On the hardnesses of several quantum decoding problems

Kao-Yueh Kuo1 · Chung-Chin Lu1

Received: 21 January 2019 / Accepted: 16 February 2020 / Published online: 27 February 2020
© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract
We classify the time complexities of three decoding problems for quantum stabilizer codes: quantum bounded distance decoding (QBDD), quantum maximum likelihood decoding (QMLD), and quantum minimum error probability decoding (QMEPD). For QBDD, we show that it is NP-hard based on Fujita’s result, and cover the gap of full row rank of check matrices, like what Berlekamp, McEliece, and Tilborg suggested in 1978. Then, we give some insight into the quantum decoding problems to clarify that the degeneracy property is implicitly embedded in any decoding algorithm, independent of the typical definition of degenerate codes. Then, over the depolarizing channel model, we show that QMLD and QMEPD are NP-hard. The NP-hardnesses of these decoding problems indicate that decoding general stabilizer codes is extremely difficult, strengthening the foundation of quantum code-based cryptography.

Keywords Quantum error correction codes · Quantum stabilizer codes · Decoding hardness · Degeneracy property · Quantum cryptography · Computational complexity

1 Introduction

For classical binary linear codes, Berlekamp et al. [1] considered the classical bounded distance decoding (CBDD) and asked a simpler decision problem \texttt{Coset Weights}. They proved that \texttt{Coset Weights} is NP-complete so that CBDD is NP-hard. In the theory of computation [2], a decision (yes or no) problem is NP-complete if it is in NP.

This work was supported by the Ministry of Science and Technology, Taiwan, under Contract MOST 101-2221-E-007-096-MY3. Part of this work was presented at the 2012 International Symposium on Information Theory and its Applications (ISITA 2012), Hawaii, USA, October 28–31, 2012. This work has an arXiv version (arxiv:1306.5173).

1 Department of Electrical Engineering, National Tsing Hua University, Hsinchu 30013, Taiwan

Kao-Yueh Kuo
d9761808@oz.nthu.edu.tw

Chung-Chin Lu
cclu@ee.nthu.edu.tw
and all NP problems are reducible to it in polynomial time. A computational problem (not necessarily a decision problem) is NP-hard if an NP-complete problem is reducible to it in polynomial time. The fact that CBDD is NP-hard indicates that it may be impossible to find a polynomial-time decoding algorithm for general classical binary linear codes. But McEliece then pointed out that the result actually provides a foundation of code-based cryptography [3]. The importance of code-based cryptography has grown recently because code-based cryptosystems appear to have strong resistance against the attacks performed by quantum computers [4,5].

It is known that quantum stabilizer codes can be related to classical self-orthogonal codes [6–8]. But Poulin and Chung [9] pointed out that decoding stabilizer codes could be very different from decoding classical codes, since rather than finding a most likely error, finding a most likely error coset is desired. Later, Hsieh and Le Gall [10] showed that, over a special Pauli channel regarding Hamming weight as the weight metric, the quantum decoding problems are NP-hard, no matter whether a most likely error or a most likely error coset is desired. More recently, Fujita [11] showed that, regarding the generalized weight as the weight metric, a bounded distance decoding for stabilizer codes, as a decision problem, is NP-complete. The generalized weight is an important metric since it is usually used to define the minimum distance of stabilizer codes [7,8,12] to directly reflect the error correction capability in number of qubits. And when stabilizer codes are used over the depolarizing channel, a direct extension of the classical binary symmetric channel [13], the generalized weight can be used to determine the probability of an error (as in Eq. (14), Sect. 5). However, the complexity (hardness) of an optimal decoding over the depolarizing channel, i.e., finding a most likely error coset under the generalized weight, is still unknown in the literature.

In this paper, we classify the hardnesses of several quantum decoding problems including the aforementioned optimal decoding problem. In the beginning, regarding the generalized weight, but regardless of any specific channel model, quantum bounded distance decoding (QBDD) is considered. Fujita considered a similar problem (see Lemma 2 of [11]) without restricting the check matrix to be of full row rank. We will take this restriction and show that QBDD is NP-hard. Then, over the depolarizing channel, quantum maximum likelihood decoding (QMLD) and quantum minimum error probability decoding (QMEPD) are considered, where the first is to find a most likely error and the second is to find a most likely error coset. Assisted by the NP-hardness of QBDD, we will show that both QMLD and QMPED are also NP-hard.

The paper is organized as follows: In Sect. 2, the foundation of stabilizer codes is reviewed and the required notations are defined. In Sect. 3, QBDD is considered and shown to be NP-hard. In Sect. 4, we give some insight into the quantum decoding problems to have more clarification on the degeneracy property. In Sect. 5, QMLD and QMEPD over the depolarizing channel are considered and both shown to be NP-hard. In Sect. 6, a conclusion is given.
2 Stabilizer codes

In this section, we define the state space we work with and stabilizer codes. The stabilizer codes will be related to even-length classical binary codes under the symplectic inner product and the generalized weight [6–8,12,14,15].

Let $V_1$ be the state space of one qubit, which is a 2-dimensional complex inner product space spanned by an orthonormal computational basis $\{|0\rangle, |1\rangle\}$. Let $G_1 \triangleq \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$ be the Pauli Group on $V_1$, where

$$I \triangleq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X \triangleq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z \triangleq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad Y \triangleq iXZ.$$

Then, $G_n \triangleq G_1^\otimes n$ is the Pauli group on the state space $V \triangleq V_1^\otimes n$ of $n$ qubits. It is known that two elements in $G_n$ either commute or anti-commute. For each $g \in G_n$, it has a tensor product representation

$$g = i^{m_0}\sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n,$$

where $m_0 \in \{0, 1, 2, 3\}$ and $\sigma_j \in \{I, X, Y, Z\}$ for all $j$. Let $w(g)$ be the weight of $g$, which is defined as the number of non-identity terms in the tensor product representation of $g$. For example, $g = i(X \otimes I \otimes Y \otimes Z) \in G_4$ has $w(g) = 3$. Since an error possibly affecting a state in $V$ can be written as a linear combination of the elements in $G_n$, according to the error discretization theorem (Theorem 10.2 of [14]), we can correct a state of $n$ qubits having errors in $\leq t$ qubits if (and only if) all error patterns $E \in G_n$ of weight $w(E) \leq t$ are correctable. It is known that such an error correction capability can be achieved by an $[[n, k, d]]$ stabilizer code with $d \geq 2t + 1$ [7,8].

