Noname manuscript No.
(will be inserted by the editor)

An Optimal Quantum Error-Correcting Procedure Using Quantifier Elimination

Ying-Ji Sun · **Ming Xu** · **Yuxin Deng**

Received: date / Accepted: date

Abstract Quantum communication channels suffer from various noises, which are mathematically modelled by error super-operators. To combat these errors, it is necessary to design recovery super-operators. This paper aims to construct the optimal recovery that maximizes the minimum fidelity through the noisy channel. It is typically a MAX-MIN problem, out of the scope of convex optimization. Compared to existing methods, our method is exact and complete by reduction to quantifier elimination over real closed fields in a fragment of two alternative quantifier blocks. Finally the complexity is shown to be in **EXP**.

Keywords quantum error-correction · quantifier elimination · complexity

1 Introduction

Quantum communication channels are often affected by various noises, which potentially bring disastrous outcomes. So it is necessary to combat the errors caused by those noises for protecting the information resource. To achieve this goal, the theory of error-correction, including quantum error-correction (QEC), came into being and was increasingly developed in the past decades [5]. Nowadays, it is also closely related to many important topics in quantum information theory, such as quantum process tomography [21] and fault-tolerant quantum computation [1].

Ying-Ji Sun
Shanghai Key Lab of Trustworthy Computing, East China Normal University, Shanghai, 200062, China
E-mail: 51184506039@stu.ecnu.edu.cn

Ming Xu
Shanghai Key Lab of Trustworthy Computing, East China Normal University, Shanghai, 200062, China
E-mail: mxu@cs.ecnu.edu.cn
Orcid=0000-0002-9906-5677

Yuxin Deng
Shanghai Key Lab of Trustworthy Computing, East China Normal University, Shanghai, 200062, China
E-mail: yxdeng@sei.ecnu.edu.cn

Classical error-correction employs the scheme of redundancy. For 1-bit data, the simplest way is to send multiple copies of the input data, and determine the output data by a majority vote among the receiving information (under the fair assumption that the error rate is not too high). More generally, $[n,k]$-linear codes $\mathscr{C}$ with $n \geq k$ are invented to encode k-bit data into n-bit data (called *codewords*). Then $\mathscr{C}$ is characterized as the linear space, w.r.t. addition modulo 2, spanned by all its codewords. When a linear code has the minimum Hamming distance at least $2d+1$ over its nonzero codewords, it can correct errors up to d bits [12].

Errors in the classical world are exclusively bit-flip, but in the quantum world they could be bit-flip, phase-flip, or even more complicated ones. In 1995, Shor constructed the first quantum error-correcting code for any 1-qubit error [18]. The Shor code, a $[9,1]$-linear code, prepares a highly entangled 9-bit state to correct bit-flip and phase-flip, i.e. any 1-qubit error. Here, the highly entangled states are introduced to represent duplicated states, since cloning quantum information is generally impossible [24]. When errors occur independently on multiple qubits, the method would still be applicable.

More generally, suppose $\mathscr{C}_1$ and $\mathscr{C}_2$ are $[n,k_1]$- and $[n,k_2]$-linear codes respectively, satisfying $\mathscr{C}_2 \subset \mathscr{C}_1$ and both $\mathscr{C}_1$ and $\mathscr{C}_2^{\perp}$ (the orthonormal complement of $\mathscr{C}_2$) can correct errors on up to d bits, Calderbank and Shor constructed an $[n,k_1-k_2]$-linear code that can correct any d-qubit error [4]. As a special case, the Steane code [19], constructed from the $[7,4]$-Hamming code and its dual (a $[7,3]$-linear code), is a $[7,1]$-linear code that can correct any 1-qubit error. Actually, all these codes, uniformly named by Calderbank–Shor–Steane codes (CSS codes for short), are a subclass of stabilizer codes [9], which lays a unified foundation for QEC.

However, the QEC theory is much more involved and challenging partially due to the following two issues:

1. Since the quantum state space is a continuum, most errors are neither simply bit-flip nor phase-flip. It is generic to model them by super-operators (to be defined in Sect. 2, together with other notions and notations).
2. The aforementioned codes aim at correcting the corrupted information to some extent, rather than recovering the corrupted information to the original information.

So it motivates people to consider

Problem 1 Given an error super-operator $\mathscr{E}$, is there a recovery super-operator $\mathscr{R}$ that perfectly corrects it, i.e. $\mathscr{R} \circ \mathscr{E} = \mathscr{I}$, the identity super-operator?

In 1997, Knill and Laflamme established the profound result:

Theorem 1 ([10]) *An error super-operator $\mathscr{E} = \{\mathbf{E}_k \,|\, k \in [m]\}$ with $[m] = \{0,1,\ldots, m-1\}$ is perfectly correctable if and only if it satisfies that*

1. *for each pair $i, j \in [m]$, there is a constant $\alpha_{i,j}$ such that $\mathbf{E}_j^{\dagger}\mathbf{E}_i = \alpha_{i,j}\mathbf{I}$, and*
2. *all these constants $\alpha_{i,j}$ form a positive Hermitian matrix $(\alpha_{i,j})_{m\times m}$.*

It implies not all errors are perfectly correctable, as the necessary and sufficient condition in Theorem 1 is nontrivial. A simple example is given below.

Example 1 Consider the error super-operator $\mathscr{E}_0 = \{\mathbf{E}_0, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3\}$, where

$$\mathbf{E}_0 = \tfrac{16}{25}\,\mathbf{I}\otimes\mathbf{I}, \qquad \mathbf{E}_1 = \tfrac{12}{25}\,\mathbf{I}\otimes\mathbf{X}, \qquad \mathbf{E}_2 = \tfrac{12}{25}\,\mathbf{X}\otimes\mathbf{I} \qquad \text{and} \qquad \mathbf{E}_3 = \tfrac{9}{25}\,\mathbf{X}\otimes\mathbf{X}.$$

The matrix $\mathbf{X} = |0\rangle\langle 1| + |1\rangle\langle 0|$ is the Pauli X-matrix (corresponding to the bit-flip). It is not difficult to check that for each pair $i, j \in [4]$ with $i \neq j$, there is no constant $\alpha_{i,j}$ such that $\mathbf{E}_j^\dagger \mathbf{E}_i = \alpha_{i,j}\mathbf{I}$, which violates the condition of Theorem 1. Hence such an error $\mathscr{E}_0$ cannot be corrected perfectly.

Even so, people might still expect to correct errors as perfectly as possible. In this paper, we will study the following optimal QEC problem. (Particularly, the optimality is specified in terms of fidelity, which is a distance measure such that closer distances yield larger fidelities, and will be defined in the formula (6).)

Problem 2 Given an error super-operator $\mathscr{E}$, what is the optimal recovery super-operator $\mathscr{R}$ that maximizes the minimum fidelity over all initial quantum states ρ, i.e. $\underline{\mathrm{Fid}}(\mathscr{R}\circ\mathscr{E}) = \min_\rho \mathrm{Fid}(\mathscr{R}\circ\mathscr{E}, \rho)$?

The optimal error-correction is formally described by

$$\max_{\mathscr{R}} \underline{\mathrm{Fid}}(\mathscr{R}\circ\mathscr{E}) = \max_{\mathscr{R}} \min_{\rho} \mathrm{Fid}(\mathscr{R}\circ\mathscr{E}, \rho). \tag{1}$$

Obviously, it is a nonlinear MAX-MIN problem. To solve it, we will reduce it to the quantified constraint on $\mathscr{R}$:

$$\forall \mathscr{R}' : \underline{\mathrm{Fid}}(\mathscr{R}'\circ\mathscr{E}) \leq \underline{\mathrm{Fid}}(\mathscr{R}\circ\mathscr{E}), \tag{2}$$

where $\forall$ is a universal quantifier which means "for each". Any solution of the latter is an optimal recovery of the former. Hence the main task of this paper is formulating and solving the quantified constraint. Our contributions are three-fold:

1. Problem 2 (the optimal QEC problem) is solved, which is open in [26].
2. Our method is based on the technique of quantifier elimination, which is absolutely exact.
3. The complexity of the proposed method is shown to be in **EXP**, which sets an upper bound of Problem 2.

