Quantum Algorithm for Petz Recovery Channels and Pretty Good Measurements

András Gilyén,[1,2,*] Seth Lloyd,[3,†] Iman Marvian,[4,‡] Yihui Quek,[5,§] and Mark M. Wilde[6,7,‖]

[1]*Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, California 91125, USA*
[2]*Simons Institute for the Theory of Computing, Berkeley, California 94720, USA*
[3]*Department of Mechanical Engineering and Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*
[4]*Department of Physics and Department of Electrical and Computer Engineering, Duke University, Durham, North Carolina 27708, USA*
[5]*Information Systems Laboratory, Stanford University, Stanford, California 94305, USA*
[6]*Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, and Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA*
[7]*Stanford Institute for Theoretical Physics, Stanford University, Stanford, California 94305, USA*

(Received 21 July 2020; revised 14 March 2022; accepted 7 April 2022; published 1 June 2022)

The Petz recovery channel plays an important role in quantum information science as an operation that approximately reverses the effect of a quantum channel. The pretty good measurement is a special case of the Petz recovery channel, and it allows for near-optimal state discrimination. A hurdle to the experimental realization of these vaunted theoretical tools is the lack of a systematic and efficient method to implement them. This Letter sets out to rectify this lack: Using the recently developed tools of quantum singular value transformation and oblivious amplitude amplification, we provide a quantum algorithm to implement the Petz recovery channel when given the ability to perform the channel that one wishes to reverse. Moreover, we prove that, in some sense, our quantum algorithm's usage of the channel implementation cannot be improved by more than a quadratic factor. Our quantum algorithm also provides a procedure to perform pretty good measurements when given multiple copies of the states that one is trying to distinguish.

DOI: 10.1103/PhysRevLett.128.220502

Introduction.—Pretty good measurements [1–5] and Petz recovery channels [6–10] are workhorses of quantum information theory: They are used ubiquitously to prove basic results in quantum communication and measurement [11]. Although important for attaining quantum channel capacities [12–16] and performing state discrimination [1–4,9], these useful theoretical constructions are less common in experiment, for the simple reason that there has not been a systematic method for performing them efficiently in practice. Our goal here is to fill this gap.

The Petz recovery channel was introduced in the context of quantum sufficiency in Refs. [6,7] and later rediscovered in Ref. [9] in the context of quantum error correction. It can be understood as a critical part of a quantum version of the Bayes theorem (see Sec. IV in Ref. [17]). To review it, let us begin with the classical case. A classical channel with input system X and output system Y over the alphabets $\mathcal{X}$, $\mathcal{Y}$ is a conditional probability distribution $\{p_{Y|X}(y|x)\}_{x\in\mathcal{X},y\in\mathcal{Y}}$. We consider a probability distribution $p_X(x)$ over the alphabet $\mathcal{X}$ as the input to the channel. It then follows from the Bayes theorem that $p_X(x)p_{Y|X}(y|x) = p_Y(y)p_{X|Y}(x|y)$, where $p_Y(y) = \sum_x p_X(x)p_{Y|X}(y|x)$. Hence, for all $x \in \mathcal{X}, y \in \mathcal{Y}$, we define the "reversal channel" via the formula

$$p_{X|Y}(x|y) = \frac{p_X(x)p_{Y|X}(y|x)}{\sum_x p_X(x)p_{Y|X}(y|x)}. \tag{1}$$

This channel acts on the output system Y. If the particular distribution $p_Y(y)$ defined above is "sent in" through this channel, then the input $p_X(x)$ is recovered perfectly: $p_X(x) = \sum_y p_{X|Y}(x|y)p_Y(y)$. The computation of the reversal channel $p_{X|Y}(x|y)$ requires a specification of the input probability distribution $p_X(x)$ and the forward channel $p_{Y|X}(y|x)$. The Petz recovery channel is a quantum generalization of the reversal channel above: It is a function of a quantum channel $\mathcal{N}$ and an input state σ to the channel, with the former generalizing $p_{Y|X}(y|x)$ and the latter $p_X(x)$. We discuss it in more detail in what follows.

The Petz recovery channel appears often in quantum information as a proof tool, showing that near-optimal recovery from undesired quantum operations is possible. Reference [9] demonstrated how this recovery channel can be an effective means for reversing the effects of noise. Thereafter, Ref. [18] showed that the Petz recovery channel (therein called "transpose channel") is a universal recovery operation for approximate quantum error correction, which

performs comparably to the best possible one in terms of worst-case fidelity (see also [19,20]). The Petz recovery channel also goes by the name "pretty good recovery," as used in Refs. [21,22], due to the result of Ref. [9]. Yet another application comes from the field of quantum communication: Reference [16] showed explicitly how to use the Petz recovery channel in a decoder to achieve the coherent information rate of quantum communication. It has also found use in developing physically meaningful refinements of quantum entropy inequalities [23–27]. See [28–32] for further uses.

As an application of our results, our quantum algorithm can be used to implement the pretty good measurement (PGM) [1–5]. This measurement was used in Refs. [12,15] as part of a coding scheme to approach the Holevo information rate for classical communication over a quantum channel. It has also been instrumental in proving bounds for quantum algorithms. Reference [33] showed that the PGM is an optimal measurement for solving the dihedral hidden subgroup problem and that it is helpful in proving a lower bound on the sample complexity of this problem. Similar techniques have been used for quantum probably-approximately-correct learning [34]. Reference [35] showed how to implement the PGM for pure states, while our algorithm for Petz recovery channels is capable of performing the PGM in the general case.

We now begin the technical part of our Letter, starting with an explicit description of the Petz recovery channel and the resources that we work with for its implementation.

