PHYSICAL REVIEW A, VOLUME 65, 032306

Strictly contractive quantum channels and physically realizable quantum computers

Maxim Raginsky*
Center for Photonic Communication and Computing, Department of Electrical and Computer Engineering, Northwestern University, Evanston, Illinois 60208-3118

(Received 13 June 2001; published 13 February 2002)

We study the robustness of quantum computers under the influence of errors modeled by strictly contractive channels. A channel T is defined to be strictly contractive if, for any pair of density operators ρ, σ in its domain, $\|T\rho-T\sigma\|_1 \leqslant k\|\rho-\sigma\|_1$ for some $0 \leqslant k < 1$ (here $\|\cdot\|_1$ denotes the trace norm). In other words, strictly contractive channels render the states of the computer less distinguishable in the sense of quantum detection theory. Starting from the premise that all experimental procedures can be carried out with finite precision, we argue that there exists a physically meaningful connection between strictly contractive channels and errors in physically realizable quantum computers. We show that, in the absence of error correction, sensitivity of quantum memories and computers to strictly contractive errors grows exponentially with storage time and computation time, respectively, and depends only on the constant k and the measurement precision. We prove that strict contractivity rules out the possibility of perfect error correction, and give an argument that approximate error correction, which covers previous work on fault-tolerant quantum computation as a special case, is possible.

DOI: 10.1103/PhysRevA.65.032306 PACS number(s): 03.67.Lx, 03.65.Ta

I. INTRODUCTION

Since it was first realized [1] that maintaining reliable operation of a large-scale (multiqubit) quantum computer in the presence of environmental noise, as well as under the combined influence of unavoidable imprecisions in state preparation, manipulation, and measurement, will pose quite a formidable obstacle to any experimental realization of the computer [2], many researchers have expended a considerable effort devising various schemes for the ''stabilization of quantum information.'' These schemes include, e.g., quantum error-correcting codes (QECC's) [3], noiseless quantum codes [4], decoherence-free subspaces [5], and noiseless subsystems [6]. (The last three of these schemes boil down to essentially the same thing, but are arrived at by different means.) However, each of these schemes relies for its efficacy upon explicit assumptions about the nature of the error mechanism. Quantum error-correcting codes [3], for instance, perform best when different qubits in the computer are affected by independent errors. On the other hand, stabilization strategies that are designed to handle collective errors [4–6] make extensive use of various symmetry arguments in order to demonstrate existence of the so-called ''noiseless subsystems,'' i.e., subsystems that are effectively decoupled from the environment, even though the computer as a whole certainly remains affected by errors.

In a recent publication [7], Zanardi unified the description of all above-mentioned schemes via a common algebraic framework, thereby reducing the conditions for efficient stabilization of quantum information to those based on symmetry considerations. The validity of this framework will ultimately be decided by the experiment, but it is also quite important to test its applicability in a theoretical setting that would make as minimal of an assumption as possible concerning the exact nature of the error mechanism, and yet would serve as an abstract embodiment of the concept of a physically realizable (i.e., nonideal) quantum computer.

In this respect, the assumption of a finite precision [8] of all physically realizable state preparation, manipulation, and registration procedures is particularly important, and can even be treated as an empirical given. This premise is general enough to subsume (a) fundamental limitations imposed by the laws of quantum physics (e.g., impossibility of reliable discrimination between any two density operators with nonorthogonal supports), (b) practical constraints imposed by the specific experimental setting (e.g., impossibility of synthesizing any quantum state or any quantum operation with arbitrary precision), and (c) environment-induced noise.

As a rule, imprecisions in the preparation and measurement procedures will give rise to imprecisions in the building blocks of the computer (gates) because the precision of any experimental characterization of these gates will always be affected by the precision of the preparation and measurement steps involved in such characterization. Conversely, precision of quantum gates will affect precision of measurements because the closeness of conditional probability measures (say, in total variation norm [9]), conditioned on the gate used, is bounded above by the closeness of any two quantum gates in question [10].

The central goal of this paper is to offer an argument that the concept of a *strictly contractive* quantum channel yields a natural (and very economical) embodiment of the above finite-precision assumption. Defining a suitable distance function $d(\cdot,\cdot)$ on the set of density operators, we say that a channel T is strictly contractive (with respect to d) if there exists some $k \in [0,1)$ such that, for any pair ρ, σ of density operators, we have the uniform estimate

$$d(T\rho,T\sigma) \leqslant k d(\rho,\sigma). \tag{1}$$

For instance, the much studied depolarizing channel is strictly contractive (with respect to the trace-norm distance,

*FAX: (847) 491-4455; electronic address: maxim @northwestern.edu to be defined later). If we assume the dominant error mechanism of the computer to be strictly contractive, then the constant k can be thought of as a quantitative measure of the computer's (im)precision. While this approach may certainly be criticized as reductionist [11], its merit lies in the fact that it brings out many essential features of physically realizable quantum computers without invoking more specific assumptions.

Let us give a "sneak preview" of what is coming up. First of all, we establish that the set of all strictly contractive channels on a particular quantum system (computer) **Q** is dense in the set of all channels on **Q**. Since finite-precision measurements cannot distinguish a dense subset from its closure [12], we draw the conclusion that strictly contractive quantum channels (SCQC's) serve as a physically meaningful abstract model of errors in physically realizable computers. This conclusion is further supported by the fact that, in the presence of a strictly contractive error mechanism, the probability of correctly discriminating between any two equiprobable quantum states is bounded away from unity (or, equivalently, no two density operators in the image of a SCQC have orthogonal supports). Next we use a particularly important property of SCQC's, namely, existence and uniqueness of their fixed points to obtain uniform dimension-independent estimates of decoherence rates of noisy quantum memories and computers. We also take up the question of the possibility of the error correction (stabilization). In this regard, we obtain a rather strong result that strictly contractive channels admit no noiseless subsystems. The proof of this claim utilizes ideas from the representation theory of operator algebras [13,14] and depends in an essential way on the property of strict contractivity.

The paper is organized as follows. In Sec. II we introduce the necessary background on quantum states and channels, as well as some relevant facts from the operator theory. Strictly contractive quantum channels are introduced in Sec. III, where we show that the set of strictly contractive channels is dense in the set of all channels. Then, in Sec. IV, we give an interpretation of strict contractivity in the framework of optimum quantum hypothesis testing (Sec. IV A) and then use the fixed point theorem for strictly contractive channels to obtain estimates on decoherence rates of noisy quantum memories and computers (Sec. IV B). In Sec. IV C, we present the proof of nonexistence of noiseless subsystems in the presence of SCQC's. The possibility of approximate error correction is addressed in Sec. IV D. Finally, in Sec. V, we present concluding remarks and outline some open questions and directions for future research.

II. PRELIMINARIES

A. On notation

In this paper we will adhere to the following notational conventions. First of all, the operator adjoint to X will be denoted by X^*, as is usually done in mathematical physics literature. Second, density operators will be denoted by ρ and σ (with subscripts, whenever necessary). We will use capital Latin letters to denote all other operators; whenever no ambiguity may arise, the action of a mapping X on a density operator ρ will be written as $X\rho$. Finally, the Pauli matrices will be written as ς_i, $i \in \{1,2,3\}$.

B. States

Let $\mathcal{H}$ be a finite-dimensional Hilbert space associated with the computer **Q**, and let $\mathcal{B}(\mathcal{H})$ be the algebra of all bounded operators on $\mathcal{H}$ [since $\dim\mathcal{H}<\infty$, the qualification "bounded" is patently unnecessary, but we will retain the notation $\mathcal{B}(\mathcal{H})$, following standard usage]. The set

$$\mathcal{S}(\mathcal{H}) := \{\rho \in \mathcal{B}(\mathcal{H}) \,|\, \rho \geqslant 0; \operatorname{tr}\rho = 1\} \tag{2}$$

is the set of all density operators (states) of **Q**. We can define a few norms on $\mathcal{B}(\mathcal{H})$; since $\mathcal{H}$ is finite-dimensional, all norm topologies on it are equivalent. First, we have the operator norm

$$\|X\| := \sup_{\psi\in\mathcal{H};\|\psi\|=1} \|X\psi\|, \quad \forall \;\; X \in \mathcal{B}(\mathcal{H}). \tag{3}$$

We can also define the class of Schatten p-norms [15]. For any $X \in \mathcal{B}(\mathcal{H})$, we let $|X| := (X^*X)^{1/2}$, so that

$$\|X\|_p := (\operatorname{tr}|X|^p)^{1/p}, \quad \forall \;\; X \in \mathcal{B}(\mathcal{H}); p = 1,2, \ldots . \tag{4}$$

