0x32E8AB
$[[31, 21, 3]]$	0x6A45F67
$[[45, 13, 5]]$	0x3A23AD59
$[[51, 35, 3]]$	0xE326E7B34B1
$[[55, 15, 4]]$	0xDDD946DFD
$[[63, 51, 3]]$	0x3F566ED27179461
$[[63, 39, 5]]$	0xA35C93F631679
$[[63, 27, 7]]$	0x3320C9F34AF3
$[[85, 69, 3]]$	0x35ABEA2C24A198F4BB4D
$[[85, 53, 5]]$	0x3FECD96C8FA9F07243
$[[89, 23, 9]]$	0x1764DDCBD3B8989
$[[93, 73, 3]]$	0xEC77E31E49181E3F23EFB
$[[93, 63, 5]]$	0x703365A734791C2C4EAF
$[[93, 43, 7]]$	0x1A97E0808F8470F23D
$[[93, 13, 11]]$	0x3E3E4297282E6B
$[[127, 113, 3]$	0x1BE0B087462729A5EBB8F32455B3FB5
$[[127, 99, 5]$	0x3190488E5B884A8F2CBF766953B65
$[[127, 85, 7]$	0x7B58F033D746D85D06A9F911B4B
$[[127, 71, 9]$	0xE2053619F3BBDFFAD8BB92E3F
$[[127, 57, 11]$	0x1363666EFD9347B31283796F
$[[127, 43, 13]$	0x2612A3178A1AD1832FE6A5
$[[127, 29, 15]]$	0x73DFA983C0D3A089566B

TABLE I
CSS QUANTUM ERROR CORRECTING OBTAINED FROM BCH CODES.

equivalent BCH codes in terms of length and dimension, BCH codes are generally slightly better. For instance, for a given depolarization rate, the Reed-Muller code $[[64, 20, 8]]$ and the BCH code $[[63, 27, 7]]$ will have the same decoding performance since their error correction threshold are identical. However, the dimension parameter of the BCH code is larger than that of the Reed-Muller code. Syndrome decoding for a $[[N, K, D]]$ quantum code requires the storage of $\sum_{i=0}^{t} 3^i \binom{N}{i}$ correction patterns with $t = \lfloor \frac{D-1}{2} \rfloor$. Therefore, for instance for the Reed-Muller code $[[64, 20, 8]]$, 1143265 correction patterns have to be stored. The requirement is quite limited. However, the syndrome is 44 qubits wide and then a direct access to the storage would require a huge memory of 2^{44} entries. The most common solution is to sort the syndrome values in increasing or decreasing order and then to access the correction table by dichotomic search. In this example, a maximum of 21 accesses are required. This technique can be improved by the use of hash tables but at the cost of increasing memory area. With our method, once the syndrome has been computed, only two decoding of the binary $[64, 42, 8]$ Reed-Muller code are needed. These decodings can be made by the Reed procedure. Alternatively, we can also resort to the syndrome decoding on binary codes. In this case, the table will contain 43745 decoding pattern and the syndrome are then 22 bits wide. However, two decodings are required, each of them needing at most 16 memory access. Thus, a maximum of 32 accesses are required. In this situation, our procedure is less efficient in terms of memory accesses, but it has a smaller memory requirement. However, it is well known that the complexity of syndrome decoding grows exponentially with the minimum distance of the code. In the case of the $[[127, 29, 15]]$ quantum BCH code more than 1.9×10^{14} correction patterns need to be stored, representing more than 1500 terabytes. On the other hand, with our decoding procedure, two decodings of the binary $[127, 78, 15]$ BCH code are required. BCH codes with even larger lengths and minimum distances are widespreadly used in current telecommunication systems. In the general case, if we use a classical self-orthogonal Reed-Muller code $RM(r, m)$ with $r \leq \frac{m-1}{2}$ in the CSS construction framework, we obtain a quantum code, whose length, dimension and minimum distance are respectively $n = 2^m$, $n - 2\sum_{i=0}^{r} \binom{m}{i}$ and 2^{r+1}. Therefore, if we use the Reed majority vote decoding procedure, the time complexity of our decoding method is then $O(n \log^{m-r-1} n)$ with a very low memory complexity. For the same code, the syndrome method requires the storage of $\binom{n}{2^r}$ syndromes of size $2\sum_{i=0}^{r} \binom{m}{i}$ in qubits. For a classical BCH code of length n and designed distance δ, the encoding rate depends on the size of the cyclotomic classes of the powers of the primitive n-th root α. In the case of a primitive BCH code, we have $n = 2^m - 1$ for some integer m and each cyclotomic class is of length m. In the worst case where successive powers of α belong to different cyclotomic classes, the dimension of the code is $n - m\delta$. The quantum code obtained by CSS construction has then n for length, $n - 2m\delta$ for dimension and δ for designed distance. The total time decoding cost by Berlekamp algorithm or Euclidean algorithm is then $O(n\delta + \delta^2)$ and the space complexity is very low. With the syndrome decoding $\binom{n}{\lfloor \frac{d-1}{2} \rfloor}$ syndromes of size $2m\delta$ in qubits have to be stored. In the case of an unprimitive BCH code, again $\binom{n}{\lfloor \frac{d-1}{2} \rfloor}$ syndromes have to be stored. The singleton bound implies that syndromes are at least $\delta - 1$ qubits long. The asymptotic cost of Berlekamp and Euclidean algorithm is unchanged. In conclusion, for quantum Reed-Muller and BCH codes, the complexity of the decoding method described in this article grows polynomially with the length and minimum distance of the codes. For these codes the space complexity of the syndrome decoding grows exponentially. If linear programming techniques or GRAND algorithms are used, the decoding process is then either suboptimal or has an exponential time complexity. Therefore, the described method gives a viable alternative for the decoding of these quantum codes.