Petz recovery channel.—The Petz recovery channel is a function of a quantum state σ_A on a system A and a quantum channel $\mathcal{N}_{A\to B}$ taking system A to a system B. It is given explicitly as follows [10]:

$$\mathcal{P}^{\sigma,\mathcal{N}}_{B\to A}(\omega_B) := \sigma_A^{1/2}\mathcal{N}^\dagger(\mathcal{N}(\sigma_A)^{-1/2}\omega_B\mathcal{N}(\sigma_A)^{-1/2})\sigma_A^{1/2}, \quad (2)$$

where $\mathcal{N}^\dagger$ is the Hilbert-Schmidt adjoint [11] of the channel $\mathcal{N}$ and we have omitted the system labels of $\mathcal{N}_{A\to B}$ for brevity.

It is a composition of three completely positive maps:

$$(\cdot) \to [\mathcal{N}(\sigma_A)]^{-1/2}(\cdot)[\mathcal{N}(\sigma_A)]^{-1/2}, \quad (3)$$

$$(\cdot) \to \mathcal{N}^\dagger(\cdot), \quad (4)$$

$$(\cdot) \to \sigma_A^{1/2}(\cdot)\sigma_A^{1/2}. \quad (5)$$

None of these maps are trace preserving individually, but overall the map in Eq. (2) is trace preserving on the support of the state $\mathcal{N}(\sigma_A)$ [23]. We note here that the main idea behind our algorithm is to implement the Petz recovery channel as a composition of the three maps given in Eqs. (3)–(5), while taking into account the fact that the overall map in Eq. (2) is trace preserving in order to implement it deterministically with some desired accuracy.

Block encoding.—The Petz recovery channel depends on the state σ_A, and so our algorithm needs some form of access to it. In order to cover a wide range of scenarios, we employ the block-encoding formalism, which generalizes the most common input models for matrices used in quantum algorithms [36,37].

Let $\|\cdot\|$ denote the spectral norm of a matrix (also known as the Schatten ∞-norm). For a complex matrix A and $\alpha \geq \|A\|$, the matrix A/α can be represented as the upper-left block of a unitary matrix:

$$U = \begin{bmatrix} A/\alpha & \cdot \\ \cdot & \cdot \end{bmatrix} \Leftrightarrow A = \alpha(\langle 0| \otimes I)U(|0\rangle \otimes I). \quad (6)$$

The unitary matrix U is said to be a *block encoding* of A. Henceforth, we do not write identity operators explicitly, but we instead include system subscripts as a guide. If the linear map A/α acts on a qubits, then the unitary U can be thought of as a probabilistic implementation of this map: Given an a-qubit input state $|\psi\rangle$, applying the unitary U to the state $|0\rangle|\psi\rangle$, measuring the first system, and postselecting on the $|0\rangle$ outcome, the second system contains a state proportional to $A|\psi\rangle/\alpha$.

This generalizes the two most relevant input models in our case. If we are given copies of the quantum state σ_A, then we can implement an (approximate) block encoding of σ_A by using density matrix exponentiation [38,39] and "taking the logarithm" of the time evolution [37]. Alternatively, if we have access to a quantum circuit U^σ_{RA} that prepares a purification $|\psi^\sigma\rangle_{RA} := U^\sigma_{RA}|0\rangle_R|0\rangle_A$ of σ_A, such that $\mathrm{Tr}_R[|\psi^\sigma\rangle\langle\psi^\sigma|_{RA}] = \sigma_A$, then we can directly implement an exact block encoding of σ_A with only two uses of U^σ_{RA} as follows [36,37]:

$$V^\sigma_{RAA'} := (U^\sigma_{RA})^\dagger(I_R \otimes \mathrm{SWAP}_{AA'})U^\sigma_{RA} = \begin{bmatrix} \sigma_A & \cdot \\ \cdot & \cdot \end{bmatrix}, \quad (7)$$

where system A' is isomorphic to system A.

Assumptions.—The resources that we use for implementing the Petz recovery channel are as follows: (i) Quantum circuits U^{σ_A} and $U^{\mathcal{N}(\sigma_A)}$ that are (approximate) block encodings of σ_A and $\mathcal{N}(\sigma_A)$, respectively, and (ii) a quantum circuit $U^{\mathcal{N}}_{E'A\to EB}$ that implements the channel $\mathcal{N}$, in the sense that $U^{\mathcal{N}}_{E'A\to EB}|0\rangle_{E'} =: V^{\mathcal{N}}_{A\to EB}$, where $V^{\mathcal{N}}_{A\to EB}$ is an isometric extension of $\mathcal{N}$ satisfying $\mathrm{Tr}_E[V^{\mathcal{N}}_{A\to EB}(\omega_A)(V^{\mathcal{N}}_{A\to EB})^\dagger] = \mathcal{N}(\omega_A)$, for every input density operator ω_A.

We note that, given an efficient description of the channel $\mathcal{N}$ in terms of its Kraus operators, the unitary $U^{\mathcal{N}}_{E'A\to EB}$ can be efficiently implemented on a quantum computer [40]. Also, given copies or "purified access" to σ_A, we can achieve the corresponding access to $\mathcal{N}(\sigma_A)$ after applying $U^{\mathcal{N}}_{E'A\to EB}$, which then results in an efficient block encoding for $\mathcal{N}(\sigma_A)$.