The Schatten 1-norm is better known as the trace norm; in the case $p=2$, we recover the Hilbert-Schmidt norm. In fact, for any $X \in \mathcal{B}(\mathcal{H})$, $\|X\|_p \to \|X\|$ as $p\to\infty$. For this reason, we can identify the operator norm $\|\cdot\|$ with $\|\cdot\|_\infty$. All these norms possess a very important property of unitary invariance [15]: for any unitaries U, V, and any $X \in \mathcal{B}(\mathcal{H})$, we have

$$\|UXV\|_p = \|X\|_p, \quad p = 1,2,\ldots,\infty. \tag{5}$$

The trace norm can be given a natural interpretation as a distance between density operators [16]. First of all, for any $\rho \in \mathcal{S}(\mathcal{H})$, we have $\|\rho\|_1 = 1$. Of especial importance is the fact that, for any pair ρ, $\sigma \in \mathcal{S}(\mathcal{H})$, the trace-norm distance $\|\rho-\sigma\|_1$ achieves its maximum value of 2 if and only if $\rho\sigma=0$ (i.e., if and only if ρ and σ have orthogonal supports). In the case of two pure states $|\phi\rangle\langle\phi|$ and $|\psi\rangle\langle\psi|$, this condition reduces to $\langle\phi|\psi\rangle=0$, i.e., the corresponding state vectors ϕ, $\psi \in \mathcal{H}$ are orthogonal. As we will see in Sec. IV, the trace-norm distance also figures prominently in the framework of optimal quantum hypothesis testing.

To close our discussion of states, we give two important characterizations of the trace-norm distance. Let X be a self-adjoint operator. Then we can write X as a difference of two positive operators with orthogonal supports: $X = X_+ - X_-$, where $X_\pm := (|X| \pm X)/2$. This is referred to as the orthogonal decomposition of X. Then $|X| = X_+ + X_-$, and

$$\|X\|_1 = \|X_+\|_1 + \|X_{-1}\|_1 \equiv \operatorname{tr} X_+ + \operatorname{tr} X_- . \tag{6}$$

Now let ρ, σ be a pair of density operators. Writing $\rho-\sigma = R_+ - R_-$, we observe that $\operatorname{tr}(\rho-\sigma)=0$ implies $\operatorname{tr} R_+ = \operatorname{tr} R_-$, and hence

$$\|\rho-\sigma\|_1 = 2 \operatorname{tr} R_+ . \tag{7}$$

Another useful relation is

$$\|\rho-\sigma\|_1=2\max_{0\leqslant F\leqslant \mathbb{1}} \operatorname{tr} F(\rho-\sigma), \tag{8}$$

where $\mathbb{1}$ is the identity operator, and the inequality $0\leqslant F\leqslant \mathbb{1}$ should be taken to mean $F\geqslant 0$ and $\mathbb{1}-F\geqslant 0$. In fact, since the set of all such F is convex, the maximum of the linear functional in Eq. (8) is attained on an extreme point of $\{F|0\leqslant F\leqslant \mathbb{1}\}$, namely, on the projector P_+ defined by

$$P_+R_+=R_+, \quad P_+R_-=0. \tag{9}$$

C. Channels

In quantum theory, the reversible evolutions of a closed quantum system correspond to the automorphisms $\mathcal{S}(\mathcal{H})\to U\mathcal{S}(\mathcal{H})U^*$ with a unitary U, i.e., for any $\rho\in\mathcal{S}(\mathcal{H})$, we have $\rho\mapsto T_U\rho:=U\rho U^*$. The map T_U: $\mathcal{S}(\mathcal{H})\to\mathcal{S}(\mathcal{H})$ is affine, trace-preserving, and positive (we will call a map positive if it takes positive operators to positive operators). Since any affine map on density operators can be uniquely extended to a linear map on self-adjoint operators [17], we can take T_U to be linear. Most importantly, T_U is invertible with $T_U^{-1}\rho:=U^*\rho U$.

The general irreversible evolution T: $\mathcal{S}(\mathcal{H})\to\mathcal{S}(\mathcal{H})$ of an open quantum system will no longer be given by an automorphism $U\cdot U^*$. We must accordingly modify the requirements imposed on T. It is obvious that we have to drop the invertibility condition, so that T is now a trace-preserving positive linear map on $\mathcal{S}(\mathcal{H})$ (we can then extend it, by linearity, to self-adjoint trace-class operators). However, positivity alone is not sufficient. In order for T to represent a physically admissible evolution, it must be *completely positive* [18], i.e., the map $T\otimes \mathrm{id}_n$, where id_n is the identity operator on the space $M_n(\mathbb{C})$ of $n\times n$ complex matrices, must be positive for all n. Unitary evolutions T_U obviously satisfy all these requirements. In fact, we can also include such transformations as measurements into this framework by requiring all admissible evolutions to be trace-nonincreasing completely positive linear maps on $\mathcal{S}(\mathcal{H})$, i.e., for any $\rho\in\mathcal{S}(\mathcal{H})$, we have $\operatorname{tr} T\rho\leqslant\operatorname{tr}\rho$, so that

$$\rho\mapsto\frac{T\rho}{\operatorname{tr} T\rho}. \tag{10}$$

Then $\operatorname{tr} T\rho$ can be naturally interpreted as the conditional probability of transformation T occurring, given that the system is initially in the state ρ. We will call any trace-preserving completely positive linear map on $\mathcal{S}(\mathcal{H})$ a *channel*.

There are many useful structure theorems for completely positive maps. For instance, the Kraus representation theorem [12] states that, for any completely positive map T: $\mathcal{B}(\mathcal{H})\to\mathcal{B}(\mathcal{H})$, there exists a collection $\{K_i\}$ of bounded operators such that

$$T(X)=\sum_i K_iXK_i^*, \quad \forall \quad X\in\mathcal{B}(\mathcal{H}). \tag{11}$$

If T is trace-nonincreasing, then we have the bound

$$\sum_i K_i^*K_i\leqslant\mathbb{1}, \tag{12}$$

where equality is achieved if and only if T is trace-preserving. In addition, if T is a *unital* channel, i.e., $T(\mathbb{1})=\mathbb{1}$, then we also have

$$\sum_i K_iK_i^*=\mathbb{1}. \tag{13}$$

Now we must adopt a suitable metric on the set of all completely positive maps on $\mathcal{B}(\mathcal{H})$. One possible candidate is the metric induced by the operator norm

$$\|T\|:=\sup_{X\in\mathcal{B}(\mathcal{H});\|X\|=1}\|T(X)\|. \tag{14}$$

Unfortunately, the operator norm is rather ill behaved [19]: it is not stable with respect to tensor products. In particular, if T is a positive map, then the norm $\|T\otimes\mathrm{id}_n\|$ can in general increase with n. A good choice then is the metric induced by the *norm of complete boundedness* [19] (or cb- norm), defined as

$$\|T\|_{\mathrm{cb}}:=\sup_n\|T\otimes\mathrm{id}_n\|. \tag{15}$$

This norm has appeared, under different guises, in Refs. [16], [20], and [21]. For any self-adjoint trace-class operator X on $\mathcal{H}$ and any two maps S,T on $\mathcal{B}(\mathcal{H})$ with finite cb-norm (in the case of finite-dimensional $\mathcal{H}$, this is always true [19]), we have the relations [20]

$$\|T(X)\|_1\leqslant\|T\|_{\mathrm{cb}}\|X\|_1, \tag{16}$$

$$\|TS\|_{\mathrm{cb}}\leqslant\|T\|_{\mathrm{cb}}\|S\|_{\mathrm{cb}}, \tag{17}$$

$$\|T\otimes S\|_{\mathrm{cb}}=\|T\|_{\mathrm{cb}}\|S\|_{\mathrm{cb}}. \tag{18}$$

Furthermore, for any channel T, we have [22] $\|T\|_{\mathrm{cb}}=1$.

If two channels T,S are close in cb-norm, then, for any density operator ρ, the corresponding states $T\rho,S\rho$ are close in trace norm since, from Eq. (16), it follows that

$$\|T\rho-S\rho\|_1=\|(T-S)\rho\|_1\leqslant\|T-S\|_{\mathrm{cb}}. \tag{19}$$

In fact, the above estimate cannot be loosened by adjoining a second system with the Hilbert space $\mathcal{K}$ in some state σ, entangling the two systems through some channel K on $\mathcal{S}(\mathcal{H}\otimes\mathcal{K})$, and then comparing the channels $T\otimes R$ and $S\otimes R$, where R is some suitably chosen channel on $\mathcal{S}(\mathcal{K})$. This is evident from the estimate

$$\|(T\otimes R)K(\rho\otimes\sigma)-(S\otimes R)K(\rho\otimes\sigma)\|_1\leqslant\|T-S\|_{\mathrm{cb}}, \tag{20}$$

which can be easily obtained by repeated application of Eqs. (16)–(18). In other words, as far as the cb-norm distinguishability criterion is concerned, entangling the system with an auxiliary system will not improve the distinguishability of the channels T and S. The cb-norm, however, is an extremely strong distinguishability measure: its definition already accounts for optimization with respect to entanglement and input states over Hilbert spaces of very large (but finite) dimension. There exist weaker measures of the channel distinguishability (such as the channel fidelity [23]), which describe how channels may be distinguished with only finite resources. Using these weaker criteria, one may show that entanglement does improve practical distinguishability of both states and channels [24].