1.1 Related work

Yamamoto *et al.* considered the optimal QEC problem in [26]. After relaxing the range of the matrix for encoding the density operator ρ, the original problem was reduced to the semi-definite programming (SDP) problem, and therefore a lower bound of $\underline{\mathrm{Fid}}(\mathscr{R}\circ\mathscr{E})$ was obtained, as well as a lower bound of $\max_{\mathscr{R}} \underline{\mathrm{Fid}}(\mathscr{R}\circ\mathscr{E})$, which explained why the authors called the procedure as the suboptimal one. Later, Yamamoto resorted to the technique of sum of squares (SOS) to attack the original problem when the quantum system is of 1-qubit [25]. The method, however, is not effective for the quantum system of 2-qubit or more, due to the theoretical bottleneck of SOS. Compared with the above existing works, our method adopts the technique of quantifier

elimination (QE) effective for quantum systems of arbitrarily many qubits. The complexity is also provided as **EXP**.

When the initial density operator $\rho_0 = \sum_{k\in[m]} p_k |\psi_k\rangle\langle\psi_k|$ with some discrete probabilistic distribution $\{p_k \,|\, k \in [m]\}$ is fixed, the minimum fidelity $\min_\rho \mathrm{Fid}(\mathscr{R}\circ\mathscr{E},\rho)$ would degenerate as the entanglement fidelity $\mathrm{Fid}(\mathscr{R}\circ\mathscr{E},\rho_0)$ or ensemble average fidelity $\sum_{k\in[m]} p_k \mathrm{Fid}^2(\mathscr{R}\circ\mathscr{E},|\psi_k\rangle\langle\psi_k|)$. Then the technique of SDP and convex optimization can be applied to find the optimal recovery without any relaxation [7, 11]. For the average entanglement fidelity $\sum_{k\in[m]} p_k \cdot \mathrm{Fid}(\mathscr{R}\circ\mathscr{E},|\psi_k\rangle\langle\psi_k|)$, to speed up the procedure, Fletcher *et al.* focused only on large eigenvalues of syndrome subspaces and neglected others, thus getting the near-optimal recovery [8]. More progresses on approximate QEC can be found in [13].

On the other hand, the technique of QE had been applied to solve several problems in quantum information theory. Using QE over real closed fields [20], the problems of entanglement, s-distillability, (s,t)-hidden variable model, n-dimensional quantum representation, s-Birkhoff property, s-shot zero-error capacity, and additive minimal output entropy, w.r.t. integer *constants* s,t,n, are shown to be decidable; while the same problems w.r.t. integer *parameters* s,t,n are undecided [23]. Unfortunately, the fidelity of quantum automata that can model a series of nondeterministic noisy channels is generally undecidable [3, 23]. It is obtained by a reduction from the undecidable Post's correspondence problem [16]. This paper reveals a new decidable problem in quantum information theory.

Organization Section 2 recalls some notions and notations from quantum computation. The optimal QEC is formulated as polynomial formulas in Sect. 3, and is solved in **EXP** in Sect. 4. Section 5 is the conclusion.

2 Preliminaries

First of all, we recall some useful notions and notations from quantum computation. Interested readers can refer to [15] for more details.

Let $[m]$ ($m \in \mathbb{Z}^+$) denote the finite set $\{0,1,\ldots,m-1\}$. Let $\mathscr{H}$ be a Hilbert space with dimension n throughout this paper, and $\{|i\rangle \,|\, i \in [n]\}$ be a basis of $\mathscr{H}$. Then any element $|\psi\rangle$ of $\mathscr{H}$ can be expressed by

$$|\psi\rangle = \sum_{i\in[n]} c_i |i\rangle \tag{3}$$

where $c_i \in \mathbb{C}$ ($i \in [n]$) and $\sum_{i\in[n]} |c_i|^2 = 1$. In other words, the element $|\psi\rangle$ is determined by those complex coefficients c_i ($i \in [n]$) under a given basis $\{|i\rangle \,|\, i \in [n]\}$.

Let $\mathscr{L}_\mathscr{H}$ be the set of linear operators on $\mathscr{H}$. For conciseness, we will omit such a subscript $\mathscr{H}$ if it is clear from the context. A linear operator ρ is *Hermitian*, if $\rho^\dagger = \rho$ where $\dagger$ denotes Hermitian adjoint; in addition it is *positive* if $\langle\psi|\rho|\psi\rangle$ is a nonnegative real number for any element $|\psi\rangle \in \mathscr{H}$. Clearly, positive operators are Hermitian. A *density operator* on $\mathscr{H}$ is a positive linear operator ρ with trace $\mathrm{tr}(\rho) = 1$. If $\rho = |\psi\rangle\langle\psi|$ for some $|\psi\rangle \in \mathscr{H}$, ρ is said to be *pure*; otherwise it is *mixed*. Let $\mathscr{D}$ be the set of density operators on $\mathscr{H}$.

A *super-operator* $\mathscr{F}$ on $\mathscr{H}$ is a linear operator on $\mathscr{L}_{\mathscr{H}}$; in addition it is *completely positive* if for any Hilbert space $\mathscr{H}'$, the trivially extended operator $\mathscr{I}_{\mathscr{H}'} \otimes \mathscr{F}$ maps the set of positive operators in $\mathscr{L}_{\mathscr{H}' \otimes \mathscr{H}}$ to itself, where $\otimes$ denotes tensor product and $\mathscr{I}_{\mathscr{H}'}$ denotes the identity super-operator on $\mathscr{L}_{\mathscr{H}'}$. Let $\mathscr{S}$ be the set of completely positive super-operators on $\mathscr{H}$. By Kraus representation [15, Thm. 8.3], a super-operator $\mathscr{F}$ is completely positive iff there are m linear operators $\mathbf{F}_0, \mathbf{F}_1, \ldots, \mathbf{F}_{m-1} \in \mathscr{L}$ with $m \leq n^2$, such that for any $\rho \in \mathscr{L}$,

$$\mathscr{F}(\rho) = \sum_{k \in [m]} \mathbf{F}_k \rho \mathbf{F}_k^\dagger. \tag{4}$$

In other words, the super-operator $\mathscr{F}$ is determined by those complex matrices $\mathbf{F}_k$ ($k \in [m]$), in which the number of complex entries is totally bounded by $mn^2 \leq n^4$. We assume w.l.o.g. the description of $\mathscr{F}$ is given by those Kraus operators $\{\mathbf{F}_k \,|\, k \in [m]\}$. Note that the Kraus representation of a super-operator is not unique in general. A super-operator $\mathscr{F} = \{\mathbf{F}_k \,|\, k \in [m]\}$ is *complete* (or equivalently *trace-preserving*) if

$$\sum_{k \in [m]} \mathbf{F}_k^\dagger \mathbf{F}_k = \mathbf{I}, \tag{5}$$

where $\mathbf{I}$ is the identity matrix. Specifically, the right hand side of the matrix equation (5) is Hermitian, and thus the matrix equation amounts to n^2 equations over $\mathbb{R}$, consisting of

- n equations over $\mathbb{R}$ on diagonal entries $\langle i| \sum_{k \in [m]} \mathbf{F}_k^\dagger \mathbf{F}_k |i\rangle = 1$ ($i \in [n]$), and
- $n(n-1)/2$ equations over $\mathbb{C}$ on upper-triangular entries $\langle i| \sum_{k \in [m]} \mathbf{F}_k^\dagger \mathbf{F}_k |j\rangle = 0$ ($i, j \in [n]$ with $i < j$).

The composition of super-operators is given by $\mathscr{F}_2 \circ \mathscr{F}_1(\rho) = \mathscr{F}_2(\mathscr{F}_1(\rho))$ for any $\rho \in \mathscr{L}$.

