YITP-24-60

Explicit decoders using fixed-point amplitude amplification based on QSVT

Takeru Utsumi[1] and Yoshifumi Nakata[2]

[1]Graduate School of Arts and Sciences, The University of Tokyo, Komaba, Meguro-ku, Tokyo 153-8902, Japan
[2]Yukawa Institute for Theoretical Physics, Kyoto University, Kitashirakawa, Sakyo-ku, Kyoto 606-8502, Japan

arXiv:2405.06051v6 [quant-ph] 5 Mar 2026

Reliably transmitting quantum information via a noisy quantum channel is a central challenge in quantum information science. While constructing a decoder is crucial to this goal, little was known about quantum circuit implementations of decoders that reach high communication rates. In this paper, we provide two decoders with explicit quantum circuits capable of recovering quantum information when the decoupling condition is satisfied, i.e., when quantum information is in principle recoverable. These are applicable to both entanglement-assisted and non-assisted settings. By developing a technique that relies on a symmetric structure of the decoders, we show that they are applicable to any noise model. As a consequence, for any noisy channel, our decoders can be used to achieve a communication rate arbitrarily close to the quantum capacity by increasing the number of channel uses. To construct the decoders, we employ the fixed-point amplitude amplification (FPAA) based on the quantum singular value transformation (QSVT), extending a previous approach applicable only to erasure noise. Our constructions offer advantages in the computational cost, largely reducing the circuit complexity compared to previous explicit decoders. Through an investigation of the decoding problem, unique advantages of the QSVT-based FPAA are highlighted.

Takeru Utsumi: takeru-utsumi@g.ecc.u-tokyo.ac.jp
Yoshifumi Nakata: yoshifumi.nakata@yukawa.kyoto-u.ac.jp

1 Introduction

Protecting quantum information from the effects of noise is crucial for transmitting quantum information over noisy quantum channels. A standard technique is to use quantum error correcting codes (QECCs), in which quantum information is encoded before the system experiences noise and is decoded afterward. The QECCs are also of significant importance in fundamental physics, such as the black hole information paradox [1–3], the AdS/CFT correspondence [4, 5], topological orders [6–8], and quantum chaos [9–11].

The importance of high-performance QECCs, especially those capable of transmitting quantum information at high rates, is growing with the recent advancement of quantum technology. In particular, achieving the optimal communication rate, i.e., the *quantum capacity*, is one of the main goals of quantum information theory. A standard approach to this goal relies on the concept of *decoupling* [12–14], which provides a necessary and sufficient condition for the recoverability of quantum information from a noisy system. The decoupling approach is, however, for investigating the capability of encoders and offers little insight into explicit decoding strategies. Explicitly constructing decoders whose rate approaches the quantum capacity has long been a central challenge.

Some progress has been made so far on QECCs with specific structures aimed at achieving high communication rates. For instance, a Clifford-based polar code provides an explicit decoder for Pauli noise that reaches a rate near the quantum capacity [15]. In another approach, [16] and subsequent works [17, 18] developed belief-propagation decoders for pure-state classical-quantum channels, which achieve the classical capacity. There is also an approach based on CSS-

type encoding with decoding via measurements of complementary observables [19, 20]. Despite the significance of the decoding problem, however, only a handful of results have been obtained in general cases [21–23] due to its inherent difficulties. Exploring general decoders can be beneficial towards achieving high-performance QECCs or the quantum capacity.

Among the previously proposed decoders applicable to general noise, to the best of our knowledge, the only one known to be explicit and approximately achieve the quantum capacity is based on the Petz recovery map [24, 25]. Since the map is known to attain near-optimal recovery error [21], and also to exhibit favorable second-order performance [26], it can serve as a high-performance decoder. However, implementing the Petz recovery map with a quantum circuit requires significant computational costs [27–30]. From a practical point of view, it is desirable to develop explicit quantum circuit constructions with reduced computational costs.

An explicit decoder with smaller computational cost is possibly constructed by following the approach of Yoshida and Kitaev [31]. They proposed a decoding protocol, which we call the *Yoshida–Kitaev (YK) decoder*, for the Hayden–Preskill (HP) protocol [1], a specific noisy model of the qubit-erasure noise with a unitary encoding, relevant to a toy model of a quantum black hole. The proposal consists of two steps: first, a decoding protocol with post-selection is considered, and then the protocol is lifted up to a decoding quantum circuit without post-selection through a non-trivial use of the *amplitude amplification (AA)* algorithm [32–34]. This two-step construction provides an explicit quantum circuit and successfully decodes the HP protocol, contributing to high-energy physics (see, e.g., [35, 36]). However, the second step with the AA algorithm, as well as the proof technique, is specifically tailored to the HP protocol. As a result, the approach is not applicable to other noise models, limiting its impact on quantum information theory. This naturally raises the question: *can the two-step construction be extended to construct a decoder applicable to an arbitrary noise model?* If this question is answered affirmatively and the resulting decoder achieves a high communication rate, it contributes to the field of quantum information.

The key to extending the construction would lie in upgrading the step with the AA using recently proposed quantum algorithms. In the past decade, significant progress has been made in quantum algorithms, including the AA algorithm [32–34]. The *fixed-point amplitude amplification (FPAA)* [37–39] is one of the improved ones applicable to broader situations. An approach to the FPAA is based on the *quantum singular value transformation (QSVT)* [40–42], exhibiting a unique property not found in other AA-type algorithms (see 2.6). The distinctive feature of the QSVT-based FPAA may help achieve tasks beyond the reach of any other AA-type algorithms. This observation may also be of theoretical interest as it will offer concrete examples in applications that highlight the unique advantages of the QSVT-based FPAA.

In this paper, by building upon these recent advances, we construct two explicit decoding circuits applicable to arbitrary noisy channels. One is a *generalized YK* decoder, and the other is a *Petz-like* decoder. Both of them are obtained by upgrading the two-step construction with the unique advantages of the QSVT-based FPAA. The Petz-like decoder is a more concise alternative to the Petz recovery map, suggesting that a full implementation of the map is not necessary for decoding. These decoders are applicable to both the entanglement-assisted and non-assisted settings. We show that these decoders can recover quantum information when the decoupling condition is satisfied. Since the decoupling is necessary and sufficient for recovery, the decoders succeed in recovering quantum information whenever it is in principle possible. This implies that, in the i.i.d. setting, both decoders with suitably chosen encoders asymptotically achieve a rate arbitrarily close to the quantum capacity. The technical contribution lies in a novel proof method relying solely on a general structure of the construction, by which the original method's limitations in applicability can be circumvented. Specifically, we exploit a symmetry of the two-step construction and apply the Powers–Størmer inequality [43, 44], a powerful tool of mathematical physics.

Furthermore, taking advantage of explicit constructions, we provide an in-depth analysis of the circuit complexity of the decoders. We show that both of our decoding circuits largely reduce the

circuit complexity. The complexity remains exponential in the number of qubits, which should be the case due to the inherent computational hardness of a general decoding problem [45–47]. Nevertheless, we have succeeded in reducing the exponent of the exponential scaling compared to the previously known explicit decoding circuits [28], resulting in a significant improvement. We also provide a simple criterion to determine which of the two decoders, the generalized YK and the Petz-like decoders, has smaller complexity. Although the criterion depends on many factors, we show that the generalized YK decoder always has smaller complexity when an encoder is an isometry and noisy channels have the maximum number of Kraus operators.

Our constructions, among the first few to provide decoders achieving a rate arbitrarily close to the quantum capacity with explicit quantum circuit implementations, contribute to the main challenge in quantum information theory. Additionally, from a quantum algorithms perspective, our construction works with the QSVT-based FPAA but fails with other known AA-type algorithms, clearly exemplifying the separation between these algorithms in a concrete and practically relevant problem. Although such a separation was previously pointed out [41], to our knowledge, few concrete examples were found in the literature. Moreover, our example highlights the situation in which the separation becomes particularly pronounced. Specifically, the unique advantages of the QSVT-based FPAA stand out when the algorithm is necessarily applied to a subsystem of an entangled system, which is precisely the case in the decoding problem. This observation provides insights into future applications of the QSVT-based algorithms.

This paper is organized as follows. We start with preliminaries in 2. Our main results are summarized in 3. The proofs of our results are provided in 4. We conclude with a summary and outlooks in 5.

2 Preliminaries

We here introduce our notation and our setting. We then briefly overview an implicit decoder commonly used in the decoupling approach. We also provide quick overviews of the Petz recovery map and the original two-step construction of the YK decoder for the HP protocol [31]. We then concisely highlight the properties of several known AA-type algorithms and provide a brief introduction to the QSVT-based FPAA.

2.1 Notation

Throughout this paper, we denote by $\mathcal{S}(\mathcal{H})$ a set of all quantum states on a Hilbert space $\mathcal{H}$. While we usually denote a pure state by $|\varphi\rangle$, the corresponding density operator is sometimes described as φ, namely, $\varphi = |\varphi\rangle\langle\varphi|$. We use a superscript to represent a system on which operators and maps are defined. For instance, an operator on a system AB and a superoperator from A to B are denoted by φ^{AB} and $\mathcal{T}^{A\to B}$, respectively. The superscript is omitted when it is clear from the context. A reduced density operator on A of φ^{AB} is described as φ^A, i.e., $\varphi^A = \mathrm{Tr}_B\, \varphi^{AB}$, where Tr_B is the partial trace over B.

For an operator M, we denote the complex conjugate and the transpose in a given basis by M^* and M^T, respectively, and denote the Hermitian conjugate by $M^\dagger$. The identity operation is denoted by $\mathbb{I}$ and id for operators and superoperators, respectively. We often omit the identity operators and superoperators for simplicity.

A Hilbert space, such as $\mathcal{H}^{A'}$ or $\mathcal{H}^{\hat{A}}$, is isomorphic to $\mathcal{H}^A$: it has the same dimension and the same fixed basis as $\mathcal{H}^A$. This applies not only to the system A, but also to any systems, such as $\mathcal{H}^{B'}$ and $\mathcal{H}^{\hat{C}}$. We write the dimension of a Hilbert space $\mathcal{H}$ as d, and for instance, denote by d_A the dimension of $\mathcal{H}^A$.

We omit the symbol of the tensor product between vectors and denote it as $|\varphi\rangle \otimes |\psi\rangle = |\varphi\rangle|\psi\rangle$, for simplicity, when it is clear from the context. We denote by $|\Phi\rangle$ a maximally entangled state (MES) defined in an orthonormal computational basis. For instance, the MES between A and $\hat{A}$ is

$$|\Phi\rangle^{A\hat{A}} = \frac{1}{\sqrt{d_A}} \sum_{i=1}^{d_A} |i\rangle^A |i\rangle^{\hat{A}}, \tag{1}$$

where $\{|i\rangle\}_i$ is the computational basis in A and $\hat{A}$, respectively. Note that a MES in an arbitrary basis can be transformed into the MES in the computational basis by applying an appropriate unitary to one of the local systems. Also, note that $\sqrt{d_A}|\Phi\rangle^{AA'} = \sum_i |i\rangle^A |i\rangle^{A'} = \sum_i |e_i\rangle^A |e_i^*\rangle^{A'}$ holds for any orthonormal basis $\{|e_i\rangle^A\}_i$. Here, the complex conjugate is taken with respect to

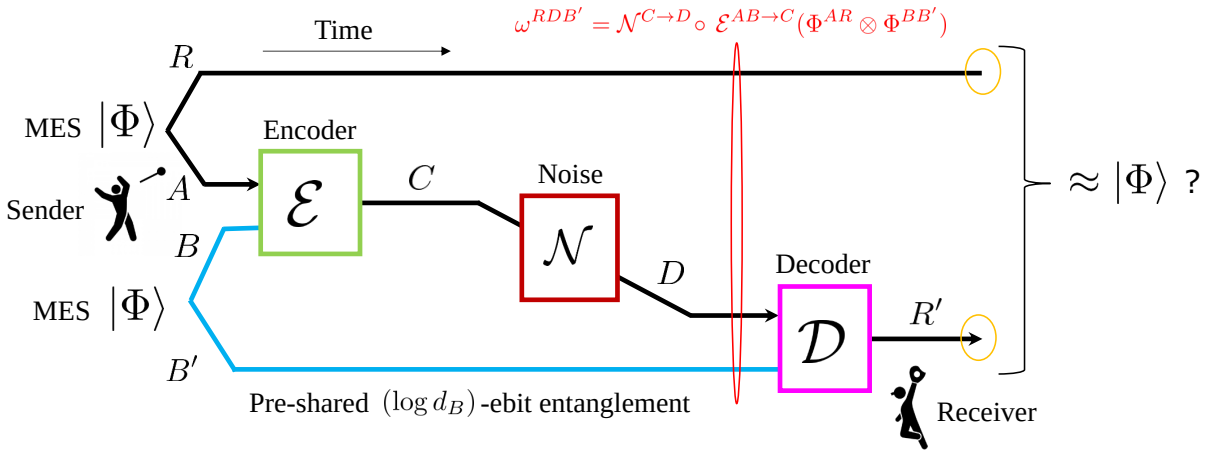


Figure 1: A diagram of our setting. Time flows from left to right. The boxes represent quantum channels. The purpose of the sender and the receiver is to transmit quantum information via a noisy channel $\mathcal{N}^{C\to D}$, which is equivalent to preserving the maximally entangled state between A and R. They may share $(\log d_B)$-ebit entanglement in advance, which is used during the encoding and decoding operations. When $d_B = 1$, this corresponds to the entanglement-non-assisted setting, while $d_B \neq 1$ corresponds to the entanglement-assisted setting with a limited or unlimited amount of entanglement, depending on whether d_B is bounded or arbitrarily large, respectively.

the computational basis; that is, when $|e_i\rangle^A = \sum_j c_{ij}|j\rangle^A$, it is given by $|e_i^*\rangle^{A'} = \sum_j c_{ij}^*|j\rangle^{A'}$. We denote the completely mixed state (CMS) by π, such as $\pi^A = \mathbb{I}^A/d_A$.

The circuit complexity of $\mathcal{T}$ is denoted by $\mathcal{C}(\mathcal{T})$. This is the minimum total number of single- and two-qubit unitary gates required to perform $\mathcal{T}$, allowing for ancillae polynomial in the number of qubits.

For a matrix M, the Schatten-p norm is defined by $\|M\|_p := \left(\mathrm{Tr}\left[(\sqrt{M^\dagger M})^p\right]\right)^{1/p}$. We particularly use the trace norm, the Hilbert–Schmidt norm, and the operator norm, corresponding to $p = 1, 2, \infty$, respectively. The trace norm has the contraction property such that for $\varphi^{AB} \in \mathcal{S}(\mathcal{H}^{AB})$ and $\psi^{AB} \in \mathcal{S}(\mathcal{H}^{AB})$,

$$\|\varphi^A - \psi^A\|_1 \leq \|\varphi^{AB} - \psi^{AB}\|_1. \tag{2}$$

The fidelity between $\varphi \in \mathcal{S}(\mathcal{H})$ and $\psi \in \mathcal{S}(\mathcal{H})$ is defined by $\mathrm{F}(\varphi, \psi) := \left\|\sqrt{\varphi}\sqrt{\psi}\right\|_1^2$. The fidelity is rephrased using the purified states of φ and ψ as

$$\mathrm{F}(\varphi^A, \psi^A) = \max_V |\langle\varphi|^{AC} V^{B\to C} |\psi\rangle^{AB}|^2, \tag{3}$$

where the maximization is taken over all isometries $V^{B\to C}$. We supposed $d_C \geq d_B$ without loss of generality. This is called the *Uhlmann's theorem* [48]. The trace norm and the fidelity are related by the Fuchs–van de Graaf inequalities [49, 50]:

$$1 - \sqrt{\mathrm{F}(\varphi, \psi)} \leq \frac{1}{2}\|\varphi - \psi\|_1 \leq \sqrt{1 - \mathrm{F}(\varphi, \psi)}. \tag{4}$$

We use the quantum collision entropy. For $\varphi^A \in \mathcal{S}(\mathcal{H}^A)$ it is given by

$$H_2(A)_\varphi = -\log \mathrm{Tr}[(\varphi^A)^2]. \tag{5}$$

This satisfies $0 \leq H_2(A)_\varphi \leq \log d_A$.

2.2 Our setting

We consider the following general setting, which is common in quantum communication. See also Fig. 1. A sender aims to transmit $(\log d_A)$-qubit quantum information using a given noisy channel $\mathcal{N}^{C\to D}$ and possibly a pre-shared entanglement $|\Phi\rangle^{BB'}$, where B and B' are with the sender and receiver, respectively. When they share no entanglement, we set $d_B = 1$ and call this the entanglement-non-assisted setting. Otherwise, it is the entanglement-assisted setting, with a limited or unlimited amount of entanglement depending on whether d_B is bounded or arbitrarily large, respectively. The sender encodes the system A with B using an encoding channel $\mathcal{E}^{AB\to C}$. The qubits in C are then transmitted to the receiver through the noisy channel $\mathcal{N}^{C\to D}$. The receiver obtains the output system D of the noisy channel and applies a recovery channel, i.e., a decoder $\mathcal{D}^{DB'\to R'}$ onto the system DB'. For simplicity, we denote by $\mathcal{F}^{AB\to D}$ the composite channel $\mathcal{N}^{C\to D} \circ \mathcal{E}^{AB\to C}$.

Following the convention, we introduce a reference system R isomorphic to A with $d_R = d_A$, and prepare the systems A and R to be in a MES

$|\Phi\rangle^{AR}$. We denote by $\omega^{RDB'}$ the state after the noise, i.e., just before the decoder:

$$\omega^{RDB'} := \mathcal{F}^{AB\to D}(\Phi^{AR} \otimes \Phi^{BB'}). \tag{6}$$

The recovery error of quantum information by a decoder $\mathcal{D}^{DB'\to R'}$ is defined as [1]

$$\Delta(\mathcal{D}|\mathcal{F}) := \frac{1}{2}\|\Phi^{RR'} - \mathcal{D}^{DB'\to R'}(\omega^{RDB'})\|_1. \tag{7}$$

The main concern in this paper is to explicitly construct a decoder $\mathcal{D}^{DB'\to R'}$ for a given channel $\mathcal{F}^{AB\to D}$. We assume that the descriptions of the encoding map $\mathcal{E}$ and the noisy channel $\mathcal{N}$ are known, so that the decoder can depend on their details. It is also assumed that every operation, except for the noisy channel $\mathcal{N}$, can be performed noiselessly. This is a common assumption in studies of information transmission. For practical implementation, however, it is also important to relax this assumption, which we will mention in 5.

2.3 Decoupling and quantum capacity

A standard approach to evaluating the recovery error is to estimate how much quantum information is leaked to an "environment" of the noisy channel. This is specifically quantified by the degree of decoupling.

Let $V_{\mathcal{F}}^{AB\to ED}$ be a Stinespring isometry [54] of the channel $\mathcal{F}^{AB\to D} = \mathcal{N}^{C\to D} \circ \mathcal{E}^{AB\to C}$ by an environment E. That is, the channel $\mathcal{F}^{AB\to D}$ is represented as

$$\mathcal{F}^{AB\to D}(\cdot) = \mathrm{Tr}_E\left[V_{\mathcal{F}}^{AB\to ED}(\cdot)(V_{\mathcal{F}}^{AB\to ED})^\dagger\right]. \tag{8}$$

For convenience, we also introduce a purified state of $\omega^{RDB'}$ in Eq. (6) as

$$|\omega\rangle^{REDB'} := V_{\mathcal{F}}^{AB\to ED}|\Phi\rangle^{AR}|\Phi\rangle^{BB'}. \tag{9}$$

The following is called the decoupling approach.

Proposition 1 (Decoupling approach [12–14])**.** *Suppose $|\omega\rangle^{REDB'}$ is a pure state. If there exists a state τ^E such that $\|\omega^{RE} - \pi^R \otimes \tau^E\|_1 \le \epsilon$, then there exists a quantum channel $\mathcal{D}^{DB'\to R'}_{\mathrm{Uhlmann}}$ that satisfies*

$$\frac{1}{2}\left\|\Phi^{RR'} - \mathcal{D}^{DB'\to R'}_{\mathrm{Uhlmann}}(\omega^{RDB'})\right\|_1 \le \sqrt{\epsilon}. \tag{10}$$

[1] It is known that the recovery errors defined by other metrics, such as the diamond norm, are closely related to the recovery error we adopt [23, 50–53].

This proposition is a straightforward consequence of the Uhlmann's theorem (Eq. (3)) together with Eqs. (2) and (4). See, e.g., [12–14]. The condition that there exists τ^E such that

$$\|\omega^{RE} - \pi^R \otimes \tau^E\|_1 \le \epsilon, \tag{11}$$

is called a *decoupling condition*, and, in fact, it is known to be necessary and sufficient for the recoverability of quantum information.

The decoupling approach is particularly strong in the study of the maximum possible communication rate of quantum information, i.e., the quantum capacity, either in one-shot or asymptotic settings. We now briefly describe the relation between the decoupling condition and the quantum capacity, as well as the construction of an explicit decoder.

Suppose that quantum information is transmitted through N independent and identical uses of a noisy channel $\mathcal{N}_1^{A_1\to C_1}$, namely, $\mathcal{N}^{A\to C} = (\mathcal{N}_1^{A_1\to C_1})^{\otimes N}$. An (asymptotically) achievable rate is given by $\mathrm{R} := \lim_{N\to\infty}\frac{1}{N}\log d_A$ under the assumption that there exists a sequence of pairs of an encoder and a decoder such that the recovery error tends to zero as $N\to\infty$. The quantum capacity is defined as the supremum of the achievable rate for the channel $\mathcal{N}_1$.