Before we go on, we must mention that, for the present purposes, we only need to consider channels that map operators on some Hilbert space $\mathcal{H}$ to operators on the same Hilbert space. In general, this does not have to be true. For instance, if the Hilbert space in question is a tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$, then the partial trace over $\mathcal{H}_2$ can be treated as a channel $\mathrm{tr}_2 : \mathcal{S}(\mathcal{H}_1 \otimes \mathcal{H}_2) \rightarrow \mathcal{S}(\mathcal{H}_1)$.

D. Some facts from operator theory

We close Sec. II by listing some facts from operator theory, which will be necessary in the sequel. Let $\mathcal{X}$ be a metric space with the corresponding metric $d(\cdot,\cdot)$. An operator A: $\mathcal{X} \rightarrow \mathcal{X}$ is called a *contraction* if, for any $x, y \in \mathcal{X}$, $d(Ax,Ay) \leqslant d(x,y)$, and a *strict contraction* if there exists some $k \in [0,1)$ such that $d(Ax,Ay) \leqslant k d(x,y)$. If $\mathcal{X}$ is a complete metric space, then the contraction mapping principle [25] states that any strict contraction A on $\mathcal{X}$ has a unique fixed point. In other words, the problem $Ax = x$ has a unique solution on $\mathcal{X}$. If $\mathcal{Y}$ is a closed subset of $\mathcal{X}$, then it follows that any strict contraction A: $\mathcal{Y} \rightarrow \mathcal{Y}$ has a unique fixed point on $\mathcal{Y}$.

Strict contractivity is a remarkably strong property. Indeed, if we pick any $y \in \mathcal{Y}$, then the sequence of iterates $A^n y$ converges to the fixed point y_0 of A exponentially fast, because

$$d(A^n y, y_0) = d(A^n y, A^n y_0) \leqslant k^n d(y, y_0). \tag{21}$$

This fact is of tremendous use in numerical analysis when one wants to solve a fixed-point problem $Ay = y$ via iteration method with some initial guess $\hat{y}$. If the operator A is a strict contraction on a closed subset of a complete metric space, then for any choice of $\hat{y}$, the iteration method is guaranteed to zero in on the solution in $O(\log \epsilon^{-1})$ steps, where ϵ is the desired precision.

It should be noted that the existence and uniqueness of a fixed point of some operator A are, by themselves, not sufficient to guarantee convergence of the sequence of iterates $A^n y$ for any point y in the domain of A. Indeed, according to the Leray-Schauder-Tychonoff theorem [25], any continuous map on a compact convex subset of a locally convex space $\mathcal{X}$ has at least one fixed point. Furthermore, any weak contraction on a compact subset $\mathcal{C}$ of a Banach space, i.e., a map W: $\mathcal{C} \rightarrow \mathcal{C}$ with the property $\|Wx - Wy\| < \|x - y\|$ for any x, $y \in \mathcal{C}$, has a unique fixed point [26]. The key to the rapid convergence in Eq. (21) is the fact that a strict contraction A: $\mathcal{Y} \rightarrow \mathcal{Y}$ shrinks distances between points of $\mathcal{Y}$ *uniformly*.

III. STRICTLY CONTRACTIVE QUANTUM CHANNELS

A. Definition and examples

Let $\mathcal{H}$ be the finite-dimensional Hilbert space associated with some quantum system **Q**. Then, as follows easily from Eq. (16), any channel T on $\mathcal{S}(\mathcal{H})$ is a contraction

$$\|T\rho - T\sigma\|_1 \leqslant \|\rho - \sigma\|_1, \quad \forall \quad \rho, \sigma \in S(\mathcal{H}). \tag{22}$$

In other words, no channel can make any ρ, σ more distinguishable. For a channel T, we define the *contractivity modulus*

$$\kappa(T) := \sup_{\rho,\sigma \in S(\mathcal{H})} \frac{\|T\rho - T\sigma\|_1}{\|\rho - \sigma\|_1}. \tag{23}$$

Any channel T with $\kappa(T) < 1$ is *strictly contractive*, and thus has a unique fixed point $\rho_T \in \mathcal{S}(\mathcal{H})$.

The depolarizing channel D_p, $0 < p < 1$, whose action on an arbitrary $\rho \in \mathcal{S}(\mathcal{H})$ is given by

$$D_p \rho := p \frac{\mathbb{1}}{d} + (1-p)\rho, \tag{24}$$

where $d = \dim \mathcal{H}$, is manifestly strictly contractive with $\kappa(D_p) = 1 - p$. The maximally mixed state $\mathbb{1}/d$ is the unique fixed point of D_p for any p. When $d = 2$, so that $\mathcal{H} = \mathbb{C}^2$, the action of D_p on $\mathcal{S}(\mathcal{H})$ can be visualized as a uniform rescaling of the Bloch-Poincaré ball by a factor of $\kappa(D_p)$, and the term "strictly contractive" thus becomes especially apt. It also turns out that, for any two depolarizing channels D_p and D_q, their tensor product is also strictly contractive. In order to show this, we use the fact that a density operator on $\mathbb{C}^2 \otimes \mathbb{C}^2$ can be written as [27]

$$\rho = \frac{1}{4}\left(\mathbb{1} \otimes \mathbb{1} + \sum_k \alpha_k \mathsf{s}_k \otimes \mathbb{1} + \sum_k \beta_k \mathbb{1} \otimes \mathsf{s}_k + \sum_{k,l} \theta_{kl} \mathsf{s}_k \otimes \mathsf{s}_l \right), \tag{25}$$

where the vector $\boldsymbol{\alpha} := (\alpha_1, \alpha_2, \alpha_3)$ and $\boldsymbol{\beta} := (\beta_1, \beta_2, \beta_3)$ are the *coherence vectors* of the first and second qubit, respectively, while the matrix Θ with entries θ_{kl} is called the *correlation tensor* of ρ. The action of the depolarizing channel on an arbitrary operator $X \in \mathcal{B}(\mathbb{C}^2)$ can be described as

$$D_p(X) = p(\mathrm{tr}\, X)\frac{\mathbb{1}}{2} + (1-p)X \tag{26}$$

[if X is a density operator, this reduces to Eq. (24)]. Thus $D_p \mathsf{s}_k = (1-p)\mathsf{s}_k$, which yields

$$(D_p \otimes D_q)\rho = \frac{1}{4}\left(\mathbb{1} \otimes \mathbb{1} + (1-p)\sum_k \alpha_k \mathsf{s}_k \otimes \mathbb{1} + (1-q)\sum_k \beta_k \mathbb{1} \otimes \mathsf{s}_k + (1-p)(1-q)\sum_{k,l} \theta_{kl} \mathsf{s}_k \otimes \mathsf{s}_l \right). \tag{27}$$

It is then straightforward to verify that $T_{pq} := D_p \otimes D_q$ is strictly contractive with $\kappa(T_{pq}) = \max[(1-p),(1-q)]$. In particular, the channel $D_p \otimes D_p$ is strictly contractive with $\kappa(D_p \otimes D_p) = \kappa(D_p) = 1 - p$. Strict contractivity of the product channel $D_p \otimes D_p$ provides an alternate explanation of the fact that the use of entanglement cannot improve the distinguishability of classical signals transmitted through the depolarizing channel [28].