Rewriting the Petz recovery channel.—Equation (4) calls for the application of the adjoint $\mathcal{N}^\dagger$ of the channel $\mathcal{N}$. We now explain how this can be accomplished using $U^{\mathcal{N}}_{E'A\to EB}$. The action of the adjoint on an arbitrary operator ω_B is given by $\mathcal{N}^\dagger(\omega_B) = \langle 0|_{E'} U^{\mathcal{N}\dagger}(I_E \otimes \omega_B) U^{\mathcal{N}} |0\rangle_{E'}$ [11]. Let $\Gamma_{E\tilde{E}} \coloneqq |\Gamma\rangle\langle\Gamma|_{E\tilde{E}}$ denote an operator proportional to the maximally entangled state on E and a reference system $\tilde{E}$, where $|\Gamma\rangle_{E\tilde{E}} \coloneqq \sum_{i=0}^{d_E-1} |i\rangle_E |i\rangle_{\tilde{E}}$ and d_E is the dimension of system E. Then extending the identity operator with $\Gamma_{E\tilde{E}}$, we rewrite the previous identity as

$$\mathcal{N}^\dagger(\omega_B) = \mathrm{Tr}_{\tilde{E}}[\langle 0|_{E'} (U^{\mathcal{N}}_{E'A\to EB})^\dagger (\Gamma_{E\tilde{E}} \otimes \omega_B) U^{\mathcal{N}}_{E'A\to EB} |0\rangle_{E'}]. \tag{8}$$

Now the interpretation of the adjoint map as a probabilistic quantum operation is clear: The adjoint map $\mathcal{N}^\dagger$ acting on the operator ω_B can be applied by tensoring in the maximally entangled state $\Gamma_{E\tilde{E}}/d_E$, performing the inverse of the unitary $U^{\mathcal{N}}$, measuring the system E', accepting if the all-zeros outcome occurs, and, finally, ignoring the system $\tilde{E}$ (which corresponds to tracing it out).

Thus, our plan is to implement the linear extension of the adjoint map, as given in Eq. (8). Sandwiching this between the other two maps in Eqs. (3) and (5) comprising the Petz recovery channel, we obtain the following isometric extension of the Petz recovery channel:

$$V^{\mathcal{P}}_{B\to\tilde{E}A} \coloneqq (\langle 0|_{E'} \otimes I_{\tilde{E}} \otimes \sigma_A^{1/2})(U^{\mathcal{N}}_{E'A\to EB})^\dagger \times (|\Gamma\rangle_{E\tilde{E}} \otimes [\mathcal{N}(\sigma_A)]^{-1/2}). \tag{9}$$

Tracing over $\tilde{E}$ then implements the Petz recovery channel $\mathcal{P}^{\sigma,\mathcal{N}}_{B\to A}(\omega_B)$. Note that, in the rewriting above, the implementation of the adjoint map discussed in the preceding paragraph is no longer contiguous. It proceeds in two phases: the application of the unitary $(U^{\mathcal{N}}_{E'A\to EB})^\dagger$ before multiplication by $\sigma_A^{1/2}$ (which applies Eq. (5)) and the measurement and postselection after that step.

Quantum singular value transformation.—Our implementation is based on quantum singular value transformation (QSVT) [37]. QSVT transforms the singular values of a block-encoded matrix and, thus, provides an efficient means of quantum matrix arithmetic. Often we need to rely on approximations, and so, when doing so, we keep track of the error or precision δ, as well as the subnormalization factor α: We say that U is an (α,δ)-block encoding of A if $\|A - \alpha(\langle 0| \otimes I) U (|0\rangle \otimes I)\| \le \delta$.

In what follows, we manipulate block encodings U^ρ of density operators ρ. The power of QSVT is that it allows for transforming U^ρ to a block encoding of $\tilde{f}(\rho)$, where $\tilde{f}$ is a function applied to the singular values of its argument. More precisely, $\tilde{f}$ denotes a polynomial approximation of some function f; in view of the maps given in Eqs. (3) and (5) above, the particular functions of interest here are $f_1(x) \coloneqq x^{-1/2}$ and $f_2(x) \coloneqq x^{1/2}$.

The complexity of realizing the transformed block-encoding unitary $U^{\tilde{f}(\rho)}$ is stated in terms of the number of uses of U^ρ (which dominates the overall gate complexity), and it depends on the parameters of the functional approximation $\tilde{f}$. For a function f, let $\|f(x)\|_{\mathcal{I}} \coloneqq \sup_{x\in\mathcal{I}} |f(x)|$. Using techniques from Ref. [41], for the two functions above, one can find polynomial approximations $\tilde{f}_1$ and $\tilde{f}_2$ such that $(\theta^{1/2}/2)\|\tilde{f}_1(x) - x^{-1/2}\|_{[\theta,1]} \le \delta$ and $\frac{1}{2}\|\tilde{f}_2(x) - x^{1/2}\|_{[\theta,1]} \le \delta$ for $\theta, \delta \in (0, 1/2]$. If ρ has minimum singular value $\lambda_{\min}$, then it suffices to set $\theta \le \lambda_{\min}$. Since $1/\lambda_{\min}$ behaves like a "condition number" for ρ, being proportional to the difficulty of transforming ρ, we denote it with the symbol κ and employ this notation later. Indeed, using the functional approximations from Refs. [41,41], QSVT achieves the desired transformations up to the errors indicated above, with $\mathcal{O}((1/\theta)\log(1/\delta))$ uses of U^ρ.

The quantum algorithm.—We implement the isometric extension of the Petz recovery channel given in Eq. (9). This consists of applying the maps in Eqs. (3)–(5) sequentially, with the first and third steps employing QSVT. Equation (9) also has a measurement component as the final step, arising from the implementation of the map in Eq. (4). By exploiting the trace-preserving property of the Petz recovery channel, we amplify the probability of success of this measurement (i.e., the projection onto $|0\rangle_{E'}$) using oblivious amplitude amplification [42], which is a special case of QSVT [37]. Overall, the implementation is precise up to ε error in diamond distance [43] (see [11] for a definition of diamond distance). Theorem 1 below states the guarantees of this technique.