Stabilizer codes are defined in the following manner. Let $S$ be a subgroup of $G_n$ such that $-I \notin S$. Then, $S$ is abelian and can be generated by a set of $n - k$ independent generators as

$$S = \langle g_1, g_2, \ldots, g_{n-k} \rangle \quad (1)$$

for some integer $k \in [0, n]$. The subgroup $S$ has a fixed subspace $C(S)$ in $V$ defined as

$$C(S) \triangleq \{|\psi\rangle \in V \mid g|\psi\rangle = |\psi\rangle \forall g \in S\},$$

which has dimension $2^k$. The subspace $C(S)$ is called an $[[n, k]]$ stabilizer code with a stabilizer group $S$. Most properties of $C(S)$ can be studied through $S$. The normalizer $\mathcal{N}(S)$ of $S$ in $G_n$ is defined as

$$\mathcal{N}(S) \triangleq \{h \in G_n \mid hg = gh \forall g \in S\}.$$
Let $K \triangleq \{ \pm I, \pm iI \}$ and $SK \triangleq S \vee K = \{ \pm g, \pm ig | g \in S \}$. Then, it is known that the minimum distance $d$ of the stabilizer code $C(S)$ can be defined as

$$d \triangleq \min \{ w(g) | g \in N(S) \setminus SK \}. \quad (2)$$

Now we relate stabilizer codes to classical binary linear codes. Let $\varphi : G_n \to \mathbb{Z}_2^{2^n}$ be a group epimorphism defined by

$$\varphi(g) = \varphi(i^{m_0} \sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n)$$

$$= (x_1 x_2 \cdots x_n | z_1 z_2 \cdots z_n) = (x | z)$$

for all $g \in G_n$ under the mapping:

$$\begin{array}{c|cccc}
\sigma_j & I & X & Y & Z \\
x_j & 0 & 1 & 1 & 0 \\
z_j & 0 & 0 & 1 & 1 \\
\end{array}$$

Let $g, h$ be any two elements in $G_n$. The epimorphism $\varphi$ gives us the relation $\varphi(gh) = \varphi(g) + \varphi(h)$ of group operations. Define

$$\Lambda \triangleq \begin{bmatrix}
O_{n \times n} & I_{n \times n} \\
I_{n \times n} & O_{n \times n}
\end{bmatrix}.$$ 

Then, we have $gh = hg$ iff $\varphi(g) \Lambda \varphi(h)^T = 0$, i.e., $\varphi(g)$ and $\varphi(h)$ are orthogonal with respect to (w.r.t.) the symplectic inner product [7]. Use the $n - k$ generators of $S$ in (1) to define an $(n - k) \times 2n$ binary matrix

$$H \triangleq \begin{bmatrix}
\varphi(g_1) \\
\vdots \\
\varphi(g_{n-k})
\end{bmatrix}_{(n-k) \times 2n}.$$ 

(3)

Since $g_i$’s are independent generators of $S$, the rows $\varphi(g_i)$’s in $H$ are linear independent so that $H$ is of full row rank. Also since $S$ is abelian, we have $H \Lambda H^T = O$ so that the row space $\text{Row}(H)$ of $H$ is a classical binary linear code $C = \varphi(SK) \subseteq \mathbb{Z}_2^{2^n}$ which is self-orthogonal w.r.t. the symplectic inner product. $H$ is called a check matrix of the stabilizer code $C(S)$. Now for each $(x | z) \in \mathbb{Z}_2^{2^n}$, define the generalized weight of $(x | z)$ as

$$gw(x | z) \triangleq w_H(x) + w_H(z) - w_H(xz),$$

where $w_H(x)$ is the Hamming weight of $x$ and $xz$ is the bitwise AND of $x$ and $z$. A property of the generalized weight is

$$gw(x | z) \geq \max \{ w_H(x), w_H(z) \} \quad (4)$$

\* Springer
and note that \( w(g) = gw(\varphi(g)) \) for all \( g \in G_n \). Let \( C_1 \triangleq \{ v \in \mathbb{Z}_{2^n} | vAH^T = 0 \} \) be the symplectic dual of \( C \). Then, \( \varphi^{-1}(C_+) = \mathcal{N}(S) \), and the minimum distance \( d \) of \( C(S) \) in (2) can be evaluated by
\[
d = \min\{gw(v) \mid v \in C_+ \setminus C\}. \tag{5}
\]

### 3 Quantum bounded distance decoding

In this section, we will review the syndrome measurement of stabilizer codes and then define the quantum bounded distance decoding (QBDD). We will consider the constraint that the check matrix in QBDD is of full row rank. Without this constraint, Fujita [11] considered this problem as a decision problem and proved that it is NP-complete. Then, he used this fact as a foundation to propose stabilizer code-based cryptosystems. To further strengthen this foundation, we will prove that QBDD is NP-hard in this section. The NP-hardness of QBDD will then help us to classify the hardnesses of the decoding problems in the next section.

Now we briefly review the syndrome measurement of stabilizer codes (see Section 10.5 of [14] for details). Consider an \([n, k]\) stabilizer code \( C(S) \) as in Sect. 2. Assume that an uncoded state of \( k \) qubits is encoded to a coded state \(|\psi\rangle \in C(S)\) of \( n \) qubits. Let \( \rho \triangleq |\psi\rangle \langle \psi| \) be the channel input and \( E(\rho) = E\rho E^\dagger \) be the channel output, provided that the error is some \( E \in G_n \). To perform the error detection, the \( n-k \) generators of \( S \) are used to form \( n-k \) syndrome measurements
\[
\{(I + g_i)/2, (I - g_i)/2\}, \quad i = 1, 2, \ldots, n-k.
\]

For each generator \( g_i \) of \( S \), we have either \( Eg_i = g_i E \) with measurement output being \(+1\) or \( Egi = -g_i E \) with measurement output being \(-1\), while the post-measurement state remains unchanged as \( E\rho E^\dagger \) with probability one. Assume that the measurements are performed and the results form an \( n-k \) tuple \( \beta = (\beta_1, \beta_2, \ldots, \beta_{n-k}) \in \{+1, -1\}^{n-k} \). Map \( \beta \) to a binary vector \( s = (s_1, s_2, \ldots, s_{n-k}) \in \mathbb{Z}_{2}^{n-k} \) by \( s_i = 0 \) if \( \beta_i = +1 \) and \( s_i = 1 \) if \( \beta_i = -1 \) for all \( i \). By the discussion in Sect. 2, we have \( Eg_i = g_i E \) iff \( \varphi(E) \Lambda \varphi(g_i)^T = 0 \). Let \( H \) be defined as in (3). Then, we have \( s = \varphi(E) \Lambda H^T \), i.e., \( s \) can be regarded as a classical binary syndrome vector generated by the error vector \( \varphi(E) \) and the check matrix \( H \) under the symplectic inner product.