In fact, since the trace-norm distance between any two density operators on $\mathbb{C}^2$ is just the Euclidean distance between their Bloch-Poincaré vectors, any strictly contractive channel on $\mathcal{S}(\mathbb{C}^2)$ can be pictured as a rescaling of the Bloch-Poincaré ball (which may not be isotropic, as long as the maximum of the scaling ratio over all directions is strictly less than 1), possibly followed by translation and rotation. As shown in Ref. [29], for any channel T on $\mathcal{B}(\mathbb{C}^2)$ [which is just the space $M_2(\mathbb{C})$ of 2×2 complex matrices], there exist unitaries U,V and vectors $\mathbf{v},\mathbf{t}\in\mathbb{R}^3$ such that

$$T\rho = U[T_{\mathbf{v},\mathbf{t}}(V\rho V^*)]U^*, \tag{28}$$

where the action of $T_{\mathbf{v},\mathbf{t}}$ is defined, with respect to the basis $\{\mathbb{1},\varsigma_1,\varsigma_2,\varsigma_3\}$, as

$$T_{\mathbf{v},\mathbf{t}}(w_0\mathbb{1}+\mathbf{w}\cdot\varsigma) := w_0\mathbb{1}+[\mathbf{t}+(\operatorname{diag}\mathbf{v})\mathbf{w}]\cdot\varsigma. \tag{29}$$

Assuming that $\mathbf{v}$ and $\mathbf{t}$ are such that the map T is indeed a channel [29], we see that T is strictly contractive whenever $\max_{i\in\{1,2,3\}}|v_i|<1$. In fact, the contractivity modulus of T satisfies

$$\kappa(T) = \max_{i\in\{1,2,3\}}|v_i|. \tag{30}$$

If T_1, T_2 are unital strictly contractive channels on $\mathcal{S}(\mathbb{C}^2)$, then the product channel $T_1\otimes T_2$ is strictly contractive on $\mathcal{S}(\mathbb{C}^2\otimes\mathbb{C}^2)$. Given a representation (28) of a channel T on $\mathcal{S}(\mathbb{C}^2)$, we see that T is unital if and only if $\mathbf{t}\equiv 0$. Specifically, for T_1 and T_2 we have

$$T_1\rho = U_1[T_{\mathbf{v}_1,0}(V_1\rho V_1^*)]U_1^*, \tag{31}$$

$$T_2\rho = U_2[T_{\mathbf{v}_2,0}(V_2\rho V_2^*)]U_2^*. \tag{32}$$

Thus the action of the channel $T_1\otimes T_2$ on a density operator ρ over $\mathbb{C}^2\otimes\mathbb{C}^2$ is a successive application of the unitary channel $(V_1\otimes V_2)\cdot(V_1^*\otimes V_2^*)$, the rescaling transformation $T_{\mathbf{v}_1,0}\otimes T_{\mathbf{v}_2,0}$, and the unitary channel $(U_1\otimes U_2)\cdot(U_1^*\otimes U_2^*)$ to ρ. By unitary invariance of the trace norm, we only need to consider the effect of $T_{\mathbf{v}_1,0}\otimes T_{\mathbf{v}_2,0}$. Writing ρ in the form of Eq. (25), we obtain

$$(T_{\mathbf{v}_1,0}\otimes T_{\mathbf{v}_2,0})\rho = \frac{1}{4}\left(\mathbb{1}\otimes\mathbb{1}+\sum_k v_k^{(1)}\alpha_k\varsigma_k\otimes\mathbb{1}+\sum_k v_k^{(2)}\beta_k\mathbb{1}\otimes\varsigma_k+\sum_{k,l} v_k^{(1)}v_l^{(2)}\theta_{kl}\varsigma_k\otimes\varsigma_l\right), \tag{33}$$

where $v_j^{(i)}$, $i\in\{1,2\}$, $j\in\{1,2,3\}$, denotes the jth component of $\mathbf{v}_i$. By inspection,

$$\kappa(T_1\otimes T_2) = \max_{i,j}|v_j^{(i)}|. \tag{34}$$

If at least one of the channels T_1 and T_2 is not unital, the tensor product channel $T=T_1\otimes T_2$ may not be strictly contractive, even if T_1 and T_2 are. This stems from the fact that, in this case, the effect of T on the correlation tensor Θ of ρ is determined not only by T, but also by ρ through the coherence vectors $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$.

It is quite easy to see that any unital strictly contractive channel maps all states to mixed states. Let $d=\dim\mathcal{H}$. Then, for any unit vector $\psi\in\mathcal{H}$, we have

$$\left\| |\psi\rangle\langle\psi| - \frac{\mathbb{1}}{d}\right\|_1 = \frac{2(d-1)}{d} \tag{35}$$

(this can be readily proved by expanding $\mathbb{1}$ with respect to an orthonormal basis containing ψ). Now suppose that T is a strictly contractive unital channel that maps $|\psi\rangle\langle\psi|$ to some other pure state $|\phi\rangle\langle\phi|$. Then

$$\left\| T|\psi\rangle\langle\psi| - \frac{T\mathbb{1}}{d}\right\|_1 = \left\| |\psi\rangle\langle\phi| - \frac{\mathbb{1}}{d}\right\|_1 = \frac{2(d-1)}{d}. \tag{36}$$

Furthermore, we must also have

$$\left\| T|\psi\rangle\langle\psi| - \frac{T\mathbb{1}}{d}\right\|_1 \leqslant \kappa(T)\left\| |\psi\rangle\langle\psi| - \frac{\mathbb{1}}{d}\right\|_1. \tag{37}$$

Hence, $\kappa(T)\geqslant 1$, which is a contradiction, since $\kappa(T)<1$ for any strictly contractive channel.

We can show that there exist channels that are not strictly contractive, and yet contain no pure states in their image. Let T be an arbitrary channel on $\mathcal{S}(\mathcal{H})$. According to the Leray-Schauder-Tychonoff theorem, T has at least one fixed point on $\mathcal{S}(\mathcal{H})$. Let us adjoin another system with the associated Hilbert space $\mathcal{K}$. Then the channel $T\otimes\mathrm{id}$ on $\mathcal{S}(\mathcal{H}\otimes\mathcal{K})$ cannot be strictly contractive because, for any fixed point ρ_T of T and any $\sigma\in\mathcal{S}(\mathcal{K})$, the product density operator $\rho_T\otimes\sigma$ is a fixed point of $T\otimes\mathrm{id}$. The channel $T\otimes\mathrm{id}$ is not even weakly contractive, because it preserves the trace-norm distance between any two of its fixed points. However, if the image of $\mathcal{S}(\mathcal{H})$ under T contains no pure states, then the image of $\mathcal{S}(\mathcal{H}\otimes\mathcal{K})$ under $T\otimes\mathrm{id}$ contains no pure states either because of the relation [30]

$$\inf_{\rho\in\mathcal{S}(\mathcal{H})} S(T\rho) = \inf_{\rho\in\mathcal{S}(\mathcal{H}\otimes\mathcal{K})} S([T\otimes\mathrm{id}]\rho), \tag{38}$$

where $S(\rho)$ is the von Neumann entropy of the state ρ.

B. Strictly contractive channels are dense in the set of all channels

As we have mentioned in the Introduction, finite-precision measurements cannot distinguish a dense subset from its closure. Let us make this statement more precise. Suppose we are presented with some quantum system $\mathbf{Q}$ in an unknown state ρ, and we are trying to estimate the state. Any physically realizable apparatus will have finite resolution ϵ, so that all states ρ' with $\|\rho-\rho'\|_1<\epsilon$ are considered indistinguishable from ρ. Now, if $\mathcal{H}$ is the Hilbert space associated with $\mathbf{Q}$, and if Σ is a dense subset of $\mathcal{S}(\mathcal{H})$, then, by the definition of a dense subset, for any $\epsilon>0$ and any $\rho\in\mathcal{S}(\mathcal{H})$, there will always be some $\sigma\in\Sigma$ such that $\|\rho-\sigma\|_1<\epsilon$.

The same reasoning also applies to distinguishability of quantum channels, except now the appropriate measure of closeness is furnished by the cb-norm. Thus, if an experiment utilizes some apparatus with resolution ϵ, then any two channels T,S with $\|T-S\|_{\text{cb}}<\epsilon$ are considered indistinguishable from each other. There is, however, no fundamental difference between the distinguishability of states and channels because any experiment purporting to distinguish any two channels T and S consists in preparing the apparatus in some state ρ and then making some measurements that would tell the states $T\rho$ and $S\rho$ apart from each other. Then, since for any state ρ_1 $\|T\rho-S\rho\|_1\leqslant\|T-S\|_{\text{cb}}$, the resolving power of the apparatus that will distinguish between T and S is limited by the resolving power of the apparatus that will distinguish between $T\rho$ and $S\rho$.

In this regard, we have the following.

Proposition 1. Let $C(\mathcal{H})$ be the set of all channels on $\mathcal{S}(\mathcal{H})$, where $\mathcal{H}$ is the Hilbert space associated with the system **Q**. Then the set $C_{\text{sc}}(\mathcal{H})$ of all strictly contractive channels on $\mathcal{S}(\mathcal{H})$ is a $\|\cdot\|_{\text{cb}}$-dense convex subset of $C(\mathcal{H})$.