Given a super-operator $\mathscr{F} \in \mathscr{S}$ and a density operator $\rho \in \mathscr{D}$, the fidelity is defined as

$$\mathrm{Fid}(\mathscr{F}, \rho) = \mathrm{tr}\left(\sqrt{\rho^{1/2} \mathscr{F}(\rho) \rho^{1/2}}\right). \tag{6}$$

When $\rho = |\psi\rangle\langle\psi|$ is pure, it is simply

$$\mathrm{Fid}(\mathscr{F}, |\psi\rangle\langle\psi|) = \mathrm{tr}\left(\sqrt{|\psi\rangle\langle\psi| \mathscr{F}(\rho) |\psi\rangle\langle\psi|}\right) = \sqrt{\langle\psi| \mathscr{F}(\rho) |\psi\rangle}. \tag{7}$$

From the definition, we can see that $0 \leq \mathrm{Fid}(\mathscr{F}, \rho) \leq 1$, and that $\mathrm{Fid}(\mathscr{F}, \rho) = 1$ holds for any $\rho \in \mathscr{D}$ iff $\mathscr{F} = \mathscr{I}$, the identity super-operator. Furthermore, the (minimum) fidelity of $\mathscr{F}$ is defined as

$$\underline{\mathrm{Fid}}(\mathscr{F}) = \min_{\rho \in \mathscr{D}} \mathrm{Fid}(\mathscr{F}, \rho) = \min_{|\psi\rangle \in \mathscr{H}} \mathrm{Fid}(\mathscr{F}, |\psi\rangle\langle\psi|), \tag{8}$$

where the last equation follows from the joint concavity [15, Ex. 9.19].

Finally we address: the MAX-MAX problem $\max_{\mathscr{R}\in\mathscr{S}}\max_{\rho\in\mathscr{D}}\mathrm{Fid}(\mathscr{R}\circ\mathscr{E},\rho)$ is in the scope of convex optimzation while the MAX-MIN problem $\max_{\mathscr{R}\in\mathscr{S}}\min_{\rho\in\mathscr{D}}\mathrm{Fid}(\mathscr{R}\circ\mathscr{E},\rho)$ not, due to the strong concavity [15, Thm. 9.7] that

$$\mathrm{Fid}\left(\sum_{k\in[m]}p_k\mathscr{F}_k,\sum_{k\in[m]}q_k\rho_k\right)\geq\sum_{k\in[m]}\sqrt{p_kq_k}\,\mathrm{Fid}(\mathscr{F}_k,\rho_k)\tag{9}$$

holds for any discrete probabilistic distributions $\{p_k\,|\,k\in[m]\}$ and $\{q_k\,|\,k\in[m]\}$.

3 Formulation as Polynomial Formulas

For the given error super-operator $\mathscr{E}=\{\mathbf{E}_k\,|\,k\in[m]\}\in\mathscr{S}$, we suppose that all entries in $\mathbf{E}_k$ ($k\in[m]$) are rational, i.e. the real and imaginary parts of each entry are rational, for facilitating the complexity analysis. How to extend it to operate with irrational entries will be mentioned later.

The optimal error-correction

$$\max_{\mathscr{R}\in\mathscr{S}}\underline{\mathrm{Fid}}(\mathscr{R}\circ\mathscr{E})=\max_{\mathscr{R}\in\mathscr{S}}\min_{|\psi\rangle\in\mathscr{H}}\mathrm{Fid}(\mathscr{R}\circ\mathscr{E},|\psi\rangle\langle\psi|)\tag{10}$$

is resolved by some optimal recovery $\mathscr{R}$ that is complete, which can be obtained as a solution to the following quantified constraint $\Phi(\mathscr{R})$:

$$\mathrm{complete}(\mathscr{R})\wedge\forall\mathscr{R}':[\mathrm{complete}(\mathscr{R}')\rightarrow\underline{\mathrm{Fid}}(\mathscr{R}'\circ\mathscr{E})\leq\underline{\mathrm{Fid}}(\mathscr{R}\circ\mathscr{E})].\tag{11}$$

We aim to formulate the constraint (11) as a formula in the decidable theory—real closed fields [20]. Recall that:

Definition 1 The theory of real closed fields is a first-order theory $Th(\mathbb{R};+,\cdot;=,>;0,1)$, in which

- the domain is $\mathbb{R}$,
- the functions are addition '$+$' and multiplication '$\cdot$',
- the predicates are equality '$=$' and order '$>$', and
- the constants are 0 and 1.

Commonly speaking, elements in $Th(\mathbb{R};+,\cdot;=,>;0,1)$ are $\mathbb{Q}$-polynomial[1] formulas that are composed from polynomial equations and inequalities (as atomic formulas) using logic connectives "$\neg,\wedge,\vee,\rightarrow,\leftrightarrow$" and quantifiers "$\forall,\exists$" shown in Table 1.

[1] It refers to polynomial with rational coefficients. As all entries in the input $\mathscr{E}$ are supposed to be rational, we would simply write 'polynomial' for '$\mathbb{Q}$-polynomial' afterwards, unless it is specified otherwise.

Table 1 Logic connectives and quantifiers

Symbol	Symbol name	Meaning	Example
$\neg$	negation	not	$\neg A$
$\wedge$	conjunction	and	$A \wedge B$
$\vee$	disjunction	or	$A \vee B$
$\rightarrow$	implication	imply	$A \rightarrow B$
$\leftrightarrow$	bicondition	if and only if	$A \leftrightarrow B$
$\forall$	universal quantifier	for each	$\forall x$
$\exists$	existential quantifier	there exists a	$\exists x$

Note 1 Here x is a variable, and A, B are formulas.

For instance,

$$\forall x : [x^2 + y^2 < 1 \rightarrow x \leq \tfrac{4}{5}] \qquad \text{and} \qquad \exists x : ax^2 + bx + c = 0$$

are elements in $Th(\mathbb{R}; +, \cdot; =, >; 0, 1)$, and thus are decidable, as the former holds iff $y \geq \frac{3}{5} \vee y \leq -\frac{3}{5}$ and the latter holds iff $[a \neq 0 \wedge b^2 \geq 4ac] \vee [a = 0 \wedge b \neq 0] \vee a = b = c = 0$. Whereas,

$$\forall x : x > \sin(2xy) \qquad \text{and} \qquad \pi - x = 5$$

are not, since neither the function 'sin' in the former nor the constant 'π' in the latter can be expressed under $Th(\mathbb{R}; +, \cdot; =, >; 0, 1)$.

In the formulating subprocedure, we first rewrite the function '$\underline{\text{Fid}}$' with the function 'Fid'. After introducing the pure states $|\psi\rangle$ and $|\psi'\rangle$ that minimize the fidelities of $\mathscr{R} \circ \mathscr{E}$ and $\mathscr{R}' \circ \mathscr{E}$ respectively, we can obtain the equivalence

$$\begin{aligned} \Phi(\mathscr{R}) \equiv\ & \text{complete}(\mathscr{R}) \wedge \\ & \exists\, |\psi\rangle\ \forall\, |\varphi\rangle : \{\text{Fid}(\mathscr{R} \circ \mathscr{E}, |\psi\rangle\langle\psi|) \leq \text{Fid}(\mathscr{R} \circ \mathscr{E}, |\varphi\rangle\langle\varphi|) \wedge \\ & \forall \mathscr{R}' : [\text{complete}(\mathscr{R}')\ \rightarrow \\ & \exists\, |\psi'\rangle : (\text{Fid}(\mathscr{R}' \circ \mathscr{E}, |\psi'\rangle\langle\psi'|) \leq \text{Fid}(\mathscr{R} \circ \mathscr{E}, |\psi\rangle\langle\psi|) \wedge \\ & \forall\, |\varphi'\rangle : \text{Fid}(\mathscr{R}' \circ \mathscr{E}, |\psi'\rangle\langle\psi'|) \leq \text{Fid}(\mathscr{R}' \circ \mathscr{E}, |\varphi'\rangle\langle\varphi'|))]\}. \end{aligned} \tag{12}$$