The above discussion suggests a bounded distance decoding that, given a check matrix \( H_{(n-k) \times 2n} \) and a syndrome vector \( s \in \mathbb{Z}_{2}^{n-k} \), we need to find an error vector \( e \in \mathbb{Z}_{2}^{2n} \) such that \( e\Lambda H^T = s \) and \( gw(e) \leq t \) for some integer \( t \geq 0 \). This is a classical computational problem. Once a solution \( e \) is found, up to a global phase, any \( \tilde{E} \in \varphi^{-1}(e) \) can be an error correction operator applying to the post-measurement state \( E\rho E^\dagger \). Now we define the decoding problem of finding such an \( e \) as

**Quantum bounded distance decoding (QBDD)**

**INPUT:** A full row rank \( m \times 2n \) binary matrix \( H \) satisfying \( H\Lambda H^T = O \), a binary vector \( s \in \mathbb{Z}_{2}^{m} \), and an integer \( t \geq 0 \).

**OUTPUT:** A binary vector \( e \in \mathbb{Z}_{2}^{2n} \) satisfying \( gw(e) \leq t \) and \( e\Lambda H^T = s \), or a failure indication if such an \( e \) does not exist.
We remark that even if the channel error $E \in G_n$ has a weight $w(E) \leq t$ and the check matrix $H$ corresponds to a stabilizer code with a minimum distance $d \geq 2t + 1$, there may still exist more than one solution $e$ to QBDD. This phenomenon is different from the classical decoding due to the evaluation of $d$ in (5). However, all these solutions will correspond to the same error correction effect. To see that, first recall $d = \min\{gw(u) \mid u \in C^\perp \setminus C\}$, where $C = \text{Row}(H) = \varphi(\mathcal{SK})$. And consider the \textit{stabilizer property} that for all $g \in G_n$,

$$g \rho g^\dagger = \rho \iff g \in \mathcal{SK},$$

where $\mathcal{SK} = \{\pm g, \pm ig \mid g \in S\}$. So if $d \geq 2t + 1$, $w(E) \leq t$, and QBDD has multiple solutions, then any two solutions $e_1$ and $e_2$ will satisfy $e_2 = e_1 + v$ for some $v \in C = \varphi(\mathcal{SK})$, i.e., $e_1$ and $e_2$ correspond to two errors $E_1 \in \varphi^{-1}(e_1)$ and $E_2 \in \varphi^{-1}(e_2)$ satisfying $E_2 = E_1 g$ for some $g \in \mathcal{SK}$. So

$$E_1^\dagger(E \rho E^\dagger)E_1 = g E_2^\dagger(E \rho E^\dagger)E_2 g^\dagger = (E_2^\dagger E)g \rho g^\dagger(E^\dagger E_2) = E_2^\dagger(E \rho E^\dagger)E_2$$

by (6), no matter $g$ and $E_1^\dagger E$ commute or anti-commute. Thus, $E_1^\dagger$ and $E_2^\dagger$ have the same error correction effect. The phenomenon that distinct operators can result in the same error correction effect is sometimes called the \textit{degeneracy property} [9,10]. But whether a stabilizer code is degenerate/nondegenerate depends on how the set of correctable error patterns is defined. For quantum bounded distance decoding, the set of correctable error patterns is usually defined as $E_C(d) \triangleq \{E \in G_n \mid w(E) \leq \lfloor \frac{d-1}{2} \rfloor\}$ with $d = \min\{gw(g) \mid g \in N(S) \setminus \mathcal{SK}\}$. In this case, a stabilizer code $\mathcal{C}(S)$ is nondegenerate iff $E_C(d) = E_C(d')$ with $d' \triangleq \min\{w(g) \mid g \in N(S) \setminus K\}$. For this, we have more clarification in Sect. 4.

The hardness of QBDD reflects the hardness of attacking a quantum code-based cryptosystem like the one in [11] when this kind of system is protected through bounded artificial noise like McEliece’s suggestion [3]. To classify the hardness of QBDD, we at first deal with a decision (yes or no) problem:

**Coset generalized weights (CGW)**

**INPUT**: An $m \times 2n$ binary matrix $H$ satisfying $H A H^T = O$, a binary vector $s \in \mathbb{Z}_2^m$, and an integer $t \geq 0$.

**QUESTION**: There exists a binary vector $e \in \mathbb{Z}_2^{2n}$ satisfying $gw(e) \leq t$ and $e \Lambda H^T = s$.

Fujita also considered this decision problem and showed that it is NP-complete in Lemma 2 of [11]. For convenience, we restate the result as

**Theorem 1** \textit{CGW is NP-complete, even if $H = [H_X|O]$ or $H = [O|H_Z]$.}

In order to know the hardness of QBDD, we need the constraint that the check matrix is of full row rank. So we restrict CGW as follows: If $H = [O|H_Z]$ is assumed in CGW, we say that CGW becomes a restricted problem CGW$_Z$. If $H = [O|H_Z]$ is further assumed to have full row rank, we say that CGW$_Z$ becomes a further restricted problem CGW$_ZF$. We define the two problems for clarity:
CGW<sub>Z</sub>

**INPUT:** An \( m \times 2n \) binary matrix \( H = [O|H_Z] \), a binary vector \( s \in \mathbb{Z}_2^m \), and an integer \( t \geq 0 \).

**QUESTION:** There exists a binary vector \( e \in \mathbb{Z}_2^{2n} \) satisfying \( g_w(e) \leq t \) and \( e \Lambda H^T = s \).

CGW<sub>ZF</sub>

**INPUT:** An \( m' \times 2n \) binary matrix \( H' = [O|H_Z'] \) having full row rank, a binary vector \( s' \in \mathbb{Z}_2^{m'} \), and an integer \( t' \geq 0 \).

**QUESTION:** There exists a binary vector \( e \in \mathbb{Z}_2^{2n} \) satisfying \( g_w(e) \leq t' \) and \( e \Lambda H'^T = s' \).

Note that an \( H = [O|H_Z] \) already satisfies \( H \Lambda H^T = O \). The problem CGW<sub>Z</sub> is already NP-complete, as stated in Theorem 1. Similar to a remark in [1], the NP-completeness of CGW<sub>Z</sub> will imply the NP-completeness of CGW<sub>ZF</sub>. We prove this statement rigorously in

**Theorem 2** CGW<sub>Z</sub> is polynomial-time reducible to CGW<sub>ZF</sub>, and hence, CGW<sub>ZF</sub> is also NP-complete.