Proof. We show convexity first. Suppose T_1, $T_2\in C_{\text{sc}}(\mathcal{H})$. Define the channel $S:=\lambda T_1+(1-\lambda)T_2$, $0<\lambda<1$. Then, for any ρ, $\sigma\in\mathcal{S}(\mathcal{H})$, we have the estimate

$$\begin{aligned}\|S\rho-S\sigma\|_1&\leqslant\lambda\|T_1\rho-T_1\sigma\|_1+(1-\lambda)\|T_2\rho-T_2\sigma\|_1\\&\leqslant[\lambda\kappa(T_1)+(1-\lambda)\kappa(T_2)]\|\rho-\sigma\|_1.\end{aligned}\tag{39}$$

Defining $\kappa:=\max[\kappa(T_1),\kappa(T_2)]$, we get

$$\|S\rho-S\sigma\|_1\leqslant\kappa\|\rho-\sigma\|_1.\tag{40}$$

Since T_1, T_2 are strictly contractive, $\kappa<1$, and therefore $S\in C_{\text{sc}}(\mathcal{H})$. To prove density, let us fix some $\sigma\in\mathcal{S}(\mathcal{H})$. Now the map $K_\sigma:\ \rho\in\mathcal{S}(\mathcal{H})\mapsto\sigma$ is obviously a channel, which is furthermore trivially strictly contractive because it maps all density operators ρ to σ. Given $\epsilon>0$, pick some positive n such that $1/n<\epsilon$. For any $T\in C(\mathcal{H})$, define

$$T_n:=\frac{1}{2n}K_\sigma+\left(1-\frac{1}{2n}\right)T.\tag{41}$$

Clearly, $T_n\in C_{\text{sc}}(\mathcal{H})$, and the estimate

$$\|T-T_n\|_{\text{cb}}=\frac{1}{2n}\|T-K_\sigma\|_{\text{cb}}\leqslant\frac{1}{n}<\epsilon\tag{42}$$

finishes the proof. ■

This proposition indicates that, as far as physically realizable (finite-precision) measurements go, there is no way to distinguish any channel T from some strictly contractive T' with $\|T-T'\|_{\text{cb}}<\epsilon$, where ϵ is the resolution of the measuring apparatus. In this regard, it is interesting to mention that any channel T with $\|T-\text{id}\|_{\text{cb}}<\epsilon$ (for some sufficiently small $\epsilon>0$) cannot be distinguished from a depolarizing channel. Indeed, let M be the channel that maps all density operators ρ to the maximally mixed state $\mathbb{1}/d$, where $d=\dim\mathcal{H}$. Then it suffices to pick some

$$n>\frac{\|M-\text{id}\|_{\text{cb}}}{\epsilon-\|T-\text{id}\|_{\text{cb}}},\tag{43}$$

so that

$$\|T-D_{1/n}\|_{\text{cb}}\leqslant\|T-\text{id}\|_{\text{cb}}+(1/n)\|M-\text{id}\|_{\text{cb}}<\epsilon.\tag{44}$$

We note that a convex combination of any channel with a strictly contractive channel is a strictly contractive channel. Let $T\in C$ be an arbitrary channel, and suppose that $T'\in C_{\text{sc}}$ [from now on, we will not mention the Hilbert space $\mathcal{H}$ when talking about channels on $\mathcal{S}(\mathcal{H})$, unless this omission might cause ambiguity]. Define, for some $0<\lambda<1$, the channel $S:=\lambda T+(1-\lambda)T'$. Then

$$\begin{aligned}\|S\rho-S\sigma\|_1&\leqslant\lambda\|T\rho-T\sigma\|_1+(1-\lambda)\|T'\rho-T'\sigma\|_1\\&\leqslant[\lambda+(1-\lambda)\kappa(T')]\|\rho-\sigma\|_1.\end{aligned}\tag{45}$$

Since $\lambda+(1-\lambda)\kappa(T')<1$, we conclude that $S\in C_{\text{sc}}$.

Finally, we mention that Proposition 1 implies that the set $C_{\text{sc}}^{\mathbb{1}}$ of all unital strictly contractive channels is a dense convex subset of the set $C^{\mathbb{1}}$ of all unital channels.

IV. IMPLICATIONS FOR QUANTUM INFORMATION PROCESSING

A. Optimum quantum decision strategies

In this section we explore an interesting connection between the contractivity modulus of a channel and quantum detection theory [31]. The archetypal problem in quantum detection theory is that of optimum M-ary detection. A quantum system is prepared in a state ρ, drawn from a collection $\{\rho_i\}_{i=1}^M$ of M density operators, where ρ_i is selected with probability π_i. Our task is to determine, as accurately as possible, which state ρ_i has been drawn. On this system we can perform a measurement described by a positive operator-valued measure (POVM), i.e., a collection $\{F_i\}_{i=1}^M$ of operators that satisfy

$$0\leqslant F_i\leqslant\mathbb{1},\quad i=1,\ldots,M,\tag{46}$$

$$\sum_{i=1}^M F_i=\mathbb{1}.\tag{47}$$

We seek a POVM that would solve the optimization problem

$$\overline{P_c}=\max_{\{F_i\}}\sum_{i=1}\pi_i\operatorname{tr}F_i\rho_i,\tag{48}$$

subject to the constraints (46) and (47). The quantity being maximized in Eq. (48) is the probability of correct decision using the POVM $\{F_i\}$. We will only consider the case $M=2$, wherein the system can be in the state ρ_1 with probability π_1, or in the state ρ_2 with probability $\pi_2\equiv1-\pi_1$. In this case, we are considering two-element POVM's $\{F,\mathbb{1}-F\}$ with $0\leqslant F\leqslant\mathbb{1}$, and the optimization problem (48) takes the form

$$\overline{P_c} = \max_{0 \leqslant F \leqslant \mathbb{1}} [\pi_1 \operatorname{tr} F\rho_1 + \pi_2 \operatorname{tr}(\mathbb{1} - F)\rho_2], \tag{49}$$

or, equivalently,

$$\overline{P_c} = \pi_2 + \max_{0 \leqslant F \leqslant \mathbb{1}} \operatorname{tr}[F(\pi_1\rho_1 - \pi_2\rho_2)]. \tag{50}$$

We interpret $\operatorname{tr} F\rho_1$ as the conditional probability that the measurement using the POVM $\{F, \mathbb{1} - F\}$ correctly determines the state of the system to be ρ_1, similarly, $\operatorname{tr}(\mathbb{1} - F)\rho_2$ is the conditional probability that the state ρ_2 is identified correctly. Then $\operatorname{tr} F\rho_2$ and $\operatorname{tr}(\mathbb{1} - F)\rho_1$, respectively, are the conditional probabilities of mistaking ρ_2 for ρ_1 and vice versa.

We can easily show that

$$\overline{P_c} = \tfrac{1}{2} + \tfrac{1}{2}\|\pi_1\rho_1 - \pi_2\rho_2\|_1. \tag{51}$$

Writing down the orthogonal decomposition $\pi_1\rho_1 - \pi_2\rho_2 = R_+ - R_-$, we get $\operatorname{tr} R_+ = \pi_1 - \pi_2 + \operatorname{tr} R_-$. Now

$$\max_{0 \leqslant F \leqslant \mathbb{1}} \operatorname{tr} F(R_+ - R_-) = \operatorname{tr} R_+, \tag{52}$$

where the maximum is attained by choosing F to be the projection operator with $FR_+ = R_+$ and $FR_- = 0$. Since

$$\operatorname{tr}|\pi_1\rho_1 - \pi_2\rho_2| = \operatorname{tr} R_+ + \operatorname{tr} R_- = 2 \operatorname{tr} R_+ + \pi_2 - \pi_1, \tag{53}$$

we finally arrive at Eq. (51), which clearly exhibits the role of the trace-norm distance in optimum quantum hypothesis testing. It can be proved [32] that $\overline{P_c} = 1$ if and only if $\rho_1\rho_2 = 0$, in which case $\|\pi_1\rho_1 - \pi_2\rho_2\|_1 = \pi_1 + \pi_2 = 1$.

Now suppose that the state of the system is given by one of two equiprobable density operators ρ_1, ρ_2. Suppose, furthermore, that $\rho_1\rho_2 = 0$, so that $\|\rho_1 - \rho_2\|_1 = 2$. Then there exists a measurement that would correctly distinguish between ρ_1 and ρ_2 with probability 1. Since any channel T will generally decrease the trace-norm distance $\|\rho_1 - \rho_2\|_1$, it can happen that the states $T\rho_1$ and $T\rho_2$ no longer have orthogonal supports, and thus the optimum decision strategy will fail with nonzero probability $P_e \equiv 1 - \widetilde{P}_c$.

If T is a weakly contractive channel, then no two density operators in its image have orthogonal supports, but the probability of error P_e can, in principle, be made arbitrarily small. If, however, T is strictly contractive, then we have the following trivial, but important Lemma.