The right hand side can be simplified as

$$\begin{aligned} & \text{complete}(\mathscr{R}) \wedge \\ & \exists\, |\psi\rangle\ \forall\, |\varphi\rangle : \{\text{Fid}(\mathscr{R} \circ \mathscr{E}, |\psi\rangle\langle\psi|) \leq \text{Fid}(\mathscr{R} \circ \mathscr{E}, |\varphi\rangle\langle\varphi|) \wedge \\ & \forall \mathscr{R}' : [\text{complete}(\mathscr{R}')\ \rightarrow \\ & \exists\, |\psi'\rangle : \text{Fid}(\mathscr{R}' \circ \mathscr{E}, |\psi'\rangle\langle\psi'|) \leq \text{Fid}(\mathscr{R} \circ \mathscr{E}, |\psi\rangle\langle\psi|)]\}, \end{aligned} \tag{13}$$

since the required

$$\underline{\text{Fid}}(\mathscr{R}' \circ \mathscr{E}) \leq \text{Fid}(\mathscr{R}' \circ \mathscr{E}, |\psi'\rangle\langle\psi'|) \leq \text{Fid}(\mathscr{R} \circ \mathscr{E}, |\psi\rangle\langle\psi|) = \underline{\text{Fid}}(\mathscr{R} \circ \mathscr{E})$$

could be implied by $\exists\,|\psi'\rangle : \mathrm{Fid}(\mathscr{R}'\circ\mathscr{E},|\psi'\rangle\langle\psi'|) \leq \mathrm{Fid}(\mathscr{R}\circ\mathscr{E},|\psi\rangle\langle\psi|)$. Then, we can easily rewrite the constraint (13) in prefix normal form as

$$\exists\,|\psi\rangle\ \forall\,|\varphi\rangle\ \forall\mathscr{R}'\ \exists\,\left|\psi'\right\rangle : \begin{cases} \mathrm{complete}(\mathscr{R}) \wedge \\ \mathrm{Fid}(\mathscr{R}\circ\mathscr{E},|\psi\rangle\langle\psi|) \leq \mathrm{Fid}(\mathscr{R}\circ\mathscr{E},|\varphi\rangle\langle\varphi|) \wedge \\ [\mathrm{complete}(\mathscr{R}') \rightarrow \\ \mathrm{Fid}(\mathscr{R}'\circ\mathscr{E},\left|\psi'\right\rangle\left\langle\psi'\right|) \leq \mathrm{Fid}(\mathscr{R}\circ\mathscr{E},|\psi\rangle\langle\psi|)] \end{cases}, \quad (14)$$

whose solutions are exactly the projection, from $(\mathscr{R},|\psi\rangle)$-coordinates to $\mathscr{R}$-ones, of solutions of the following constraint

$$\forall\,|\varphi\rangle\ \forall\mathscr{R}'\ \exists\,\left|\psi'\right\rangle : \begin{cases} \mathrm{complete}(\mathscr{R}) \wedge \\ \mathrm{Fid}(\mathscr{R}\circ\mathscr{E},|\psi\rangle\langle\psi|) \leq \mathrm{Fid}(\mathscr{R}\circ\mathscr{E},|\varphi\rangle\langle\varphi|) \wedge \\ [\mathrm{complete}(\mathscr{R}') \rightarrow \\ \mathrm{Fid}(\mathscr{R}'\circ\mathscr{E},\left|\psi'\right\rangle\left\langle\psi'\right|) \leq \mathrm{Fid}(\mathscr{R}\circ\mathscr{E},|\psi\rangle\langle\psi|)] \end{cases}. \quad (15)$$

The constraint (15) is a quantified formula in the fragment of two alternative quantifier blocks. In the following we will further encode it as a polynomial formula. To this end, it suffices to encode all subformulas in the constraint (15) as polynomial formulas. We encode them in three steps.

1. By Kraus representation, we predefine $\mathscr{R} = \{\mathbf{R}_k \,|\, k \in [n^2]\}$ where $\mathbf{R}_k = (r_{k,i,j})_{n\times n}$ ($k \in [n^2]$ and $i,j \in [n]$) are matrices of complex parametric entries. So the completeness is encoded as

$$\mathrm{complete}(\mathscr{R}) \equiv \sum_{k\in[n^2]} \mathbf{R}_k^\dagger \mathbf{R}_k = \mathbf{I}, \quad (16)$$

   which is indeed a polynomial formula, involving at most
   - $2n^4$ real variables (converted from n^4 complex variables) and
   - n^2 quadratic equations over $\mathbb{R}$ (converted from the Hermitian matrix equation).

   The same encoding can be applied to the subformula $\mathrm{complete}(\mathscr{R}')$ by predefining $\mathscr{R}' = \{\mathbf{R}'_k \,|\, k \in [n^2]\}$ where $\mathbf{R}'_k = (r'_{k,i,j})_{n\times n}$ ($k \in [n^2]$ and $i,j \in [n]$) are matrices of complex parametric entries. We denote all parameters introduced here by $\mathbf{r} = (r_{k,i,j})_{k\in[n^2];i,j\in[n]}$ and $\mathbf{r}' = (r'_{k,i,j})_{k\in[n^2];i,j\in[n]}$.
2. Since $|\psi\rangle$ and $|\varphi\rangle$ are pure states, we predefine $|\psi\rangle = \sum_{i\in[n]} x_i\,|i\rangle$ and $|\varphi\rangle = \sum_{i\in[n]} y_i\,|i\rangle$ where x_i and y_i ($i \in [n]$) are complex parameters, subject to the purity $\sum_{i\in[n]} |x_i|^2 = 1$ and $\sum_{i\in[n]} |y_i|^2 = 1$. The encoding of the purity depends on the corresponding quantifier, which will be delivered in the next step. Under the

purity, we have

$$\begin{aligned}
&\mathrm{Fid}(\mathscr{R}\circ\mathscr{E},|\psi\rangle\langle\psi|)\le\mathrm{Fid}(\mathscr{R}\circ\mathscr{E},|\varphi\rangle\langle\varphi|)\\
\equiv\ &\langle\psi|\mathscr{R}\circ\mathscr{E}(|\psi\rangle\langle\psi|)\,|\psi\rangle\le\langle\varphi|\mathscr{R}\circ\mathscr{E}(|\varphi\rangle\langle\varphi|)\,|\varphi\rangle\\
\equiv\ &\underbrace{\left(\sum_{j\in[n]}x_j^*\langle j|\right)}_{\deg=1}\underbrace{\mathscr{R}}_{\deg=2}\circ\underbrace{\mathscr{E}}_{\deg=0}\underbrace{\left(\sum_{i,j\in[n]}x_ix_j^*|i\rangle\langle j|\right)}_{\deg=2}\underbrace{\left(\sum_{i\in[n]}x_i|i\rangle\right)}_{\deg=1}\le\\
&\underbrace{\left(\sum_{j\in[n]}y_j^*\langle j|\right)}_{\deg=1}\underbrace{\mathscr{R}}_{\deg=2}\circ\underbrace{\mathscr{E}}_{\deg=0}\underbrace{\left(\sum_{i,j\in[n]}y_iy_j^*|i\rangle\langle j|\right)}_{\deg=2}\underbrace{\left(\sum_{i\in[n]}y_i|i\rangle\right)}_{\deg=1},
\end{aligned}\tag{17}$$

which results in a polynomial formula, involving at most

- $2n^4+4n$ real variables (converted from n^4+2n complex variables) and
- one sextic inequality. (Details on the degree accumulation can be seen from the underbraced notes of (17).)

The same encoding can be applied to the subformula $\mathrm{Fid}(\mathscr{R}'\circ\mathscr{E},|\psi'\rangle\langle\psi'|)\le\mathrm{Fid}(\mathscr{R}\circ\mathscr{E},|\psi\rangle\langle\psi|))$ by predefining $|\psi'\rangle=\sum_{i\in[n]}x_i'|i\rangle$ where x_i' ($i\in[n]$) are complex parameters, subject to the purity $\sum_{i\in[n]}|x_i'|^2=1$. We denote all parameters introduced here by $\mathbf{x}=(x_i)_{i\in[n]}$, $\mathbf{y}=(y_i)_{i\in[n]}$ and $\mathbf{x}'=(x_i')_{i\in[n]}$.