As established in the quantum capacity theorem [52, 55–58], when the sender and receiver share no entanglement in advance, the quantum capacity $Q(\mathcal{N}_1)$ is given by the regularized coherent information:

$$Q(\mathcal{N}_1) = \lim_{N\to\infty}\frac{1}{N} I_{\mathrm{c}}((\mathcal{N}_1^{A_1\to C_1})^{\otimes N}), \tag{12}$$

where $I_{\mathrm{c}}(\mathcal{T}^{A\to B}) = \max_{\rho^A}\left[H(\mathcal{T}^{A\to B}(\rho^A)) - H(\bar{\mathcal{T}}^{A\to E}(\rho^A))\right]$ is the coherent information of a quantum channel $\mathcal{T}^{A\to B}$ [50, 53, 59]. Here, $H(\rho^A) = -\mathrm{Tr}[\rho^A\log\rho^A]$ is the von Neumann entropy of a state ρ^A and $\bar{\mathcal{T}}^{A\to E}$ is a complementary channel of $\mathcal{T}^{A\to B}$. The maximization is taken over all states on the input system of $\mathcal{T}^{A\to B}$. Note that achieving the quantum capacity, which may exceed the one-shot coherent information of a quantum channel $I_{\mathrm{c}}(\mathcal{N}_1^{A_1\to C_1})$ due to its superadditivity, generally requires encoding and decoding collectively over N-block uses of the channel $\mathcal{N}_1$. On the other hand, in the case that unlimited pre-shared entanglement is available, the entanglement-assisted quantum capacity $Q_{\mathrm{E}}(\mathcal{N}_1)$ is given by the mutual information

of a quantum channel [59–61]:

$$Q_{\mathrm{E}}(\mathcal{N}_1) = \frac{1}{2} I(\mathcal{N}_1^{A_1 \to C_1}), \tag{13}$$

where $I(\mathcal{T}^{A\to B}) = \max_{|\rho\rangle^{AA'}} [H(\mathcal{T}^{A\to B}(\rho^A)) + H(\rho^A) - H(\mathcal{T}^{A\to B}(|\rho\rangle\langle\rho|^{AA'}))]$ is the mutual information of a quantum channel $\mathcal{T}^{A\to B}$ [53, 59]. The maximization is taken over all purifications $|\rho\rangle^{AA'}$ of the state ρ^A with a reference system A'. Unlike the coherent information of a quantum channel $I_{\mathrm{c}}(\mathcal{T}^{A\to B})$, the mutual information of a quantum channel $I(\mathcal{T}^{A\to B})$ is additive, and thus Eq. (13) does not involve regularization via a limit over N.

From the discussion of the decoupling and the random encoding (see, e.g., [12–14, 50, 53, 62]), it is known that, in the entanglement-non-assisted setting, when the achievable rate R is below the quantum capacity $Q(\mathcal{N}_1)$, there exists a suitable isometric encoder that achieves decoupling with asymptotically vanishing error: $\epsilon \to 0$ as $N \to \infty$. This is also the case in the entanglement-assisted setting with unlimited entanglement, where R must satisfy $\mathrm{R} < Q_{\mathrm{E}}(\mathcal{N}_1)$. Then, Proposition 1 implicitly provides a decoder under which the recovery error asymptotically tends to zero. This guarantees the existence of a decoder that can be used to achieve the communication rate asymptotically approaching the quantum capacity; however, this does not provide an explicit procedure for constructing the decoder, and all details, including its computational cost, remain unclear[2].

Constructing a high-performance decoder explicitly in the form of quantum circuits poses significant challenges. The decoupling approach offers guidance toward this goal, as the relation between the decoupling and the quantum capacity implies that by designing decoders under the decoupling condition, we obtain explicit decoders that can be used to asymptotically achieve a rate approaching the quantum capacity. Hereafter, to construct explicit decoders, we investigate a general channel $\mathcal{N}$ and the one-shot scenario. For discussing the quantum capacity, it suffices to apply the decoder to the case $\mathcal{N} = \mathcal{N}_1^{\otimes N}$ and consider the asymptotic limit.

[2]In recent work, explicit algorithms directly addressing the Uhlmann's theorem have also been explored; see Refs. [63, 64].

2.4 Petz recovery map

One of the explicit decoders we may use is the Petz recovery map [24, 25], which has been intensely studied [26, 59, 65, 66]. The Petz recovery map is developed from a quantum analog of Bayes theorem based on the idea that there can be a reverse channel that counteracts the effect of noise. The general form of the Petz recovery map is determined by a map $\mathcal{T}$ and a reference state σ, given by

$$\mathcal{P}^{B\to A}_{\sigma,\mathcal{T}}(\cdot) = (\sigma^A)^{\frac{1}{2}} (\mathcal{T}^{A\to B})^\dagger \Big([\mathcal{T}(\sigma^A)]^{-\frac{1}{2}} (\cdot) [\mathcal{T}(\sigma^A)]^{-\frac{1}{2}} \Big) (\sigma^A)^{\frac{1}{2}}, \tag{14}$$

where $(\mathcal{T}^{A\to B})^\dagger$ is the adjoint map of $\mathcal{T}^{A\to B}$ with respect to the Hilbert–Schmidt inner product. The Petz recovery map is composed of three CP maps:

$$(\cdot) \to [\mathcal{T}(\sigma^A)]^{-\frac{1}{2}} (\cdot) [\mathcal{T}(\sigma^A)]^{-\frac{1}{2}}, \tag{15}$$

$$(\cdot) \to (\mathcal{T}^{A\to B})^\dagger (\cdot), \tag{16}$$

$$(\cdot) \to (\sigma^A)^{\frac{1}{2}} (\cdot) (\sigma^A)^{\frac{1}{2}}, \tag{17}$$

and achieves the perfect recovery for the reference state σ^A, i.e., $\mathcal{P}^{B\to A}_{\sigma,\mathcal{T}}(\mathcal{T}^{A\to B}(\sigma^A)) = \sigma^A$.

For the recovery error of the Petz recovery map, the following is known.

Proposition 2 (Barnum-Knill's theorem [21])**.** *For any state ρ^A and any channel $\mathcal{T}^{A\to B}$, it holds that*

$$\mathrm{F}\big(\rho^{AR}, \mathcal{P}^{B\to A}_{\rho,\mathcal{T}} \circ \mathcal{T}^{A\to B}(\rho^{AR})\big) \geq \big[\max_{\mathcal{R}} \mathrm{F}\big(\rho^{AR}, \mathcal{R}^{B\to A} \circ \mathcal{T}^{A\to B}(\rho^{AR})\big)\big]^2, \tag{18}$$

where $\rho^{AR} = |\rho\rangle\langle\rho|^{AR}$ is a purified state of ρ^A. The maximum is taken over all quantum channels $\mathcal{R}^{B\to A}$.

This proposition guarantees that if there exists a decoder that recovers information with a small error, the Petz recovery map also recovers it with a small error.

To apply the Petz recovery map to our setting, let F be the system such that $ABF = ED$, and a unitary $U^L_{\mathcal{F}}$ be defined by

$$V^{AB\to ED}_{\mathcal{F}} = U^L_{\mathcal{F}} |0\rangle^F, \tag{19}$$

where $L = ABF = ED$. Using this unitary, Eq. (8) is rephrased as

$$\mathcal{F}^{AB\to D}(\cdot) = \mathrm{Tr}_E \left[U^L_{\mathcal{F}} (\cdot \otimes |0\rangle\langle 0|^F) (U^L_{\mathcal{F}})^\dagger \right]. \tag{20}$$

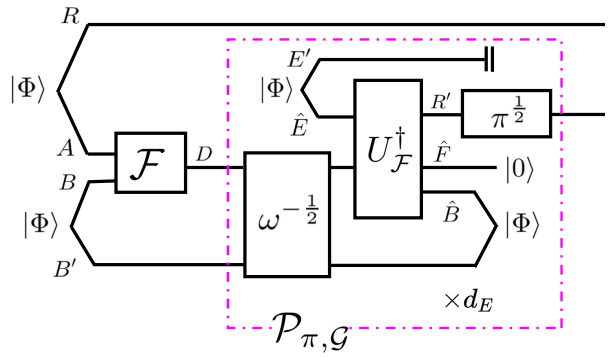


Figure 2: A diagram of the Petz recovery map applied to our setting. The dash-dotted box corresponds to the Petz recovery map $\mathcal{P}_{\pi,\mathcal{G}}$ given in Eq. (21). The boxes of $(\omega^{DB'})^{-1/2}$ and $(\pi^{R'})^{1/2}$ represent that $(\cdot) \to (\omega^{DB'})^{-1/2}(\cdot)(\omega^{DB'})^{-1/2}$ and $(\cdot) \to (\pi^{R'})^{1/2}(\cdot)(\pi^{R'})^{1/2}$, respectively. The double vertical lines represent that the qubits of that system are traced out.

We use $\mathcal{G}^{A\to DB'}(\cdot) \coloneqq \mathcal{F}^{AB\to D}(\cdot \otimes \Phi^{BB'})$ and fix the reference state to be the CMS π^A. The explicit form of the Petz recovery map in our setting is then given by

$$\begin{aligned}&\mathcal{P}^{DB'\to R'}_{\pi,\mathcal{G}}(\omega^{RDB'})\\ &= d_E \operatorname{Tr}_{E'}\Big[(\pi^{R'})^{1/2}\langle\Phi|^{\hat{B}B'}\langle 0|^{\hat{F}}(U^{\hat{L}}_{\mathcal{F}})^\dagger\\ &\qquad\big[(\omega^{DB'})^{-1/2}\omega^{RDB'}(\omega^{DB'})^{-1/2}\otimes\Phi^{\hat{E}E'}\big]\\ &\qquad U^{\hat{L}}_{\mathcal{F}}|\Phi\rangle^{\hat{B}B'}|0\rangle^{\hat{F}}(\pi^{R'})^{1/2}\Big],\end{aligned} \tag{21}$$

where $\hat{L}$ is equal to $R'\hat{F}\hat{B} = \hat{E}D$. See also the diagram in Fig. 2.

By combining Proposition 2 with Proposition 1 and the Fuchs–van de Graaf inequalities Eq. (4), we derive the following statement, which relates the recovery error of the Petz recovery map $\mathcal{P}^{DB'\to R'}_{\pi,\mathcal{G}}$ against $\mathcal{F}^{AB\to D}$ to the decoupling condition: if there exists a state τ^E such that $\|\omega^{RE} - \pi^R \otimes \tau^E\|_1 \le \epsilon$, then the recovery error of the Petz recovery map in the above setting is given by

$$\Delta(\mathcal{P}_{\pi,\mathcal{G}}|\mathcal{F}) \le 2\epsilon^{1/4}. \tag{22}$$

As discussed in 2.3, the decoupling is asymptotically achieved by an appropriately chosen encoder. Since the upper bound on the recovery error of $\mathcal{P}_{\pi,\mathcal{G}}$ also asymptotically tends to zero with such an encoder, its communication rate can approach the quantum capacity.

Although it is not clear from the definition how the Petz recovery map can be implemented by quantum circuits, an algorithmic implementation was provided in [28]. The algorithm is based on the fact that the Petz recovery map is a CPTP map as a whole, which allows its implementation through the direct use of the QSVT. However, its circuit complexity grows exponentially with the number of qubits due to the full implementation of the CP maps in Eqs. (15) to (17).

2.5 Two-step construction of a decoder for the Hayden–Preskill protocol

In [31], a decoding circuit was provided for recovering quantum information in the HP protocol [1]. The HP protocol formulates the information paradox of black holes based on the qubit-erasure noise with a restriction that the encoding operation is given by a random unitary dynamics. That is, the encoder $\mathcal{E}$ and the noise $\mathcal{N}$ in Fig. 1 are given by a random unitary and the partial trace over a subsystem E of C, respectively, where $AB = C$.

The construction of a decoder consists of two steps. The first step is to construct a decoding protocol with post-selection. This is achieved by "emulating" the dynamics of the encoding unitary and the erasure noise in the receiver's local system and teleporting the output of the noise by performing the measurement in a maximally entangled basis. More specifically, after preparing the emulated systems in the receiver's local system, the receiver measures the output of the noise and the corresponding emulated output in the maximally entangled basis. If a desired outcome is obtained, the emulated output becomes as if it were in the same quantum state as that of the noisy output. In this case, the effect of the erasure noise is canceled by the dynamics emulated in advance in the local system, and the receiver succeeds in recovering quantum information. Note that this protocol does not succeed with certainty as it requires post-selection.

In the second step of the construction, this post-selection is removed by replacing the measurement with the AA algorithm. This replacement can be understood as aiming to amplify the probability of obtaining the desired outcome. As a result, a decoding quantum circuit for the HP protocol without post-selection is constructed.

The reason for this construction to work, or more specifically the AA algorithm to work, strongly relies on the specific properties of the HP protocol, as we will later elaborate on. The proof technique is also fully tailored to the HP protocol

and cannot be simply generalized to other noise models. Hence, this decoding strategy with a standard AA algorithm for the HP protocol cannot be directly applied to general noisy situations.

2.6 Various amplitude amplification protocols

The AA algorithm is a common technique to enhance the measurement probability to obtain a desired output, and it provides a quadratic speedup over classical algorithms. Various amplitude amplification protocols have been proposed so far, and each has different features.

To remind the standard AA algorithm, let an initial state and a desired state be $|\psi\rangle$ and $|\xi\rangle$, respectively. We consider iteratively applying unitaries $I - 2|\xi\rangle\langle\xi|$ and $I - 2|\psi\rangle\langle\psi|$, t times to the initial state. This iterative application approximately achieves the state transformation, such as

$$|\psi\rangle \mapsto |\xi\rangle, \quad \text{if } t = \lfloor \pi/(4|\langle\xi|\psi\rangle|) \rfloor. \tag{23}$$

One feature of this standard AA algorithm is that this desired state is not a fixed point of the operation. That is, if the number t of iterations exceeds the value in Eq. (23), the resulting state becomes different from $|\xi\rangle$. This is known as an *overcook* problem [67]. For this reason, it is crucial to precisely know the value of $|\langle\xi|\psi\rangle|$ in advance.

The overcook problem is circumvented by the FPAA [39]. The FPAA algorithm also consists of the iterations of unitaries, but there is a threshold number $t_{\rm th}$ of iterations such that

$$|\psi\rangle \mapsto e^{i\chi}|\xi\rangle, \quad \forall t \geq t_{\rm th} = \mathcal{O}(1/|\langle\xi|\psi\rangle|), \tag{24}$$

is approximately achieved, where χ is an unknown phase. Unlike the standard AA algorithm, if $t \geq t_{\rm th}$, the state always stays in this form. As the unknown phase χ is typically not important in many applications of the AA algorithm, the FPAA should resolve the overcook problem. Importantly, the FPAA works if a lower bound on $|\langle\psi|\xi\rangle|$ is known in advance, and precise estimation of the value is not necessary.

While the FPAA may be sufficient in most applications, one can get rid of the unknown phase χ by the QSVT-based FPAA [40–42]. We will describe the QSVT-based FPAA in more detail in the next section. The QSVT-based FPAA iterates certain unitaries t times, and one can approximately achieve

$$|\psi\rangle \mapsto |\xi\rangle, \quad \forall t \geq t_{\rm th} = \mathcal{O}(1/|\langle\xi|\psi\rangle|), \tag{25}$$

without any unknown phases that could be problematic depending on the goals. As pointed out in [41], this is one of the unique features of the QSVT-based FPAA, which may help in achieving tasks that are not achievable by any other AA-type algorithms. Constructing explicit examples of such tasks, especially those of practical importance or those contributing to existing problems, is of theoretical interest.

2.7 Quantum singular value transformation-based fixed-point amplitude amplification

Our construction of decoders employs the QSVT-based FPAA. We here introduce it briefly. For further details, see, e.g., [40–42].

We first introduce a notion of block-encoding [40, 68]. When a certain operator of interest Λ such that $\|\Lambda\|_\infty \leq 1$ is encoded as a block of a larger unitary U:

$$U = \begin{array}{c} \\ \Pi_2 \end{array} \begin{array}{c} \begin{array}{cc} \Pi_1 & \end{array} \\ \begin{pmatrix} \Lambda & \cdot \\ \cdot & \cdot \end{pmatrix} \end{array} \longleftrightarrow \Lambda = \Pi_2 U \Pi_1, \tag{26}$$

the unitary U is called a block-encoding of Λ. Here, Π_1 and Π_2 are projectors which specify the top-left block of U. The normalization $\|\Lambda\|_\infty \leq 1$ ensures that U is a unitary with appropriate choices of the remaining blocks of U.

The QSVT [40, 41] is a powerful technique to transform Λ to its even or odd polynomial function, by multiple uses of U and $U^\dagger$. In this study, we only focus on degree-t real odd polynomials $Q_{t,\phi}$ that satisfy $|Q_{t,\phi}(x)| \leq 1$ for all $x \in [-1, 1]$, where $\phi = (\phi_1, \phi_2, \ldots, \phi_t)$ is a sequence of parameters with $\phi_j \in (-\pi, \pi]$ for $j = 1, 2, \ldots, t$, which determines the form of the polynomial $Q_{t,\phi}$.

The QSVT with a real polynomial is such that it uses U and $U^\dagger$ a total of $2t$ times to perform the transformation:

$$U = \begin{array}{c} \\ \Pi_2 \end{array} \begin{array}{c} \begin{array}{cc} \Pi_1 & \end{array} \\ \begin{pmatrix} \Lambda & \cdot \\ \cdot & \cdot \end{pmatrix} \end{array} \tag{27}$$

$$\xrightarrow{\text{QSVT}} G_{t,\phi} = \begin{array}{c} \\ \Pi_2' \end{array} \begin{array}{c} \begin{array}{cc} \Pi_1' & \end{array} \\ \begin{pmatrix} Q_{t,\phi}(\Lambda) \otimes |0\rangle\langle 0| & \cdot \\ \cdot & \cdot \end{pmatrix} \end{array}, \tag{28}$$

where $\Pi'_m = \Pi_m \otimes |0\rangle\langle 0|$ for $m = 1, 2$, the projectors with an ancilla qubit. When $Q_{t,\phi}$ is odd, its action on a matrix is defined by

$$Q_{t,\phi}(\Lambda) = \sum_\mu Q_{t,\phi}(s_\mu)|\xi_\mu\rangle\langle\psi_\mu|, \tag{29}$$

where $\Lambda = \sum_\mu s_\mu|\xi_\mu\rangle\langle\psi_\mu|$ is the singular value decomposition of Λ. The unitary $G_{t,\phi}$ is constructed from U as follows. Let $W_m(\theta) := e^{i\theta(2\Pi_m - \mathbb{I})}$ for $m = 1, 2$ and $\theta \in (-\pi, \pi]$, and define $W_{t,\phi}$ as

$$W_{t,\phi} := W_2(\phi_t)U \prod_{j=1}^{(t-1)/2} W_1(\phi_{2j})U^\dagger W_2(\phi_{2j-1})U. \tag{30}$$

Then, $G_{t,\phi}$ is given by

$$G_{t,\phi} := W_{t,\phi} \otimes |+\rangle\langle +| + W_{t,-\phi} \otimes |-\rangle\langle -|. \tag{31}$$

The unitary $G_{t,\phi}$ constructed in this way satisfies

$$(\Pi_2 \otimes \langle 0|)G_{t,\phi}(\Pi_1 \otimes |0\rangle) = Q_{t,\phi}(\Lambda), \tag{32}$$

as indicated by Eq. (28).

Note that, to implement the QSVT in practice, one needs to compute the sequence of phases ϕ corresponding to a given $Q_{t,\phi}$. It is known that we can compute it in $\mathcal{O}(\mathrm{poly}(t))$ time even by a classical computer [69–73].

By choosing a polynomial $Q_{t,\phi}$ appropriately, we can implement various useful quantum algorithms within the QSVT framework. In this work, we particularly consider a real odd polynomial that closely approximates the sign function:

$$\mathrm{sign}(x) = \begin{cases} 1 & (x > 0) \\ 0 & (x = 0) \\ -1 & (x < 0)\,. \end{cases} \tag{33}$$

This case is referred to as the QSVT-based FPAA, also known as the singular vector transformation [40, 41]. The following lemma ensures that there exists a polynomial Q_t^{sign} that well approximates the sign function.

Lemma 3 (Polynomial approximation of the sign function [40–42, 74–78])**.** *For $\delta \in (0, 1/2)$ and $\beta \in (0, 1)$, and for any odd integer $t \geq \lceil \frac{8e}{\beta} \log(2/\delta) \rceil$, there exists a real polynomial $Q_t^{\mathrm{sign}}(x)$ of degree t such that*

- $|Q_t^{\mathrm{sign}}(x)| \leq 1$ *for* $x \in [-1, 1]$,
- $|Q_t^{\mathrm{sign}}(x) - \mathrm{sign}(x)| \leq \delta$ *for* $x \in [-1, -\beta] \cup [\beta, 1]$.

To perform the QSVT-based FPAA, we take the phase sequence $\phi = (\phi_1, \ldots, \phi_t)$ in the QSVT so that the polynomial $Q_{t,\phi}$ becomes Q_t^{sign}. With this polynomial, the matrix Λ is mapped to $Q_t^{\mathrm{sign}}(\Lambda) \approx \mathrm{sign}(\Lambda) = \sum_\mu |\xi_\mu\rangle\langle\psi_\mu|$. We thus obtain an operation that transforms the right singular vectors $|\psi_\mu\rangle$ to the corresponding left singular vectors $|\xi_\mu\rangle$, without introducing any unknown phases.

The range of the degree t of Q_t^{sign} is determined as follows. Let $\gamma_{\delta,\beta}$ be given by

$$\gamma_{\delta,\beta} = 2\Big\lceil \max\Big\{ \frac{e}{2\beta}\sqrt{W\Big(\frac{8}{\pi\delta^2}\Big)W\Big(\frac{512}{e^2\pi\delta^2}\Big)}, \sqrt{2}\,W\Big(\frac{4}{\beta\delta}\sqrt{\frac{2}{\pi}W\Big(\frac{8}{\pi\delta^2}\Big)}\Big)\Big\}\Big\rceil + 1, \tag{34}$$

with the Lambert W function $W(x)$ [79]. Then, for any odd integer $t \geq \gamma_{\delta,\beta}$, there is a degree-$t$ polynomial that approximates $\mathrm{sign}(x)$ within error δ over $|x| \in [\beta, 1]$ [76]. Since $W(x) \leq \log x$ holds for $x > e$ [80, 81], we obtain $\gamma_{\delta,\beta} \leq \lceil \frac{8e}{\beta} \log(2/\delta) \rceil$ for $\delta \in (0, 1/2)$ and $\beta \in (0, 1)$. As a result, it suffices to set t to an odd integer satisfying $t \geq \lceil \frac{8e}{\beta} \log(2/\delta) \rceil$.

3 Main results

In this section, we summarize our results. We provide explicit quantum circuit constructions of two decoders and evaluate their performance. The generalized YK decoder is presented in 3.1, and the Petz-like decoder in 3.2. We investigate the complexity of the decoders in 3.3 and 3.4.

Both decoders are constructed by the extended two-step construction. We first provide a protocol with post-selection and then transform the protocol into the one without post-selection. To achieve the latter, we use the QSVT-based FPAA algorithm, which is crucial for circumventing issues that arise if other AA-type algorithms are used.