Lemma 1. Let T be a strictly contractive channel. Then, for any pair ρ_1, ρ_2 of equiprobable density operators, the optimum decision strategy for $T\rho_1$ and $T\rho_2$ is such that

$$\overline{P_c} \leqslant \frac{1 + \kappa(T)}{2} < 1. \tag{54}$$

Proof. Fix a pair ρ_1, ρ_2 of density operators. Then, using Eq. (51), we get

$$\overline{P_c} = \tfrac{1}{2} + \tfrac{1}{4}\|T\rho_1 - T\rho_2\|_1 \leqslant \tfrac{1}{2} + \frac{\kappa(T)}{4}\|\rho_1 - \rho_2\|_1. \tag{55}$$

Since $\|\rho_1 - \rho_2\|_1 \leqslant 2$, we obtain Eq. (54). ■

We note that the statement of the above Lemma can be extended to general channels. For instance, if T is a channel with the property that there exists at least one pair ρ, σ of density operators such that $\|T\rho - T\sigma\|_1 = \|\rho - \sigma\|_1$, then the bound (54) is obviously

$$\overline{P_c} \leqslant 1. \tag{56}$$

If T is a weakly contractive channel, then the inequality (56) becomes strict, but $\overline{P_c}$ can, at least, in principle, be made arbitrarily close to 1. This is decidedly not the case for a strictly contractive channel, in which case Lemma 1 states that for any pair of equiprobable density operators ρ, σ, the probability $\overline{P_c}$ of correctly discriminating between them is bounded away from 1.

The discussion in this section lends further support to our argument that strictly contractive channels serve as an abstract model of errors in physically realizable quantum computers. In any realistic setting, no event occurs with the probability exactly equal to unity. For instance, we can never prepare a pure state $|\psi\rangle\langle\psi|$, but rather a mixture $(1 - \epsilon)|\psi\rangle\langle\psi| + \epsilon\rho$, where both ϵ and ρ depend on the particulars of the preparation procedure. Similarly, the measuring device that would ideally identify $|\psi\rangle\langle\psi|$ perfectly will instead be realized by $(1 - \delta)|\psi\rangle\langle\psi| + \delta F$, where δ and the operator F, $0 \leqslant F \leqslant \mathbb{1}$, are again determined by practice. If we assume that, in any physically realizable computer, all state preparation, manipulation and registration procedures can be carried out with finite precision, then it is reasonable to expect that there exist strict bounds on all probabilities that figure in the description of the computer's operation.

B. Decoherence rates of noisy quantum memories and computers

So far, we have established two important properties of strictly contractive channels. First, any channel T can be approximated, in cb-norm, by a strictly contractive channel T', and there will always be some finite-precision measurement that will not be able to distinguish T from T'. Second, any measurement that would, in principle, distinguish some pair ρ, σ of density operators with certainty, will fail with probability at least $[1 - \kappa(T)]/2$ in the presence of a strictly contractive error channel T. The latter statement can also be phrased as follows: no two density operators in the image $T\mathcal{S}(\mathcal{H})$ of $\mathcal{S}(\mathcal{H})$ under some $T \in C_{\mathrm{sc}}$ have orthogonal supports; furthermore, the trace-norm distance between any two density operators in $T\mathcal{S}(\mathcal{H})$ is bounded from above by $2\kappa(T)$.

In this section, we obtain dimension-independent estimates on decoherence rates of quantum memories and computers under the influence of strictly contractive noise and without any error correction (the possibility of error correction will be addressed in Sec. IV C and Sec. IV D).

We treat quantum memories (registers) first. Suppose that we want to store some state $\rho_0 \in \mathcal{S}(\mathcal{H})$ for time t in the presence of errors modeled by some strictly contractive channel T. Let τ be the decoherence time scale, with $\tau \ll t$, and let $n = \lceil t/\tau \rceil$. The final state of the register is then $\rho_n = T^n \rho_0$. If ρ_T is the unique fixed point of T, then

$$\|\rho_n - \rho_T\|_1 = \|T^n \rho_0 - T^n \rho_T\|_1 \leqslant \kappa(T)^n \|\rho_0 - \rho_T\|_1 . \quad (57)$$

In other words, the state ρ_0, stored in a quantum register in the presence of strictly contractive noise T, evolves to the fixed state ρ_T of T, and the convergence is incredibly rapid. Let us consider a numerical example. Suppose that $\kappa(T) = 0.9$, and that initially the states ρ_0 and ρ_T have orthogonal supports, so $\|\rho_0 - \rho_T\|_1 = 2$. Then, after $n = 10$ iterations (i.e., $t = 10\tau$), we have $\|\rho_n - \rho_T\| \leqslant 0.697$, and the probability of correct discrimination between ρ_n and ρ_T is only 0.674. Note that the decoherence rate estimate

$$r(n;\rho_0,T) := \frac{\|\rho_n - \rho_T\|_1}{\|\rho_0 - \rho_T\|_1} \leqslant \kappa(T)^n \quad (58)$$

does not depend on the dimension of $\mathcal{H}$, but only on the contractivity modulus $\kappa(T)$ and on the relative storage duration n. In other words, quantum registers of *any* size are equally sensitive to strictly contractive errors.

Obtaining estimates on decoherence rates of computers is not so simple because, in general, the sequence $\{\rho_n\}$, where ρ_n is the overall state of the computer after n computational steps, does not have to be convergent. Let us first fix the model of a quantum computer. We define [33] an *ideal quantum circuit of size n* to be an ordered n-tuple of unitaries U_i, where each U_i is a tensor product of elements of some set $\mathcal{G}$ of universal gates [34]. The set $\mathcal{G}$ will in, general, be a dense subgroup of the group $U(\mathcal{H})$ of all unitary operators on $\mathcal{H}$. For some error channel T, a *T-noisy quantum circuit of size n with k error locations* is an ordered $(n+k)$-tuple containing n channels $\hat{U}_i := U_i \cdot U_i^*$, where the unitaries U_i are of the form described above, as well as k instances of T. We will assume, for simplicity, that each T is preceded and followed by some $\hat{U}_i$ and $\hat{U}_{i+1}$, respectively. Based on this definition, the "noisiest" computer for fixed T and n is modeled by a T-noisy quantum circuit of size n with n error locations, i.e., a $2n$-tuple of the form $(\hat{U}_1, T, \hat{U}_2, T, \ldots, \hat{U}_n, T)$. If the initial state of the computer is ρ_0, then we will use the notation

$$\rho_n = \left(\prod_{i=1}^{n} T\hat{U}_i \right) \rho_0 \quad (59)$$

to signify the state of the computer after n computational steps. In the above expression, the product sign should be understood in the sense of composition $T \circ \hat{U}_n \circ \cdots \circ T \circ \hat{U}_1$.

Given an arbitrary sequence of computational steps, the sequence $\{\rho_n\}$, defined by Eq. (59) (assuming that n is sufficiently large, i.e., the computation is sufficiently long) need not be convergent. However, if the channel T is strictly contractive, then, for any $\epsilon > 0$, there exists some N_0 such that, for any pair of initial states ρ_0, $\sigma_0 \in \mathcal{S}(\mathcal{H})$, the states ρ_n, σ_n, $n \geqslant N_0$, will be indistinguishable from each other. In other words, any two sufficiently lengthy computations will yield nearly the same final state. Using Eq. (59), as well as unitary invariance of the trace norm, we obtain

$$\|\rho_n - \sigma_n\|_1 = \left\| \left(\prod_{i=1}^{n} T\hat{U}_i \right) (\rho_0 - \sigma_0) \right\|_1 \leqslant \kappa(T)^n \|\rho_0 - \sigma_0\|_1 . \quad (60)$$

Now suppose that, at the end of the computation, we perform a measurement with precision ϵ, i.e., any two states ρ, σ with $\|\rho - \sigma\|_1 < \epsilon$ are considered indistinguishable. Then, if the computation takes at least $N_0 = \lceil \log(\epsilon/2)/\log \kappa(T) \rceil$ steps, we will have $\|\rho_n - \sigma_n\|_1 < \epsilon$ for all $n \geqslant N_0$. For a numerical illustration, we take $\kappa(T) = 0.9$ and $\epsilon = 0.01$, which yields $N_0 = 50$. In other words, the result of any computation that takes more than 50 steps in the presence of a strictly contractive channel T with $\kappa(T) = 0.9$ is untrustworthy since we will not be able to distinguish between any two states ρ and σ with $\|\rho - \sigma\|_1 < 0.01$. Again, N_0 depends only on the contractivity modulus of T and on the measurement precision ϵ, not on the dimension of $\mathcal{H}$, at least not explicitly. We note that, if the state of the computer is a density operator over a 2^k-dimensional Hilbert space, then any efficient quantum computation will take $O(\mathrm{Poly}(k))$ steps, and therefore the sensitivity of the computer to errors grows exponentially with k.