3. Finally we encode the whole constraint (15) as

$$\begin{aligned}
&\Phi(\mathscr{R},|\psi\rangle))\\
\equiv\ &\forall\,|\varphi\rangle\ \forall\mathscr{R}'\ \exists\,\left|\psi'\right\rangle:\Psi(\mathscr{R},|\psi\rangle,|\varphi\rangle,\mathscr{R}',\left|\psi'\right\rangle)\\
\equiv\ &\forall\mathbf{y}\,\forall\mathbf{r}'\,\exists\mathbf{x}':\left\{\|\mathbf{x}\|^2=1\wedge\left[\|\mathbf{y}\|^2=1\to\left(\|\mathbf{x}'\|^2=1\wedge\Upsilon(\mathbf{r},\mathbf{x},\mathbf{y},\mathbf{r}',\mathbf{x}')\right)\right]\right\},
\end{aligned}\tag{18}$$

where $\Upsilon(\mathbf{r},\mathbf{x},\mathbf{y},\mathbf{r}',\mathbf{x}')$ is the polynomialization of $\Psi(\mathscr{R},|\psi\rangle,|\varphi\rangle,\mathscr{R}',|\psi'\rangle)$ as described above. Thereby we obtain the desired polynomial formula (18), which involves at most

- $4n^4+6n$ real variables from real and imaginary parts of $\mathbf{r},\mathbf{r}',\mathbf{x},\mathbf{y},\mathbf{x}'$,
- $2n^2+3$ quadratic equations from the completeness and the purity, and
- 2 sextic inequalities from the order between fidelities.

Example 2 Let us consider the optimal QEC for the error super-operator $\mathscr{E}_0$ shown in Example 1. We will formulate it as a polynomial formula.

We first introduce the required real variables as follows.

- $\mathbf{a}=\Re(\mathbf{x})$ and $\mathbf{b}=\Im(\mathbf{x})$ where $\mathbf{x}=(x_i)_{i\in[4]}$ encodes the pure state $|\psi\rangle$,
- $\mathbf{c}=\Re(\mathbf{y})$ and $\mathbf{d}=\Im(\mathbf{y})$ where $\mathbf{y}=(y_i)_{i\in[4]}$ encodes the pure state $|\varphi\rangle$,
- $\mathbf{a}'=\Re(\mathbf{x}')$ and $\mathbf{b}'=\Im(\mathbf{x}')$ where $\mathbf{x}'=(x_i')_{i\in[4]}$ encodes the pure state $|\psi'\rangle$,
- $\mathbf{u}=\Re(\mathbf{r})$ and $\mathbf{v}=\Im(\mathbf{r})$ where $\mathbf{r}=(r_{k,i,j})_{k\in[16];i,j\in[4]}$ encodes the super-operator $\mathscr{R}$, and
- $\mathbf{u}'=\Re(\mathbf{r}')$ and $\mathbf{v}'=\Im(\mathbf{r}')$ where $\mathbf{r}'=(r'_{k,i,j})_{k\in[16];i,j\in[4]}$ encodes the super-operator $\mathscr{R}'$.

For the input $\mathscr{E}_0 = \{\mathbf{E}_{k'} \,|\, k' \in [4]\}$, its entries are directly referred to as real constants $e_{k',i,j}$ $(k', i, j \in [4])$.

We then encode the purity, the completeness and the fidelity in turn. For purity, we encode:

- $|\psi\rangle$ as $\|\mathbf{x}\|^2 = 1$, i.e. $\sum_{i\in[4]} a_i^2 + b_i^2 = 1$,
- $|\varphi\rangle$ as $\|\mathbf{y}\|^2 = 1$, i.e. $\sum_{i\in[4]} c_i^2 + d_i^2 = 1$, and
- $|\psi'\rangle$ as $\|\mathbf{x}'\|^2 = 1$, i.e. $\sum_{i\in[4]} (a_i')^2 + (b_i')^2 = 1$.

Denote the resulting polynomial formulas by PURE($\mathbf{a}, \mathbf{b}$), PURE($\mathbf{c}, \mathbf{d}$) and PURE($\mathbf{a}'$, $\mathbf{b}'$) respectively.

For completeness, we have:

- complete$(\mathscr{R}) \equiv \sum_{k\in[16]} \mathbf{R}_k^\dagger \mathbf{R}_k = \mathbf{I}$, which is exactly

$$\begin{aligned}
&\bigwedge_{i,j\in[4]} \sum_{k\in[16],l\in[4]} r_{k,l,i}^* r_{k,l,j} = \delta_{i,j} \\
\equiv &\bigwedge_{i,j\in[4]} \sum_{k\in[16],l\in[4]} (u_{k,l,i} - \mathrm{i}v_{k,l,i})(u_{k,l,j} + \mathrm{i}v_{k,l,j}) = \delta_{i,j} \\
\equiv &\bigwedge_{i,j\in[4]} \left(\begin{array}{l} \displaystyle\sum_{k\in[16],l\in[4]} u_{k,l,i}u_{k,l,j} + v_{k,l,i}v_{k,l,j} = \delta_{i,j} \wedge \\ \displaystyle\sum_{k\in[16],l\in[4]} u_{k,l,i}v_{k,l,j} - v_{k,l,i}u_{k,l,j} = 0 \end{array} \right),
\end{aligned}$$

  where $\delta_{i,j}$ is the Kronecker δ-function that is 1 if $i = j$ and 0 otherwise.
- complete$(\mathscr{R}') \equiv \sum_{k\in[16]} (\mathbf{R}_k')^\dagger (\mathbf{R}_k) = \mathbf{I}$, which is exactly

$$\bigwedge_{i,j\in[4]} \left(\sum_{k\in[16],l\in[4]} u'_{k,l,i}u'_{k,l,j} + v'_{k,l,i}v'_{k,l,j} = \delta_{i,j} \wedge \sum_{k\in[16],l\in[4]} u'_{k,l,i}v'_{k,l,j} - v'_{k,l,i}u'_{k,l,j} = 0 \right).$$

Denote the resulting polynomial formulas by COMPLETE($\mathbf{u}, \mathbf{v}$) and COMPLETE $(\mathbf{u}', \mathbf{v}')$ respectively.

For the given $\mathbf{E}_{k'} = (e_{k',i,j})_{4\times4}$ $(k', i, j \in [4])$, we encode the square of the fidelity as[2]

$$\begin{aligned}
\mathrm{Fid}^2(\mathscr{R}\circ\mathscr{E}, |\psi\rangle\langle\psi|) &= \langle\psi| \mathscr{R}\circ\mathscr{E}(|\psi\rangle\langle\psi|) |\psi\rangle \\
&= \sum_{k\in[16],k'\in[4]} \langle\psi| \mathbf{R}_k\mathbf{E}_{k'} |\psi\rangle\langle\psi| \mathbf{E}_{k'}^\dagger\mathbf{R}_k^\dagger |\psi\rangle \\
&= \sum_{k\in[16],k'\in[4]} |\langle\psi| \mathbf{R}_k\mathbf{E}_{k'} |\psi\rangle|^2,
\end{aligned}$$

[2] We prefer to encode the square of the fidelity here, rather than the fidelity, since the latter is generally expressed as a square root of an SOS polynomial. The order between fidelities could be correspondingly replaced with the order between their squares.