**Proof** Suppose we have a polynomial-time algorithm for CGW<sub>ZF</sub>. Given an instance of CGW<sub>Z</sub> with some \( H = [O|H_Z]_{m \times 2n} \), \( s \in \mathbb{Z}_2^m \), and \( t \geq 0 \), assume rank(\( H \)) = \( m' \). Then, \( m' \leq n \). We also have \( m' \leq n \) from \( H \Lambda H^T = O \). Let \( H_Z' \) in CGW<sub>ZF</sub> consist of \( m' \) rows of \( H_Z \) so that Row(\( H' \)) = Row(\( H \)). Constructing such an \( H_Z' \) can be done in polynomial time, as a remark in Sect. IV of [1]. Once this is done, then \( H = RH' \) for some \( m \times m' \) binary matrix \( R \). The matrix \( R \) can also be constructed in polynomial time. (For example, first put \( H' \) in a reduced row echelon form \( \hat{H}' = E H' \), which can be done in polynomial time. Then, it is trivial to find a unique \( \hat{R} \) satisfying \( H = \hat{R} \hat{H}' = \hat{R} E H' \), which implies \( R = \hat{R} E \).) Assume that rows \( j_1, j_2, \ldots, j_{m'} \) of \( H_Z \) compose the rows of \( H_Z' \). By the given \( s = (s_1 \ s_2 \ \ldots \ s_m) \), let \( s'_t = (s_{j_1} \ s_{j_2} \ \ldots \ s_{j_{m'}}) \). Then, any \( u \in \mathbb{Z}_2^{2n} \) satisfying \( u \Lambda H^T = s \) will satisfy \( u \Lambda H'^T = s'_t \). And if such a \( u \) exists, we must have \( s'_t \Lambda H'^T R^T = u \Lambda H'^T = s \). Thus, if the equality \( s'_t \Lambda H'^T R^T = s \) does not hold, then the answer to CGW<sub>Z</sub> is negative. If the equality \( s'_t \Lambda H'^T R^T = s \) holds, then let \( t' = t \) and use the polynomial-time algorithm to solve CGW<sub>ZF</sub>. If the answer to CGW<sub>ZF</sub> is negative, then the answer to CGW<sub>Z</sub> is also negative by our construction of \( H_Z' \). Conversely, if the answer to CGW<sub>ZF</sub> is positive, then there exists a vector \( e \in \mathbb{Z}_2^{2n} \) satisfying \( g_w(e) \leq t \) and \( e \Lambda H'^T = s' \). Then, this \( e \) also satisfies \( e \Lambda H'^T R^T = s' \Lambda R^T = s \) so that the answer to CGW<sub>Z</sub> is also positive. We have shown that CGW<sub>Z</sub> is polynomial-time reducible to CGW<sub>ZF</sub>. By Theorem 1, CGW<sub>Z</sub> is NP-complete and so does CGW<sub>ZF</sub>.

Many known results of quantum decoding hardnesses [10,11] are based on the Coset Weight [1] without specifying the gap of full row rank check matrices. Theorem 2 slightly covers the gap. It is trivial that CGW<sub>ZF</sub> is polynomial-time reducible to QBDD. Thus, by Theorem 2 and by symmetry, we have

**Corollary 1** QBDD is NP-hard, even if \( H = [H_X|O] \) or \( H = [O|H_Z] \).

We have shown that QBDD is NP-hard by considering the practical constraint that the check matrix is of full row rank, which makes the foundation of stabilizer code-
based cryptography more concrete. This will also be helpful when we classify the hardnesses of the decoding problems in the next section.

4 Some Insight into the Quantum Decoding Problems

In this section, we give some insight into the quantum decoding problems, starting from classical syndrome decoding to optimal quantum decoding, by group quotients, relating to the degeneracy property.

We reconstruct the classical standard array [16] for convenience of discussion. Recall the notations in Sect. 2. For a check matrix $H_{(n-k)\times 2n}$ generating a self-orthogonal $C \subset \mathbb{Z}_2^{2n}$, we have the symplectic dual $C^\perp \supseteq C$ generated by some $G_{(n+k)\times 2n}$ s.t. $G \Lambda H^T = O$. Consider the quotient group $\mathbb{Z}_2^{2n} / C^\perp = \{ e + C^\perp \mid e \in \mathbb{Z}_2^{2n} \}$. This group quotient partitions $\mathbb{Z}_2^{2n}$ into $|Z_2^{2n}| / |C^\perp| = 2^{n-k}$ disjoint cosets. Given some error $e$, all elements in the same coset $e + C^\perp$ have the same syndrome $s$ for some $s \in \mathbb{Z}^{n-k}_2$, i.e., $u \Lambda H^T = s$ for all $u \in e + C^\perp$. For the coset associated with the syndrome $s \in \mathbb{Z}^{n-k}_2$, we select a coset leader $e_s$ by minimum weight, i.e.,

$$e_s = \arg \min_{e \in \mathbb{Z}_2^{2n}: e \Lambda H^T = s} wt(e), \quad (8)$$

for some weight function $wt(\cdot)$. This is the most often way to select coset leasers because in many channel models, the probability $P(e)$ of an error $e$ is a decreasing function of $wt(e)$. There are $2^{n-k}$ syndromes $s$'s associated with the $2^{n-k}$ disjoint cosets $e_s + C^\perp$. So we can write down the quotient group by partition

$$\mathbb{Z}_2^{2n} / C^\perp = \{ e_s + C^\perp \mid s \in \mathbb{Z}_2^{n-k} \}.$$

List all elements in $C^\perp$ by $v_1 = 0, v_2, \cdots, v_{|C^\perp|} \text{ where } |C^\perp| = 2^{n+k}$. And list all $e_s$'s by $e_1 = 0, e_2, \cdots, e_{|C|} \text{ where } |C| = 2^{n-k}$. Then we can write down the standard array [16] for syndrome decoding:

$$\begin{bmatrix} e_1 + C^\perp = C^\perp \\
 e_2 + C^\perp \\
 \vdots \\
 e_{|C|} + C^\perp \end{bmatrix} \rightarrow \begin{bmatrix} e_1 = 0 & v_2 & \cdots & v_{|C^\perp|} \\
 e_2 & e_2 + v_2 & \cdots & e_2 + v_{|C^\perp|} \\
 \vdots & \vdots & \ddots & \vdots \\
 e_{|C|} & e_{|C|} + v_2 & \cdots & e_{|C|} + v_{|C^\perp|} \end{bmatrix}. \quad (9)$$

Regardless of the orthogonality and the weight function to be used, the array (9) defines a classical syndrome decoding (CSD) that when a syndrome $s$ is measured, then the coset leader $e_s$ is selected to perform the error correction. The set of correctable error patterns is

$$\mathcal{E}_{C^\perp} = \{ e_s \mid s \in \mathbb{Z}_2^{n-k} \},$$

and the uncorrectable error probability is $1 - P(\mathcal{E}_{C^\perp}) = 1 - \sum_{s \in \mathbb{Z}_2^{n-k}} P(e_s)$. But a complete CSD becomes hard when $(n - k)$ goes asymptotically large. An alternative
way is to decode the code up to some designed correction capability $t$ in polynomial time (which is very important for long codes such as Goppa codes [17,18]). By classical coding theory [16],

\[ \mathcal{E}_{C^\perp} \supseteq \mathcal{E}_{C^\perp}(d') \triangleq \left\{ e \in \mathbb{Z}_2^{2n} | wt(e) \leq \left\lfloor \frac{d' - 1}{2} \right\rfloor \right\} \]