3.1 Generalized YK decoder

In 3.1.1, we investigate a decoding protocol with post-selection that works for general encoding maps and noisy channels. We then show in 3.1.2 that the protocol can be lifted up to a decoder, by using the QSVT-based FPAA.

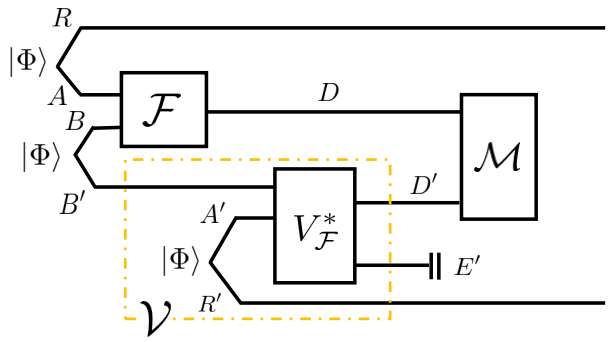


Figure 3: A diagram of the protocol with post-selection for the generalized YK decoder. The double vertical lines represent that the qubits of that system are traced out. The dash-dotted box corresponds to the isometry map $\mathcal{V}^{B'\to D'E'R'}$ defined in Eq. (35).

3.1.1 Decoding protocol with post-selection

The decoding protocol with post-selection consists of the following three steps. See Fig. 3 as well.

1. The receiver prepares ancilla qubits in the system $A'R'$, and then generates a MES $\Phi^{A'R'}$, which is regarded as a copy of the MES Φ^{AR}.

2. The receiver applies an isometry $(V_{\mathcal{F}}^{A'B'\to E'D'})^*$ onto $A'B'$, where $V_{\mathcal{F}}^{AB\to ED}$ is a Stinespring isometry of $\mathcal{F}^{AB\to D}$ and E is an environment of the channel $\mathcal{F}$. The complex conjugate is taken in the computational basis.

3. The receiver performs a binary measurement $\mathcal{M} := \{|\Phi\rangle\langle\Phi|^{DD'}, \mathbb{I}^{DD'} - |\Phi\rangle\langle\Phi|^{DD'}\}$ on DD'. When the former result of the measurement $\mathcal{M}$ is obtained, this protocol succeeds.

Note that, in this protocol, all the systems with a prime, i.e., A', B', R', D', and E', in addition to the output system D of the channel $\mathcal{F}$ are in the hands of the receiver. Thus, the above protocol can be executed by the receiver.

The Stinespring dilation $V_{\mathcal{F}}^{AB\to ED}$ in the step 2 is not uniquely determined from a given channel $\mathcal{F}^{AB\to D}$; the dilation has the freedom of applying additional isometries on the environment E. However, the protocol works for any choice of $V_{\mathcal{F}}^{AB\to ED}$. The receiver can choose an arbitrary Stinespring dilation of the channel $\mathcal{F}^{AB\to D}$.

For future use, we denote the operation up to the step 2 of the above protocol by an isometry map $\mathcal{V}^{B'\to D'E'R'}$. That is,

$$\begin{aligned}&\mathcal{V}^{B'\to D'E'R'}(\cdot)\\ &:= (V_{\mathcal{F}}^{A'B'\to E'D'})^*(\cdot\otimes\Phi^{A'R'})(V_{\mathcal{F}}^{A'B'\to E'D'})^{\mathsf{T}}.\end{aligned} \tag{35}$$

We denote by p_{succ} and ζ_{succ} the success probability and the output state after the success of $\mathcal{M}$ in the step 3, respectively. The reduced state on RR' of ζ_{succ} is given by

$$\begin{aligned}&\zeta_{\mathrm{succ}}^{RR'}\\ &= \mathrm{Tr}_{DD'E'}\left[\frac{1}{p_{\mathrm{succ}}}|\Phi\rangle\langle\Phi|^{DD'}\mathcal{V}^{B'\to D'E'R'}(\omega^{RDB'})\right].\end{aligned} \tag{36}$$

In 4.1.1, we compute p_{succ} and the fidelity between $\zeta_{\mathrm{succ}}^{RR'}$ and $\Phi^{RR'}$, and then obtain

$$p_{\mathrm{succ}} = \frac{d_B}{d_D}2^{-H_2(RE)_\omega}, \tag{37}$$

$$\mathrm{F}(\zeta_{\mathrm{succ}}^{RR'}, \Phi^{RR'}) = \frac{1}{d_A}2^{H_2(RE)_\omega - H_2(E)_\omega}. \tag{38}$$

The second equation, Eq. (38), implies that if ω^{RE} decouples as $\omega^{RE}\approx\pi^R\otimes\omega^E$, the fidelity after post-selection becomes $\mathrm{F}(\zeta_{\mathrm{succ}}^{RR'}, \Phi^{RR'})\approx 1$. In other words, the MES can be successfully recovered if the measurement is successful and the decoupling condition is sufficiently satisfied. However, the success probability p_{succ} is exponentially small, even when ω^{RE} decouples. This means that the decoding protocol with post-selection fails in most cases.

3.1.2 Construction of the generalized YK decoder

We now consider upgrading the decoding protocol with post-selection to a decoder without post-selection by the QSVT-based FPAA algorithm. Let us first outline how this could be achieved.

Compared to the standard situations of using AA-type algorithms, we need a more careful analysis since we can manipulate only a part of the system. To clarify this point, we denote by $|\omega_0\rangle^{REDD'E'R'}$ a purified state after the step 2, that is, we purify the state before the measurement in Fig. 3 by an environment E of the channel $\mathcal{F}$. We may divide this state into RE, which we have no access to, and $DD'E'R'$, which we can manipulate. This leads to the Schmidt decomposition:

$$|\omega_0\rangle^{REDD'E'R'} = \sum_\mu \sqrt{\lambda_\mu}|\eta_\mu\rangle^{RE}|\psi_\mu\rangle^{DD'E'R'}, \tag{39}$$

with Schmidt coefficients $\{\sqrt{\lambda_\mu}\}_\mu$, and orthonormal bases $\{|\eta_\mu\rangle^{RE}\}_\mu$ and $\{|\psi_\mu\rangle^{DD'E'R'}\}_\mu$ in RE and $DD'E'R'$, respectively. By applying an AA-type algorithm to $DD'E'R'$ of $|\omega_0\rangle^{REDD'E'R'}$, we aim to achieve the transformation:

$$|\psi_\mu\rangle^{DD'E'R'} \mapsto |\xi_\mu\rangle^{DD'E'R'}, \tag{40}$$

for each μ, where $\{|\xi_\mu\rangle^{DD'E'R'}\}_\mu$ is the Schmidt basis of the post-selected state after the measurement in the step 3. As it is post-selected by the MES $|\Phi\rangle\langle\Phi|^{DD'}$ and due to the symmetry of the state, we can show that

$$|\xi_\mu\rangle^{DD'E'R'} = |\Phi\rangle^{DD'}|\eta_\mu^*\rangle^{E'R'}, \tag{41}$$

where the complex conjugate acts on the coefficients when the state is expanded in the computational basis. Hence, if we can achieve the transformation given by Eq. (40) for all μ simultaneously while maintaining the superposition, the entire state is transformed as

$$|\omega_0\rangle^{REDD'E'R'} \mapsto |\Phi\rangle^{DD'} \sum_\mu \sqrt{\lambda_\mu}|\eta_\mu\rangle^{RE}|\eta_\mu^*\rangle^{E'R'}. \tag{42}$$

Assuming the decoupling between R and E, we can further show that this is close to $|\Phi\rangle^{DD'}|\tau\rangle^{EE'}|\Phi\rangle^{RR'}$. This statement is nontrivial, and we use the Powers–Størmer inequality [43, 44] to prove it. As a result, we obtain the MES $|\Phi\rangle^{RR'}$ between the reference R and the subsystem R' in the receiver's hands, completing the recovery of quantum information. See 4.1.2 for the details.

The remaining and crucial question is how we could simultaneously achieve the transformation in Eq. (40) for all μ. The standard AA fails to achieve this because the number of iterations of operations is sensitive to the exact value of $|\langle\xi_\mu|\psi_\mu\rangle|$ (see Eq. (23)), which differs for each μ in general. Thus, although we could achieve Eq. (40) for some μ, other states will be overcooked or undercooked, which ends up in a failure of achieving the transformation in Eq. (42). Note that this issue does not arise if all the inner products $|\langle\xi_\mu|\psi_\mu\rangle|$ are almost the same. This is the case for the HP protocol and is why the original decoding protocol [31] for the HP protocol works with the standard AA algorithm.

An issue still arises even if we use the original FPAA [39]. Although the overcook and undercook problems can be circumvented (see Eq. (24)), it eventually results in

$$|\Phi\rangle^{DD'} \sum_\mu e^{i\chi_\mu}\sqrt{\lambda_\mu}|\eta_\mu\rangle^{RE}|\eta_\mu^*\rangle^{E'R'}. \tag{43}$$

Again, this fails to achieve Eq. (42). This FPAA does not work since we need to operate on the state in a superposition, making the unknown phase χ_μ a relative one. The phase χ_μ generally depends on the overlap between the input and output states, $\langle\xi_\mu|\psi_\mu\rangle$, and computing it would not be straightforward. This concern was pointed out in [41] as a general remark.

For these reasons, the only AA-type algorithm that we can employ to achieve Eq. (42) is the one based on the QSVT, which in fact works well for our purpose (see Eq. (25)). We emphasize here that the reason why only the QSVT-based FPAA works is that, in the decoding task, we have access only to one part of the entangled systems. In this situation, the superposition makes the relative phases, that arise from other AA-type algorithms, harmful and results in the failure of decoding. Hence, our decoding protocol can be considered as a concrete and practical example that highlights the unique feature of the QSVT-based FPAA compared to other AA-type algorithms.

We now explain a concrete algorithm for constructing a decoder. Let $G_{t,\phi}$ be the unitary corresponding to the QSVT-based FPAA, where $t \in \mathbb{N}$ and $\phi = (\phi_1, \phi_2, \ldots, \phi_t) \in (-\pi, \pi]^t$ are the parameters of the algorithm. We replace the step 3 in the previous section with the application of the unitary $G_{t,\phi}$.

3'. The receiver prepares an auxiliary single-qubit state $|0\rangle^H$ in a system H, and then applies a unitary $G_{t,\phi}^{DD'E'R'H}$, with appropriate t and ϕ to approximate the sign function.

The details of the unitary $G_{t,\phi}$ will be explained later in this section.

This replacement allows us to obtain a decoder without post-selection, i.e., the generalized YK decoder. All together, the decoding CPTP map is given by

$$\begin{aligned}\mathcal{D}_{t,\phi}^{DB'\to R'}(\cdot) &\coloneqq \mathrm{Tr}_{DD'E'H}\big[G_{t,\phi}^{DD'E'R'H}\big(\mathcal{V}^{B'\to D'E'R'}(\cdot) \\ &\qquad \otimes |0\rangle\langle 0|^H\big)(G_{t,\phi}^{DD'E'R'H})^\dagger\big],\end{aligned} \tag{44}$$

where $\mathcal{V}^{B'\to D'E'R'}$ is defined in Eq. (35). See Fig. 4 as well.

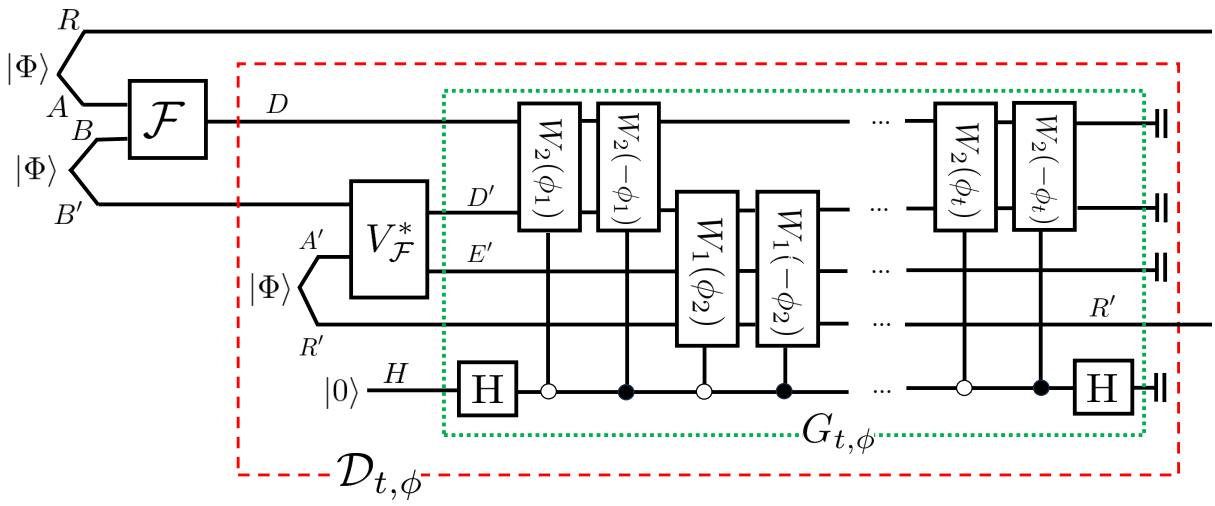


Figure 4: A diagram of the generalized YK decoder. Open circles imply that the gates are controlled by $|0\rangle$, while closed circles indicate the ones controlled by $|1\rangle$. The gate H is the single-qubit Hadamard gate. The red dashed and green dotted boxes correspond to the generalized YK decoder $\mathcal{D}_{t,\phi}$ defined in Eq. (44), and the unitary $G_{t,\phi}$ by the QSVT-based FPAA algorithm given in Eq. (53), respectively. The unitary $W_m(\theta)$ $(m = 1, 2)$ is defined in Eq. (51).

This construction of the generalized YK decoder is an extension of the original one for the HP protocol. However, it is not straightforward to analyze its decoding performance, as the original analysis is based on the specific details of the HP protocol and cannot be applied to any other noise. By developing a proof technique that relies on the symmetric structure of the generalized YK decoder, we prove the following theorem.

Theorem 4 (Performance of the generalized YK decoder)**.** *For a channel $\mathcal{F}^{AB\to D}$, let $\bar{\mathcal{F}}^{AB\to E}$ be its complementary channel, ω^{RE} be the state given by*

$$\omega^{RE} = \bar{\mathcal{F}}^{AB\to E}(\Phi^{AR} \otimes \pi^{B}), \tag{45}$$

and $\lambda_{\min}(\omega^{RE})$ be the non-zero minimum eigenvalue of ω^{RE}. Suppose that there exists a state τ^{E} such that $\|\omega^{RE} - \pi^{R} \otimes \tau^{E}\|_1 \leq \epsilon$. Then, for any $\delta \in (0, 1)$ and any odd integer t satisfying

$$t \geq \left\lceil 16e\sqrt{\frac{d_D}{d_B \lambda_{\min}(\omega^{RE})}} \log(2/\delta) \right\rceil, \tag{46}$$

there exist $\phi = (\phi_1, \phi_2, \ldots, \phi_t) \in (-\pi, \pi]^t$ such that the recovery error $\Delta(\mathcal{D}_{t,\phi}|\mathcal{F})$ of the generalized YK decoder $\mathcal{D}^{DB'\to R'}_{t,\phi}$ is given by

$$\Delta(\mathcal{D}_{t,\phi}|\mathcal{F}) \leq \sqrt{\epsilon} + \delta, \tag{47}$$

and the circuit complexity of $\mathcal{D}^{DB'\to R'}_{t,\phi}$ is

$$\mathcal{C}(\mathcal{D}_{t,\phi}) = \mathcal{O}\Big(t\big(\mathcal{C}(U_{\mathcal{F}}) + \log(d_D^2 d_E/d_B)\big)\Big), \tag{48}$$

and $\mathcal{O}\big(\log(d_D^2 d_E/d_B)\big)$ ancilla qubits suffice. Here, $\mathcal{C}(U_{\mathcal{F}})$ is circuit complexity of a unitary $U^L_{\mathcal{F}}$ such that $U^L_{\mathcal{F}}|0\rangle^F$ is a Stinespring isometry of $\mathcal{F}^{AB\to D}$, and $L = ABF = ED$.

Theorem 4 shows in Eq. (47) that the recovery error is dependent on ϵ and δ. While ϵ is an upper bound on the degree of decoupling and depends only on the channel $\mathcal{F}$, δ can be chosen arbitrarily small. One may hence think that the limit $\delta \to 0$ should be taken. This is true if the recovery error is the only concern. However, there is a trade-off relation between the recovery error and the circuit complexity, which is characterized by the parameter δ. In fact, Eqs. (46) and (48) show that the circuit complexity of the generalized YK decoder depends on δ, such as $\log(1/\delta)$. Hence, the complexity increases if one wishes to achieve small errors. This trade-off is naturally expected due to the implementation using quantum algorithms. Exponentially small δ is feasible since the dependence of the complexity on $1/\delta$ is only logarithmic.

Since $\mathcal{F}^{AB\to D} = \mathcal{N}^{C\to D} \circ \mathcal{E}^{AB\to C}$, Theorem 4 states that when the encoding map $\mathcal{E}$ is appropriately chosen against a given noise $\mathcal{N}$, or equivalently when the encoder $\mathcal{E}$ is chosen to satisfy the decoupling condition with small error, then the generalized YK decoder achieves a small error in recovering quantum information. In particular, consider the case where $\mathcal{N} = \mathcal{N}_1^{\otimes N}$ and $d_B = 1$. As explained in 2.3, if the achievable rate R is

below the quantum capacity $Q(\mathcal{N}_1)$, there exists a suitable encoder that satisfies the decoupling condition with ϵ vanishing in the limit of increasing number of channel uses. Hence, by setting δ in Theorem 4 to the value which vanishes in the limit, such as $1/d_A$, the generalized YK decoder can be used to achieve a rate arbitrarily close to the quantum capacity $Q(\mathcal{N}_1)$. This also applies to the entanglement-assisted setting with unlimited entanglement, while the achievable rate in this case approximates the entanglement-assisted quantum capacity $Q_{\mathrm{E}}(\mathcal{N}_1)$. Note that the generalized YK decoder remains explicit for any finite value of N.

In 3.3, we provide an in-depth comparison of the complexity with that of the algorithmic implementation of the Petz recovery map. We here mention that the number t is dominant unless $\mathcal{C}(U_{\mathcal{F}})$ is exponentially large. The number t arises from the QSVT-based FPAA algorithm and is known to be an optimal order [38, 39, 41]. Hence, the quantum circuit implementation of the generalized YK decoder cannot be significantly improved. Note that, while t is independent of the choice of the dilation of $\mathcal{F}^{AB\to D}$, the whole complexity is dependent on the choice due to the factor $\mathcal{C}(U_{\mathcal{F}}) + \log(d_D^2 d_E/d_B)$ in Eq. (48). Hence, using the unitary $U_{\mathcal{F}}^L$ which minimizes $\mathcal{C}(U_{\mathcal{F}}) + \log(d_D^2 d_E/d_B)$ results in the smallest complexity.

Another factor to be noted in the complexity is $\sqrt{d_D/d_B}$ in Eq. (46), where d_D is the dimension of the output of the noisy channel $\mathcal{N}^{C\to D}$ and d_B is that of the pre-shared entanglement. In the simplest case, where the encoding map is given by a unitary on AB that is set to the same size as the input system C of the noisy channel $\mathcal{N}^{C\to D}$, we have $\sqrt{d_D/d_B} = \sqrt{d_A d_D/d_C}$. In this case, the complexity depends on d_A and the ratio d_D/d_C between the dimensions of the input C and the output D of the noisy channel. If the encoding is non-unitary, this is not the case, and one may expect that the complexity could be decreased by increasing d_B. This might be done by, e.g., fictitiously adding more entanglement at the outset, and by discarding it in the encoding process. This trick, however, does not affect the total complexity due to the other factor $[\lambda_{\min}(\omega^{RE})]^{-1/2}$. As $|\omega\rangle^{REDB'}$ is pure, $\lambda_{\min}(\omega^{RE}) = \lambda_{\min}(\omega^{DB'})$, where $\lambda_{\min}(\omega^{DB'})$ is non-zero minimum eigenvalue of $\omega^{DB'}$. This implies that, even if we fictitiously add extra entanglement of dimension d_{extra} for increasing d_B, the value of $\lambda_{\min}(\omega^{DB'})$ changes by factor $1/d_{\mathrm{extra}}$, which cancels the increase of d_B in the complexity.

Before we move on, we explain the construction of the QSVT-based FPAA unitary $G_{t,\phi}^{DD'E'R'H}$ (see also 2.7). To this end, we introduce two projectors:

$$\Pi_1^{D'E'R'} := (V_{\mathcal{F}}^{A'B'\to E'D'})^* (\mathbb{I}^{B'} \otimes |\Phi\rangle\langle\Phi|^{A'R'})(V_{\mathcal{F}}^{A'B'\to E'D'})^{\mathsf{T}}, \quad (49)$$

$$\Pi_2^{DD'} := |\Phi\rangle\langle\Phi|^{DD'}, \quad (50)$$

and unitaries:

$$W_m(\theta) := e^{i\theta(2\Pi_m - \mathbb{I})}, \quad (51)$$

where $m = 1, 2$ and $\theta \in (-\pi, \pi]$. Let $W_{t,\phi}^{DD'E'R'}$ be a unitary given by

$$W_{t,\phi}^{DD'E'R'} := W_2(\phi_t)^{DD'} \prod_{j=1}^{(t-1)/2} \Big[W_1(\phi_{2j})^{D'E'R'} W_2(\phi_{2j-1})^{DD'} \Big]. \quad (52)$$

The unitary $G_{t,\phi}^{DD'E'R'H}$ is then defined by

$$G_{t,\phi}^{DD'E'R'H} := W_{t,\phi}^{DD'E'R'} \otimes |+\rangle\langle+|^H + W_{t,-\phi}^{DD'E'R'} \otimes |-\rangle\langle-|^H, \quad (53)$$

where H is a single-qubit auxiliary system. The unitary $G_{t,\phi}^{DD'E'R'H}$ has the block matrix representation as

$$G_{t,\phi}^{DD'E'R'H} = \begin{pmatrix} Q_{t,\phi}(\Pi_2^{DD'}\Pi_1^{D'E'R'}) \otimes |0\rangle\langle 0|^H & \cdot \\ \cdot & \cdot \end{pmatrix}, \quad (54)$$

where $Q_{t,\phi}$ is a polynomial determined by degree t and the phase sequence $\phi = (\phi_1, \ldots, \phi_t)$. When we choose an appropriate t and ϕ, the polynomial $Q_{t,\phi}$ well approximates the sign function, by which we can realize the QSVT-based FPAA. More detailed analysis for its circuit complexity is explained in 4.1.2.