in which $\langle\psi|\mathbf{R}_k\mathbf{E}_{k'}|\psi\rangle$ ($k\in[16]$ and $k'\in[4]$) can be expanded as

$$\begin{aligned}
&\sum_{i,j,l,\tilde{i},\tilde{j},\tilde{l}\in[4]}(a_{\tilde{l}}-\mathrm{i}b_{\tilde{l}})\left\langle\tilde{l}\right|(u_{k,i,j}+\mathrm{i}v_{k,i,j})|i\rangle\langle j|e_{k',\tilde{i},\tilde{j}}\left|\tilde{i}\right\rangle\left\langle\tilde{j}\right|(a_l+\mathrm{i}b_l)|l\rangle\\
=&\sum_{i,j,l\in[4]}(a_i-\mathrm{i}b_i)(u_{k,i,j}+\mathrm{i}v_{k,i,j})e_{k',j,l}(a_l+\mathrm{i}b_l)\\
=&\sum_{i,j,l\in[4]}\begin{pmatrix}e_{k',j,l}[u_{k,i,j}(a_ia_l+b_ib_l)-v_{k,i,j}(a_ib_l-b_ia_l)]+\\ \mathrm{i}e_{k',j,l}[u_{k,i,j}(a_ib_l-b_ia_l)+v_{k,i,j}(a_ia_l+b_ib_l)]\end{pmatrix}
\end{aligned}$$

and thereby $|\langle\psi|\mathbf{R}_k\mathbf{E}_{k'}|\psi\rangle|^2$ is

$$\begin{aligned}
&\left[\sum_{i,j,l\in[4]}e_{k',j,l}[u_{k,i,j}(a_ia_l+b_ib_l)-v_{k,i,j}(a_ib_l-b_ia_l)]\right]^2+\\
&\left[\sum_{i,j,l\in[4]}e_{k',j,l}[u_{k,i,j}(a_ib_l-b_ia_l)+v_{k,i,j}(a_ia_l+b_ib_l)]\right]^2.
\end{aligned}$$

In details, for instance, when k' takes 1, we have

$$\begin{aligned}
|\langle\psi|\mathbf{R}_k\mathbf{E}_1|\psi\rangle|^2=&\left[\sum_{i\in[4]}\begin{pmatrix}\frac{12}{25}[u_{k,i,2}(a_ia_1+b_ib_1)-v_{k,i,2}(a_ib_1-b_ia_1)]+\\ \frac{12}{25}[u_{k,i,1}(a_ia_2+b_ib_2)-v_{k,i,1}(a_ib_2-b_ia_2)]+\\ \frac{12}{25}[u_{k,i,4}(a_ia_3+b_ib_3)-v_{k,i,4}(a_ib_3-b_ia_3)]+\\ \frac{12}{25}[u_{k,i,3}(a_ia_4+b_ib_4)-v_{k,i,3}(a_ib_4-b_ia_4)]\end{pmatrix}\right]^2+\\
&\left[\sum_{i\in[4]}\begin{pmatrix}\frac{12}{25}[u_{k,i,2}(a_ib_1-b_ia_1)+v_{k,i,2}(a_ia_1+b_ib_1)]+\\ \frac{12}{25}[u_{k,i,1}(a_ib_2-b_ia_2)+v_{k,i,1}(a_ia_2+b_ib_2)]+\\ \frac{12}{25}[u_{k,i,4}(a_ib_3-b_ia_3)+v_{k,i,4}(a_ia_3+b_ib_3)]+\\ \frac{12}{25}[u_{k,i,3}(a_ib_4-b_ia_4)+v_{k,i,3}(a_ia_4+b_ib_4)]\end{pmatrix}\right]^2.
\end{aligned}$$

Denote the resulting polynomial by $\mathrm{FID}^2(\mathbf{u},\mathbf{v},\mathbf{a},\mathbf{b})$. The same encoding can be applied to $\mathrm{Fid}^2(\mathscr{R}\circ\mathscr{E},|\varphi\rangle\langle\varphi|)$ and $\mathrm{Fid}^2(\mathscr{R}'\circ\mathscr{E},|\psi'\rangle\langle\psi'|)$, and produce the polynomials $\mathrm{FID}^2(\mathbf{u},\mathbf{v},\mathbf{c},\mathbf{d})$ and $\mathrm{FID}^2(\mathbf{u}',\mathbf{v}',\mathbf{a}',\mathbf{b}')$ respectively.

Combining all of the above components, we eventually obtain the desired polynomial formula

$$\begin{aligned}
&\Phi(\mathscr{R},|\psi\rangle)\\
\equiv&\forall|\varphi\rangle\ \forall\mathscr{R}'\ \exists\left|\psi'\right\rangle:\Psi(\mathscr{R},|\psi\rangle,|\varphi\rangle,\mathscr{R}',\left|\psi'\right\rangle)\\
\equiv&\forall\mathbf{y}\,\forall\mathbf{r}'\,\exists\mathbf{x}':\left\{\|\mathbf{x}\|^2=1\wedge\left[\|\mathbf{y}\|^2=1\rightarrow\begin{pmatrix}\|\mathbf{x}'\|^2=1\wedge\\ \Upsilon(\mathbf{r},\mathbf{x},\mathbf{y},\mathbf{r}',\mathbf{x}')\end{pmatrix}\right]\right\}\\
\equiv&\forall\{\mathbf{c},\mathbf{d}\}\,\forall\{\mathbf{u}',\mathbf{v}'\}\,\exists\{\mathbf{a}',\mathbf{b}'\}:\left\{\mathrm{PURE}(\mathbf{a},\mathbf{b})\wedge\left[\mathrm{PURE}(\mathbf{c},\mathbf{d})\ \rightarrow\right.\right.\\
&\left.\left.\begin{pmatrix}\mathrm{PURE}(\mathbf{a}',\mathbf{b}')\wedge\mathrm{COMPLETE}(\mathbf{u},\mathbf{v})\wedge\mathrm{FID}^2(\mathbf{u},\mathbf{v},\mathbf{a},\mathbf{b})\leq\mathrm{FID}^2(\mathbf{u},\mathbf{v},\mathbf{c},\mathbf{d})\wedge\\ [\mathrm{COMPLETE}(\mathbf{u}',\mathbf{v}')\rightarrow\mathrm{FID}^2(\mathbf{u}',\mathbf{v}',\mathbf{a}',\mathbf{b}')\leq\mathrm{FID}^2(\mathbf{u},\mathbf{v},\mathbf{a},\mathbf{b})]\end{pmatrix}\right]\right\}.
\end{aligned}$$

Due to page limit, the polynomial formula that is instantiated with the values of $e_{k',i,j}$ ($k',i,j \in [4]$) is omitted here. The complete description could be found at `https://github.com/yjs4869/quantum-2019`.

A further simplification We notice that

$$(c^* \langle\psi|)\rho(c|\psi\rangle) = |c|^2 \langle\psi|\rho|\psi\rangle = \langle\psi|\rho|\psi\rangle$$
$$(c|\psi\rangle)(c^* \langle\psi|) = |c|^2 |\psi\rangle\langle\psi| = |\psi\rangle\langle\psi|$$

hold for any unit complex number c. Thus we can suppose w.l.o.g. that the first parameter x_0 of $\mathbf{x}$ for encoding $|\psi\rangle$ is real, since:

- if the first parameter x_0 is already real, it is trivially achieved;
- otherwise, $c\mathbf{x}$ with $c = x_0^*/|x_0|$, whose first parameter is real, also suffices to encode $|\psi\rangle$.

Similarly, we can save one real variable for each of $\mathbf{y}, \mathbf{x}'$. The same trick can be also applied to encode Kraus elements $\mathbf{R}_k$ and $\mathbf{R}'_k$ ($k \in [n^2]$), and thus save n^2 real variable for each of $\mathbf{r}, \mathbf{r}'$. For instance, $\Im(x_0), \Im(y_0), \Im(x'_0)$ and $\Im(r_{k,0,0}), \Im(r'_{k,0,0})$ ($k \in [n^2]$) can be supposed w.l.o.g. to be zero in encoding the pure states $|\psi\rangle, |\varphi\rangle, |\psi'\rangle$ and the super-operators $\mathscr{R}, \mathscr{R}'$, respectively. Therefore, the polynomial formula (18) involves at most $4n^4 - 2n^2 + 6n - 3$ real variables from real and imaginary parts of $\mathbf{r}, \mathbf{r}', \mathbf{x}, \mathbf{y}, \mathbf{x}'$.

4 Solving Polynomial Formulas

In this section we will solve the polynomial constraint (18) by the quantifier elimination over real closed fields, a classic algorithm in computational algebraic geometry. The complexity of our procedure will be also provided.