Theorem 1.—Let N_σ, $N_{\mathcal{N}(\sigma)}$, and $N_{\mathcal{N}}$ denote the number of elementary quantum gates needed to realize the unitaries U^{σ_A}, $U^{\mathcal{N}(\sigma_A)}$, and $U^{\mathcal{N}}_{E'A\to EB}$, respectively (noting that in our applications $N_{\mathcal{N}(\sigma)} \le N_\sigma + N_{\mathcal{N}}$). Let κ_σ denote an upper bound on the reciprocal of the minimum nonzero eigenvalue of σ_A, and, correspondingly, let $\kappa_{\mathcal{N}(\sigma)}$ denote the same for $\mathcal{N}(\sigma_A)$. There exists a quantum algorithm realizing the channel $\tilde{\mathcal{P}}^{\sigma_A,\mathcal{N}}_{B\to A}$, which is an approximate implementation of the ideal Petz recovery channel in Eq. (2), in the sense that

$$\|\tilde{\mathcal{P}}^{\sigma_A,\mathcal{N}}_{B\to A} - \mathcal{P}^{\sigma_A,\mathcal{N}}_{B\to A}\|_\diamond \le \varepsilon, \tag{10}$$

with gate complexity (up to polylogarithmic factors)

$$\tilde{\mathcal{O}}\left[\sqrt{d_E \kappa_{\mathcal{N}(\sigma)}}[\kappa_{\mathcal{N}(\sigma)} N_{\mathcal{N}(\sigma)} + N_{\mathcal{N}} + N_\sigma \min(\kappa_\sigma, d_E \kappa_{\mathcal{N}(\sigma)}/\varepsilon^2)]\right]. \tag{11}$$

In Eq. (11), d_E is the dimension of the system E, which is not smaller than the Kraus rank of the channel $\mathcal{N}(\cdot)$.

In Supplemental Material [44], we provide a modified algorithm that substitutes the dependence on d_E in Eq. (11) with the rank of the state $\tilde{\mathcal{N}}(\sigma)$, where $\tilde{\mathcal{N}}$ is a channel complementary to $\mathcal{N}$ [11]. For certain choices of $\mathcal{N}$ and σ, this provides a dramatic reduction in the run-time.

We now break the algorithm down into its four steps and analyze each step individually (assuming without loss of generality that $\varepsilon = \mathcal{O}(1)$). We indicate the steps using the numbers (1)–(4).

(1) To simulate the first step of the Petz recovery channel, as described by Eq. (3), we transform the block encoding of $\mathcal{N}(\sigma_A)$ to a $(2\sqrt{\kappa_{\mathcal{N}(\sigma)}}, (\mathcal{O}(\varepsilon)/\sqrt{d_E}))$-block encoding $U_{R'B}^{\tilde{f}_1[\mathcal{N}(\sigma_A)]}$ of $[\mathcal{N}(\sigma_A)]^{-1/2}$ using QSVT, which has gate complexity $\mathcal{O}(\kappa_{\mathcal{N}(\sigma)} N_{\mathcal{N}(\sigma)} \log(d_E/\varepsilon))$. Then the following error bound holds:

$$\|\tilde{f}_1(\mathcal{N}(\sigma_A)) - (\mathcal{N}(\sigma_A))^{-1/2}\| \leq \mathcal{O}(\varepsilon)/\sqrt{d_E}, \quad (12)$$

which suffices for our purposes, as shown later.

(2) Let $\tilde{E}$ be a system with dimension equal to that of E. The second step of the algorithm is simply to prepare the maximally entangled state $|\Phi\rangle_{E\tilde{E}} := |\Gamma\rangle_{E\tilde{E}}/\sqrt{d_E}$ alongside the state prepared above and then apply the unitary $(U_{AE'\to BE}^{\mathcal{N}})^\dagger$. Note that $|\Phi\rangle_{E\tilde{E}}$ is a normalized quantum state, introducing an additional factor of $1/d_E$ in the output density operator, which resurfaces in the subnormalization factor of the overall unitary (see Eq. (15)). The maximally entangled state $|\Phi\rangle_{E\tilde{E}}$ is prepared by means of a unitary $U_{E\tilde{E}}^{\Phi}$ acting on the state $|0\rangle_{E\tilde{E}}$, so that $|\Phi\rangle_{E\tilde{E}} := U_{E\tilde{E}}^{\Phi}|0\rangle_{E\tilde{E}}$. Note that the unitary $U_{E\tilde{E}}^{\Phi}$ is easy to implement. For example, if systems E and $\tilde{E}$ consist of qubits, one can apply Hadamard gates on the qubits of E and CNOT gates between pairs of qubits of E and $\tilde{E}$. In this step, we have described the first half of the procedure for implementing a linear extension of Eq. (4); the final part, which consists of measurement and postselection, is deferred to the fourth step.

(3) The third step of the algorithm is to apply an approximation of the map in Eq. (5) that conjugates the state by $\sigma_A^{1/2}$. Analogous to the first step, we transform the block encoding of σ_A to a $(2, (\mathcal{O}(\varepsilon)/\sqrt{d_E \kappa_{\mathcal{N}(\sigma)}}))$-block encoding $U_{R''A}^{\tilde{f}_2(\sigma_A)}$ of $\tilde{f}_2(\sigma_A)$ using QSVT, which has gate complexity $\mathcal{O}(\kappa_\sigma N_\sigma \log((d_E \kappa_{\mathcal{N}(\sigma)})/\varepsilon))$. Then the following error bound holds:

$$\|\tilde{f}_2(\sigma_A) - \sigma_A^{1/2}\| \leq \mathcal{O}(\varepsilon)/\sqrt{d_E \kappa_{\mathcal{N}(\sigma)}}. \quad (13)$$

We can now apply the unitary $U_{R''A}^{\tilde{f}_2(\sigma_A)}$ to the output of step 2. In detail, letting ρ_A denote the output state of step 2, we tensor in the state $|0\rangle\langle 0|_{R''}$ to the input state ρ_A and perform the unitary $U_{R''A}^{\tilde{f}_2(\sigma_A)}$.