3.2 Petz-like decoder

Using a similar technique, we can construct the Petz-like decoder, which is a simplification of the

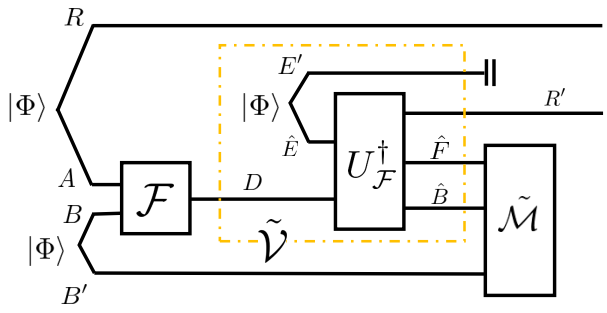


Figure 5: A diagram of the protocol with post-selection for the Petz-like decoder. The dash-dotted box represents the isometry map $\tilde{\mathcal{V}}$ in Eq. (55).

Petz recovery map. We first introduce a decoding protocol with post-selection in 3.2.1. Combining it with the QSVT-based FPAA algorithm, we explicitly construct the Petz-like decoder in 3.2.2 [3].

3.2.1 Decoding protocol with post-selection

The decoding protocol with post-selection is as follows. See also Fig. 5. Similarly to the generalized YK decoder, we denote a Stinespring isometry of $\mathcal{F}^{AB\to D}$ by $U_{\mathcal{F}}^{L}|0\rangle^{F}$ as given in Eqs. (19) and (20). Note that the protocol works for any choice of $U_{\mathcal{F}}$.

1. The receiver prepares ancilla qubits in the system $\hat{E}E'$, and then generates a MES $\Phi^{\hat{E}E'}$.
2. The receiver applies the unitary $(U_{\mathcal{F}}^{\hat{L}})^{\dagger}$, where $\hat{L} = R'\hat{F}\hat{B} = \hat{E}D$.
3. The receiver performs a binary measurement $\tilde{\mathcal{M}} := \{|0\rangle\langle 0|^{\hat{F}} \otimes |\Phi\rangle\langle\Phi|^{\hat{B}B'}, \mathbb{I}^{\hat{F}\hat{B}B'} - |0\rangle\langle 0|^{\hat{F}} \otimes |\Phi\rangle\langle\Phi|^{\hat{B}B'}\}$ on $\hat{F}\hat{B}B'$. When the former result of the measurement $\tilde{\mathcal{M}}$ is obtained, this protocol succeeds.

In this protocol, all the systems with a prime or a hat, and the channel output D, are in the hands of the receiver. Below, we denote by $\tilde{\mathcal{V}}^{D\to E'R'\hat{F}\hat{B}}$ an isometry map of the operation up to the step 2; that is,

$$\tilde{\mathcal{V}}^{D\to E'R'\hat{F}\hat{B}}(\cdot) := (U_{\mathcal{F}}^{\hat{L}})^{\dagger}(\cdot \otimes \Phi^{\hat{E}E'})U_{\mathcal{F}}^{\hat{L}}. \tag{55}$$

[3] While we assume that the state on BB' is the MES $|\Phi\rangle^{BB'}$, the Petz-like decoder works even for an arbitrary state $|\rho\rangle^{BB'}$ (one example: the thermofield double state). In such cases, replacing every $|\Phi\rangle^{BB'}$ which appears in this section with $|\rho\rangle^{BB'}$ should suffice.

Conditioned by the success of the measurement $\tilde{\mathcal{M}}$, the reduced state on the system RR' is given by

$$\tilde{\zeta}_{\mathrm{succ}}^{RR'} = \mathrm{Tr}_{E'\hat{E}\hat{B}B'}\Big[\frac{1}{\tilde{p}_{\mathrm{succ}}}(|0\rangle\langle 0|^{\hat{F}} \otimes |\Phi\rangle\langle\Phi|^{\hat{B}B'}) \tilde{\mathcal{V}}^{D\to E'R'\hat{F}\hat{B}}(\omega^{RDB'})\Big], \tag{56}$$

where $\tilde{p}_{\mathrm{succ}}$ is the success probability of $\tilde{\mathcal{M}}$, and $\omega^{RDB'} = \mathcal{F}^{AB\to D}(\Phi^{AR} \otimes \Phi^{BB'})$. It is straightforward to show that

$$\tilde{p}_{\mathrm{succ}} = \frac{d_A}{d_E} 2^{-H_2(RE)_\omega}, \tag{57}$$

$$\mathrm{F}(\tilde{\zeta}_{\mathrm{succ}}^{RR'}, \Phi^{RR'}) = \frac{1}{d_A} 2^{H_2(RE)_\omega - H_2(E)_\omega}. \tag{58}$$

See 4.2 for the details.

As mentioned before, $U_{\mathcal{F}}^{L}$ is not uniquely determined from $\mathcal{F}^{AB\to D}$. Although this decoding protocol works for any choice of $U_{\mathcal{F}}$, the decoding performance depends on the choice, which is unlike the generalized YK decoder. In fact, the success probability $\tilde{p}_{\mathrm{succ}}$ is inverse-proportional to d_E, which implies that it succeeds with higher probability if a smaller environment of the channel $\mathcal{F}^{AB\to D}$ is chosen. Even though decoupling is satisfied, the probability $\tilde{p}_{\mathrm{succ}}$ is exponentially small. On the other hand, the fidelity is the same as that of the generalized YK decoder. It is independent of the choice of $U_{\mathcal{F}}$, and we have $\mathrm{F}(\tilde{\zeta}_{\mathrm{succ}}^{RR'}, \Phi^{RR'}) \approx 1$ when the decoupling is satisfied as $\omega^{RE} \approx \pi^{R} \otimes \omega^{E}$.

3.2.2 Construction of the Petz-like decoder

We now use the QSVT-based FPAA algorithm to amplify the success probability of the measurement $\tilde{\mathcal{M}}$. For the same reasons as the generalized YK decoder, the amplification cannot be achieved with other known AA-type algorithms.

To describe the unitary $\tilde{G}_{t,\phi}$ corresponding to the QSVT-FPAA, let us define two projectors as

$$\tilde{\Pi}_1^{E'R'\hat{F}\hat{B}} := (U_{\mathcal{F}}^{\hat{L}})^{\dagger}(|\Phi\rangle\langle\Phi|^{\hat{E}E'} \otimes \mathbb{I}^{D})U_{\mathcal{F}}^{\hat{L}}, \tag{59}$$

$$\tilde{\Pi}_2^{\hat{F}\hat{B}B'} := |0\rangle\langle 0|^{\hat{F}} \otimes |\Phi\rangle\langle\Phi|^{\hat{B}B'}. \tag{60}$$

By replacing Π_m with $\tilde{\Pi}_m$ in the definition of $W_m(\theta)$ $(m = 1, 2)$ in Eq. (51) and the following the constructions by Eqs. (52) and (53), we define the unitary $\tilde{G}_{t,\phi}^{E'R'\hat{F}\hat{B}B'H}$.

The Petz-like decoder $\tilde{\mathcal{D}}_{t,\phi}^{DB'\to R'}$ is given by replacing the step 3 with the following. See Fig. 6 as well.

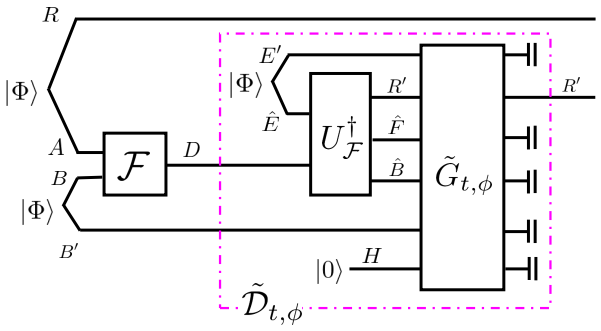


Figure 6: A diagram of the Petz-like decoder $\tilde{\mathcal{D}}_{t,\phi}$, which is given in Eq. (61), corresponds to the dash-dotted box. Note that $\tilde{G}_{t,\phi}$ consists of repeated applications of unitaries, which is similar to Fig. 4.

3'. The receiver prepares an auxiliary state $|0\rangle^H$ in the system H and applies the unitary $\tilde{G}_{t,\phi}^{E'R'\hat{F}\hat{B}B'H}$.

With this modification, the Petz-like decoder is explicitly given by

$$\begin{aligned}&\tilde{\mathcal{D}}_{t,\phi}^{DB'\to R'}(\cdot)\\ &:= \mathrm{Tr}_{E'\hat{F}\hat{B}B'H}\big[\tilde{G}_{t,\phi}^{E'R'\hat{F}\hat{B}B'H}\big(\tilde{\mathcal{V}}^{D\to E'R'\hat{F}\hat{B}}(\cdot)\\ &\qquad\otimes|0\rangle\langle 0|^H\big)\big(\tilde{G}_{t,\phi}^{E'R'\hat{F}\hat{B}B'H}\big)^\dagger\big]. \quad (61)\end{aligned}$$

The number $t\in\mathbb{N}$ and the phases $\phi\in(-\pi,\pi]^t$ are chosen such that the QSVT realizes an approximation of the sign function.

The following theorem provides the performance of the Petz-like decoder.

Theorem 5 (Performance of the Petz-like decoder)**.** *For a given channel $\mathcal{F}^{AB\to D}$, let $\bar{\mathcal{F}}^{AB\to E}$ be its complementary channel, ω^{RE} be the state given by*

$$\omega^{RE}=\bar{\mathcal{F}}^{AB\to E}(\Phi^{AR}\otimes\pi^B), \quad (62)$$

and $\lambda_{\min}(\omega^{RE})$ be the non-zero minimum eigenvalue of ω^{RE}. Suppose that there exists a state τ^E such that $\|\omega^{RE}-\pi^R\otimes\tau^E\|_1\le\epsilon$. Then, for any $\delta\in(0,1)$, and any odd integer t satisfying

$$t\ge\left\lceil 16e\sqrt{\frac{d_E}{d_A\lambda_{\min}(\omega^{RE})}}\log(2/\delta)\right\rceil, \quad (63)$$

there exist $\phi=(\phi_1,\phi_2,\ldots,\phi_t)\in(-\pi,\pi]^t$ such that the recovery error $\Delta(\tilde{\mathcal{D}}_{t,\phi}|\mathcal{F})$ of the Petz-like decoder $\tilde{\mathcal{D}}_{t,\phi}^{DB'\to R'}$ is given by

$$\Delta(\tilde{\mathcal{D}}_{t,\phi}|\mathcal{F})\le\sqrt{\epsilon}+\delta, \quad (64)$$

and the circuit complexity of $\tilde{\mathcal{D}}_{t,\phi}^{DB'\to R'}$ is

$$\mathcal{C}(\tilde{\mathcal{D}}_{t,\phi})=\mathcal{O}\Big(t\big(\mathcal{C}(U_{\mathcal{F}})+\log(d_Dd_E^2/d_A)\big)\Big), \quad (65)$$

and $\mathcal{O}\big(\log(d_Dd_E^2/d_A)\big)$ ancilla qubits suffice. Here, $\mathcal{C}(U_{\mathcal{F}})$ is circuit complexity of a unitary $U_{\mathcal{F}}^L$ such that $U_{\mathcal{F}}^L|0\rangle^F$ is the Stinespring isometry of $\mathcal{F}^{AB\to D}$, and $L=ABF=ED$.

Theorem 5 has many similarities to Theorem 4 about the generalized YK decoder, such as that the recovery error depends on the degree ϵ of decoupling as well as the parameter δ that characterizes the trade-off relation between the recovery error and the circuit complexity of the decoder. From the upper bound on the recovery error in Eq. (64), we observe that, with a suitable encoder and δ, the Petz-like decoder can also be used to achieve a rate arbitrarily close to the quantum capacity by increasing the number of channel uses, in the entanglement-non-assisted setting. In the entanglement-assisted setting with unlimited entanglement, it achieves a rate arbitrarily close to the entanglement-assisted quantum capacity.

On the other hand, the complexity of the Petz-like decoder differs from that of the generalized YK decoder. The number t, as well as the remaining part in $\mathcal{C}(\tilde{\mathcal{D}}_{t,\phi})$, explicitly depends on d_E. This implies that the complexity depends on the choice of the dilation of $\mathcal{F}^{AB\to D}$, which reflects the aforementioned fact that the success probability of the protocol with post-selection is dependent on d_E. Hence, it is desirable to use a dilated unitary $U_{\mathcal{F}}^L$ with a small environment E. In the next section, we compare in detail the complexities of decoders and clarify in what cases one decoder has smaller complexity than the other.

As we will explain in the next section, the Petz-like decoder has a smaller circuit complexity than the algorithmic implementation of the original Petz recovery map [28], when δ is appropriately chosen. This is for two reasons. First, the Petz-like decoder is not exactly the same as the Petz recovery map. Although the Petz recovery map is known to be a good decoder, it is not necessary to implement the full map if one is interested in using the map as a decoder. This is one of the implications of our results. Second, the algorithmic implementation of the Petz recovery map [28] relies on the direct use of the QSVT to implement three CP maps that compose the Petz recovery map, which leads to high complexity. Due to

Table 1: A table of notation that we use in 3.3. We use the numbers of qubits in the systems.

k	The number of logical qubits in A: $k = \log d_A$.
n_{in}	The number of input qubits of the channel $\mathcal{N}$: $n_{\text{in}} = \log d_C$.
n_{out}	The number of output qubits of the channel $\mathcal{N}$: $n_{\text{out}} = \log d_D$.
b	The number of ebits shared by the sender and the receiver in advance: $b = \log d_B$.
κ	The number of qubits in the environment E, which is equal to the logarithm of #Kraus ops.: $\kappa = \log d_E = \log(\#\text{Kraus ops.})$.

the aforementioned simplification, we can cleverly use the QSVT-based FPAA instead of such direct uses of the QSVT, resulting in smaller computational cost.

3.3 Comparison of the circuit complexities

We compare the circuit complexities of the generalized YK decoder, the Petz-like decoder, and the algorithmic implementation of the original Petz recovery map [28]. We derive a simple criterion that ensures the generalized YK decoder has smaller complexity compared to the Petz-like decoder. We also demonstrate that the Petz-like decoder has substantially smaller complexity than the algorithmic implementation of the original Petz recovery map [28].

In the comparison, we sometimes use the number of qubits in each system instead of the dimensions. We denote the number of qubits in A, B, C, D, and E by k, b, n_{in}, n_{out}, and κ, respectively. See Table 1. Note that κ is the logarithm of the number of the Kraus operators of the channel $\mathcal{F}^{AB\to D}$, i.e., $\kappa = \log d_E = \log(\#\text{Kraus ops.})$. While this number depends on how the channel is dilated, we take the minimum possible number of Kraus operators in the comparison below, as we are interested in minimizing the complexity.

We first compare the complexity of the generalized YK decoder with that of the Petz-like decoder. As explained in 3.1.2, the number t is the significant factor in the complexity. We denote the numbers t for the generalized YK decoder and for the Petz-like decoder by t_{gYK} and t_{Pl}, respectively. That is,

$$t_{\text{gYK}} = \Theta\Big(\big[2^{b-n_{\text{out}}}\lambda_{\min}(\omega^{RE})\big]^{-1/2}\log(1/\delta)\Big), \tag{66}$$

$$t_{\text{Pl}} = \Theta\Big(\big[2^{k-\kappa}\lambda_{\min}(\omega^{RE})\big]^{-1/2}\log(1/\delta)\Big). \tag{67}$$

See Eq. (46) and Eq. (63). Comparing t_{gYK} and t_{Pl}, we find that

$$t_{\text{gYK}} \le t_{\text{Pl}} \iff k - b \le \kappa - n_{\text{out}}. \tag{68}$$

The left-hand side of the right condition in Eq. (68) is given by the number of logical qubits k that the sender intends to transmit and the number of pre-shared ebits b. On the other hand, the right-hand side depends on the quantities κ and n_{out} that are the properties of the channel $\mathcal{F}^{AB\to D}$. To better understand the condition in Eq. (68), we consider a couple of concrete instances below, assuming an isometric encoder for simplicity. In these cases, κ corresponds to the logarithm of the number of Kraus operators of the noisy channel $\mathcal{N}^{C\to D}$.

For a given noisy channel $\mathcal{N}^{C\to D}$, the right-hand side of Eq. (68) represents a property of the noise. Hence, the number of logical qubits k and that of pre-shared entanglement b determine which decoder has smaller complexity. In general, the generalized YK decoder has an advantage when b is large, and as b becomes smaller, the advantage shifts to the Petz-like decoder. To observe this more concretely, we note that $0 \le b \le n_{\text{in}} - k$. When the sender and the receiver pre-share the maximal amount of entanglement, i.e., $b = n_{\text{in}} - k$, Eq. (68) is rephrased as $k \le \frac{1}{2}(n_{\text{in}} - n_{\text{out}} + \kappa)$. In particular, if the input and the output systems of the channel $\mathcal{N}^{C\to D}$ are

identical, i.e., $n_{\rm in} = n_{\rm out}$, it reduces to

$$t_{\rm gYK} \leq t_{\rm Pl} \iff k \leq \frac{1}{2}\kappa. \tag{69}$$

Hence, the generalized YK decoder has smaller complexity than the Petz-like decoder unless the number of logical qubits exceeds half of the logarithm of the number of Kraus operators of the noisy channel.

In contrast, when no entanglement is shared in advance: $b = 0$, Eq. (68) reduces to

$$t_{\rm gYK} \leq t_{\rm Pl} \iff k \leq \kappa - n_{\rm out}. \tag{70}$$

Whether the right-hand side holds or not depends on the details of the noise. For instance, the amplitude damping on each qubit violates the inequality on the right-hand side. For such noises or the choice of large k, the Petz-like decoder has smaller complexity than the generalized YK decoder.

We may also use the fact that k should necessarily satisfy $k \leq n_{\rm in}$ for the recovery to be possible. This leads to a trivial inequality $k+n_{\rm out}-\kappa \leq n_{\rm in} + n_{\rm out} - \kappa$. Furthermore, κ always satisfies $\kappa \leq n_{\rm in}+n_{\rm out}$, since κ is the logarithm of the number of Kraus operators. If a given noisy channel $\mathcal{N}$ has the property that $\kappa = n_{\rm in}+n_{\rm out}$, it follows that

$$k + n_{\rm out} - \kappa \leq 0 \leq b, \tag{71}$$

for any b. Hence, for the noise with the maximum possible number of Kraus operators, the generalized YK decoder has smaller complexity than the Petz-like decoder no matter how much entanglement is pre-shared.

We next compare the complexity of the Petz-like decoder with an algorithmic implementation of the original Petz recovery map provided in [28]. The following corollary can be derived by applying the algorithmic implementation to the Petz recovery map in our setting. In this corollary, $\|\cdot\|_\diamond$ denotes the diamond norm [50, 82, 83].

Corollary 6 (Algorithmic implementation of the Petz recovery map [28])**.** *Let $\mathcal{P}_{\pi,\mathcal{G}}^{DB'\to R'}$ be the decoder based on the Petz recovery map defined in Eq. (21). Then, there exists a quantum algorithm realizing the map $\tilde{\mathcal{P}}_{\pi,\mathcal{G}}^{DB'\to R'}$, which satisfies*

$$\|\tilde{\mathcal{P}}_{\pi,\mathcal{G}}^{DB'\to R'} - \mathcal{P}_{\pi,\mathcal{G}}^{DB'\to R'}\|_\diamond \leq \varepsilon, \tag{72}$$

with circuit complexity

$$\begin{aligned}&\mathcal{C}(\tilde{\mathcal{P}}_{\pi,\mathcal{G}})\\ &= \mathcal{O}\Big(t_{\rm Petz}\Big(\mathcal{C}(U_{\mathcal{F}}) + \log(d_B d_E) + \frac{\mathcal{C}(U_\omega)}{\lambda_{\min}(\omega^{RE})}\\ &\qquad \log\big(\frac{d_E}{\varepsilon}\big) + d_A \log(d_A) \log\big(\frac{d_E}{\varepsilon\lambda_{\min}(\omega^{RE})}\big)\Big)\Big),\end{aligned} \tag{73}$$

where $t_{\rm Petz}$ is given by

$$t_{\rm Petz} = \left\lfloor \pi\sqrt{\frac{d_E}{\lambda_{\min}(\omega^{RE})}} \right\rfloor, \tag{74}$$

and $\mathcal{C}(U_\omega)$ is circuit complexity of a unitary $U_\omega^{DB'P}$ such that, for any system P,

$$\omega^{DB'} = {\rm Tr}_P[U_\omega^{DB'P}|0\rangle\langle 0|^{DB'P}(U_\omega^{DB'P})^\dagger]. \tag{75}$$

From Eqs. (22) and (72), the recovery error of $\tilde{\mathcal{P}}_{\pi,\mathcal{G}}$ is bounded as

$$\Delta(\tilde{\mathcal{P}}_{\pi,\mathcal{G}}|\mathcal{F}) \leq 2\epsilon^{1/4} + \varepsilon, \tag{76}$$

when there exists τ^E such that $\|\omega^{RE} - \pi^R \otimes \tau^E\|_1 \leq \epsilon$.

We clarify the condition that the Petz-like decoder has smaller complexity than the algorithmic implementation of the Petz recovery map. First, when $\mathcal{C}(U_{\mathcal{F}})$ is larger than the other terms, Eqs. (65) and (73) approximately reduce to

$$\mathcal{C}(\tilde{\mathcal{D}}_{t,\phi}) \approx \mathcal{O}(t_{\rm Pl}\mathcal{C}(U_{\mathcal{F}})), \tag{77}$$

$$\mathcal{C}(\tilde{\mathcal{P}}_{\pi,\mathcal{G}}) \approx \mathcal{O}(t_{\rm Petz}\mathcal{C}(U_{\mathcal{F}})), \tag{78}$$

respectively. In this case, we only need to compare $t_{\rm Pl}$ with $t_{\rm Petz}$, which satisfies $t_{\rm Pl} = \Theta(\frac{\log(1/\delta)}{\sqrt{d_A}} t_{\rm Petz})$. Hence, as far as $\delta = \Omega(2^{-\sqrt{d_A}})$, the Petz-like decoder has smaller complexity than the algorithmic implementation of the original Petz recovery map. For instance, by taking $\delta = 1/d_A$, the Petz-like decoder achieves a reduced circuit complexity by a leading factor of $\sqrt{d_A} = 2^{k/2}$, implying that the exponent of the exponential scaling in the circuit complexity changes to a smaller one.