Let us consider some cases where the sequence $\{\rho_n\}$ does converge. Suppose first that the channel $T \in C_{\mathrm{sc}}$ is unital. Then, since each channel $\hat{U}_i$ is unital as well, the sequence $\{\rho_n\}$ converges exponentially fast to the maximally mixed state $\mathbb{1}/d$, where $d = \dim\mathcal{H}$. If the computation employs a static algorithm, i.e., $\hat{U}_i = \hat{U}$ for all i (this is true, e.g., in the case of Grover's search algorithm [35]), then the channel $S := T\hat{U}$ is also strictly contractive, and $\kappa(S) = \kappa(T)$ by unitary invariance of the trace norm. Denoting the fixed point of S by ρ_S, we then have

$$\|\rho_n - \rho_S\|_1 = \|S^n \rho_0 - S^n \rho_S\|_1 \leqslant \kappa(T)^n \|\rho_n - \rho_S\|_1 , \quad (61)$$

i.e., the output state of any sufficiently lengthy computation with a static algorithm will be indistinguishable from the fixed point ρ_S of $S = T\hat{U}$.

C. Impossibility of perfect error correction

After we have seen in the preceding section that quantum memories and computers are ultrasensitive to errors modeled by strictly contractive channels, we must address the issue of error correction (stabilization of quantum information). Since we have not made any specific assumptions (beyond strict contractivity) about the errors affecting the computer, it is especially important to investigate the possibility of error correction, if only to determine the limitations on the robustness of physically realizable quantum computers from the foundational standpoint.

First of all, strict contractivity rules out the possibility of perfect quantum error-correcting codes [3]. Let us recall the basics of QECC's. We seek to protect a quantum system with a k-dimensional Hilbert $\mathcal{H}$ space by realizing it as a subspace $\mathcal{K}$ (called the *code*) of a larger n-dimensional Hilbert space $\mathcal{H}_c$, known as the *coding space*. In other words, the Hilbert space $\mathcal{H}$ is embedded in the coding space $\mathcal{H}_c$ via the isometric encoding operator $V_{\mathrm{enc}}: \mathcal{H}\to\mathcal{K}$. Now, for any channel T on $\mathcal{S}(\mathcal{H}_c)$, a theorem of Knill and Laflamme [3] asserts that a subspace $\mathcal{K}$ of $\mathcal{H}_c$ can serve as a *T-corrrecting code* if and only if there exists some channel S on $\mathcal{S}(\mathcal{H}_c)$ such that $ST|_{\mathcal{K}}=\mathrm{id}$. In other words, S is the left inverse of the restriction of T to $\mathcal{S}(\mathcal{K})$. However, if the channel T on $\mathcal{S}(\mathcal{H}_c)$ is strictly contractive, then no subspace $\mathcal{K}$ of $\mathcal{H}_c$ is a T-correcting code. Suppose, to the contrary, that such a subspace $\mathcal{K}$ exists, and let $\{e_\mu\}$ be any orthonormal basis of $\mathcal{K}$. Then there also exists some channel S on $\mathcal{S}(\mathcal{H}_c)$ that satisfies the Knill-Laflamme condition for T and $\mathcal{K}$. Thus

$$\|ST(|e_\mu\rangle\langle e_\mu|-|e_\nu\rangle\langle e_\nu|)\|_1=\||e_\mu\rangle\langle e_\mu|-|e_\nu\rangle\langle e_\nu|\|_1 \tag{62}$$

for all μ, ν. But, using Eq. (16) and strict contractivity of T, we also have

$$\||e_\mu\rangle\langle e_\mu|-|e_\nu\rangle\langle e_\nu|\|_1\leqslant\kappa(T)\||e_\mu\rangle\langle e_\mu|-|e_\nu\rangle\langle e_\nu|\|_1, \tag{63}$$

which yields $\kappa(T)\equiv 1$. Since T is strictly contractive, this is a contradiction, and therefore no subspace $\mathcal{K}$ of $\mathcal{H}_c$ is a T-correcting code.

Before we go on, we must mention that the Knill-Laflamme theorem provides also for approximately correctable channels. That is, let $\{K_i\}$ be the set of the Kraus operators of some channel T on $\mathcal{S}(\mathcal{H}_c)$. For any subset Λ of $\{K_i\}$, we can define the completely positive map T_Λ via

$$T_\Lambda(X):=\sum_{K_i\in\Lambda}K_iXK_i^*,\quad\forall\ X\in\mathcal{B}(\mathcal{H}_c). \tag{64}$$

Then a subspace $\mathcal{K}$ of $\mathcal{H}_c$ can serve as a T_Λ-correcting code if there exists some channel S on $\mathcal{S}(\mathcal{H}_c)$ such that $ST_\Lambda|_{\mathcal{K}}\propto\mathrm{id}$. If $\|T-T_\Lambda\|_{\mathrm{cb}}$ is sufficiently small, then the errors modeled by the channel T are approximately correctable. Thus, in and of itself, the impossibility of perfect error correction for strictly contractive channels is not likely to be a serious problem.

However, strict contractivity also proscribes the existence of noiseless subsystems in the sense of Knill-Laflamme-Viola [6] and Zanardi [7], the essence of which we now summarize. Given some quantum system (computer) **Q** with the associated finite-dimensional Hilbert space $\mathcal{H}$, we consider the error channel T with Kraus operators K_i. We define the *interaction algebra* $\mathfrak{K}$ of T as a *-algebra generated by K_i. It is obvious that $\mathfrak{K}$ is an algebra with identity because of the condition $\Sigma_iK_i^*K_i=\mathbb{1}$. However, since the Kraus representation of a channel T is not unique, we must make sure that, for any two choices $\{K_i\}$ and $\{K_\mu\}$ of Kraus representations of T, the corresponding interaction algebras are equal. Using the fact that any two Kraus representations of a channel are connected via

$$K_i=\sum_\mu v_{i\mu}K_\mu, \tag{65}$$

where $v_{i\mu}$ are the entries of a matrix V with $V^*V=\mathbb{1}$ (assuming that one of the sets $\{K_i\}$ and $\{K_\mu\}$ is padded with zero operators in order to ensure that they have the same cardinality), we see that it is indeed the case that the interaction algebra of a channel T does not depend on the particular choice of the Kraus operators.

The existence of noiseless subsystems of **Q** with respect to T hinges on the reducibility of the interaction algebra $\mathfrak{K}$. Since $\mathfrak{K}$ is a uniformly closed *-subalgebra of $\mathcal{B}(\mathcal{H})$, it is a finite-dimensional C^*-algebra, and is therefore isomorphic to a direct sum of r full matrix algebras, each of which appears with multiplicity m_i and has dimension n_i^2 (i.e., it is an algebra of $n_i\times n_i$ complex matrices). Thus $\dim\mathfrak{K}=\Sigma_{i=1}^r n_i^2$. The *commutant* $\mathfrak{K}'$ of $\mathfrak{K}$ is defined as the set of all operators $X\in\mathcal{B}(\mathcal{H})$ that commute with all $K\in\mathfrak{K}$. From the Wedderburn theorem [15] it follows that each $K\in\mathfrak{K}$ has the form

$$K=\bigoplus_{i=1}^r\mathbb{1}_{m_i}\otimes K_i,\quad K_i\in M_{n_i}(\mathbb{C}), \tag{66}$$

and that each $K'\in\mathfrak{K}'$ has the form

$$K'=\bigoplus_{i=1}^r K_i'\otimes\mathbb{1}_{n_i},\quad K_i'\in M_{m_i}(\mathbb{C}). \tag{67}$$

Thus $\dim\mathfrak{K}'=\Sigma_{i=1}^r m_i^2$. We have the corresponding isomorphism

$$\mathcal{H}\simeq\bigoplus_{i=1}^r\mathbb{C}^{m_i}\otimes\mathbb{C}^{n_i}, \tag{68}$$

and each factor $\mathbb{C}^{m_i}$ is referred to as a *noiseless subsystem* because it is effectively decoupled from the error channel T. It is rather obvious that, in order to be of any use, a noiseless subsystem must be nontrivial, i.e., at least two-dimensional. Now, if the interaction algebra $\mathfrak{K}$ is irreducible, then $\dim\mathfrak{K}'=1$, and no noiseless subsystems exist. There is a simple criterion of irreducibility of an algebra, the Schur's lemma [14], which states that a *-algebra $\mathfrak{A}$ is irreducible if and only if its commutant $\mathfrak{A}'$ consists of complex multiples of the identity. We are now ready to state two main results of this section.