Let us summarize the algorithm up to this point. We have described the addition of auxiliary systems as happening separately in each step. However, we are free to tensor them in to the input state ω_B at the start, enlarging the input state to $|0\rangle\langle 0|_{R''} \otimes |0\rangle\langle 0|_{E\tilde{E}} \otimes |0\rangle\langle 0|_{R'} \otimes \omega_B$. Then to this state, we apply the following product of unitaries:

$$\tilde{W} := U_{R''A}^{\tilde{f}_2(\sigma_A)} (U_{E'A\to EB}^{\mathcal{N}})^\dagger (U_{E\tilde{E}}^{\Phi} \otimes U_{R'B}^{\tilde{f}_1(\mathcal{N}(\sigma_A))}), \quad (14)$$

where $U_{R''A}^{\tilde{f}_2(\sigma_A)}$ and $U_{R'B}^{\tilde{f}_1(\mathcal{N}(\sigma_A))}$ are implemented using QSVT. The unitary $\tilde{W}$ approximates the isometric extension in Eq. (9) and can be represented as the following block encoding:

$$\tilde{W} = \begin{bmatrix} \frac{1}{4}\sqrt{\frac{1}{d_E \kappa_{\mathcal{N}(\sigma)}}}\tilde{V}_{B\to\tilde{E}A}^{\mathcal{P}} & \cdot \\ \cdot & \cdot \end{bmatrix}, \quad (15)$$

where the linear operator $\tilde{V}_{B\to\tilde{E}A}^{\mathcal{P}}$ is an approximate isometric extension of the Petz recovery channel and is defined through its action on a ket $|\psi\rangle_B$ as

$$\tilde{V}_{B\to\tilde{E}A}^{\mathcal{P}}|\psi\rangle_B := \tilde{f}_2(\sigma_A)(V_{A\to EB}^{\mathcal{N}})^\dagger \tilde{f}_1(\mathcal{N}(\sigma_A))|\Gamma\rangle_{E\tilde{E}}|\psi\rangle_B. \quad (16)$$

After applying $\tilde{W}$ to the enlarged input state, we would like to measure the $R''E'R'$ systems and obtain the all-zeros state as the outcome (which corresponds to the top-left block of $\tilde{W}$). Receiving this outcome signals the successful implementation of the desired map $\tilde{V}_{B\to\tilde{E}A}^{\mathcal{P}}$, up to a subnormalization factor of $4\sqrt{\kappa_{\mathcal{N}(\sigma)} d_E}$. To compare this to the ideal isometric extension in Eq. (9), we should account for the accumulated errors due to the approximate implementations of $\mathcal{N}(\sigma_A)^{-1/2}$ and $\sigma_A^{1/2}$ in $\tilde{W}$. It follows that

$$\|\tilde{V}_{B\to\tilde{E}A}^{\mathcal{P}} - V_{B\to\tilde{E}A}^{\mathcal{P}}\| \leq \mathcal{O}(\varepsilon), \quad (17)$$

where $\tilde{V}_{B\to\tilde{E}A}^{\mathcal{P}}$ is defined in Eq. (16) and $V_{B\to\tilde{E}A}^{\mathcal{P}}$ in Eq. (9). To see this, observe that the left-hand side of Eq. (17) can be bounded from above by the following quantity:

$$\begin{aligned} &\|\sigma_A^{1/2} - \tilde{f}_2(\sigma_A)\| \|(V_{A\to EB}^{\mathcal{N}})^\dagger \mathcal{N}(\sigma_A)^{-1/2}|\Gamma\rangle_{E\tilde{E}}\| \\ &+ \|\tilde{f}_2(\sigma_A)(V_{A\to EB}^{\mathcal{N}})^\dagger\| \|\|\Gamma\rangle_{E\tilde{E}}\| \|\mathcal{N}(\sigma_A)^{-1/2} - \tilde{f}_1[\mathcal{N}(\sigma_A)]\|, \end{aligned} \quad (18)$$

which follows from applying the triangle inequality and submultiplicativity of the spectral norm. Noting that $|\Gamma\rangle_{E\tilde{E}}$ is the unnormalized maximally entangled vector, we further bound the following terms:

$$\|(V_{A\to EB}^{\mathcal{N}})^\dagger \mathcal{N}(\sigma_A)^{-1/2}|\Gamma\rangle_{E\tilde{E}}\| \leq \sqrt{d_E \kappa_{\mathcal{N}(\sigma_A)}}, \quad (19)$$

$$\|\tilde{f}_2(\sigma_A)(V_{A\to EB}^{\mathcal{N}})^\dagger\| \|\|\Gamma\rangle_{E\tilde{E}}\| \leq 2\sqrt{d_E}. \quad (20)$$

The second bound follows because $\tilde{f}_2(\sigma_A)$ is a block encoding with norm at most 2. Putting Eqs. (18)–(20) together with the bounds in Eqs. (12) and (13), we conclude an overall error between $V^{\mathcal{P}}$ and $\tilde{V}^{\mathcal{P}}$ of $\mathcal{O}(\varepsilon)$.