The advantage of the Petz-like decoder remains even when $\mathcal{C}(U_{\mathcal{F}})$ is not dominant. To see this, suppose that ε in Eq. (73) is $\varepsilon = \mathcal{O}(\delta)$ with sufficiently small δ. The complexity of the algorithmic implementation of the Petz recovery map reduces

Table 2: The circuit complexity of our decoders in particular noise models. We denote $\min_i p_i$ by $p_{\min}$. The constant γ is assumed to be $1/2$ or less. We have assumed a unitary encoding by a polynomial-sized quantum circuit, so $k+b = n_{\rm in}$. We have also assumed the decoupling condition $\omega^{RE} \approx \pi^R \otimes \omega^E$, which leads to $\lambda_{\min}(\omega^{RE}) \approx \lambda_{\min}(\omega^E)/d_A$ with $\lambda_{\min}(\omega^E)$ being the non-zero minimum eigenvalue of $\omega^E = \bar{\mathcal{N}}^{C\to E}(\pi^C)$. The part $\mathrm{poly}(\cdot)$ comes from the term associated with the dilated unitary of the noise, and from the term logarithmic in dimensions in Eqs. (48) and (65).

	Generalized YK decoder $\mathcal{C}(\mathcal{D}_{t,\phi})$	Petz-like decoder $\mathcal{C}(\tilde{\mathcal{D}}_{t,\phi})$
Pauli noise	$[(2^k/p_{\min}^{n/2})\log(1/\delta)]\mathrm{poly}(n,k)$	$[(2/p_{\min}^{1/2})^n \log(1/\delta)]\mathrm{poly}(n,k)$
Amplitude damping noise	$[2^k(2/\gamma)^{n/2}\log(1/\delta)]\mathrm{poly}(n,k)$	$[(4/\gamma)^{n/2}\log(1/\delta)]\mathrm{poly}(n,k)$
Erasure noise	$[2^k \log(1/\delta)]\mathrm{poly}(n_{\rm in}, n_{\rm out}, k)$	$[2^{n_{\rm in}-n_{\rm out}}\log(1/\delta)]\mathrm{poly}(n_{\rm in}, n_{\rm out}, k)$

to

$$\mathcal{C}(\tilde{\mathcal{P}}_{\pi,\mathcal{G}}) \approx \mathcal{O}\Big(t_{\rm Petz}\log(1/\delta)\mathrm{poly}(n_{\rm in}, n_{\rm out}, k) \Big(\frac{1}{\lambda_{\min}(\omega^{RE})} + 2^k\Big)\Big) \tag{79}$$

$$= \mathcal{O}\Big(t_{\rm Pl}\mathrm{poly}(n_{\rm in}, n_{\rm out}, k) 2^{k/2}\Big(\frac{1}{\lambda_{\min}(\omega^{RE})} + 2^k\Big)\Big). \tag{80}$$

Here, we used in the second equation that $t_{\rm Pl} = \Theta(\frac{\log(1/\delta)}{\sqrt{d_A}} t_{\rm Petz})$ and assumed that $\mathcal{C}(U_{\mathcal{F}}^L)$ is polynomial in qubits, which further implies that $\mathcal{C}(U_\omega^{DB'P})$ is polynomial. On the other hand, the complexity of the Petz-like decoder in this case is

$$\mathcal{C}(\tilde{\mathcal{D}}_{t,\phi}) = \mathcal{O}(t_{\rm Pl}\mathrm{poly}(n_{\rm in}, n_{\rm out}, k)). \tag{81}$$

Since this corresponds to the first line of Eq. (80), the Petz-like decoder has smaller circuit complexity than the algorithmic implementation of the Petz recovery map. As the second line of Eq. (80) is at least an order of $2^{k/2}$, a significant reduction in the circuit complexity is achieved in this case as well.

From these comparisons of explicit quantum circuit implementations, we conclude that, for isometry encoding and noisy channels with the maximum number of Kraus operators, the circuit complexity increases in the following order: the generalized YK decoder, the Petz-like decoder, and the algorithmic implementation of the Petz recovery map. For channels with fewer Kraus operators, the Petz-like decoder may have smaller complexity than the generalized YK decoder, depending on more specific noise properties. However, both decoders have smaller complexity than the algorithmic implementation of the Petz recovery map.

Note that, although all the complexities are exponential in the number of qubits, this must be the case as it is in general computationally hard to decode quantum information [45–47].

3.4 Application to concrete noisy models

We consider several noises for demonstration. We investigate the noises that independently act on each qubit, such as the independent Pauli noise, the independent amplitude damping noise, and the qubit-erasure noise. If the input system C of the noisy channel $\mathcal{N}^{C\to D}$ is equal to the output system D of it, we denote by S the system as $S = C = D$, and by n the number of these qubits as $n = n_{\rm in} = n_{\rm out}$.

In Table 2, we summarize the circuit complexities of our decoders. From these results, we find that the complexities become smaller in more noisy situations, such as for large $p_{\min} = \min_{i=0,1,2,3} p_i$ in the Pauli noise or large γ in the amplitude damping noise.

- Independent Pauli noise

The first example is the independent Pauli noise. A Stinespring isometry of the single-qubit Pauli noise is given by

$$V_{\mathcal{N}}^{S\to ES} = \sum_{i=0}^{3} \sqrt{p_i}|e_i\rangle^E \otimes \sigma_i^S, \tag{82}$$

where $\sum_{i=0}^3 p_i = 1$ and $(\sigma_i^S) = (\mathbb{I}^S, X^S, Y^S, Z^S)$. Since the number of qubits of the system S is n, and the logarithm of the number of the Kraus

operators $\kappa = 2n$, we can rephrase Eq. (68) as

$$n - k + b \geq 0 \iff t_{\mathrm{gYK}} \leq t_{\mathrm{Pl}}. \tag{83}$$

Since $k \leq n - b$ is always satisfied, the generalized YK decoder has smaller complexity than the Petz-like decoder for the independent Pauli noise.

- Independent amplitude damping noise

The second example is the amplitude damping noise for $\{|0\rangle^S, |1\rangle^S\}$, which independently acts on each qubit. The single-qubit amplitude damping noise is represented by an isometry

$$\begin{aligned} V_{\mathcal{N}}^{S\to ES} = \sqrt{\gamma}|e_0\rangle^E \otimes |0\rangle\langle 1|^S \\ + |e_1\rangle^E \otimes (|0\rangle\langle 0|^S + \sqrt{1-\gamma}|1\rangle\langle 1|^S), \end{aligned} \tag{84}$$

where $\gamma \in [0, 1]$. As $n = \kappa$, Eq. (68) becomes

$$b - k \geq 0 \iff t_{\mathrm{gYK}} \leq t_{\mathrm{Pl}}. \tag{85}$$

Hence, when the number of pre-shared entanglement b is more than the number of the logical qubits k, the generalized YK decoder has smaller complexity than the Petz-like decoder.

- Qubit-erasure noise

The third example is the qubit-erasure noise, which erases κ qubits out of n_{in} input qubits. The erased qubits are randomly chosen, but it is assumed that the receiver knows which qubits were erased. In this case, it holds that $n_{\mathrm{in}} = n_{\mathrm{out}} + \kappa$. Thus, Eq. (68) becomes

$$n_{\mathrm{in}} - 2n_{\mathrm{out}} - k + b \geq 0 \iff t_{\mathrm{gYK}} \leq t_{\mathrm{Pl}}. \tag{86}$$

Especially, when there is no pre-shared entanglement, $b = 0$, and the communication rate k/n_{in} is given by $k/n_{\mathrm{in}} = n_{\mathrm{out}}/n_{\mathrm{in}} - 1/2$, which is approximately half of the quantum capacity, Eq. (86) does not hold, and the Petz-like decoder has smaller complexity than the generalized YK decoder. On the other hand, when the maximal amount of entanglement is pre-shared, i.e., $b = n_{\mathrm{in}} - k$, Eq. (86) is rephrased as $k \leq n_{\mathrm{in}} - n_{\mathrm{out}} = \kappa$. Hence, if more than k qubits are erased by the noise, the generalized YK decoder has smaller complexity than the Petz-like decoder.

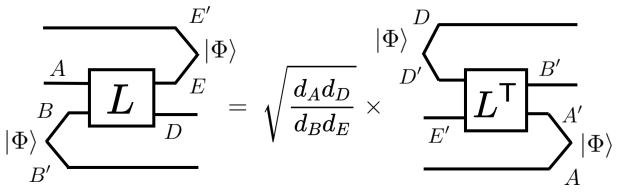


Figure 7: A diagram of the transpose of a matrix L sandwiched by two MESs

4 Proofs

In this section, we provide proofs of the main results. In 4.1 and 4.2, we show the statements about the generalized YK decoder and the Petz-like decoder, respectively.

4.1 Proofs: the generalized YK decoder

We first consider the decoding protocol with post-selection, and provide the success probability and the fidelity after the post-selection. We then prove Theorem 4.

4.1.1 Success probability and fidelity in the decoding protocol with post-selection

Before proving Theorem 4, we first derive Eqs. (37) and (38) here. To this end, we introduce an important lemma, which will be used frequently in what follows. Its proof is straightforward by direct calculation. See Fig. 7 for the diagram of the statement.

Lemma 7 (Transpose of a matrix sandwiched by two MESs)**.** *For any linear operator $L^{AB\to ED}$, i.e., $d_E d_D \times d_A d_B$ matrix, it holds that*

$$\begin{aligned} &\langle\Phi|^{EE'}(\mathbb{I}^{B'E'} \otimes L^{AB\to ED})|\Phi\rangle^{BB'} \\ &= \sqrt{\frac{d_A d_D}{d_B d_E}}\langle\Phi|^{AA'}((L^{A'B'\to E'D'})^{\mathsf{T}} \otimes \mathbb{I}^{AD})|\Phi\rangle^{DD'}. \end{aligned} \tag{87}$$

This is a linear operator from AE' to $B'D$. The transpose is taken with respect to the basis that defines each MES.

We consider our decoding protocol with post-selection. The input state of the decoding protocol is given by

$$\omega^{RDB'} = \mathcal{F}^{AB\to D}(\Phi^{AR} \otimes \Phi^{BB'}). \tag{88}$$

By including the environment E, its purified state is

$$|\omega\rangle^{REDB'} = V_{\mathcal{F}}^{AB\to ED}|\Phi\rangle^{AR}|\Phi\rangle^{BB'}. \tag{89}$$

Using Lemma 7 for $L = V_{\mathcal{F}}^*$, the state $\zeta_{\rm succ}^{RR'}$ on the system RR' after the post-selection is rewritten as

$$\zeta_{\rm succ}^{RR'} = \frac{1}{p_{\rm succ}} \mathrm{Tr}_{E'} \left[\langle \Phi |^{DD'} (V_{\mathcal{F}}^{A'B' \to E'D'})^* (\omega^{RDB'} \otimes \Phi^{A'R'}) (V_{\mathcal{F}}^{A'B' \to E'D'})^{\mathsf{T}} |\Phi\rangle^{DD'} \right] \tag{90}$$

$$= \frac{1}{p_{\rm succ}} \mathrm{Tr}_{E'} \left[\langle \Phi |^{DD'} (V_{\mathcal{F}}^{A'B' \to E'D'})^* |\Phi\rangle^{A'R'} \omega^{RDB'} \langle \Phi |^{A'R'} (V_{\mathcal{F}}^{A'B' \to E'D'})^{\mathsf{T}} |\Phi\rangle^{DD'} \right] \tag{91}$$

$$= \frac{1}{p_{\rm succ}} \frac{d_B d_E}{d_A d_D} \mathrm{Tr}_{E'} \left[\langle \Phi |^{\hat{B}B'} (V_{\mathcal{F}}^{R'\hat{B} \to \hat{E}D})^\dagger |\Phi\rangle^{\hat{E}E'} \omega^{RDB'} \langle \Phi |^{\hat{E}E'} V_{\mathcal{F}}^{R'\hat{B} \to \hat{E}D} |\Phi\rangle^{\hat{B}B'} \right] \tag{92}$$

$$= \frac{1}{p_{\rm succ}} \frac{d_B}{d_A d_D} \langle \Phi |^{\hat{B}B'} (V_{\mathcal{F}}^{R'\hat{B} \to \hat{E}D})^\dagger (\omega^{RDB'} \otimes \mathbb{I}^{\hat{E}}) V_{\mathcal{F}}^{R'\hat{B} \to \hat{E}D} |\Phi\rangle^{\hat{B}B'}. \tag{93}$$

Here, we used Lemma 7 in the third equation. The success probability of the measurement $\mathcal{M}$ is then given as

$$p_{\rm succ} = \frac{d_B}{d_A d_D} \mathrm{Tr}[\langle \Phi |^{\hat{B}B'} (V_{\mathcal{F}}^{R'\hat{B} \to \hat{E}D})^\dagger (\omega^{RDB'} \otimes \mathbb{I}^{\hat{E}}) V_{\mathcal{F}}^{R'\hat{B} \to \hat{E}D} |\Phi\rangle^{\hat{B}B'}] \tag{94}$$

$$= \frac{d_B}{d_D} \mathrm{Tr} \left[(\mathbb{I}^R \otimes V_{\mathcal{F}}^{R'\hat{B} \to \hat{E}D} (\pi^{R'} \otimes \Phi^{\hat{B}B'}) (V_{\mathcal{F}}^{R'\hat{B} \to \hat{E}D})^\dagger) (\omega^{RDB'} \otimes \mathbb{I}^{\hat{E}}) \right] \tag{95}$$

$$= \frac{d_B}{d_D} \mathrm{Tr}[(\mathbb{I}^R \otimes \omega^{DB'\hat{E}})(\omega^{RDB'} \otimes \mathbb{I}^{\hat{E}})] \tag{96}$$

$$= \frac{d_B}{d_D} \mathrm{Tr}[(\omega^{DB'})^2] \tag{97}$$

$$= \frac{d_B}{d_D} 2^{-H_2(RE)_\omega}. \tag{98}$$

Since the state $|\omega\rangle^{REDB'}$ is pure, we here used that $\mathrm{Tr}[(\omega^{DB'})^2] = \mathrm{Tr}[(\omega^{RE})^2] = 2^{-H_2(RE)_\omega}$.

The fidelity after the post-selection is calculated from $\zeta_{\rm succ}^{RR'}$ as follows:

$$\mathrm{F}(\zeta_{\rm succ}^{RR'}, \Phi^{RR'}) = \frac{1}{p_{\rm succ}} \frac{d_B}{d_A d_D} \mathrm{Tr}[\Phi^{RR'} \langle \Phi |^{\hat{B}B'} (V_{\mathcal{F}}^{R'\hat{B} \to \hat{E}D})^\dagger (\omega^{RDB'} \otimes \mathbb{I}^{\hat{E}}) V_{\mathcal{F}}^{R'\hat{B} \to \hat{E}D} |\Phi\rangle^{\hat{B}B'}] \tag{99}$$

$$= \frac{1}{p_{\rm succ}} \frac{d_B}{d_A d_D} \mathrm{Tr}[V_{\mathcal{F}}^{R'\hat{B} \to \hat{E}D} (\Phi^{RR'} \otimes \Phi^{\hat{B}B'}) (V_{\mathcal{F}}^{R'\hat{B} \to \hat{E}D})^\dagger (\omega^{RDB'} \otimes \mathbb{I}^{\hat{E}})] \tag{100}$$

$$= \frac{1}{p_{\rm succ}} \frac{d_B}{d_A d_D} \mathrm{Tr}[\omega^{R\hat{E}DB'} (\omega^{RDB'} \otimes \mathbb{I}^{\hat{E}})] \tag{101}$$

$$= \frac{1}{p_{\rm succ}} \frac{d_B}{d_A d_D} \mathrm{Tr}[(\omega^{RDB'})^2] \tag{102}$$

$$= \frac{1}{p_{\rm succ}} \frac{d_B}{d_A d_D} 2^{-H_2(RDB')_\omega}. \tag{103}$$

Substituting Eq. (98), we obtain that

$$\mathrm{F}(\zeta_{\rm succ}^{RR'}, \Phi^{RR'}) = \frac{1}{d_A} 2^{H_2(RE) - H_2(RDB')} \tag{104}$$

$$= \frac{1}{d_A} 2^{H_2(RE) - H_2(E)}, \tag{105}$$

where we used $H_2(RDB')_\omega = H_2(E)_\omega$ since $|\omega\rangle^{REDB'}$ is pure. Thus, we obtain Eqs. (37) and (38).

4.1.2 Proof of Theorem 4

To show Theorem 4, we use the QSVT-based FPAA algorithm instead of the measurement $\mathcal{M}$. We again mention that our situation differs from the common situation for the AA algorithm since the receiver has access only to a part of the whole system; the reference R and environment E are not with the receiver. This issue will be circumvented by the QSVT-based FPAA.

First, we specify the input and output states of the QSVT-based FPAA. We denote the input state by

$$\omega_0^{RDD'E'R'} := \mathcal{V}^{B' \to D'E'R'} (\omega^{RDB'}), \tag{106}$$

where $\omega^{RDB'}$ is given by Eq. (88), and $\mathcal{V}^{B' \to D'E'R'}$ is the isometry map such that

$$\mathcal{V}^{B' \to D'E'R'}(\cdot) = (V_{\mathcal{F}}^{A'B' \to E'D'})^* (\cdot \otimes \Phi^{A'R'}) (V_{\mathcal{F}}^{A'B' \to E'D'})^{\mathsf{T}}. \tag{107}$$

To introduce a target state, we define a pure state $|\omega_{\rm targ}\rangle^{RR'EE'}$ by

$$|\omega_{\rm targ}\rangle^{RR'EE'} := \sqrt{d_A d_E \omega^{RE}} |\Phi\rangle^{RER'E'}. \tag{108}$$

A reduced state on RR', i.e., $\omega_{\mathrm{targ}}^{RR'}$, is our target state, to which we aim to transform the input state $\omega_0^{RDD'E'R'}$. This is because, if there exists a state τ^E such that $\|\omega^{RE} - \pi^R \otimes \tau^E\|_1 \leq \epsilon$, it holds that

$$\frac{1}{2}\left\|\omega_{\mathrm{targ}}^{RR'} - \Phi^{RR'}\right\|_1 \leq \sqrt{\epsilon}. \tag{109}$$

This follows from the following proposition, which considers, in a slightly more general case, the so-called *canonical purification* [84].

The canonical purification for a state ρ^A is defined as $|\rho_{\mathrm{c}}\rangle^{AA'} := \sqrt{d_A \rho^A}|\Phi\rangle^{AA'} = \sum_i \sqrt{p_i}|e_i\rangle^A|e_i^*\rangle^{A'}$, where $\sum_i p_i |e_i\rangle\langle e_i|^A$ is the eigenvalue decomposition of ρ^A. Note that $\sqrt{d_A}|\Phi\rangle^{AA'} = \sum_i |i\rangle^A|i\rangle^{A'} = \sum_i |e_i\rangle^A|e_i^*\rangle^{A'}$, where $\{|i\rangle\}_i$ is the computational basis. The canonical purification satisfies the following.

Proposition 8. *Let $|\rho_{\mathrm{c}}\rangle^{AA'}$ and $|\sigma_{\mathrm{c}}\rangle^{AA'}$ be the canonical purifications of states ρ^A and σ^A, respectively. Then, it holds that*

$$\frac{1}{2}\left\||\rho_{\mathrm{c}}\rangle\langle\rho_{\mathrm{c}}|^{AA'} - |\sigma_{\mathrm{c}}\rangle\langle\sigma_{\mathrm{c}}|^{AA'}\right\|_1 \leq \sqrt{\|\rho^A - \sigma^A\|_1}. \tag{110}$$

While this proposition may be derived readily from results in [85], we provide a proof for completeness.

Proof of Proposition 8. Let us start by evaluating the Euclidean norm of the difference between $|\rho_{\mathrm{c}}\rangle^{AA'}$ and $|\sigma_{\mathrm{c}}\rangle^{AA'}$:

$$\begin{aligned}
&\left\||\rho_{\mathrm{c}}\rangle^{AA'} - |\sigma_{\mathrm{c}}\rangle^{AA'}\right\| \\
&= \left\|\sqrt{d_A\rho^A}|\Phi\rangle^{AA'} - \sqrt{d_A\sigma^A}|\Phi\rangle^{AA'}\right\| && (111)\\
&= \sqrt{\mathrm{Tr}[\rho^A] + \mathrm{Tr}[\sigma^A] - 2\,\mathrm{Tr}\left[\sqrt{\rho^A}\sqrt{\sigma^A}\right]} && (112)\\
&= \left\|\sqrt{\rho^A} - \sqrt{\sigma^A}\right\|_2 && (113)\\
&\leq \sqrt{\|\rho^A - \sigma^A\|_1}. && (114)
\end{aligned}$$

In the last line, we used the well-known Powers–Størmer inequality [43, 44]: for any positive semidefinite operators L and M, $\|L^{1/2} - M^{1/2}\|_2 \leq \|L - M\|_1^{1/2}$ holds. Then, since $\frac{1}{2}\||v\rangle\langle v| - |w\rangle\langle w|\|_1 \leq \||v\rangle - |w\rangle\|$ for any pure states $|v\rangle$ and $|w\rangle$, we obtain

$$\frac{1}{2}\left\||\rho_{\mathrm{c}}\rangle\langle\rho_{\mathrm{c}}|^{AA'} - |\sigma_{\mathrm{c}}\rangle\langle\sigma_{\mathrm{c}}|^{AA'}\right\|_1 \leq \sqrt{\|\rho^A - \sigma^A\|_1}. \tag{115}$$

□

By taking ρ^A and σ^A in Proposition 8 as ω^{RE} and $\pi^R \otimes \tau^E$, respectively, and using the contraction property of the trace norm under the partial trace over EE', we obtain Eq. (109). This implies that the state $\omega_{\mathrm{targ}}^{RR'}$ is $\sqrt{\epsilon}$-close to the MES $\Phi^{RR'}$ when the decoupling is satisfied with error ϵ. Hence, we aim to transform the input state to the target state: $\omega_0^{RDD'E'R'} \mapsto \omega_{\mathrm{targ}}^{RR'} \approx \Phi^{RR'}$, ensuring that the recovery is successful when $\omega^{RE} \approx \pi^R \otimes \tau^E$.