(and further $\mathcal{E}_{C^\perp} \nsubseteq \mathcal{E}_{C^\perp}(d' + 2)$ if stated more precisely) with $d'$ the minimum distance of $C^\perp$. A typical classical bounded distance decoding (CBDD) is to decode the code up to the designed correction capability $t' = \left\lfloor \frac{d' - 1}{2} \right\rfloor$, i.e., the set of correctable error patterns becomes $\mathcal{E}_{C^\perp}(d')$. Although CBDD corrects less errors than that of CSD, $P(\mathcal{E}_{C^\perp}(d'))$ is more analytical than $P(\mathcal{E}_{C^\perp})$. To help the following discussion, we write down the hints to prove

\[ \mathcal{E}_{C^\perp} \supseteq \mathcal{E}_{C^\perp}(d'). \]  

First, an error $e$ in $\mathcal{E}_{C^\perp}(d')$ is either $0$ or not in the first row of (9). Next, by group theory [19], two elements $e$ and $e'$ in $\mathbb{Z}_2^{2n}$ are in distinct cosets (different rows of (9)) iff $e + e' \notin C^\perp$. Then, since $C^\perp \setminus \{0\}$ has minimum weight $d'$, the set $\mathcal{E}_{C^\perp} \setminus \{0\}$ must contain $\mathcal{E}_{C^\perp}(d') \setminus \{0\}$ so that $\mathcal{E}_{C^\perp} \supseteq \mathcal{E}_{C^\perp}(d')$.

We now turn to the quantum case. The stabilizer property (6), (7) implies the degeneracy property that if two errors $E \in \varphi^{-1}(e)$ and $E' \in \varphi^{-1}(e')$ satisfy $e + e' \in C$, then the two errors have the same syndrome and correspond to equivalent error correction effect. Since $C^\perp \supseteq C$, we can further consider the group quotient $C^\perp/C = \{v + C | v \in C^\perp\}$ with $|C^\perp/C| = |C^\perp|/|C| = 2^k$. A straightforward way to do a partition is by diagonalizing $H = [I \ A | B \ D]$ and write down the standard form [8,15] for stabilizer codes:

\[
\begin{bmatrix}
 n-k & k & n-k & k \\
 I & A & B & D \\
 k & k & & \\
 O & I & D^T & O \\
 O & O & A^T & I \\
 n-k & & O & O
\end{bmatrix}
= \begin{bmatrix}
 H \\
 L_X \\
 L_Z \\
 T
\end{bmatrix}
= \begin{bmatrix}
 G \\
 L \\
 T
\end{bmatrix}.
\]

(11)

Since $C = \text{Row}(H)$ and $C^\perp = \text{Row}(G) = \text{Row}([H \ L])$, a partition can be written as $C^\perp/C = \{v + C | v \in \text{Row}(L)\}$, where $|\text{Row}(L)| = 2^{2k}$. We can similarly list all $v \in \text{Row}(L)$ as $v_1 = 0$, $v_2$, $\ldots$, $v_{2^{2k}}$ and write down the quantum standard array...
with classical coset leaders

\[
\begin{bmatrix}
e_1 + C^\perp = C^\perp \\
e_2 + C^\perp \\
\vdots \\
e_{|C|} + C^\perp 
\end{bmatrix}
\rightarrow
\begin{bmatrix}
e_1 + C = C \\
e_2 + C \\
\vdots \\
e_{|C|} + C 
\end{bmatrix}
\]

(12)

It is interesting that now the rule of the kernel \( C \) is similar to the rule of the zero state \( \mathbf{0} \) in (9). This can also be observed from the encoding process [8,15] that \( \varphi(S) = C \) and all operators in \( S \) are needed to create the state \( |O\rangle = \sum_{g \in S} |0\rangle^\otimes n \) like a zero state of the stabilizer code \( C(S) \). And for decoding, it is known that good quantum codes can be constructed from classical codes with existed classical decoding algorithms reused [20,21]. So a convenient way to define the set of correctable error patterns for \( C(S) \) is

\[
\mathcal{E}_C = \{ E \in \mathcal{G}_n | \varphi(E) \in \{ e_1, e_2, \ldots, e_{|C|} \} \}.
\]

Then, distinct correctable errors produce linearly independent results recognized by distinct syndromes. By definition, the code is nondegenerate [7,8] (or called pure because the linearly independent results are orthogonal for stabilizer codes). More specifically, a bounded distance decoding may be performed due to efficiency, and then, the set of correctable error patterns is now

\[
\mathcal{E}_C(d') = \left\{ E \in \mathcal{G}_n | gw(\varphi(E)) \leq \left\lfloor \frac{d'-1}{2} \right\rfloor \right\}
\]

with \( d' = \min\{gw(v) | v \in C^\perp \setminus \{0\} \} \). It is clear that \( \mathcal{E}_C(d') \subseteq \mathcal{E}_C \) and the code is still nondegenerate. But if \( E \in \varphi^{-1}(e_s) \) is correctable, then all elements in \( \varphi^{-1}(e_s + C) \) are correctable. Theoretically, one can use the stabilizer property to extremely enlarge the set of correctable error patterns as

\[
\hat{\mathcal{E}}_C(d') \triangleq \{ EF | E \in \mathcal{E}_C(d'), F \in \varphi^{-1}(C) \} = \mathcal{E}_C(d') \cup SK.
\]

Then, the code is always degenerate, no matter that it is initially using a decoding algorithm for \( \mathcal{E}_C(d') \), i.e., treating the code as a nondegenerate code. So we have the clarification that the degeneracy property is implicitly embedded in any decoding strategy, but whether a code is degenerate or not depends on the definition of the set of correctable error patterns.

We continue to clarify that how degenerate codes are defined typically. For a stabilizer code \( C(S) \), consider the associated syndrome decoding defined by \( \mathcal{E}_C \) and the implicit set of correctable error patterns