(4) Finally, we move on to the last step, which is a measurement of the $R''E'R'$ systems. Equation (15) makes it clear that the probability p_{success} of measuring the all-zeros state, at this point, is approximately $1/(16 d_E \kappa_{\mathcal{N}(\sigma)})$. We would like to amplify this probability, and so we use oblivious amplitude amplification to implement an approximate projection onto this state. This, too, can be achieved using QSVT techniques [37] and requires a number of repetitions of $\tilde{W}$ that scales as $\mathcal{O}(1/\sqrt{p_{\text{success}}})$, which in this case is $N_{\text{rep}} := \mathcal{O}(\sqrt{d_E \kappa_{\mathcal{N}(\sigma)}})$. After applying (robust) oblivious amplitude amplification (see Theorem 28 in Ref. [46]), we obtain a unitary that is a $(1, \mathcal{O}(\varepsilon))$-block encoding of the isometric extension $V^{\mathcal{P}}_{B\to\tilde{E}A}$, providing an $\mathcal{O}(\varepsilon)$-approximate implementation of the Petz recovery channel.

The complexity of our algorithm is given by N_{rep} times the complexity of implementing $\tilde{W}$. As we discussed previously, the cost of implementing the first step in $\tilde{W}$ is $\mathcal{O}(\kappa_{\mathcal{N}(\sigma)} N_{\mathcal{N}(\sigma)} \log(d_E/\varepsilon))$. The complexity of implementing the second step is $\mathcal{O}(N_{\mathcal{N}} + \log d_E)$, where the logarithmic term is the cost of implementing $U^{\Phi}_{E\tilde{E}}$. Finally, the complexity of the third step is $\mathcal{O}(\varepsilon_\sigma N_\sigma \log((d_E \varepsilon_{\mathcal{N}(\sigma)})/\varepsilon))$. An alternative for this last step is to consider choosing a threshold θ higher than $1/\kappa_\sigma$ and approximating the square root function by constant zero below the threshold. Indeed, then choosing $\theta \approx \varepsilon^2/(d_E \kappa_{\mathcal{N}(\sigma)})$ suffices, resulting in the alternative complexity $\mathcal{O}((d_E \kappa_{\mathcal{N}(\sigma)}/\varepsilon^2)) N_\sigma \log((d_E \kappa_{\mathcal{N}(\sigma)}/\varepsilon))$ of the third step.

Lower bounds.—Our algorithm uses the forward channel unitary $U^{\mathcal{N}}_{E'A\to EB}$ about $\mathcal{O}(\sqrt{d_E \kappa_{\mathcal{N}(\sigma)}})$ times. We now prove that there is no generally applicable algorithm that uses $U^{\mathcal{N}}_{E'A\to EB}$ fewer than $\Omega(d_E^{(1/2)-\alpha} \kappa^{\alpha}_{\mathcal{N}(\sigma)})$ times, for all $\alpha \in [0, \frac{1}{2}]$, thereby ruling out the possibility of large improvements on our algorithm that would simultaneously improve the dependence on both parameters d_E and $\kappa_{\mathcal{N}(\sigma)}$.

We consider solving the problem of unstructured search of $N \geq 2$ elements with only a single marked element. Let O be a search oracle that recognizes the single marked element. Let the input state σ_A be the maximally mixed state representing a uniformly random index $i \in [N]$. The forward channel $\mathcal{N}_{A\to B}$ applies the search oracle and outputs its output, which is equal to 1 if i is the marked element and is equal to 0 otherwise. Hence, $\mathcal{N}_{A\to B}(\sigma_A) = \text{diag}(1 - (1/N), (1/N))$ and $\kappa_{\mathcal{N}(\sigma)} = d_E = N$. Let $\mathcal{P}^{\mathcal{N},\sigma_A}$ be the Petz recovery channel defined from $\mathcal{N}$ and σ_A as specified above. Now applying the exact channel $\mathcal{P}^{\mathcal{N},\sigma_A}$ on the state $\omega_B = |1\rangle\langle 1|$ finds the marked element with certainty. Thus, for every constant $c < 1$, applying a c-approximate channel $\tilde{\mathcal{P}}^{\mathcal{N},\sigma_A}$ on ω_B still finds a marked element with probability at least $1 - c$. This requires $\Omega(\sqrt{N}) = \Omega(d_E^{(1/2)-\alpha} \kappa^{\alpha}_{\mathcal{N}(\sigma)})$ uses of O, as the well-known quantum search lower bound states [47].

Pretty good measurement.—One can use our algorithm to implement the pretty good measurement [1–5], which is a special case of the Petz map. In this application, one is given a set $\{\sigma^x_B\}_x$ of states and a probability distribution p_X. Let σ_{XB} denote the following classical-quantum state: $\sigma_{XB} := \sum_x p_X(x)|x\rangle\langle x|_X \otimes \sigma^x_B$. Let $\mathcal{N}_{XB\to B} := \text{Tr}_X$ be the partial trace channel that discards system X.

We now plug these choices into Eq. (2). The adjoint map $(\mathcal{N}_{XB\to B})^\dagger$ appends the identity on system X. Let $\bar{\sigma}_B := \mathcal{N}_{XB\to B}(\sigma_{XB}) = \sum_x p_X(x)\sigma^x_B$. The resulting Petz recovery channel is as follows:

$$\mathcal{P}^{\sigma_{XB},\text{Tr}_X}_{B\to XB}(\omega_B) := \sum_x [x]_X \otimes p_X(x)(\sigma^x_B)^{1/2}(\bar{\sigma}_B)^{-1/2} \times \omega_B(\bar{\sigma}_B)^{-1/2}(\sigma^x_B)^{1/2},$$

which is known as the "pretty good instrument" [23] and where $[x] \equiv |x\rangle\langle x|$. This is a generalization of the pretty good measurement that has a quantum output in addition to the usual classical measurement output; the PGM is obtained by discarding the quantum output.