In the following, our goal is to show that the transformation from $\omega_0^{RDD'E'R'}$ to $\omega_{\mathrm{targ}}^{RR'}$ can be achieved with high accuracy by the QSVT-based FPAA algorithm. Before we consider the QSVT-based FPAA in full detail, we first examine the structures of the input and output states to construct an operator to which the QSVT-based FPAA should be applied.

Let $|\omega_0\rangle^{REDD'E'R'}$ be the purified state of $\omega_0^{RDD'E'R'}$, i.e.,

$$|\omega_0\rangle^{REDD'E'R'} = (V_{\mathcal{F}}^{A'B'\to E'D'})^*|\omega\rangle^{REDB'}|\Phi\rangle^{A'R'}. \tag{116}$$

The state $|\omega\rangle^{REDB'}$ is given by Eq. (89). Suppose $|\omega_0\rangle^{REDD'E'R'}$ has the Schmidt decomposition between RE and $DD'E'R'$ such that

$$|\omega_0\rangle^{REDD'E'R'} = \sum_{\mu=1}^{r} \sqrt{\lambda_\mu}|\eta_\mu\rangle^{RE}|\psi_\mu\rangle^{DD'E'R'}, \tag{117}$$

where $\{|\psi_\mu\rangle^{DD'E'R'}\}_\mu$ and $\{|\eta_\mu\rangle^{RE}\}_\mu$ are orthonormal bases, and r is the Schmidt rank, i.e., the number of non-zero λ_μ's. From Eq. (108) and the fact that $\omega^{RE} = \omega_0^{RE}$, it follows that the Schmidt decomposition of $|\omega_{\mathrm{targ}}\rangle^{RR'EE'}$ is given by

$$|\omega_{\mathrm{targ}}\rangle^{RR'EE'} = \sum_\mu \sqrt{\lambda_\mu}|\eta_\mu\rangle^{RE}|\eta_\mu^*\rangle^{E'R'}. \tag{118}$$

Thus, if we can transform $|\psi_\mu\rangle^{DD'E'R'}$ to $|\eta_\mu^*\rangle^{E'R'}$ for all μ, we can obtain $\omega_{\mathrm{targ}}^{RR'}$ on RR'.

To this end, we now turn to investigate the QSVT-based FPAA. Consider an operator $\Lambda^{DD'E'R'}$ defined by $\Lambda^{DD'E'R'} := \Pi_2^{DD'}\Pi_1^{D'E'R'}$, which is the subject of the QSVT-based FPAA in our protocol. Here, $\Pi_1^{D'E'R'}$ and $\Pi_2^{DD'}$ are the

projectors such that

$$\Pi_1^{D'E'R'} := (V_{\mathcal{F}}^{A'B'\to E'D'})^*(\mathbb{I}^{B'} \otimes |\Phi\rangle\langle\Phi|^{A'R'}) (V_{\mathcal{F}}^{A'B'\to E'D'})^{\mathsf{T}}, \tag{119}$$

$$\Pi_2^{DD'} := |\Phi\rangle\langle\Phi|^{DD'}. \tag{120}$$

To apply the QSVT, we need to specify the singular value decomposition of $\Lambda^{DD'E'R'}$. This can be done as follows.

We first calculate $(\Pi_1\Pi_2\Pi_1)^{DD'E'R'}$:

$$\begin{aligned}
&(\Pi_1\Pi_2\Pi_1)^{DD'E'R'} \\
&= (V_{\mathcal{F}}^{A'B'\to E'D'})^*|\Phi\rangle\langle\Phi|^{A'R'}(V_{\mathcal{F}}^{A'B'\to E'D'})^{\mathsf{T}} \\
&\qquad |\Phi\rangle\langle\Phi|^{DD'}(V_{\mathcal{F}}^{A'B'\to E'D'})^* \\
&\qquad\quad |\Phi\rangle\langle\Phi|^{A'R'}(V_{\mathcal{F}}^{A'B'\to E'D'})^{\mathsf{T}} && (121)\\
&= \frac{d_Bd_E}{d_Ad_D}(V_{\mathcal{F}}^{A'B'\to E'D'})^*|\Phi\rangle^{A'R'}\langle\Phi|^{EE'}V_{\mathcal{F}}^{AB\to ED} \\
&\qquad |\Phi\rangle\langle\Phi|^{BB'}(V_{\mathcal{F}}^{AB\to ED})^\dagger \\
&\qquad\quad |\Phi\rangle^{EE'}\langle\Phi|^{A'R'}(V_{\mathcal{F}}^{A'B'\to E'D'})^{\mathsf{T}} && (122)\\
&= \frac{d_B}{d_D}(V_{\mathcal{F}}^{A'B'\to E'D'})^* \\
&\qquad (\omega^{DB'} \otimes \Phi^{A'R'})(V_{\mathcal{F}}^{A'B'\to E'D'})^{\mathsf{T}} && (123)\\
&= \frac{d_B}{d_D}\omega_0^{DD'E'R'}, && (124)
\end{aligned}$$

where we used Lemma 7 in the second equation. We then compute $(\Lambda\Lambda^\dagger\Lambda)^{DD'E'R'}$:

$$\begin{aligned}
&(\Lambda\Lambda^\dagger\Lambda)^{DD'E'R'} \\
&= (\Pi_2\Pi_1\Pi_2\Pi_1)^{DD'E'R'} && (125)\\
&= \frac{d_B}{d_D}|\Phi\rangle\langle\Phi|^{DD'}\omega_0^{DD'E'R'} && (126)\\
&= \sum_{\mu=1}^{r}\frac{d_B\lambda_\mu}{d_D}|\Phi\rangle\langle\Phi|^{DD'}|\psi_\mu\rangle\langle\psi_\mu|^{DD'E'R'}. && (127)
\end{aligned}$$

To proceed with the calculation, we must determine $\langle\Phi|^{DD'}|\psi_\mu\rangle^{DD'E'R'}$, which is an unnormalized vector on $E'R'$. Although this is somewhat involved, it can be obtained as

$$\langle\Phi|^{DD'}|\psi_\mu\rangle^{DD'E'R'} = \sqrt{\frac{d_B\lambda_\mu}{d_D}}|\eta_\mu^*\rangle^{E'R'}. \tag{128}$$

by investigating the state after the post-selection as follows.

Let us denote by $|\zeta_{\mathrm{succ}}\rangle^{REE'R'}$ the state on $REE'R'$ after the post-selection by $|\Phi\rangle^{DD'}$, i.e.,

$$|\zeta_{\mathrm{succ}}\rangle^{REE'R'} = \frac{1}{\sqrt{p_{\mathrm{succ}}}}\langle\Phi|^{DD'}|\omega_0\rangle^{REDD'E'R'}. \tag{129}$$

The states ω_0^{RE} and $\zeta_{\mathrm{succ}}^{RE}$ are related by

$$\zeta_{\mathrm{succ}}^{RE} = \frac{d_B}{d_Dp_{\mathrm{succ}}}(\omega_0^{RE})^2. \tag{130}$$

This follows from the direct calculation:

$$\begin{aligned}
&\zeta_{\mathrm{succ}}^{RE} \\
&= \frac{1}{p_{\mathrm{succ}}}\langle\Phi|^{DD'}\omega_0^{REDD'}|\Phi\rangle^{DD'} && (131)\\
&= \frac{1}{p_{\mathrm{succ}}}\mathrm{Tr}_{R'E'}\Big[(\langle\Phi|^{DD'}(V_{\mathcal{F}}^{A'B'\to E'D'})^*|\Phi\rangle^{A'R'}) \\
&\quad |\omega\rangle\langle\omega|^{REDB'}(\langle\Phi|^{DD'}(V_{\mathcal{F}}^{A'B'\to E'D'})^*|\Phi\rangle^{A'R'})^\dagger\Big] && (132)\\
&= \frac{d_Bd_E}{d_Ad_Dp_{\mathrm{succ}}}\mathrm{Tr}_{R'E'}\Big[(\langle\Phi|^{\hat{B}B'}(V_{\mathcal{F}}^{R'\hat{B}\to\hat{E}D})^\dagger \\
&\qquad |\Phi\rangle^{\hat{E}E'})|\omega\rangle\langle\omega|^{REDB'} \\
&\qquad (\langle\Phi|^{\hat{B}B'}(V_{\mathcal{F}}^{R'\hat{B}\to\hat{E}D})^\dagger|\Phi\rangle^{\hat{E}E'})^\dagger\Big] && (133)\\
&= \frac{d_B}{d_Ad_Dp_{\mathrm{succ}}}\mathrm{Tr}_{R'}\Big[\langle\Phi|^{\hat{B}B'}(V_{\mathcal{F}}^{R'\hat{B}\to\hat{E}D})^\dagger \\
&\quad (|\omega\rangle\langle\omega|^{REDB'} \otimes \mathbb{I}^{\hat{E}})(V_{\mathcal{F}}^{R'\hat{B}\to\hat{E}D})|\Phi\rangle^{\hat{B}B'}\Big] && (134)\\
&= \frac{d_B}{d_Dp_{\mathrm{succ}}}\mathrm{Tr}_{\hat{E}DB'}\Big[(V_{\mathcal{F}}^{R'\hat{B}\to\hat{E}D})(\pi^{R'} \otimes \Phi^{\hat{B}B'}) \\
&\quad (V_{\mathcal{F}}^{R'\hat{B}\to\hat{E}D})^\dagger(|\omega\rangle\langle\omega|^{REDB'} \otimes \mathbb{I}^{\hat{E}})\Big] && (135)\\
&= \frac{d_B}{d_Dp_{\mathrm{succ}}}\mathrm{Tr}_{DB'}[\omega^{DB'}|\omega\rangle\langle\omega|^{REDB'}] && (136)\\
&= \frac{d_B}{d_Dp_{\mathrm{succ}}}(\omega^{RE})^2 && (137)\\
&= \frac{d_B}{d_Dp_{\mathrm{succ}}}(\omega_0^{RE})^2, && (138)
\end{aligned}$$

where we used Lemma 7 in the third equation. The second last equality follows, e.g., from the Schmidt decomposition of $|\omega\rangle^{REDB'}$. Note that $\omega^{RE} = \omega_0^{RE}$.

We now expand Eq. (130) based on the Schmidt decomposition of $|\omega_0\rangle^{REDD'E'R'}$ given by Eq. (117). As $|\zeta_{\mathrm{succ}}\rangle^{REE'R'}$ is given by Eq. (129), it can be written as

$$|\zeta_{\mathrm{succ}}\rangle^{REE'R'} = \sum_{\mu=1}^{r}\sqrt{\frac{\lambda_\mu}{p_{\mathrm{succ}}}}|\eta_\mu\rangle^{RE}|\check{\varphi}_\mu\rangle^{E'R'}, \tag{139}$$

where $|\check{\varphi}_\mu\rangle^{E'R'} = \langle\Phi|^{DD'}|\psi_\mu\rangle^{DD'E'R'}$ is an unnormalized vector. Hence, we can rephrase Eq. (130)

as

$$\sum_{\mu,\nu=1}^{r} \frac{\sqrt{\lambda_\mu \lambda_\nu}}{p_{\mathrm{succ}}} \langle \breve{\varphi}_\nu | \breve{\varphi}_\mu \rangle |\eta_\mu\rangle\langle\eta_\nu|^{RE} = \sum_{\mu=1}^{r} \frac{d_B \lambda_\mu^2}{d_D p_{\mathrm{succ}}} |\eta_\mu\rangle\langle\eta_\mu|^{RE}. \quad (140)$$

Since $\{|\eta_\mu\rangle^{RE}\}_\mu$ is an orthonormal basis and $\lambda_\mu \neq 0$ for $\mu = 1, 2, \ldots, r$, Eq. (140) implies that

$$\langle \breve{\varphi}_\nu | \breve{\varphi}_\mu \rangle = \frac{d_B \lambda_\mu}{d_D} \delta_{\mu\nu}, \quad (141)$$

where $\delta_{\mu\nu} = 1$ if $\mu = \nu$ and $\delta_{\mu\nu} = 0$ otherwise. By normalizing $|\breve{\varphi}_\mu\rangle$, such as $|\varphi_\mu\rangle^{E'R'} = \sqrt{d_D/(d_B\lambda_\mu)}|\breve{\varphi}_\mu\rangle^{E'R'}$, we obtain

$$|\zeta_{\mathrm{succ}}\rangle^{REE'R'} = \sum_{\mu=1}^{r} \sqrt{\frac{d_B}{d_D p_{\mathrm{succ}}}} \lambda_\mu |\eta_\mu\rangle^{RE} |\varphi_\mu\rangle^{E'R'}. \quad (142)$$

Since $|\varphi_\mu\rangle^{E'R'}$ are mutually orthonormal due to Eq. (141), Eq. (142) provides the Schmidt decomposition of $|\zeta_{\mathrm{succ}}\rangle^{REE'R'}$ between RE and $E'R'$.

Moreover, from the symmetry of $|\zeta_{\mathrm{succ}}\rangle^{REE'R'}$ between RE and $E'R'$, taking the complex conjugate of this state is equivalent to swapping RE with $E'R'$. This implies that the Schmidt basis of $|\zeta_{\mathrm{succ}}\rangle^{REE'R'}$ in RE and that in $E'R'$ are the same up to the complex conjugate. Hence, we find that $|\varphi_\mu\rangle^{E'R'} = |\eta_\mu^*\rangle^{E'R'}$. Accordingly, the Schmidt decomposition of $|\zeta_{\mathrm{succ}}\rangle^{REE'R'}$ is given by

$$|\zeta_{\mathrm{succ}}\rangle^{REE'R'} = \sum_{\mu=1}^{r} \sqrt{\frac{d_B}{d_D p_{\mathrm{succ}}}} \lambda_\mu |\eta_\mu\rangle^{RE} |\eta_\mu^*\rangle^{E'R'}. \quad (143)$$

This symmetry property solely relies on the general structure of the protocol and is of crucial importance. See also Fig. 8.

Finally, by applying $\langle\eta_\mu|^{RE}$ on the left to $|\zeta_{\mathrm{succ}}\rangle^{REE'R'}$ in its two different expressions given by Eqs. (139) and (143), we obtain Eq. (128).

We now return to determining the singular value decomposition of $\Lambda^{DD'E'R'}$. Substituting Eq. (128) into Eq. (127), it follows that

$$(\Lambda\Lambda^\dagger\Lambda)^{DD'E'R'} = \sum_{\mu=1}^{r} \Big(\frac{d_B\lambda_\mu}{d_D}\Big)^{3/2} |\Phi\rangle^{DD'} |\eta_\mu^*\rangle^{E'R'} \langle\psi_\mu|^{DD'E'R'}. \quad (144)$$

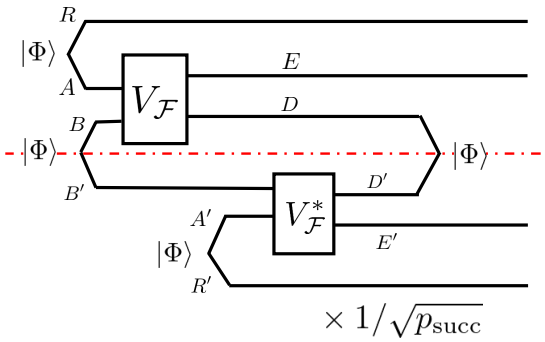


Figure 8: A diagram of the state $|\zeta_{\mathrm{succ}}\rangle^{REE'R'}$. This is symmetrical with respect to the red dash-dotted line, up to the complex conjugate. Due to this symmetry, the Schmidt basis of $|\zeta_{\mathrm{succ}}\rangle^{REE'R'}$ is given by $\{|\eta_\mu\rangle^{RE}|\eta_\mu^*\rangle^{E'R'}\}_\mu$.

Hence, the singular value decomposition of $\Lambda^{DD'E'R'}$ is uniquely determined, without any phase ambiguity in the left- and right-singular vectors, as

$$\Lambda^{DD'E'R'} = \sum_{\mu=1}^{r} \sqrt{\frac{d_B\lambda_\mu}{d_D}} |\Phi\rangle^{DD'} |\eta_\mu^*\rangle^{E'R'} \langle\psi_\mu|^{DD'E'R'}. \quad (145)$$

When some of the λ_μ's are degenerate, we fix the basis in the degenerate subspace to an arbitrary one.

Since $\Lambda^{DD'E'R'}$ is a product of two projectors $\Pi_1^{D'E'R'}$ and $\Pi_2^{DD'}$, it is naturally block-encoded in $\mathbb{I}^{DD'E'R'}$ on the subspace specified by these projectors; see also Eqs. (26) to (32) in 2.7, with $U = \mathbb{I}$. Then, the following holds as an immediate consequence of the QSVT for $\Lambda^{DD'E'R'}$ with a real odd polynomial [40–42].

Let $Q_{t,\phi}(x)$ be a degree-t real odd polynomial satisfying $|Q_{t,\phi}(x)| \leq 1$ for all $x \in [-1, 1]$. Then, there is $\phi \in (-\pi, \pi]^t$ such that

$$(\Pi_2^{DD'} \otimes \langle 0|^H) G_{t,\phi}^{DD'E'R'H} (\Pi_1^{D'E'R'} \otimes |0\rangle^H) = Q_{t,\phi}(\Lambda^{DD'E'R'}) \quad (146)$$

$$= \sum_{\mu=1}^{r} Q_{t,\phi}\Big(\sqrt{\frac{d_B\lambda_\mu}{d_D}}\Big) |\Phi\rangle^{DD'} |\eta_\mu^*\rangle^{E'R'} \langle\psi_\mu|^{DD'E'R'}, \quad (147)$$

where the unitary $G_{t,\phi}^{DD'E'R'H}$ is given by Eq. (53), with a single-qubit auxiliary system H. If we can choose the polynomial $Q_{t,\phi}$ such that $Q_{t,\phi}(\sqrt{d_B\lambda_\mu/d_D}) \approx 1$ for all $\mu = 1, 2, \ldots, r$,

we obtain desired transformation $|\psi_\mu\rangle^{DD'E'R'}$ to $|\Phi\rangle^{DD'}|\eta_\mu^*\rangle^{E'R'}$. A possible choice of such a polynomial is one that approximates the sign function. From Lemma 3, for $Q_t^{\mathrm{sign}}(\sqrt{d_B\lambda_\mu/d_D})$ to be larger than $1-\delta$ for $\mu=1,2,\ldots,r$, it suffices that $\sqrt{d_B\lambda_{\min}/d_D}\geq\beta$, where $\lambda_{\min}:=\min_{\mu\in[1,r]}\lambda_\mu$ and $\delta\in(0,1/2)$. Thus, we can take the odd integer t such that

$$t\geq\left\lceil 8e\sqrt{\frac{d_D}{d_B\lambda_{\min}(\omega^{RE})}}\log(2/\delta)\right\rceil. \tag{148}$$

We here used that $\lambda_{\min}$ corresponds to the nonzero minimum eigenvalue of ω^{RE}, $\lambda_{\min}(\omega^{RE})$, since $\omega_0^{RE}=\omega^{RE}$; see Eq. (117).

This QSVT allows us to approximately obtain a block-encoding of the operator

$$\begin{aligned}&\mathrm{sign}(\Lambda^{DD'E'R'})\otimes|0\rangle\langle 0|^H\\&=\sum_{\mu=1}^r|\Phi\rangle^{DD'}|\eta_\mu^*\rangle^{E'R'}\langle\psi_\mu|^{DD'E'R'}\otimes|0\rangle\langle 0|^H.\end{aligned} \tag{149}$$

Applying this to the state $|\omega_0\rangle^{REDD'E'R'}|0\rangle^H$, we achieve the transformation:

$$|\omega_0\rangle^{REDD'E'R'}|0\rangle^H\mapsto|\Phi\rangle^{DD'}|\omega_{\mathrm{targ}}\rangle^{REE'R'}|0\rangle^H. \tag{150}$$

Recall that the Schmidt decomposition of $|\omega_0\rangle^{REDD'E'R'}$ and $|\omega_{\mathrm{targ}}\rangle^{REE'R'}$ are given in Eqs. (117) and (118), respectively. Since the state $|\omega_{\mathrm{targ}}\rangle^{REE'R'}$ satisfies Eq. (109), we can successfully recover the MES $|\Phi\rangle^{RR'}$ for sufficiently small ϵ.

To provide a more precise analysis of the overall error, we denote the output state of the QSVT-based FPAA algorithm by

$$\begin{aligned}&|\omega_t\rangle^{REDD'E'R'H}\\&\quad:=G_{t,\phi}^{DD'E'R'H}|\omega_0\rangle^{REDD'E'R'}|0\rangle^H.\end{aligned}$$

By taking t and ϕ to approximate the sign function, we obtain the overlap between this output state and the state $|\Phi\rangle^{DD'}|\omega_{\mathrm{targ}}\rangle^{REE'R'}|0\rangle^H$ as

$$\begin{aligned}&\langle\Phi|^{DD'}\langle\omega_{\mathrm{targ}}|^{REE'R'}\langle 0|^H|\omega_t\rangle^{REDD'E'R'H}\\&=\sum_{\mu=1}^r\lambda_\mu\langle\Phi|^{DD'}\langle\eta_\mu^*|^{E'R'}\langle 0|^H\\&\qquad G_{t,\phi}^{DD'E'R'H}|\psi_\mu\rangle^{DD'E'R'}|0\rangle^H &(151)\\&=\sum_{\mu=1}^r\lambda_\mu Q_t^{\mathrm{sign}}(\sqrt{d_B\lambda_\mu/d_D}) &(152)\\&\geq(1-\delta)\sum_{\mu=1}^r\lambda_\mu &(153)\\&=1-\delta, &(154)\end{aligned}$$

where we used $\sum_{\mu=1}^r\lambda_\mu=1$. Using the Fuchs–van de Graaf inequalities and the contraction property of the trace norm under the partial trace, we obtain

$$\frac{1}{2}\|\omega_t^{RR'}-\omega_{\mathrm{targ}}^{RR'}\|_1\leq\sqrt{1-(1-\delta)^2}\leq\sqrt{2\delta}. \tag{155}$$

Using Eqs. (109), (155), and the triangle inequality, we obtain

$$\frac{1}{2}\|\omega_t^{RR'}-\Phi^{RR'}\|_1\leq\sqrt{\epsilon}+\sqrt{2\delta}, \tag{156}$$

where ϵ is the degree of decoupling. Note that the state $\omega_t^{RR'}$ is the output of the generalized YK decoder: $\mathcal{D}_{t,\phi}^{DB'\to R'}(\omega^{RDB'})=\omega_t^{RR'}$. Thus, by rescaling δ to $\delta^2/2$, we complete the evaluation of the overall recovery error of the generalized YK decoder.