\[
\hat{\mathcal{E}}_C = \mathcal{E}_C \cup SK = \{ E \in \mathcal{G}_n | \varphi(E) \in (e_1 + C) \cup (e_2 + C) \cup \cdots \cup (e_{|C|} + C) \}.
\]
It is known that
\[
\hat{E}_C \supseteq \mathcal{E}_C(d) = \left\{ E \in G_n | g w(\varphi(E)) \leq \left\lfloor \frac{d - 1}{2} \right\rfloor \right\}
\]
with \( d = \min \{gw(v) | v \in C^\perp \setminus C \} \). The proof can be referred to Theorem 1 of [6], or by using similar arguments to (10): First, an error \( E \in \mathcal{E}_C(d) \) is either in \( \varphi^{-1}(C) = SK \) (automatically corrected) or not in the inverse image of the first row of (12); next, since \( C^\perp \setminus C \) has minimum weight \( d \), the set \( \hat{E}_C \setminus \varphi^{-1}(C) \) must contain \( \mathcal{E}_C(d) \setminus \varphi^{-1}(C) \) so that \( \hat{E}_C \supseteq \mathcal{E}_C(d) \). Now we have \( \mathcal{E}_C \supseteq \mathcal{E}_C(d') \), and \( \hat{E}_C \supseteq \mathcal{E}_C(d) \supseteq \mathcal{E}_C(d') \). When \( \mathcal{E}_C(d) \supseteq \mathcal{E}_C(d') \), for any \( e \in \varphi(\mathcal{E}_C(d) \setminus \mathcal{E}_C(d')) \), there must exist another \( e' \in \varphi(\mathcal{E}_C(d)) \) s.t. \( e + e' \in C \), i.e., \( E \in \varphi^{-1}(e) \) and \( E' \in \varphi^{-1}(e') \) have the same syndrome and correspond to equivalent correction effect. These errors cannot be distinguished by syndromes and are often called degenerate errors. Typically, \( \mathcal{E}_C(d) \) is defined as the set of correctable error patterns without further specification [7,8]. Under this convention, a code \( C \) is nondegenerate (pure) iff \( \mathcal{E}_C(d') = \mathcal{E}_C(d) \). Otherwise, \( \mathcal{E}_C(d') \subsetneq \mathcal{E}_C(d) \) and the code is degenerate (impure). So typically, we have the relation for nondegenerate codes
\[
\mathcal{E}_C(d') = \mathcal{E}_C(d) \subseteq \mathcal{E}_C = \varphi^{-1}(\{e_1, e_2, \ldots, e_{|C|}\})
\]
with the associated implicit sets of correctable error patterns
\[
\hat{E}_C(d') = \hat{E}_C(d) \subseteq \hat{E}_C = \varphi^{-1}((e_1 + C) \cup (e_2 + C) \cup \cdots \cup (e_{|C|} + C)).
\]
And for degenerate codes,
\[
\mathcal{E}_C(d') \subsetneq \mathcal{E}_C(d) \subsetneq \mathcal{E}_C,
\]
but once a complete syndrome decoding for \( \mathcal{E}_C \) can be performed,
\[
\hat{E}_C(d') \subsetneq \hat{E}_C(d) \subseteq \hat{E}_C.
\]
So a degenerate decoding algorithm for \( \mathcal{E}_C(d) \) is not necessary to have better performance than that of a nondegenerate decoding algorithm for \( \mathcal{E}_C \).

To prevent any ambiguity from the dichotomy of “degenerate” described above, we will use quantum minimum error probability decoding (QMEPD) to name an optimal quantum decoding algorithm in the next section. As per previous discussion, an optimal quantum decoding is intuitively to reselect a set of new \( e'_s \) instead of \( e_s \) such that \( P(\hat{E}_C) \) is maximized. It requires that the aggregate probability \( P(e'_s + C) \triangleq \sum_{u \in C} P(e'_s + u) \) is maximized for each \( s \), i.e.,
\[
e'_s = \arg \max_{e \in \mathbb{Z}_2^n, eAH^T = s} P(e + C).
\]
If \( e_s \) in (12) are replaced by \( e'_s \), we call the array the quantum standard array with quantum coset leaders, which defines a quantum syndrome decoding optimized in the
sense of probability. There is no fixed selection of \( e'_s \) unless a channel model is given to specify \( P(\cdot) \). Upon a given channel model and some given \( s \in \mathbb{Z}_{2}^{n-k} \), a suggested method \([9,10]\) to search \( e'_s \) is to first define \( u_s = (0_s | s 0_k) \in \text{Row}(T) \) from (11), and find

\[
e'_s = \arg \max_{e \in u_s + \text{Row}(L)} P(e + C),
\]

which quickly reduces the exhaustive search size from \( |\text{Row}(G)| = 2^{n+k} \) to \( |\text{Row}(L)| = 2^{2k} \). We will rigorously prove in the next section that this is indeed an optimal quantum decoding for stabilizer codes, but over the depolarizing channel, this kind of decoding in general is still NP-hard.

5 Decoding over the depolarizing channel

The depolarizing channel is one of the most important channel models in quantum communication and quantum cryptography \([13,14,22]\). In this section, we will consider the decoding problems for finding a most likely error and for finding a most likely error coset over the depolarizing channel. Like classical decoding, it is very intuitive to consider the decoding problem for finding a most likely error, called quantum maximum likelihood decoding (QMLD). But a further analysis shows that the optimal decoding to minimize the decoding error probability is to find a most likely error coset, for which we call it quantum minimum error probability decoding (QMEPD). We will show that these two problems are NP-hard.

We assume the memoryless model that the depolarizing channel affects each qubit independently such that for some \( p \in [0, 1] \), a qubit is depolarized to be a completely mixed state \( I/2 \) with probability \( p \), and remains intact with probability \( 1 - p \). If \( \rho_1 \) is a density operator of one-qubit depolarizing channel input, then it is known that the channel output can be expressed as

\[
E(\rho) = p(I/2) + (1 - p)\rho_1 = (1 - \varepsilon)\rho_1 + (\varepsilon/3)(X\rho_1X + Y\rho_1Y + Z\rho_1Z)
\]

with \( \varepsilon = \frac{3}{4}p \).

Now consider an \([n, k, d]\) stabilizer code \( C(S) \) with \( d \geq 2t+1 \) as in Sect. 2. Again the stabilizer group \( S = (g_1, g_2, \ldots, g_{n-k}) \) has a check matrix \( H \) as in (3). Given a coded state \( |\psi\rangle \in C(S) \), let \( \rho = |\psi\rangle \langle \psi | \) be the channel input of the depolarizing channel. Then, the channel output is

\[
E(\rho) = \sum_{u \in \mathbb{Z}_{2}^{n}} (\sqrt{\lambda_u} E_u)\rho(\sqrt{\lambda_u} E_u)^{\dagger},
\]

where \( E_u = \sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n \) with \( \sigma_j \in \{ I, X, Y, Z \} \) such that \( \varphi(E_u) = u \) and \( \lambda_u = (\varepsilon/3)^{g_w(u)}(1 - \varepsilon)^{n-g_w(u)} \) since different uses of the channel are independent.