We check the necessary assumptions for our technique against what is potentially available for experiments. The isometric extension of the channel $\text{Tr}_X(\cdot)$ is simply the identity. If we have copies of σ_{XB}, then our algorithm is applicable, but it is more efficient in the case when we can prepare a purification of σ_{XB}. Applying Theorem 1, we arrive at a quantum algorithm implementing the pretty good instrument with performance guarantees as in Eqs. (10) and (11), where

$$d_E = |X|, \qquad \kappa_{\mathcal{N}(\sigma)} = \kappa_{\bar{\sigma}}, \qquad \kappa_\sigma = \min_x p_X(x)\kappa_{\sigma^x_B}. \quad (21)$$

Conclusion.—We have developed a quantum algorithm for implementing the Petz recovery channel and the pretty good measurement. This solves an important open problem in quantum computation, and, more generally, it opens up a new research paradigm for realizing fully quantum Bayesian inference on quantum computers.

We gratefully acknowledge the Simons Institute for the Theory of Computing, where part of this work was conducted. A. G. acknowledges funding provided by Samsung Electronics Co., Ltd., for the project "The Computational Power of Sampling on Quantum Computers." Additional support was provided by the Institute for Quantum Information and Matter, an NSF Physics Frontiers Center (National Science Foundation Grant No. PHY-1733907). S. L. was funded by ARO, AFOSR, and IARPA. I. M. acknowledges support from the U.S. National Science Foundation under Grant No. 1910571. Y. Q. acknowledges support from a Stanford

QFARM fellowship and from an NUS Overseas Graduate Scholarship. M. M. W. acknowledges support from the U.S. National Science Foundation under Grant No. 1714215, from Stanford QFARM, and from AFOSR under Grant No. FA9550-19-1-0369.

*gilyen@berkeley.edu
†slloyd@mit.edu
‡iman.marvian@duke.edu
§yquek@stanford.edu
‖mwilde@lsu.edu

[1] Viacheslav Belavkin, Optimal distinction of non-orthogonal quantum signals, Radio Eng. Electron. Phys. **20**, 39 (1975).
[2] Viacheslav Belavkin, Optimal multiple quantum statistical hypothesis testing, Stochastics **1**, 315 (1975).
[3] Alexander S. Holevo, On asymptotically optimal hypothesis testing in quantum statistics, Theory Probab. Appl. **23**, 411 (1979).
[4] Paul Hausladen, On the quantum mechanical channel capacity as a function of the density matrix, Bachelor's thesis, Williams College, Williamstown, Massachusetts, 1993.
[5] Paul Hausladen and William K. Wootters, A 'pretty good' measurement for distinguishing quantum states, J. Mod. Opt. **41**, 2385 (1994).
[6] Dénes Petz, Sufficient subalgebras and the relative entropy of states of a von Neumann algebra, Commun. Math. Phys. **105**, 123 (1986).
[7] Dénes Petz, Sufficiency of channels over von Neumann algebras, Q. J. Mech. Appl. Math. **39**, 97 (1988).
[8] Masanori Ohya and Denes Petz, *Quantum Entropy and Its Use* (Springer, New York, 1993).
[9] Howard Barnum and Emanuel Knill, Reversing quantum dynamics with near-optimal quantum and classical fidelity, J. Math. Phys. (N.Y.) **43**, 2097 (2002).
[10] Patrick Hayden, Richard Jozsa, Dénes Petz, and Andreas Winter, Structure of states which satisfy strong subadditivity of quantum entropy with equality, Commun. Math. Phys. **246**, 359 (2004).
[11] Mark M. Wilde, *Quantum Information Theory*, 2nd ed. (Cambridge University Press, Cambridge, England, 2017).
[12] Paul Hausladen, Richard Jozsa, Benjamin Schumacher, Michael Westmoreland, and William K. Wootters, Classical information capacity of a quantum channel, Phys. Rev. A **54**, 1869 (1996).
[13] Alexander S. Holevo, The capacity of the quantum channel with general signal states, IEEE Trans. Inf. Theory **44**, 269 (1998).
[14] Benjamin Schumacher and Michael D. Westmoreland, Sending classical information via noisy quantum channels, Phys. Rev. A **56**, 131 (1997).
[15] Salman Beigi and Amin Gohari, Quantum achievability proof via collision relative entropy, IEEE Trans. Inf. Theory **60**, 7980 (2014).
[16] Salman Beigi, Nilanjana Datta, and Felix Leditzky, Decoding quantum information via the Petz recovery map, J. Math. Phys. (N.Y.) **57**, 082203 (2016).
[17] Matthew S. Leifer and Robert W. Spekkens, Towards a formulation of quantum theory as a causally neutral theory of Bayesian inference, Phys. Rev. A **88**, 052130 (2013).
[18] Hui Khoon Ng and Prabha Mandayam, Simple approach to approximate quantum error correction based on the transpose channel, Phys. Rev. A **81**, 062342 (2010).
[19] Jon Tyson, Two-sided bounds on minimum-error quantum measurement, on the reversibility of quantum dynamics, and on maximum overlap using directional iterates, J. Math. Phys. (N.Y.) **51**, 092204 (2010).
[20] Prabha Mandayam and Hui Khoon Ng, Towards a unified framework for approximate quantum error correction, Phys. Rev. A **86**, 012335 (2012).
[21] Frederic Dupuis, Omar Fawzi, and Stephanie Wehner, Entanglement sampling and applications, IEEE Trans. Inf. Theory **61**, 1093 (2015).
[22] Joseph M. Renes, Better bounds on optimal measurement and entanglement recovery, with applications to uncertainty and monogamy relations, Phys. Rev. A **96**, 042328 (2017).
[23] Mark M. Wilde, Recoverability in quantum information theory, Proc. R. Soc. A **471**, 20150338 (2015).
[24] David Sutter, Marco Tomamichel, and Aram W. Harrow, Strengthened monotonicity of relative entropy via pinched Petz recovery map, IEEE Trans. Inf. Theory **62**, 2907 (2016).
[25] Marius Junge, Renato Renner, David Sutter, Mark M. Wilde, and Andreas Winter, Universal recovery from a decrease of quantum relative entropy, Ann. Henri Poincare **19**, 2955 (2018).
[26] Eric A. Carlen and Anna Vershynina, Recovery map stability for the data processing inequality, J. Phys. A **53**, 035204 (2020).
[27] Thomas Faulkner, Stefan Hollands, Brian Swingle, and Yixu Wang, Approximate recovery and relative entropy I. General von Neumann subalgebras, arXiv:2006.08002.
[28] Ludovico Lami, Siddhartha Das, and Mark M. Wilde, Approximate reversal of quantum Gaussian dynamics, J. Phys. A **51**, 125301 (2018).
[29] Brian G. Swingle and Yixu Wang, Recovery map for fermionic Gaussian channels, J. Math. Phys. (N.Y.) **60**, 072202 (2019).
[30] Jordan Cotler, Patrick Hayden, Geoffrey Penington, Grant Salton, Brian Swingle, and Michael Walter, Entanglement Wedge Reconstruction via Universal Recovery Channels, Phys. Rev. X **9**, 031011 (2019).
[31] Hewei Frederic Jia and Mukund Rangamani, Petz reconstruction in random tensor networks, arXiv:2006.12601.
[32] Geoff Penington, Stephen H. Shenker, Douglas Stanford, and Zhenbin Yang, Replica wormholes and the black hole interior, arXiv:1911.11977.
[33] Dave Bacon, Andrew M. Childs, and Wim van Dam, Optimal measurements for the dihedral hidden subgroup problem, Chicago J. Theor. Comput. Sci. **2006**, 2 (2006), http://cjtcs.cs.uchicago.edu/articles/2006/2/contents.html.
[34] Srinivasan Arunachalam and Ronald de Wolf, Optimal quantum sample complexity of learning algorithms, in *Proceedings of the 32nd IEEE Conference on Computational Complexity (CCC)* (IEEE, New York, 2017), Vol. 31, pp. 1–25, https://dl.acm.org/doi/abs/10.5555/3291125.3309633.
[35] Seth Lloyd, Samuel Bosch, Giacomo De Palma, Bobak Kiani, Zi-Wen Liu, Milad Marvian, Patrick Rebentrost, and