Algorithm 1 Quantifier Elimination over Real Closed Fields [2, Alg. 14.5]

$$G(\mathbf{y}) \leftarrow \mathsf{QE}(\mathrm{Q}_1 \mathbf{x}_1 \cdots \mathrm{Q}_\ell \mathbf{x}_\ell : F(\mathbf{x}_1, \ldots, \mathbf{x}_\ell, \mathbf{y}))$$

Input: $\mathrm{Q}_1 \mathbf{x}_1 \cdots \mathrm{Q}_\ell \mathbf{x}_\ell : F(\mathbf{x}_1, \ldots, \mathbf{x}_\ell, \mathbf{y})$ is a quantified polynomial formula, in which
- $\mathbf{x}_i$ ($i \in \{1, \ldots, \ell\}$) are blocks of k_i variables quantified by $\mathrm{Q}_i \in \{\forall, \exists\}$,
- $\mathbf{y}$ is a block of l free variables,
- each atomic formula in F is in the form $p \sim 0$ where $\sim \in \{<, \leq, =, \geq, >, \neq\}$,
- all distinct polynomials p, regardless of a constant factor, extracted from those atomic formulas $p \sim 0$ form a polynomial collection $\mathbb{P}$,
- s is the cardinality of $\mathbb{P}$, and
- d is the maximum degree of the polynomials in $\mathbb{P}$.

Output: $G(\mathbf{y})$ is a quantifier-free polynomial formula equivalent to $\mathrm{Q}_1 \mathbf{x}_1 \cdots \mathrm{Q}_\ell \mathbf{x}_\ell : F(\mathbf{x}_1, \ldots, \mathbf{x}_\ell, \mathbf{y})$. For each realizable sign condition of $\mathbb{P}$ w.r.t. the variable partition $\{\{\mathbf{x}_1\}, \ldots, \{\mathbf{x}_\ell\}, \{\mathbf{y}\}\}$, the sample is also provided by a routine [2, Alg. 13.2].

Complexity: $s^{(k_1+1)\cdots(k_\ell+1)(l+1)} d^{\mathscr{O}(k_1)\cdots\mathscr{O}(k_\ell)\mathscr{O}(l)}$.

There are many tools that have implemented Algorithm 1, such as REDUCE (a.k.a. REDLOG [6]) and Z3 [14].

Note that Algorithm 1 is in **2EXP** w.r.t. the number of alternative quantifier blocks and in **EXP** w.r.t. the number of variables. In our situation, the polynomial formula (18) is in a fixed fragment of two alternative quantifier blocks, and thus is solvable in **EXP**. Formally, we conclude with:

Theorem 2 *The optimal QEC problem can be solved in **EXP**.*

Proof It is completed by showing that

1. the formulating subprocedure is polynomial-time, and
2. the solving subprocedure is exponential-time.

The formulating of the formula (15) is clearly in $\mathscr{O}(n^4)$, dominated by the size of the input error super-operator $\mathscr{E}$. The encoding on the purity is in $\mathscr{O}(n)$, and that on the completeness is in $\mathscr{O}(n^5)$, since there are at most n^2 quadratic equations over $\mathbb{R}$, each equation has at most n^2 terms on the left hand side of the polynomial formula (16) and a constant on the right hand side, and each term has n quadratic monomials. In the rest of the proof, we analyze the cost of encoding the left hand side of the order (see the polynomial formula (17)) step by step.

1. Each entry of the innermost $(n \times n)$-matrix $\sum_{i,j\in[n]} x_i x_j^* |i\rangle\langle j|$ is a product of two variables. So it is plainly encoded in $\mathscr{O}(n^2)$.
2. After performing the constant super-operator $\mathscr{E}$, it results in an $(n \times n)$-matrix of quadratic polynomials as entries. Specifically, each entry has at most n^2 terms, each term has at most n^2 quadratic monomials. So it is encoded in $\mathscr{O}(n^6)$.
3. After performing the parametric super-operator $\mathscr{R}$, it results in an $(n \times n)$-matrix of quartic polynomials as entries. Specifically, each entry has at most n^2 terms, each term is a sum of at most n^2 products of quadratic monomials and quadratic polynomials, each of which consists of at most n^4 monomials. So it is encoded in $\mathscr{O}(n^{10})$.
4. After performing the outermost multiplication $\sum_{i,j\in[n]} x_j^* \langle j| \cdots x_i |i\rangle$, it results in a sextic polynomial, which is a sum of at most n^2 products of quadratic monomials and quartic polynomials, each of which consists of at most n^8 monomials. So it is still encoded in $\mathscr{O}(n^{10})$.

Encoding the right hand side of the order is similar, and thus encoding the polynomial formula (17) is in $\mathscr{O}(n^{10})$. The whole polynomial formula (18) is a fixed composition of the aforementioned subformulas—three subformulas for purity, two for completeness and two for order, which entails the formulating subprocedure is in **P**.

Then we tackle the solving subprocedure, which is invoking Algorithm 1 on the polynomial formula (18). The optimal recovery super-operators are exactly determined by satisfying samples of $\mathbf{r}$. In details, we can see the polynomial formula (18) has

- a block of $2n^4 - n^2 + 2n - 1$ universally quantified variables $\mathbf{y}$ and $\mathbf{r}'$,
- a block of $2n - 1$ existentially quantified variables $\mathbf{x}'$,
- a block of $2n^4 - n^2 + 2n - 1$ free variables $\mathbf{r}$ and $\mathbf{x}$, and
- at most $2n^2 + 5$ distinct polynomials of degree at most 6.

Thereby, the complexity of the procedure is in

$$(2n^2+5)^{(2n^4-n^2+2n)(2n)(2n^4-n^2+2n)} \times 6^{\mathscr{O}(2n^4-n^2+2n-1)\mathscr{O}(2n-1)\mathscr{O}(2n^4-n^2+2n-1)} = 2^{\mathscr{O}(n^9)},$$

an exponential hierarchy. □

In fact, as the size of the input error super-operator $\mathscr{E}$ is $N = n^4$, the relative complexity of the optimal error-correcting procedure is $2^{\mathscr{O}(N^{2.25})}$. Finally we remark that Theorem 2 is just a theoretical result that is not of practical usefulness, since even when we ignore the constant factor in the exponent of $2^{\mathscr{O}(n^9)}$ and n takes 2, the resulting complexity is still 2^{512}, which is far beyond the number ($\approx 10^{80}$) of observable atoms in the universal!

4.1 Extension to algebraic entries

In the above procedure, all entries in the input error super-operator $\mathscr{E}$ are supposed to be rational. Here we will extend those rational entries to algebraic ones. Recall that:

Definition 2 A number ω is algebraic, denoted by $\omega \in \mathbb{A}$, if there is a nonzero $\mathbb{Q}$-polynomial of least degree $f(z)$, such that $f(\omega) = 0$. Such a polynomial $f(z)$ is called the minimal polynomial f_ω of ω.

Clearly, algebraic numbers properly contain all rational complex numbers, i.e. $\mathbb{A} \supset \{a+b\mathrm{i} \,|\, a,b \in \mathbb{Q}\}$. Algebraic numbers widely occur in quantum information, such as the definition of the pure state $|+\rangle$, obtained as performing the Hadamand operator $|+\rangle\langle 0| + |-\rangle\langle 1|$ on the pure state $|0\rangle$, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. The coefficient $1/\sqrt{2}$ is algebraic but not rational.

Suppose that the input $\mathscr{E}$ involves real algebraic numbers $\Omega = (\omega_k)_{k\in[m]}$.[3] Then the polynomial formula (18) would result in an $\mathbb{A}$-polynomial formula, namely $\Phi(\mathscr{R}, |\psi\rangle, \Omega)$. To effectively tackle it, we resort to the standard encoding of real algebraic number ω that uses minimal polynomial f_ω and isolation interval $\mathbb{I}_\omega$, which is typically expressed by linear inequalities, like

$$z \in \mathbb{I}_\omega \equiv z > L \wedge z < U \tag{19}$$

for some rational endpoints L and U of $\mathbb{I}_\omega$, to distinguish ω from other real roots of f_ω. In such a way, to encode each real algebraic number ω, we need to introduce at most

- one real variable z,
- one equation $f_\omega = 0$, and
- 2 linear inequalities $z > L$ and $z < U$ from the isolation interval $\mathbb{I}_\omega$ of ω.