VII. Conclusion

In this article, we have proposed a new decoding technique for CSS quantum codes built over binary codes having algebraic decoding procedures. Examples with Reed-Muller and BCH codes have been presented and our decoding procedure has been compared to the classical syndrome decoding procedure. It was shown that for CSS quantum codes with large minimum distance, the proposed procedure is much more efficient and gives a realistic alternative to syndrome decoding.

References

[1] G Arun and Vivekanand Mishra. A review on quantum computing and communication. In *2014 2nd International Conference on Emerging Technology Trends in Electronics, Communication and Networking*, pages 1–5, 2014.

[2] Solenov D., Brieler J., and Scherrer J.F. The potential of quantum computing and machine learning to advance clinical research and change the practice of medicine. *Missouri Medicine*, 115(5):463–467, Sep-Oct 2018. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6205278.

[3] Chuang I.L., Laflamme R., Shor P.W., and Zurek W.H. Quantum computers, factoring, and decoherence. *Science*, 270(5242):1633–1635, Dec 1995. DOI: 10.1126/science.270.5242.1633.

[4] Quantum Technology, Application Consortium QUTAC, Bayerstadler A., and Becquin G. et al. Industry quantum computing applications. *EPJ Quantum Technology*, 8(25), 2021.

[5] Cheng H.-P. and Erik Deumens E. et al. Application of quantum computing to biochemical systems: A look to the future. *Frontiers in Chemistry*, 8, 2020.

[6] Sreraman M. and Linshu L. et al. Optimal architectures for long-distance quantum communication. *Scientific Reports*, 6, Feb 2016.

[7] Lago-Rivera D., Rakonjac J.V., and Grandi S. et al. Long distance multiplexed quantum teleportation from a telecom photon to a solid-state qubit. *Nature Communications*, 14, Apr 2023. https://www.nature.com/articles/s41467-023-37518-5.

[8] Gottesman D. *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, 1997. https://arxiv.org/abs/quant-ph/9705052.

[9] Leifer M.S. and Poulin D. Quantum graphical models and belief propagation. *Annals of Physics*, 323(8):1899–1946, Aug 2008. https://www.sciencedirect.com/science/article/pii/S0003491607001509.

[10] Nielsen M.A. and Chuang I.L. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[11] July X. Li and Pascal O. Vontobel. Lp decoding of quantum stabilizer codes. In *2018 IEEE International Symposium on Information Theory (ISIT)*, pages 1306–1310, 2018.

[12] Omar Fawzi, Lucien GrouÃ¨s, and Anthony Leverrier. Linear programming decoder for hypergraph product quantum codes. In *2020 IEEE Information Theory Workshop (ITW)*, pages 1–5, 2021.

[13] Daryus Chandra, Zeynep B. Kaykac Egilmez, Yifeng Xiong, Soon Xin Ng, Robert G. Maunder, and Lajos Hanzo. Universal decoding of quantum stabilizer codes via classical guesswork. *IEEE Access*, 11:19059–19072, 2023.

[14] Mark M Christiansen and Ken R Duffy. Guesswork, large deviations, and shannon entropy. *IEEE transactions on information theory*, 59(2):796–802, 2012.

[15] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996. https://arxiv.org/abs/quant-ph/9512032.

[16] Steane A. Multiple-particle interference and quantum error correction. *Proceedings of the royal society A*, 452(1954), 1996. https://arxiv.org/abs/quant-ph/9601029.

[17] Reed I.S. A class of multiple-error-correcting codes and the decoding scheme. Technical Report 44, Massachusetts Institute of Technology, October 1953.

[18] F.J. MacWilliams and N.J.A. Sloane. *The theory of error-correcting codes*. North-Holland, Amsterdam, London, New York, 1st edition, 1983. ISBN: 9780444851932.

[19] Emmanuel Abbe, Amir Shpilka, and Min Ye. Reed–muller codes: Theory and algorithms. *IEEE Transactions on Information Theory*, 67(6):3251–3277, 2020.

[20] Massey J.L. Shift-register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, IT-15(1):122–127, January 1969. http://crypto.stanford.edu/∼mironov/cs359/massey.pdf.

[21] Sugiyama Y., Kasahara M., Hirasawa S., and Namekawa T. A method for solving key equation for decoding goppa codes. *Information and Control*, 27(1):87–99, 1975. https://www.sciencedirect.com/science/article/pii/S001999587590090X.

[22] Grassl C., Beth T., and Pellizari T. Codes for the quantum erasure channel. *Physical Review*, 56(1):33–38, July 1997. https://arxiv.org/pdf/quant-ph/9610042.pdf.