David M. Arvidsson-Shukur, Quantum polar decomposition algorithm, arXiv:2006.00841.

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

[37] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe, Quantum singular value transformation and beyond: Exponential improvements for quantum matrix arithmetics, in *Proceedings of the 51st ACM Symposium on the Theory of Computing (STOC)* (Association for Computing Machinery, 2019), pp. 193–204, https://dl.acm.org/doi/10.1145/3313276.3316366.

[38] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost, Quantum principal component analysis, Nat. Phys. **10**, 631 (2014).

[39] Shelby Kimmel, Cedric Yen-Yu Lin, Guang Hao Low, Maris Ozols, and Theodore J. Yoder, Hamiltonian simulation with optimal sample complexity, npj Quantum Inf. **3**, 13 (2017).

[40] Richard Cleve and Chunhao Wang, Efficient quantum algorithms for simulating Lindblad evolution, in *Proceedings of the 44th International Colloquium on Automata, Languages, and Programming (ICALP 2017)*, edited by Ioannis Chatzigiannakis, Piotr Indyk, Fabian Kuhn, and Anca Muscholl, Leibniz International Proceedings in Informatics (LIPIcs) Vol. 80 (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2017), pp. 1–17, https://drops.dagstuhl.de/opus/volltexte/2017/7477/.

[41] András Gilyén, Quantum singular value transformation & its algorithmic applications, Ph.D. thesis, University of Amsterdam, 2019, https://dare.uva.nl/search?identifier=20e9733e-6014-402d-afa9-20f3cc4a0568.

[42] Dominic W. Berry, Andrew M. Childs, Richard Cleve, Robin Kothari, and Rolando D. Somma, Exponential improvement in precision for simulating sparse Hamiltonians, in *Proceedings of the 46th ACM Symposium on the Theory of Computing (STOC)* (Association for Computing Machinery, 2014), pp. 283–292, https://dl.acm.org/doi/10.1145/2591796.2591854.

[43] Alexei Yu Kitaev, Quantum computations: Algorithms and error correction, Russ. Math. Surv. **52**, 1191 (1997).

[44] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.128.220502 for we show how the running time of the algorithm proposed in the main text can be improved substantially in some cases. That is, we remove the dependence of the algorithm on the dimension d_E of the environment system E, and we replace this parameter with the dimension of the projection $\Pi_E^{\tilde{\mathcal{N}}(\sigma)}$ onto the support of the state $\tilde{\mathcal{N}}_{A\to E}(\sigma_A)$, where $\tilde{\mathcal{N}}_{A\to E}$ is the channel complementary to the original channel $\mathcal{N}_{A\to B}$ and defined from the unitary extension $U_{E'A\to EB}^{\mathcal{N}}$, which also includes Ref. [45].

[45] Joran van Apeldoorn and András Gilyén, Improvements in quantum SDP-solving with applications, in *Proceedings of the 46th International Colloquium on Automata, Languages, and Programming (ICALP)* (2019), Vol. 15, pp. 1–99, https://drops.dagstuhl.de/opus/volltexte/2019/10675/.

[46] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe, Quantum singular value transformation and beyond: Exponential improvements for quantum matrix arithmetics, arXiv:1806.01838.

[47] Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp, Quantum amplitude amplification and estimation, in *Quantum Computation and Quantum Information: A Millennium Volume*, Contemporary Mathematics Series Vol. 305 (American Mathematical Society, Providence, 2002), pp. 53–74.