[3] Encoding complex entries amounts to encoding their real and imaginary parts, which are clearly real. So it is generic to tackle real algebraic numbers Ω only.

For instance, the aforementioned $1/\sqrt{2}$ can be encoded as the unique solution to $z^2 = \frac{1}{2} \wedge z > 0 \wedge z < 1$.

Thereby, the $\mathbb{A}$-polynomial formula $\Phi(\mathscr{R}, |\psi\rangle, \Omega)$ can be rewritten as the $\mathbb{Q}$-polynomial formula:

$$\begin{aligned}\Phi(\mathscr{R}, |\psi\rangle, \Omega) &\equiv \exists \mathbf{z} : \left[\Phi(\mathscr{R}, |\psi\rangle, \mathbf{z}) \wedge \bigwedge_{k\in[m]} (f_{\omega_k}(z_k) = 0 \wedge z_k \in \mathbb{I}_{\omega_k}) \right] \\ &\equiv \forall \mathbf{z} : \left[\Phi(\mathscr{R}, |\psi\rangle, \mathbf{z}) \wedge \bigwedge_{k\in[m]} (f_{\omega_k}(z_k) = 0 \wedge z_k \in \mathbb{I}_{\omega_k}) \right], \end{aligned} \tag{20}$$

where $\mathbf{z} = (z_k)_{k\in[m]}$ are real variables introduced to symbolize Ω. Note that the quantifiers $\exists \mathbf{z}$ and $\forall \mathbf{z}$ are equivalent here, since for each $i \in [m]$, there is a unique solution (i.e. ω_k) to $f_{\omega_k}(z_k) = 0 \wedge z_k \in \mathbb{I}_{\omega_k}$ by the standard encoding of ω_k. The solving subprocedure for the polynomial formula (20) is in

$$\begin{aligned} & (2n^2 + 5 + 3m)^{(2n^4 - n^2 + 2n + m)(2n)(2n^4 - n^2 + 2n)} \times \\ & \max\left(6, \max_{k\in[m]} \deg(f_{\omega_k})\right)^{\mathscr{O}(2n^4 - n^2 + 2n - 1 + m)\mathscr{O}(2n-1)\mathscr{O}(2n^4 - n^2 + 2n - 1)} \\ = & \left(\max_{k\in[m]} \deg(f_{\omega_k})\right)^{\mathscr{O}(n^9 + mn^5)}, \end{aligned}$$

since we additionally introduce

- at most m universally quantified variables together with $\mathbf{y}, \mathbf{r}'$, and
- at most $3m$ distinct polynomials of degree at most $\max_{k\in[m]} \deg(f_{\omega_k})$.

Hence we still obtain an exponential complexity upper bound, when the input $\mathscr{E}$ involves algebraic numbers.

5 Conclusion

In this paper, we have presented an optimal quantum error-correcting procedure in terms of fidelity. Our method is based on quantifier elimination over real closed fields, which is exact and complete. The complexity has been shown to be in exponential time. We believe that the proposed method could be easily amended for other distance measures, like the trace distance version

$$\min_{\mathscr{R}} \max_{\rho} \mathrm{tr}(|\mathscr{R} \circ \mathscr{E}(\rho) - \rho|), \tag{21a}$$

and generally, for some $k \leq n$, the partial fidelity [22] version

$$\max_{\mathscr{R}} \min_{\rho} \sum_{i=1}^{k} \sigma_i \left(\sqrt{\rho^{1/2} \cdot \mathscr{R} \circ \mathscr{E}(\rho) \cdot \rho^{1/2}} \right), \tag{21b}$$

where $\sigma_i(\rho)$ $(1 \leq i \leq n)$ denotes the ith largest eigenvalue of ρ, and the partial trace distance [17] version

$$\max_{\mathscr{R}} \min_{\rho} \sum_{i=1}^{k} \sigma_i(|\mathscr{R} \circ \mathscr{E}(\rho) - \rho|), \tag{21c}$$

with a similar complexity of exponential hierarchy.

In the future, we would like to study how to improve the practical complexity of the proposed method. One of possible approaches is to propose a normal form on Kraus representation, so that much less variables in $\mathscr{R}$ and $\mathscr{R}'$ would be introduced in the constraint (18). It seems to produce a small constant K to the complexity 2^{Kn^9}, but not a lower-degree polynomial than n^9. Besides, we would consider the lower bound of the optimal QEC problem, which seems to be **EXP**-hard.

Acknowledgements The authors thank Yuan Feng for his valuable suggestions on an early version of the paper, and Jianling Fu for her careful proof-reading.

References

1. Abu-Nada A, Fortescue B, Byrd M (2017) Optimizing the frequency of quantum error correction. Physical Review Letters 119(19):article no. 190502
2. Basu S, Pollack R, Roy MF (2006) Algorithms in Real Algebraic Geometry, 2nd edn. Springer
3. Blondel VD, Jeandel E, Koiran P, Portier N (2005) Decidable and undecidable problems about quantum automata. SIAM Journal on Computing 34(6):1464–1473
4. Calderbank AR, Shor PW (1996) Good quantum error-correcting codes exist. Physical Review A 54(2):1098–1105
5. Devitt SJ, Munro WJ, Nemoto K (2013) Quantum error correction for beginners. Reports on Progress in Physics 76(7):article no. 076001
6. Dolzmann A, Sturm T (1997) REDLOG: Computer algebra meets computer logic. ACM SIGSAM Bulletin 31(2):2–9
7. Fletcher AS, Shor PW, Win MZ (2007) Optimum quantum error recovery using semidefinite programming. Physical Review A 75(1):article no. 012338
8. Fletcher AS, Shor PW, Win MZ (2008) Structured near-optimal channel-adapted quantum error correction. Physical Review A 77(1):article no. 012320
9. Gottesman D (1997) Stabilizer codes and quantum error correction. PhD thesis, California Institute of Technology
10. Knill E, Laflamme R (1997) Theory of quantum error-correcting codes. Physical Review A 55(2):900–911
11. Kosut RL, Shabani A, Lidar DA (2008) Quantum error correction via convex optimization. Physical Review Letters 100(2):article no. 020502
12. MacWilliams FJ, Sloane NJA (1977) The theory of error-correcting codes. North Holland Publishing Co.
13. Mandayam P, Ng HK (2012) Towards a unified framework for approximate quantum error correction. Physical Review A 86(1):article no. 012335

14. de Moura L, Bjørner N (2008) Z3: An efficient SMT solver. In: Proc. of 14th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), Springer, pp 337–340
15. Nielsen MA, Chuang IL (2000) Quantum Computation and Quantum Information. Cambridge University Press
16. Post EL (1946) A variant of a recursively unsolvable problem. Bulletin of the American Mathematical Society 52(6):264–268
17. Rastegin AE (2009) Partitioned trace distances. Quantum Information Processing 9(1):61–73
18. Shor PW (1995) Scheme for reducing decoherence in quantum computer memory. Physical Review A 52(4):R2493–R2496
19. Steane AM (1996) Error correcting codes in quantum theory. Physical Review Letters 77(5):793–797
20. Tarski A (1951) A Decision Method for Elementary Algebra and Geometry, 2nd edn. University of California Press
21. Thinh LP, Faist P, Helsen J, Elkouss D, Wehner S (2019) Practical and reliable error bars for quantum process tomography. Physical Review A 99(5):article no. 052311
22. Uhlmann A (2000) On "partial" fidelities. Reports on Mathematical Physics 45(3):407–418
23. Wolf MM, Cubitt TS, Pérez-García D (2011) Are problems in quantum information theory (un)decidable? CoRR abs/1111.5425, URL `http://arxiv.org/abs/1111.5425`
24. Wootters WK, Zurek WH (1982) A single quantum cannot be cloned. Nature 299:802–803
25. Yamamoto N (2009) Exact solution for the max-min quantum error recovery problem. In: Proc. of 48th IEEE Conference on Decision and Control (CDC), IEEE, pp 1433–1438
26. Yamamoto N, Hara S, Tsumura K (2005) Suboptimal quantum-error-correcting procedure based on semidefinite programming. Physical Review A 71(2):article no. 022322