\( \Box \) Springer
The channel output $\mathcal{E}(\rho)$ is a mixed state with ensemble

$$\{\lambda_u, E_u|\psi\rangle\}_{u \in \mathbb{Z}_2^{2n}}.$$  

Notice that a smaller $gw(u) = w(E_u)$ results in a larger $\lambda_u$ since $0 \leq \varepsilon = \frac{3}{4} p \leq \frac{3}{4}$. We first consider the decoding problem for finding a most likely error. Suppose that $\mathcal{E}(\rho)$ is received and the $n - k$ syndrome measurements by operators defined by the generators $g_i$’s of $S$ are performed, as in Sect. 3. Likewise, map the measurement results to a binary syndrome vector $s \in \mathbb{Z}_2^{n-k}$. Let $E$ be the unknown channel error operator. Given the syndrome $s \in \mathbb{Z}_2^{n-k}$, the event $(E = E_u)$ occurs with probability

$$P(E = E_u|\text{syndrome is } s) = \frac{P(E = E_u)P(\text{syndrome is } s|E = E_u)}{P(\text{syndrome is } s)} = \frac{\lambda_u P(\text{syndrome is } s|E = E_u)}{q_s} = \begin{cases} \frac{\lambda_u}{q_s} & \text{if } u \Lambda H^T = s, \\ 0 & \text{otherwise}, \end{cases}$$

where

$$q_s \triangleq P(\text{syndrome is } s) = \sum_{u \in \mathbb{Z}_2^{2n}} P(E = E_u)P(\text{syndrome is } s|E = E_u) = \sum_{u \in \mathbb{Z}_2^{2n}: u \Lambda H^T = s} \lambda_u$$

is a constant given $s$. Since a smaller $gw(u)$ results in a larger $\lambda_u$, to find a most likely error, we have

**Quantum maximum likelihood decoding (QMLD)**

**Input:** A full row rank $m \times 2n$ binary matrix $H$ satisfying $H \Lambda H^T = O$, and a binary vector $s \in \mathbb{Z}_2^m$.

**Output:** A binary vector $e \in \mathbb{Z}_2^{2n}$ satisfying $e \Lambda H^T = s$ and minimizing $gw(e)$.

Obviously, there is a polynomial-time reduction from QBDD to QMLD. So by Corollary 1, we have

**Corollary 2** QMLD is NP-hard, even if $H = [H_X|O]$ or $H = [O|H_Z]$.

Since QMLD does not limit the search scope of $gw(e)$, QMLD has better decoding performance than that of QBDD in practice. But it is known that a decoding rule based on QMLD does not minimize the decoding error probability [9,10]. To see this, again let $E$ be the unknown channel error operator. If we select $E^v_\dagger$ as the error correction operator for some $v \in \mathbb{Z}_2^{2n}$, then a successful correction will be performed...
iff \( E_v^\dagger (E \rho E^\dagger) E_v = \rho \) iff \( E_v^\dagger E \in SK \) by (6). Let \( P_s(\cdot) \triangleq P(\cdot | \text{syndrome is } s) \). In order to minimize the decoding error probability given \( s \), we have to find a \( v \in \mathbb{Z}_2^{2n} \) maximizing

\[
P(E_v^\dagger E \in SK | \text{syndrome is } s) = P_s(E_v^\dagger E \in SK)
\]

\[
= \sum_{u \in \mathbb{Z}_2^{2n}} P_s(E = E_u) P_s(E_v^\dagger E \in SK | E = E_u)
\]

\[
= \sum_{u \in \mathbb{Z}_2^{2n} : u \Lambda H^T = s} \frac{\lambda_u}{q_s} P_s(E_v^\dagger E \in SK | E = E_u) \text{ by (15)}
\]

\[
= \frac{1}{q_s} \sum_{u \in \mathbb{Z}_2^{2n} : u \Lambda H^T = s} \lambda_u
\]

\[
= \begin{cases} \frac{1}{q_s} \sum_{u \in v + \text{Row}(H) : u \Lambda H^T = s} \lambda_u & \text{if } v \Lambda H^T = s, \\ 0 & \text{otherwise} \end{cases}
\]

The last equality holds since for all \( u \in v + \text{Row}(H), u \Lambda H^T = s \) iff \( v \Lambda H^T = s \) by the fact that \( H \Lambda H^T = O \). Now let \( \alpha_v \triangleq \sum_{u \in v + \text{Row}(H)} \lambda_u \) be the aggregate probability of the coset \( v + \text{Row}(H) \). By recalling \( \lambda_u = (\varepsilon/3)^{g_w(u)} (1 - \varepsilon)^{n - g_w(u)} \), we have

**Quantum minimum error probability decoding (QMEPD)**

**Input:** A full row rank \( m \times 2n \) binary matrix \( H \) satisfying \( H \Lambda H^T = O \), a binary vector \( s \in \mathbb{Z}_2^m \), and a real number \( 0 \leq \varepsilon \leq 3/4 \).

**Output:** A binary vector \( v \in \mathbb{Z}_2^{2n} \) satisfying \( v \Lambda H^T = s \) and maximizing \( \alpha_v = \sum_{u \in v + \text{Row}(H)} (\varepsilon/3)^{g_w(u)} (1 - \varepsilon)^{n - g_w(u)} \).

Note that the optimal decoding problem can be formulated in another way by assigning each coset \( v + \text{Row}(H) \) a unique representative and limiting the output to be one of those representatives (see DQMLD in [10] or Sec. IV of [9]). But our formulation for QMEPD is an important step to classify the complexity of QMEPD. Now we show

**Theorem 3** **QMEPD is NP-hard.**

**Proof** By assuming \( H = [H_X | O] \), we reduce QMLD to QMEPD in polynomial time. Suppose we have a polynomial-time algorithm for QMEPD. Given an instance of QMLD with some \( H = [H_X | O] \) and \( s \in \mathbb{Z}_2^m \), let QMEPD have the same \( H \) and \( s \) in its inputs. Now \( | \text{Row}(H) | = 2^n \), and observe that \( \alpha_v = (1 - \varepsilon)^n \sum_{u \in v + \text{Row}(H)} (\varepsilon/3)^{g_w(u)} (1 - \varepsilon)^{n - g_w(u)} \). Let the \( \varepsilon \) in QMEPD be sufficiently small such that \( 0 < \frac{\varepsilon/3}{1 - \varepsilon} < \frac{1}{2m} \), and then, use the polynomial-time algorithm to solve QMEPD. By our selection of \( \varepsilon \), the algorithm must output a vector \( v \) such that the coset \( v + \text{Row}(H) \) contains a solution \( e \) to the problem QMLD. Suppose not, i.e., there
exists an \( e_1 \notin v + \text{Row}(H) \) such that \( e_1 \Lambda H^T = s \) and \( g_w(e_1) < g_w(e) \) with an \( e \in v + \text{Row}(H) \) having a minimum generalized weight among all vectors in the coset \( v + \text{Row}(H) \). Then, we have

\[
\alpha_{e_1} = (1 - \varepsilon)^n \sum_{u \in e_1 + \text{Row}(H)} \left( \frac{\varepsilon/3}{1 - \varepsilon} \right)^{g_w(u)}
\]

\[
\geq (1 - \varepsilon)^n \left( \frac{\varepsilon/3}{1 - \varepsilon} \right)^{g_w(e_1)}
\]

\[
\geq (1 - \varepsilon)^n \left( \frac{\varepsilon/3}{1 - \varepsilon} \right)^{g_w(e) - 1}
\]

\[
> (1 - \varepsilon)^n 2^m \left( \frac{\varepsilon/3}{1 - \varepsilon} \right)^{g_w(e)}
\]