We next investigate the circuit complexity of the generalized YK decoder. The non-trivial part is to implement the unitary $G_{t,\phi}$ in the QSVT-based FPAA algorithm, whose construction is explained in 3.1.2 (see also Fig. 4). We thus mainly focus on $\mathcal{C}(G_{t,\phi})$.

We start with a circuit implementation of $W_m(\theta)$ for $m=1,2$:

$$\begin{aligned}W_m(\theta)&=e^{i\theta(2\Pi_m-\mathbb{I})} &(157)\\&=e^{-i\theta}\mathbb{I}-(e^{-i\theta}-e^{i\theta})\Pi_m. &(158)\end{aligned}$$

To implement the unitary $W_m(\theta)$, we use the *projector-controlled NOT gate* [40, 41] that is in general defined for a projector Π^P as

$$\mathrm{C}_\Pi\mathrm{NOT}^{P\text{-}G}:=\Pi^P\otimes X^G+(\mathbb{I}^P-\Pi^P)\otimes\mathbb{I}^G. \tag{159}$$

The order of the superscripts in the left-hand side indicates the controlling and controlled systems.

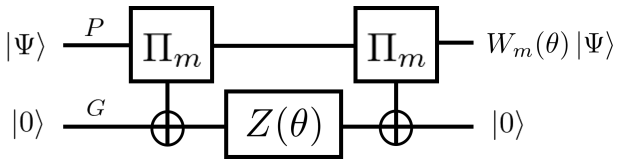


Figure 9: A quantum circuit for implementing a unitary $W_m(\theta)^P$. The box in which a projector is written implies that this projector controls the gate. The circle drawn inside the intersecting lines represents the NOT gate, i.e., the Pauli-X gate.

The gate X is the single-qubit Pauli-X gate. We also use a single-qubit rotation-Z gate:

$$Z(\theta) \coloneqq e^{-i\theta Z} \tag{160}$$
$$= e^{-i\theta}|0\rangle\langle 0| + e^{i\theta}|1\rangle\langle 1|, \tag{161}$$

where Z is the single-qubit Pauli-Z gate. It is straightforward to check that, for any state $|\Psi\rangle^P$,

$$(\mathrm{C}_\Pi\mathrm{NOT}^{P\text{-}G} Z(\theta)^G \mathrm{C}_\Pi\mathrm{NOT}^{P\text{-}G})(|\Psi\rangle^P \otimes |0\rangle^G)$$
$$= \left[e^{-i\theta}\mathbb{I}^P - (e^{-i\theta} - e^{i\theta})\Pi^P)|\Psi\rangle^P\right] \otimes |0\rangle^G \tag{162}$$
$$= W_m(\theta)^P|\Psi\rangle^P \otimes |0\rangle^G. \tag{163}$$

Hence, we can implement $W_m(\theta)^P$ by preparing a single-qubit system G and by operating a quantum circuit in Fig. 9.

To construct a circuit for $G_{t,\phi}$, we prepare another single-qubit system H for the controlled implementation of $W_m(\theta)^P$. For instance, a quantum circuit implementing

$$W_1(\phi_{2j})^{D'E'R'} W_2(\phi_{2j-1})^{DD'} \otimes |+\rangle\langle +|^H + W_1(-\phi_{2j})^{D'E'R'} W_2(-\phi_{2j-1})^{DD'} \otimes |-\rangle\langle -|^H, \tag{164}$$

is given in Fig. 10. By applying the circuit $(t-1)/2$ times with various phases and finally applying $W_2(\phi_t)^{DD'} \otimes \mathrm{H}^H$, the unitary $G_{t,\phi}$ is realized. Here, the gate H^H is the single-qubit Hadamard gate on the system H.

In the construction, the unitary $G_{t,\phi}$ is decomposed into two unitaries $\mathrm{C}_{\Pi_1}\mathrm{NOT}^{D'E'R'\text{-}G}$ and $\mathrm{C}_{\Pi_2}\mathrm{NOT}^{DD'\text{-}G}$. A quantum circuit for $\mathrm{C}_{\Pi_1}\mathrm{NOT}^{D'E'R'\text{-}G}$ is given in Fig. 11. In general, the unitary $\mathrm{C}_{|0\rangle\langle 0|}\mathrm{NOT}^{P\text{-}G}$ can be implemented using $\mathcal{O}(\log d_P)$ single- and two-qubit gates and $\mathcal{O}(\log d_P)$ ancilla qubits [86]. The unitary $U_\Phi^{A'R'}$, which is given by

$$U_\Phi^{A'R'}|0\rangle^{A'}|0\rangle^{R'} = |\Phi\rangle^{A'R'}, \tag{165}$$

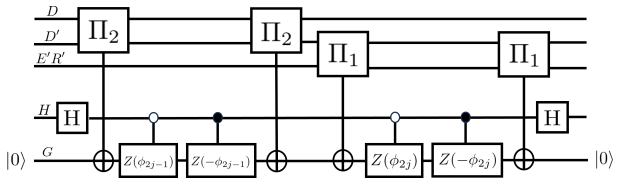


Figure 10: A quantum circuit for implementing the unitary operation $W_1(\phi_{2j})^{D'E'R'}W_2(\phi_{2j-1})^{DD'} \otimes |+\rangle\langle +|^H + W_1(-\phi_{2j})^{D'E'R'}W_2(-\phi_{2j-1})^{DD'} \otimes |-\rangle\langle -|^H$. Open circles imply that the gates are controlled by $|0\rangle$, while closed circles indicate the ones controlled by $|1\rangle$.

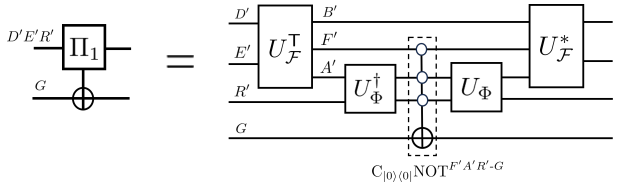


Figure 11: A quantum circuit for implementing the projector-controlled NOT gate $\mathrm{C}_{\Pi_1}\mathrm{NOT}^{D'E'R'\text{-}G}$. The dashed box represents the gate $\mathrm{C}_{|0\rangle\langle 0|}\mathrm{NOT}^{F'A'R'\text{-}G}$.

can be implemented using $\mathcal{O}(\log d_A)$ gates. Hence, in total, $\mathrm{C}_{\Pi_1}\mathrm{NOT}^{D'E'R'\text{-}G}$ can be implemented by

$$\mathcal{O}(\mathcal{C}(U_\mathcal{F}) + \log(d_A d_F)) \tag{166}$$

gates and $\mathcal{O}(\log d_A d_F)$ ancilla qubits. Similarly, $\mathrm{C}_{\Pi_2}\mathrm{NOT}^{DD'\text{-}G}$ can be implemented using $\mathcal{O}(\log d_D)$ gates and $\mathcal{O}(\log d_D)$ ancilla qubits.

In the unitary $G_{t,\phi}$, these projector-controlled NOT gates are used $\mathcal{O}(t)$ times. The total complexity of the generalized YK decoder is given by

$$\mathcal{C}(\mathcal{D}_{t,\phi}) = \mathcal{O}\Big(t(\mathcal{C}(U_\mathcal{F}) + \log(d_A d_F d_D))\Big) + \mathcal{C}(U_\mathcal{F}) + \mathcal{O}(\log d_A) \tag{167}$$
$$= \mathcal{O}\Big(t(\mathcal{C}(U_\mathcal{F}) + \log(d_D^2 d_E/d_B))\Big), \tag{168}$$

with $\mathcal{O}(\log(d_D^2 d_E/d_B))$ ancilla qubits. Here, we used $d_A d_B d_F = d_E d_D$. In Eq. (167), the first line in the right-hand side comes from $G_{t,\phi}$ and the second line comes from $\mathcal{V}^{A'B'\to E'D'}$, which is applied before $G_{t,\phi}$.

4.2 Proofs: the Petz-like decoder

Similarly to the generalized YK decoder, we first consider the decoding protocol with post-selection and then provide a sketch of a proof of Theorem 5.

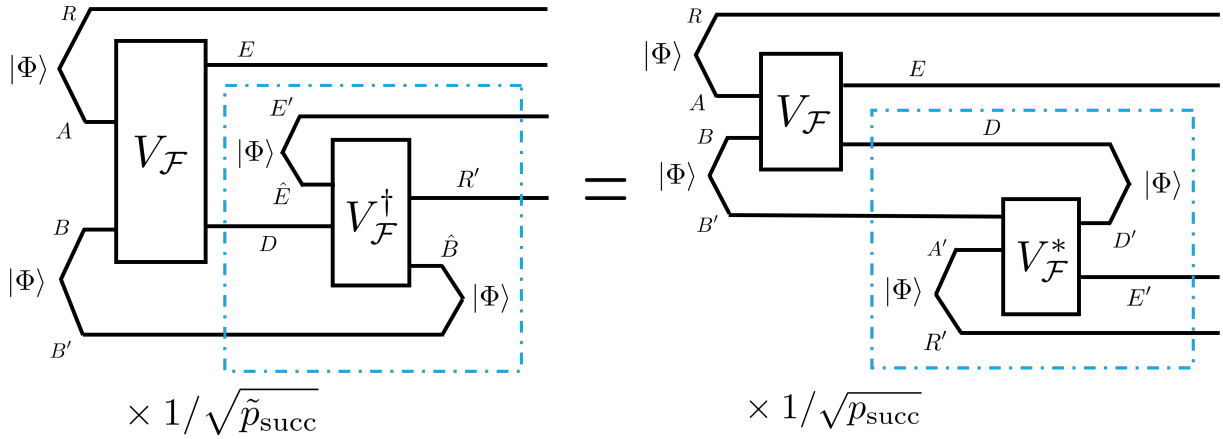


Figure 12: The equivalence of the states $\tilde{\zeta}_{\mathrm{succ}}^{REE'R'}$ and $\zeta_{\mathrm{succ}}^{REE'R'}$, which are obtained after the post-selection in the Petz-like protocol and in the generalized YK protocol, respectively. We can derive this equivalence by applying Lemma 7 onto the portion enclosed by the blue dash-dotted lines.

From Eqs. (19), (55), and (56), the success probability $\tilde{p}_{\mathrm{succ}}$ is computed as

$$\begin{aligned}\tilde{p}_{\mathrm{succ}} &= \frac{d_A}{d_E}\operatorname{Tr}\left[V_{\mathcal{F}}^{R'\hat{B}\to\hat{E}D}(\Phi^{\hat{B}B'}\otimes\pi^{R'})\right.\\ &\qquad\left.(V_{\mathcal{F}}^{R'\hat{B}\to\hat{E}D})^{\dagger}(\omega^{RDB'}\otimes\mathbb{I}^{\hat{E}})\right] &(169)\\ &= \frac{d_A}{d_E}\operatorname{Tr}\left[(\omega^{DB'})^2\right] &(170)\\ &= \frac{d_A}{d_E}2^{-H_2(DB')_\omega} &(171)\\ &= \frac{d_A}{d_E}2^{-H_2(RE)_\omega}, &(172)\end{aligned}$$

where we used $H_2(DB')_\omega = H_2(RE)_\omega$ as $|\omega\rangle^{REDB'}$ is pure. Note that the states $\omega^{RDB'}$ and $|\omega\rangle^{REDB'}$ are defined in Eqs. (88) and (89), respectively. The fidelity between $\tilde{\zeta}_{\mathrm{succ}}^{RR'}$ and $\Phi^{RR'}$ is computed as

$$\begin{aligned}&\mathrm{F}(\tilde{\zeta}_{\mathrm{succ}}^{RR'},\Phi^{RR'})\\ &= \frac{1}{d_E\tilde{p}_{\mathrm{succ}}}\operatorname{Tr}\left[V_{\mathcal{F}}^{R'\hat{B}\to\hat{E}D}(\Phi^{RR'}\otimes\Phi^{\hat{B}B'})\right.\\ &\qquad\left.(V_{\mathcal{F}}^{R'\hat{B}\to\hat{E}D})^{\dagger}(\omega^{RDB'}\otimes\mathbb{I}^{\hat{E}})\right] &(173)\\ &= \frac{1}{d_A}2^{H_2(RE)_\omega}\operatorname{Tr}\left[\omega^{R\hat{E}DB'}(\omega^{RB'D}\otimes\mathbb{I}^{\hat{E}})\right] &(174)\\ &= \frac{1}{d_A}2^{H_2(RE)_\omega-H_2(RDB')_\omega} &(175)\\ &= \frac{1}{d_A}2^{H_2(RE)_\omega-H_2(E)_\omega}, &(176)\end{aligned}$$

by using $H_2(RDB')_\omega = H_2(E)_\omega$ for $|\omega\rangle^{REDB'}$. Hence, we obtained Eqs. (57) and (58).

Let us now turn to the proof of Theorem 5. Since the proof is similar to that of Theorem 4, we provide only an outline.

We denote the input state of the QSVT-based FPAA algorithm by

$$\tilde{\omega}_0^{RE'R'\hat{F}\hat{B}B'} := \tilde{\mathcal{V}}^{D\to E'R'\hat{F}\hat{B}}(\omega^{RDB'}), \tag{177}$$

where $\tilde{\mathcal{V}}^{D\to E'R'\hat{F}\hat{B}}$ is the isometry map such that

$$\tilde{\mathcal{V}}^{D\to E'R'\hat{F}\hat{B}} = (U_{\mathcal{F}}^{\hat{L}})^{\dagger}(\cdot\otimes\Phi^{\hat{E}E'})U_{\mathcal{F}}^{\hat{L}}, \tag{178}$$

and $\hat{L} = R'\hat{F}\hat{B} = \hat{E}D$. Note that $\tilde{\omega}_0^{RE} = \omega^{RE}$. Let $|\tilde{\omega}_0\rangle^{REE'R'\hat{F}\hat{B}B'}$ be the purified state such that

$$|\tilde{\omega}_0\rangle^{REE'R'\hat{F}\hat{B}B'} = (U_{\mathcal{F}}^{\hat{L}})^{\dagger}|\omega\rangle^{REDB'}|\Phi\rangle^{\hat{E}E'}. \tag{179}$$

The state on $REE'R'$ after the post-selection is then given by

$$\begin{aligned}&|\tilde{\zeta}_{\mathrm{succ}}\rangle^{REE'R'}\\ &= \frac{1}{\sqrt{\tilde{p}_{\mathrm{succ}}}}\langle 0|^{\hat{F}}\langle\Phi|^{\hat{B}B'}|\tilde{\omega}_0\rangle^{REE'R'\hat{F}\hat{B}B'}. &(180)\end{aligned}$$

It is important to note that

$$\tilde{\zeta}_{\mathrm{succ}}^{REE'R'} = \zeta_{\mathrm{succ}}^{REE'R'}, \tag{181}$$

where the right-hand side is the state after the post-selection in the generalized YK decoding protocol. Although it may be hard to observe this relation from the construction in Fig. 5, this can be readily shown using Lemma 7 as in Fig. 12. From this relation, it turns out that the state $\tilde{\zeta}_{\mathrm{succ}}^{REE'R'}$ is also symmetric between RE and $E'R'$ up to the complex conjugate, and thus, the Schmidt basis in RE and that in $E'R'$ are complex conjugates of each other.

Suppose that the Schmidt decomposition of $|\tilde{\omega}_0\rangle^{REE'R'\hat{F}\hat{B}B'}$, divided into RE and $E'R'\hat{F}\hat{B}B'$, is given by

$$|\tilde{\omega}_0\rangle^{REE'R'\hat{F}\hat{B}B'} = \sum_{\mu=1}^{r} \sqrt{\lambda_\mu} |\eta_\mu\rangle^{RE} |\tilde{\psi}_\mu\rangle^{E'R'\hat{F}\hat{B}B'}. \tag{182}$$

As $\tilde{\omega}_0^{RE}$ is equal to $\omega_0^{RE} = \omega^{RE}$, λ_μ and $|\eta_\mu\rangle^{RE}$ are the eigenvalues and eigenvectors of ω^{RE}, respectively. Since the state $|\tilde{\zeta}_{\mathrm{succ}}\rangle$ is defined by using $|\tilde{\omega}_0\rangle$ as Eq. (180), it follows that

$$|\tilde{\zeta}_{\mathrm{succ}}\rangle^{REE'R'} = \sum_{\mu=1}^{r} \sqrt{\frac{\lambda_\mu}{\tilde{p}_{\mathrm{succ}}}} |\eta_\mu\rangle^{RE} \langle 0|^{\hat{F}} \langle \Phi|^{\hat{B}B'} |\tilde{\psi}_\mu\rangle^{E'R'\hat{F}\hat{B}B'}. \tag{183}$$

From Eq. (143) for $|\zeta_{\mathrm{succ}}\rangle$ in the generalized YK decoding protocol with post-selection and the relation in Eq. (181), we have

$$\begin{aligned} &\langle 0|^{\hat{F}} \langle \Phi|^{\hat{B}B'} |\tilde{\psi}_\mu\rangle^{E'R'\hat{F}\hat{B}B'} \\ &= \sqrt{\frac{d_B \tilde{p}_{\mathrm{succ}} \lambda_\mu}{d_D p_{\mathrm{succ}}}} |\eta_\mu^*\rangle^{E'R'} \qquad (184) \\ &= \sqrt{\frac{d_A \lambda_\mu}{d_E}} |\eta_\mu^*\rangle^{E'R'}. \qquad (185) \end{aligned}$$

Here, we substituted the success probabilities p_{succ} and $\tilde{p}_{\mathrm{succ}}$ in the generalized YK and Petz-like decoding protocols with post-selection, which are given by Eqs. (98) and (172), respectively.

We next consider the QSVT-based FPAA. The target state is, as in the case of the generalized YK decoder, given by $|\omega_{\mathrm{targ}}\rangle^{RER'E'}$ in Eq. (118). Recall that this state satisfies

$$\frac{1}{2} \|\omega_{\mathrm{targ}}^{RR'} - \Phi^{RR'}\|_1 \leq \sqrt{\epsilon}, \tag{186}$$

when the decoupling condition is satisfied with an error ϵ. Let $\tilde{\Pi}_1^{E'R'\hat{F}\hat{B}}$ and $\tilde{\Pi}_2^{\hat{F}\hat{B}B'}$ be projectors defined by

$$\tilde{\Pi}_1^{E'R'\hat{F}\hat{B}} := (U_{\mathcal{F}}^{\hat{L}})^\dagger (|\Phi\rangle\langle\Phi|^{\hat{E}E'} \otimes \mathbb{I}^D) U_{\mathcal{F}}^{\hat{L}}, \tag{187}$$

$$\tilde{\Pi}_2^{\hat{F}\hat{B}B'} := |0\rangle\langle 0|^{\hat{F}} \otimes |\Phi\rangle\langle\Phi|^{\hat{B}B'}. \tag{188}$$

From a similar calculation to the case of the generalized YK decoder, we obtain

$$(\tilde{\Pi}_1 \tilde{\Pi}_2 \tilde{\Pi}_1)^{E'R'\hat{F}\hat{B}B'} = \frac{d_A}{d_E} \tilde{\omega}_0^{E'R'\hat{F}\hat{B}B'}. \tag{189}$$

Then, letting $\tilde{\Lambda}^{E'R'\hat{F}\hat{B}B'} = (\tilde{\Pi}_2 \tilde{\Pi}_1)^{E'R'\hat{F}\hat{B}B'}$, it follows that

$$\begin{aligned} &(\tilde{\Lambda}\tilde{\Lambda}^\dagger \tilde{\Lambda})^{E'R'\hat{F}\hat{B}B'} \\ &= |0\rangle\langle 0|^{\hat{F}} \otimes |\Phi\rangle\langle\Phi|^{\hat{B}B'} \frac{d_A}{d_E} \omega_0^{E'R'\hat{F}\hat{B}B'} \qquad (190) \\ &= \sum_{\mu=1}^{r} \left(\frac{d_A \lambda_\mu}{d_E}\right)^{3/2} |\eta_\mu^*\rangle^{E'R'} \\ &\qquad |0\rangle^{\hat{F}} |\Phi\rangle^{\hat{B}B'} \langle \tilde{\psi}_\mu|^{E'R'\hat{F}\hat{B}B'}, \qquad (191) \end{aligned}$$

where we used Eqs. (182), (185), and (189). Hence, the Schmidt decomposition of $\tilde{\Lambda}^{E'R'\hat{F}\hat{B}B'}$ is uniquely determined as

$$\tilde{\Lambda}^{E'R'\hat{F}\hat{B}B'} = \sum_{\mu=1}^{r} \sqrt{\frac{d_A \lambda_\mu}{d_E}} |\eta_\mu^*\rangle^{E'R'} |0\rangle^{\hat{F}} |\Phi\rangle^{\hat{B}B'} \langle \tilde{\psi}_\mu|^{E'R'\hat{F}\hat{B}B'}. \tag{192}$$

By the QSVT-based FPAA algorithm with appropriately chosen $\phi \in (-\pi, \pi]^t$, we obtain a block-encoding $\tilde{G}_{t,\phi}^{E'R'\hat{F}\hat{B}B'H}$ of the operator

$$\begin{aligned} &\mathrm{sign}(\tilde{\Lambda}^{E'R'\hat{F}\hat{B}B'}) \otimes |0\rangle\langle 0|^H \\ &= \sum_{\mu=1}^{r} |\eta_\mu^*\rangle^{E'R'} |0\rangle^{\hat{F}} |\Phi\rangle^{\hat{B}B'} \langle \tilde{\psi}_\mu|^{E'R'\hat{F}\hat{B}B'} \otimes |0\rangle\langle 0|^H. \end{aligned} \tag{193}$$

This operator maps the state $|\tilde{\psi}_\mu\rangle^{E'R'\hat{F}\hat{B}B'} |0\rangle^H$ to $|\eta_\mu^*\rangle^{E'R'} |0\rangle^{\hat{F}} |\Phi\rangle^{\hat{B}B'} |0\rangle^H$ for each μ. Hence, the transformation:

$$\begin{aligned} &|\tilde{\omega}_0\rangle^{REE'R'\hat{F}\hat{B}B'} |0\rangle^H \\ &\qquad \mapsto |\omega_{\mathrm{targ}}\rangle^{REE'R'} |0\rangle^{\hat{F}} |\Phi\rangle^{\hat{B}B'} |0\rangle^H, \end{aligned} \tag{194}$$

is approximately achieved. By a similar technique to the generalized YK decoder, we can conclude that the Petz-like decoder $\tilde{\mathcal{D}}_{t,\phi}$ achieves

$$\frac{1}{2} \|\tilde{\mathcal{D}}_{t,\phi}^{DB'\to R'}(\omega^{RDB'}) - \omega_{\mathrm{targ}}^{RR'}\| \leq \sqrt{\delta}, \tag{195}$$

for $\delta \in (0, 1/2)$, where t is any odd number satisfying

$$t \geq \left\lceil 8e \sqrt{\frac{d_E}{d_A \lambda_{\min}(\omega^{RE})}} \log(2/\delta) \right\rceil. \tag{196}$$

We here used that $\lambda_{\min} = \lambda_{\min}(\omega^{RE})$. From Eqs. (186) and (195), by using the triangle inequality, the recovery error by the Petz-like decoder is evaluated as

$$\frac{1}{2} \|\tilde{\mathcal{D}}_{t,\phi}^{DB'\to R'}(\omega^{RDB'}) - \Phi^{RR'}\|_1 \leq \sqrt{\epsilon} + \sqrt{2\delta}. \tag{197}$$

Finally, since $\tilde{\Pi}_1^{E'R'\hat{F}\hat{B}}$ and $\tilde{\Pi}_2^{\hat{F}\hat{B}B'}$ are explicitly given by Eqs. (187) and (188), respectively, the complexity of the Petz-like decoder can be evaluated similarly to the generalized YK decoder. The circuit complexity of $\mathrm{C}_{\tilde{\Pi}_1}\mathrm{NOT}$ is

$$\mathcal{O}\Big(\mathcal{C}(U_{\mathcal{F}}) + \log d_E\Big), \tag{198}$$

and that of $\mathrm{C}_{\tilde{\Pi}_2}\mathrm{NOT}$ is

$$\mathcal{O}\big(\log d_B d_F\big). \tag{199}$$

Since they are applied $\mathcal{O}(t)$ times in the Petz-like decoder, the total complexity is given by

$$\mathcal{O}\Big(t(\mathcal{C}(U_{\mathcal{F}}) + \log\left(d_E d_B d_F\right))\Big), \tag{200}$$

with $\mathcal{O}\big(\log\left(d_E d_B d_F\right)\big)$ ancilla qubits.