\[
\geq (1 - \varepsilon)^n \sum_{u \in v + \text{Row}(H)} \left( \frac{\varepsilon/3}{1 - \varepsilon} \right)^{g_w(u)}
\]

\[
= \alpha_v,
\]

a contradiction to the maximality of \( \alpha_v \). However, we only have \( v = (x|z) \) for some \( x, z \in \mathbb{Z}_2^n \). To obtain a solution to QMLD from \( v \), let \( e' \triangleq (0|z) \in \mathbb{Z}_2^n \). First, \( e' \) satisfies \( e' \Lambda H^T = s \) since \( H = [H_X|O] \). That means \( g_w(e') \geq g_w(e) \) by the minimum of the \( g_w(e) \) in QMLD. But \( e \in v + \text{Row}(H) \) implies \( e = (x + h|z) \) for some \( h \in \text{Row}(H_X) \), so \( g_w(e) \geq w_H(z) = g_w(e') \) by (4). We have shown that \( e' \Lambda H^T = s \) and \( g_w(e') = g_w(e) \), i.e., the vector \( e' \) constructed from \( v \) is also a solution to QMLD. Thus, QMLD is polynomial-time reducible to QMEPD, as \( H = [H_X|O] \) is assumed. By Corollary 2, QMEPD is NP-hard.

Recall the quantum standard array with kernel \( C \) in (12). The QMEPD represents an algorithm that can always sort out a coset \( e_s + v + C \) with the largest aggregate probability, by any given \( s \in \mathbb{Z}_2^{2k} \) and \( \varepsilon \in [0, 3/4] \). The search can be restricted to \( 2^{2k} \) elements in \( \text{Row}(L) \) as in (13). But from problem statement, QMEPD relaxes this restriction and can accommodate more possible search methods. However, Theorem 3 proves that by varying \( p \) to a trivial value, QMEPD can solve QMLD in polynomial time and thus be NP-hard. Also note that in order to perform QMEPD practically, an auxiliary channel estimation may be needed to estimate the actual \( \varepsilon \) of the channel, and to compute \( \alpha_v \), the exponential function needs large space complexity [23,24]. However, for the time complexity, the NP-hardness of QMEPD in Theorem 3 answers the dangling problem of how hard an optimal decoding over the depolarizing channel is.

In quantum cryptography, the hardnesses of QMLD and QMEPD reflect the hardness of eavesdropping on a stabilizer code-based cryptosystem over the depolarizing channel model, i.e., the artificial noise used to protect the system is generated in some way like the depolarizing channel. Corollary 2 and Theorem 3 indicate that such a system can effectively resist the attacks based on QMLD or QMEPD.
6 Conclusion

Based on the generalized weight, we first classify the complexity of QBDD. Before giving any channel model, we give some insight into the quantum decoding problems, illustrating that degeneracy property is implicitly embedded in any decoding strategy, but whether a code is degenerate depends on the definition of the set of correctable error patterns. Then, we classify the complexities of QMLD and QMEPD over the depolarizing channel. QBDD is shown to be NP-hard based on the NP-completeness of CGW and the handling of the full row rank. QMLD and QMEPD, over the depolarizing channel, are shown to be NP-hard by showing that QBDD is reducible to QMLD and QMLD is reducible to QMEPD in polynomial time. The NP-hardnesses of these decoding problems indicate that decoding general stabilizer codes is extremely difficult, which strengthens the foundation of quantum code-based cryptography.

Funding This work was supported by the Ministry of Science and Technology, Taiwan, under Contract MOST 101-2221-E-007-096-MY3.

References

1. Berlekamp, E., McEliece, R., van Tilborg, H.: On the inherent intractability of certain coding problems. IEEE Trans. Inf. Theory 24, 384–386 (1978)
2. Sipser, M.: Introduction to the Theory of Computation. Thomson Course Technology, Boston (2006)
3. McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. Nasa dsn progress report 42-44, NASA (1978)
4. Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.): Post-Quantum Cryptography. Springer, Berlin (2009)
5. Bernstein, D.J., Lange, T., Peters, C.: Wild McEliece. In: Proceedings of Selected Areas in Cryptography, pp. 143–158 (2010)
6. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction and orthogonal geometry. Phys. Rev. Lett. 78, 405 (1997)
7. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over GF(4). IEEE Trans. Inf. Theory 44, 1369–1387 (1998)
8. Gottesman, D.: Stabilizer Codes and Quantum Error Correction. Ph.D. thesis, California Institute of Technology (1997)
9. Poulin, D., Chung, Y.: On the iterative decoding of sparse quantum codes. Quantum Inf. Comput. 8, 987–1000 (2008)
10. Hsieh, M.H., Le Gall, F.: NP-hardness of decoding quantum error-correction codes. Phys. Rev. A 83, 052331 (2011)
11. Fujita, H.: Quantum McEliece public-key cryptosystem. Quantum Inf. Comput. 12, 0181–0202 (2012)
12. Cohen, G., Encheva, S., Litsyn, S.: On binary constructions of quantum codes. IEEE Trans. Inf. Theory 45, 2495–2498 (1999)
13. Bennett, C.H., Shor, P.W.: Quantum information theory. IEEE Trans. Inf. Theory 44, 2724–2742 (1998)
14. Nielsen, M., Chuang, I.: Quantum Computation and Quantum Information. Cambridge Univ. Press, Cambridge (2000)
15. Kuo, K.Y., Lu, C.C.: A further study on the encoding complexity of quantum stabilizer codes. In: Proceedings of 2010 International Symposium on Information Theory and its Applications, pp. 1041–1044 (2010)
16. MacWilliams, F., Sloane, N.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, Amsterdam (1978)
17. Pretzel, O.: Codes and Algebraic Curves. Oxford University Press, Oxford (1998)
18. Stichtenoth, H.: Algebraic Function Fields and Codes, 2nd edn. Springer, Berlin (2008)
19. Herstein, I.N.: Abstract Algebra, 3rd edn. Wiley, Hoboken (1996)
20. Grassl, M., Beth, T.: Quantum BCH codes. In: Proceedings X. International Symposium on Theoretical Electrical Engineering, Magdeburg, pp. 207–212 (1999)

21. Hamada, M.: Concatenated quantum codes constructible in polynomial time: efficient decoding and error correction. IEEE Trans. Inf. Theory 54, 5689–5704 (2008)

22. Smith, G.: Private classical capacity with a symmetric side channel and its application to quantum cryptography. Phys. Rev. A 78, 022306 (2008)

23. Chudnovsky, D.V., Chudnovsky, G.V.: Approximations and complex multiplication according to Ramanujan. In: Ramanujan Revisited, pp. 375–472. Academic Press Inc., Boston (1988)

24. Fürer, M.: Faster integer multiplication. In: Proceedings of the 39th Annual ACM Symposium on Theory of Computing, pp. 55–67 (2007)

**Publisher’s Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.