By using $d_A d_B d_F = d_E d_D$ and rescaling δ to $\delta^2/2$, Theorem 5 is obtained.

5 Summary and outlooks

In this paper, we have presented two decoders applicable to arbitrary noisy channels with explicit circuit implementations: the generalized YK decoder and the Petz-like decoder. Both decoders can recover quantum information when the decoupling condition is satisfied, and they are applicable to entanglement-assisted and non-assisted settings. They are thus among the first few explicit decoders that can be used to asymptotically achieve communication rates arbitrarily close to the quantum capacity or the entanglement-assisted quantum capacity, with suitably chosen encoders.

Both decoders are constructed in two steps: first we consider a decoding protocol with measurement and post-selection, and then replace the measurement with the QSVT-based FPAA algorithm to construct the decoder. The two-step construction does not work with other AA-type algorithms. Hence, our constructions of decoders provide an explicit example that fully leverages and highlights the unique strength of the QSVT-based FPAA in a practical problem.

We have also investigated their circuit complexity, showing that both decoders significantly reduce the computational cost compared to the previously known algorithmic implementation of the Petz recovery map. Moreover, we have shown that the generalized YK decoder has smaller complexity than the Petz-like decoder in many situations.

As a future direction, investigating protocols in the presence of circuit-level noise, i.e., noise that occurs during operations, is important. Since it is common, in studies of theoretical limits such as the quantum capacity, to assume that every operation except for the noisy channel can be realized noiselessly, we focused on the situation without the circuit-level noise. On the other hand, research that takes the circuit-level noise into account is also emerging [87]. In our protocol, the QSVT-based FPAA may suffer from noisy operations, as mentioned in [41], since the effect of the noise may accumulate by iterating the operations. To avoid the accumulation, it is desirable to iterate the operations as few times as possible. Recalling that the number of iterations in the generalized YK decoder is related to the amount of the pre-shared entanglement (see Eq. (46)), the error accumulation is also related to the noise on the pre-share entanglement, making the investigation non-trivial. It is interesting to estimate the performance of the proposed decoders in the presence of the circuit-level noise.

From a theoretical viewpoint, it may also be interesting to address the question about whether a similar approach to that in this work functions for recovering *classical* [88, 89] or *hybrid* [90–93] information. In the former, the encoded information is classical, and the decoder is simply given by a quantum measurement. In the latter, the information is a mixture of classical and quantum, which can be decoded by the simultaneous use of a quantum measurement and a quantum decoder. In these cases, a couple of quantum measurements are known to work well, such as the pretty-good measurement [89, 94]. Our approach adapted to these settings may provide a better decoding performance.

Another direction is to relax the assumptions on the knowledge of the noisy channel [95]. While general decoders, including the proposed decoders, are constructed based on the assumption that we know the description of the noisy channel, it would not be realistic to obtain complete knowledge of the noise. If we can relax the assumption, the decoders may become more useful.

These decoders may also have potential use in

fundamental physics for exploring exotic quantum many-body phenomena that are related to the recovery of quantum information. For instance, the proposed decoders could be potentially applied to reconstructing the internal structure of a black hole from the noisy Hawking radiation [96], and to recovering the bulk structure from a part of the boundaries, such as the entanglement wedge reconstruction [97]. This is also an intriguing direction of studies with the decoders.

Acknowledgments

T. U. and Y. N. were supported by JST CREST Grant Number JPMJCR23I3. T. U. was supported by JST SPRING Grant Number JPMJSP2108. Y. N. was supported by MEXT-JSPS Grant-in-Aid for Transformative Research Areas (A) "Extreme Universe" Grant Numbers JP21H05182 and JP21H05183, by JSPS KAKENHI Grant Number JP22K03464, and JST PRESTO Grant Number JPMJPR2456. The authors thank Takaya Matsuura, Shiro Tamiya, and Ryuji Takagi for valuable discussions.

References

[1] Patrick Hayden and John Preskill. "Black holes as mirrors: quantum information in random subsystems". J. High Energy Phys. **2007**, 120 (2007).

[2] Daniel Harlow and Patrick Hayden. "Quantum computation vs. firewalls". J. High Energy Phys. **2013**, 1–56 (2013).

[3] Yoshifumi Nakata, Eyuri Wakakuwa, and Masato Koashi. "Black holes as clouded mirrors: the Hayden-Preskill protocol with symmetry". Quantum **7**, 928 (2023).

[4] Fernando Pastawski, Beni Yoshida, Daniel Harlow, and John Preskill. "Holographic quantum error-correcting codes: toy models for the bulk/boundary correspondence". J. High Energy Phys. **2015**, 1–55 (2015).

[5] Ahmed Almheiri, Xi Dong, and Daniel Harlow. "Bulk locality and quantum error correction in AdS/CFT". J. High Energy Phys. **2015**, 1–34 (2015).

[6] Eric Dennis, Alexei Kitaev, Andrew Landahl, and John Preskill. "Topological quantum memory". J. Math. Phys. **43**, 4452–4505 (2002).

[7] Alexei Kitaev. "Fault-tolerant quantum computation by anyons". Ann. Phys. **303**, 2–30 (2003).

[8] Alexei Kitaev. "Anyons in an exactly solved model and beyond". Ann. Phys. **321**, 2–111 (2006).

[9] Pavan Hosur, Xiao-Liang Qi, Daniel A. Roberts, and Beni Yoshida. "Chaos in quantum channels". J. High Energy Phys. **2016**, 1–49 (2016).

[10] Daniel A. Roberts and Beni Yoshida. "Chaos and complexity by design". J. High Energy Phys. **2017**, 1–64 (2017).

[11] Yoshifumi Nakata and Masaki Tezuka. "Hayden-Preskill recovery in Hamiltonian systems". Phys. Rev. Res. **6**, L022021 (2024).

[12] Patrick Hayden, Michał Horodecki, Andreas Winter, and Jon Yard. "A decoupling approach to the quantum capacity". Open Syst. Inf. Dyn. **15**, 7–19 (2008).

[13] Frédéric Dupuis. "The decoupling approach to quantum information theory". PhD thesis. University of Montreal. (2010).

[14] Frédéric Dupuis, Mario Berta, Jürg Wullschleger, and Renato Renner. "One-shot decoupling". Commun. Math. Phys. **328**, 251–284 (2014).

[15] Frédéric Dupuis, Ashutosh Goswami, Mehdi Mhalla, and Valentin Savin. "Polarization of quantum channels using Clifford-based channel combining". IEEE Trans. Inf. Theory **67**, 2857–2877 (2021).

[16] Joseph M. Renes. "Belief propagation decoding of quantum channels by passing quantum messages". New J. Phys. **19**, 072001 (2017).

[17] Narayanan Rengaswamy, Kaushik P. Seshadreesan, Saikat Guha, and Henry D. Pfister. "Belief propagation with quantum messages for quantum-enhanced classical communications". npj Quantum Inf. **7**, 97 (2021).

[18] Christophe Piveteau and Joseph M. Renes. "Quantum message-passing algorithm for optimal and efficient decoding". Quantum **6**, 784 (2022).

[19] Joseph M. Renes. "The physics of quantum information: Complementarity, uncertainty, and entanglement". Int. J. Quantum Inf. **11**, 1330002 (2013).

[20] Joseph M. Renes. "Quantum information

theory: Concepts and methods". De Gruyter Oldenbourg. Berlin, Boston (2022).

[21] Howard Barnum and Emanuel Knill. "Reversing quantum dynamics with near-optimal quantum and classical fidelity". J. Math. Phys. **43**, 2097–2106 (2002).

[22] Joseph M. Renes. "Uncertainty relations and approximate quantum error correction". Phys. Rev. A **94**, 032314 (2016).

[23] Yoshifumi Nakata, Takaya Matsuura, and Masato Koashi. "Decoding general error correcting codes and the role of complementarity". npj Quantum Inf. **11**, 4 (2025).

[24] Dénes Petz. "Sufficient subalgebras and the relative entropy of states of a von Neumann algebra". Commun. Math. Phys. **105**, 123–131 (1986).

[25] Dénes Petz. "Sufficiency of channels over von Neumann algebras". Q. J. Math. **39**, 97–108 (1988).

[26] Salman Beigi, Nilanjana Datta, and Felix Leditzky. "Decoding quantum information via the Petz recovery map". J. Math. Phys. **57**, 082203 (2016).

[27] Beni Yoshida. "Decoding the entanglement structure of monitored quantum circuits" (2021). arXiv:2109.08691.

[28] András Gilyén, Seth Lloyd, Iman Marvian, Yihui Quek, and Mark M. Wilde. "Quantum algorithm for Petz recovery channels and pretty good measurements". Phys. Rev. Lett. **128**, 220502 (2022).

[29] Debjyoti Biswas, Gaurav M. Vaidya, and Prabha Mandayam. "Noise-adapted recovery circuits for quantum error correction". Phys. Rev. Res. **6**, 043034 (2024).

[30] Yasuaki Nakayama, Akihiro Miyata, and Tomonori Ugajin. "The Petz (lite) recovery map for scrambling channel". Prog. Theor. Exp. Phys. **2023**, 123B04 (2023).

[31] Beni Yoshida and Alexei Kitaev. "Efficient decoding for the Hayden-Preskill protocol" (2017). arXiv:1710.03363.

[32] Lov K. Grover. "A fast quantum mechanical algorithm for database search". In Proc. the 28th ACM STOC. Pages 212–219. (1996).

[33] Gilles Brassard and Peter Høyer. "An exact quantum polynomial-time algorithm for simon's problem". In Proc. the 5th ISTCS. Pages 12–23. IEEE (1997).

[34] Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. "Quantum amplitude amplification and estimation". Contemp. Math. **305**, 53–74 (2002).

[35] Ran Li, Xuanhua Wang, Kun Zhang, and Jin Wang. "Information retrieval from Hawking radiation in the non-isometric model of black hole interior: Theory and quantum simulation". Phys. Rev. D **109**, 044005 (2024).

[36] Ran Li and Jin Wang. "Quantum information recovery from a black hole with a projective measurement". Phys. Rev. D **110**, 026010 (2024).

[37] Lov K. Grover. "Fixed-point quantum search". Phys. Rev. Lett. **95**, 150501 (2005).

[38] Scott Aaronson and Paul Christiano. "Quantum money from hidden subspaces". In Proc. the 44th ACM STOC. Pages 41–60. (2012).

[39] Theodore J. Yoder, Guang Hao Low, and Isaac L. Chuang. "Fixed-point quantum search with an optimal number of queries". Phys. Rev. Lett. **113**, 210501 (2014).

[40] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. "Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics". In Proc. the 51st ACM SIGACT STOC. Pages 193–204. (2019).

[41] András Gilyén. "Quantum singular value transformation & its algorithmic applications". PhD thesis. University of Amsterdam. (2019). url: https://hdl.handle.net/11245.1/20e9733e-6014-402d-afa9-20f3cc4a0568.

[42] John M. Martyn, Zane M. Rossi, Andrew K. Tan, and Isaac L. Chuang. "Grand unification of quantum algorithms". PRX Quantum **2**, 040203 (2021).

[43] Robert T. Powers and Erling Størmer. "Free states of the canonical anticommutation relations". Commun. Math. Phys. **16**, 1–33 (1970).

[44] Fuad Kittaneh and Hideki Kosaki. "Inequalities for the Schatten p-norm V". Publ. Res. Inst. Math. Sci. **23**, 433–443 (1987).

[45] Alexander Vardy. "The intractability of computing the minimum distance of a code". IEEE Trans. Inf. Theory **43**, 1757–1766 (1997).

[46] Kao-Yueh Kuo and Chung-Chin Lu. "On the hardness of decoding quantum stabilizer codes under the depolarizing channel".

In Proc. the ISITA 2012. Pages 208–211. (2012). url: https://ieeexplore.ieee.org/document/6400919.

[47] Pavithran Iyer and David Poulin. "Hardness of decoding quantum stabilizer codes". IEEE Trans. Inf. Theory **61**, 5209–5223 (2015).

[48] Armin Uhlmann. "The "transition probability" in the state space of a $*$-algebra". Rep. Math. Phys. **9**, 273–279 (1976).

[49] Christopher A. Fuchs and Jeroen van de Graaf. "Cryptographic distinguishability measures for quantum-mechanical states". IEEE Trans. Inf. Theory **45**, 1216–1227 (1999).

[50] John Watrous. "The theory of quantum information". Cambridge University Press. (2018).

[51] Dennis Kretschmann and Reinhard F. Werner. "Tema con variazioni: quantum channel capacity". New J. Phys. **6**, 26 (2004).

[52] Igor Devetak. "The private classical capacity and quantum capacity of a quantum channel". IEEE Trans. Inf. Theory **51**, 44–55 (2005).

[53] Sumeet Khatri and Mark M. Wilde. "Principles of quantum communication theory: a modern approach" (2024). arXiv:2011.04672.

[54] W. Forrest Stinespring. "Positive functions on C^*-algebras". Proc. Am. Math. Soc. **6**, 211–216 (1955).

[55] Seth Lloyd. "Capacity of the noisy quantum channel". Phys. Rev. A **55**, 1613 (1997).

[56] Howard Barnum, Michael A. Nielsen, and Benjamin Schumacher. "Information transmission through a noisy quantum channel". Phys. Rev. A **57**, 4153–4175 (1998).

[57] Howard Barnum, Emanuel Knill, and Michael A. Nielsen. "On quantum fidelities and channel capacities". IEEE Trans. Inf. Theory **46**, 1317–1329 (2000).

[58] Peter W. Shor. "The quantum channel capacity and coherent information". Lecture notes, MSRI Workshop on Quantum Computation (2002).

[59] Mark M. Wilde. "Quantum information theory". Cambridge University Press. (2013).

[60] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. "Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem". IEEE Trans. Inf. Theory **48**, 2637–2655 (2002).

[61] Charles H. Bennett, Igor Devetak, Aram W. Harrow, Peter W. Shor, and Andreas Winter. "The quantum reverse Shannon theorem and resource tradeoffs for simulating quantum channels". IEEE Trans. Inf. Theory **60**, 2926–2959 (2014).

[62] Rochus Klesse. "Approximate quantum error correction, random codes, and quantum channel capacity". Phys. Rev. A **75**, 062315 (2007).

[63] John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen. "Unitary complexity and the Uhlmann transformation problem" (2023). arXiv:2306.13073.

[64] Takeru Utsumi, Yoshifumi Nakata, Qisheng Wang, and Ryuji Takagi. "Quantum algorithms for Uhlmann transformation" (2025). arXiv:2509.03619.

[65] Hui Khoon Ng and Prabha Mandayam. "Simple approach to approximate quantum error correction based on the transpose channel". Phys. Rev. A **81**, 062342 (2010).

[66] Lea Lautenbacher, Fernando de Melo, and Nadja K. Bernardes. "Approximating invertible maps by recovery channels: optimality and an application to non-Markovian dynamics". Phys. Rev. A **105**, 042421 (2022).

[67] Gilles Brassard. "Searching a quantum phone book". Science **275**, 627–628 (1997).

[68] Guang Hao Low and Isaac L. Chuang. "Hamiltonian simulation by qubitization". Quantum **3**, 163 (2019).

[69] Jeongwan Haah. "Product decomposition of periodic functions in quantum signal processing". Quantum **3**, 190 (2019).

[70] Rui Chao, Dawei Ding, András Gilyén, Cupjin Huang, and Mario Szegedy. "Finding angles for quantum signal processing with machine precision" (2020). arXiv:2003.02831.

[71] Yulong Dong, Xiang Meng, K. Birgitta Whaley, and Lin Lin. "Efficient phase-factor evaluation in quantum signal processing". Phys. Rev. A **103**, 042419 (2021).

[72] Lin Lin. "Lecture notes on quantum algorithms for scientific computation". Lecture notes, University of California, Berke-

ley (2022). Available at https://math.berkeley.edu/~linlin/qasc/.

[73] Kaoru Mizuta and Keisuke Fujii. "Recursive quantum eigenvalue and singular-value transformation: analytic construction of matrix sign function by newton iteration". Phys. Rev. Res. **6**, L012007 (2024).

[74] Guang Hao Low and Isaac L. Chuang. "Hamiltonian simulation by uniform spectral amplification" (2017). arXiv:1707.05391.

[75] Lin Lin and Yu Tong. "Near-optimal ground state preparation". Quantum **4**, 372 (2020).

[76] John M. Martyn, Yuan Liu, Zachary E. Chin, and Isaac L Chuang. "Efficient fully-coherent quantum signal processing algorithms for real-time dynamics simulation". J. Chem. Phys. **158**, 024106 (2023).

[77] Kosuke Mitarai, Kiichiro Toyoizumi, and Wataru Mizukami. "Perturbation theory with quantum signal processing". Quantum **7**, 1000 (2023).

[78] Kiichiro Toyoizumi, Naoki Yamamoto, and Kazuo Hoshino. "Hamiltonian simulation using the quantum singular-value transformation: complexity analysis and application to the linearized Vlasov-Poisson equation". Phys. Rev. A **109**, 012430 (2024).

[79] Robert M. Corless, Gaston H. Gonnet, D. E. G. Hare, David J. Jeffrey, and Donald E. Knuth. "On the Lambert W function". Adv. Comput. Math. **5**, 329–359 (1996).

[80] Mehdi Hassani. "Approximation of the Lambert W function". RGMIA Res. Rep. Coll. **8**, 4 (2005). url: https://vuir.vu.edu.au/18113/.

[81] Abdolhossein Hoorfar and Mehdi Hassani. "Inequalities on the Lambert function and hyperpower function". JIPAM **9**, Article 51, 5 (2008). url: https://dornsife.usc.edu/sergey-lototsky/wp-content/uploads/sites/211/2023/12/LambertW-Ineq.pdf.

[82] Alexei Kitaev. "Quantum computations: algorithms and error correction". Russian Math. Surveys **52**, 1191–1249 (1997).

[83] John Watrous. "Notes on super-operator norms induced by Schatten norms". Quantum Inf. Comput. **5**, 58–68 (2005). url: https://dl.acm.org/doi/10.5555/2011608.2011614.

[84] Andreas Winter. ""extrinsic" and "intrinsic" data in quantum measurements: Asymptotic convex decomposition of positive operator valued measures". Commun. Math. Phys. **244**, 157–185 (2004).

[85] Koenraad M. R. Audenaert. "Comparisons between quantum state distinguishability measures". Quantum Inf. Comput. **14**, 31–38 (2014).

[86] Michael A. Nielsen and Isaac L. Chuang. "Quantum computation and quantum information". Cambridge University Press. (2010).

[87] Matthias Christandl and Alexander Müller-Hermes. "Fault-tolerant coding for quantum communication". IEEE Trans. Inf. Theory **70**, 282–317 (2024).

[88] Benjamin Schumacher and Michael D. Westmoreland. "Sending classical information via noisy quantum channels". Phys. Rev. A **56**, 131 (1997).

[89] Alexander S. Holevo. "The capacity of the quantum channel with general signal states". IEEE Trans. Inf. Theory **44**, 269–273 (1998).

[90] Igor Devetak and Peter W. Shor. "The capacity of a quantum channel for simultaneous transmission of classical and quantum information". Commun. Math. Phys. **256**, 287–303 (2005).

[91] Min-Hsiu Hsieh and Mark M. Wilde. "Entanglement-assisted communication of classical and quantum information". IEEE Trans. Inf. Theory **56**, 4682–4704 (2010).

[92] Yoshifumi Nakata, Eyuri Wakakuwa, and Hayata Yamasaki. "One-shot quantum error correction of classical and quantum information". Phys. Rev. A **104**, 012408 (2021).

[93] Eyuri Wakakuwa and Yoshifumi Nakata. "One-shot triple-resource trade-off in quantum channel coding". IEEE Trans. Inf. Theory **69**, 2400–2426 (2023).

[94] Paul Hausladen and William K. Wootters. "A 'pretty good' measurement for distinguishing quantum states". J. Mod. Opt. **41**, 2385–2390 (1994).

[95] Igor Bjelaković, Holger Boche, and Janis Nötzel. "Entanglement transmission and generation under channel uncertainty: universal quantum channel coding". Commun. Math. Phys. **292**, 55–97 (2009).

[96] Ning Bao and Yuta Kikuchi. "Hayden-preskill decoding from noisy hawking radiation". J. High Energy Phys. **02**, 017 (2021).

[97] Chi-Fang Chen, Geoffrey Penington, and Grant Salton. "Entanglement wedge reconstruction using the Petz map". J. High Energy Phys. **2020**, 1–14 (2020).