Proposition 2. Let T be a strictly contractive unital channel. Then T admits no noiseless subsystems.

Proof. Let us pick a Kraus representation $\{K_i\}$ of T, and let $\mathfrak{K}$ be the corresponding interaction algebra. We observe that if any $X\in\mathcal{B}(\mathcal{H})$ belongs to $\mathfrak{K}'$, then X is a fixed point of T on $\mathcal{B}(\mathcal{H})$. Indeed,

$$X\in\mathfrak{K}'\Rightarrow T(X)=\sum_i K_iXK_i^*=X\sum_i K_iK_i^*. \tag{69}$$

Since T is unital, $\Sigma_iK_iK_i^*=\mathbb{1}$, and thus $T(X)=X$. Now, if $X\in\mathfrak{K}'$, then $X^*\in\mathfrak{K}'$ as well, which implies that $X_1:=(X+X^*)/2$ and $X_2:=(X-X^*)/2i$ belong to $\mathfrak{K}'$. Therefore we only need to show that any self-adjoint $X \in \mathfrak{K}'$ has the form $r\mathbb{1}$ for some $r \in \mathbb{R}$. For any self-adjoint X, the operator $|X| := (X^2)^{1/2}$ belongs to the algebra generated by X^2, so

$$X = X^* \in \mathfrak{K}' \Rightarrow X_\pm := \frac{|X| \pm X}{2} \in \mathfrak{K}'. \tag{70}$$

Since $X = X_+ - X_-$ and $X_\pm \geqslant 0$, we reduce our task to proving that any positive X in $\mathfrak{K}'$ is a multiple of the identity. Without loss of generality, we may assume that $\|X\|_1 = 1$. Since $X \geqslant 0$, we must have $X \in \mathcal{S}(\mathcal{H})$; since X belongs to the commutant of $\mathfrak{K}$, it is also a fixed point of T. Thus $X = \mathbb{1}/\dim\mathcal{H}$, and the commutant $\mathfrak{K}'$ of the interaction algebra $\mathfrak{K}$ consists of complex multiples of the identity. ■

The proof of Proposition 2 depends in an essential way on the uniqueness of the fixed point of a strictly contractive channel, as well as on the condition satisfied by the Kraus operators of a unital channel. It turns out, however, that the statement of Proposition 2 can be strengthened to include *all* strictly contractive channels.

Proposition 3. Let T be a strictly contractive channel. Then T admits no noiseless subsystems.

Proof. Let $\mathfrak{K}$ be the interaction algebra of the channel T. Let us suppose, contrary to the statement of the Proposition, that T admits at least one noiseless subsystem (i.e., $\mathfrak{K}$ is reducible). That is, there exists at least one $j \in \{1, \dots, r\}$ such that $m_j, n_j \geqslant 2$ in Eqs. (66)–(68). Let $\mathcal{K}$ be some closed subspace of $\mathcal{H}$. Restricting the channel T to the set

$$\mathcal{S}(\mathcal{K}) := \{\rho \in \mathcal{S}(\mathcal{H}) \,|\, \mathrm{supp}\,\rho \subseteq \mathcal{K}\} \tag{71}$$

(where supp ρ is the orthogonal complement of ker ρ), we note that, by definition, the contractivity modulus of the restricted channel cannot exceed the contractivity modulus of T. Let $\mathcal{H}_j$ be the jth direct summand $\mathbb{C}^{m_j} \otimes \mathbb{C}^{n_j}$ in Eq. (68). Define the channel T_j as the restriction of T to $\mathcal{S}(\mathcal{H}_j)$. Then any Kraus operator of T_j has the form $\mathbb{1}_{m_j} \otimes K_\mu$ where $K_\mu \in M_n(\mathbb{C})$ and

$$\sum_\mu K_\mu^* K_\mu = \mathbb{1}_n. \tag{72}$$

Furthermore, $\kappa(T_j) \leqslant \kappa(T) < 1$. Now T_j is the channel of the form $\mathrm{id} \otimes S_j$, where S_j is the channel on $\mathcal{S}(\mathbb{C}^{n_j})$ with Kraus operators K_μ. As we have shown in Sec. III A, channels of this form are not strictly contractive (or even weakly contractive). Thus $\kappa(T_j) = 1$, and the Proposition is proved, *reductio ad absurdum*. ■

The result of Proposition 3 is quite shocking as it unequivocally rules out the existence of noiseless subsystems for any strictly contractive channel. From the standpoint of foundations of the quantum theory, the importance of Proposition 3 lies in the fact that it establishes nonexistence of noiseless subsystems for a wide class of physically realizable quantum computers on the basis of a minimal set of assumptions. Furthermore, from the mathematical point of view, it is rather remarkable that strict contractivity of a channel already implies irreducibility of its interaction algebra. We must, however, hasten to emphasize that, despite its sweeping generality, Proposition 3 should not be considered as a proof of the impossibility of building a reliable quantum computer. It merely rules out the possibility of building quantum computers with a *perfect* protection against errors modeled by strictly contractive channels.

D. Approximate error correction

At this point we must realize that the results of the preceding section are not as unexpected as they may seem. After all, nothing is perfect in the real world. Therefore, our error-correction schemes must, at best, come as close as possible to the perfect scenario. Of course, the precise criteria for determining how close a given error-correction scheme is to the "perfect case" will vary depending on the particular situation, but we can state perhaps the most obvious criterion in terms of the distinguishability of channels.

Let us first phrase everything in abstract terms. Let the error mechanism affecting the computer be modeled by some channel T. We assume that there exists some positive $\delta < 1$, which, in some way, characterizes the channel T (it could be given, e.g., by the minimum of the operator norms of the Kraus operators of T, and thus quantify the "smallest" probability of an error occurring). Let $\mathcal{H}$ be the Hilbert space associated with the computer. Then, for each $\epsilon > 0$, we define a (ϵ, δ)-*approximate error-correcting scheme* for T to consist of the following objects. (1) an integer $n > 1$; (2) a Hilbert space $\mathcal{H}_{\mathrm{ext}}$ with dim $\mathcal{H}_{\mathrm{ext}} \geqslant \dim\mathcal{H}$; (3) a channel $E: \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H}_{\mathrm{ext}})$, (4) a channel $\tilde{T}: \mathcal{S}(\mathcal{H}_{\mathrm{ext}}) \to \mathcal{S}(\mathcal{H}_{\mathrm{ext}})$, and (5) a completely positive (CP) map $T_{\mathrm{corr}}: \mathcal{S}(\mathcal{H}_{\mathrm{ext}}) \to \mathcal{S}(\mathcal{H}_{\mathrm{ext}})$, such that the channel $\tilde{T}$ depends uniquely on n, $\mathcal{H}_{\mathrm{ext}}$, T, and E; the CP map T_{corr} is correctable (say, in the Knill-Laflamme sense, or through other means, depending on the particular situation); and we have the estimate

$$\|\tilde{T} - T_{\mathrm{corr}}\|_{\mathrm{cb}} < \delta^n < \epsilon. \tag{73}$$

Let us give a concrete example in order to illustrate the above definition. Suppose that the channel T is of the form $\mathrm{id} + \mathcal{S}$ with $\|\mathcal{S}\|_{\mathrm{cb}} < \delta$. Then, for any n, we can write

$$T^{\otimes n} = \mathrm{id} + \sum_{\substack{A \subset \{1,\dots,n\} \\ 0 < |A| < n}} \bigotimes_{k=1}^{n} S^{\iota_A(k)} + S^{\otimes n}, \tag{74}$$

where $|A|$ denotes the cardinality of the set A, and $\iota_A: \{1, \dots, n\} \to \{0,1\}$ is the indicator function of A. We use the convention that, for any map M, $M^0 = \mathrm{id}$. In other words, the summation on the right-hand side of Eq. (74) consists of tensor product terms with one or more identity factors. For the last term, we have $\|\mathcal{S}^{\otimes n}\|_{\mathrm{cb}} < \delta^n$.

In this case, given some $\epsilon > 0$, we pick such n that $\delta^n < \epsilon$ and let $\mathcal{H}_{\mathrm{ext}} := \mathcal{H}^{\otimes n}$. If the CP map given by the sum of the first two terms on the right-hand side of Eq. (74) is correctable on some subspace $\mathcal{K}$ of $\mathcal{H}_{\mathrm{ext}}$, then the channel E is defined in a natural way through the composition of the following two operations: (a) adjoining additional $n-1$ copies of $\mathcal{H}$, each in some suitable state ρ_0, and (b) restricting to the subspace $\mathcal{K}$. This way, we obviously have $\tilde{T} := T^{\otimes n}$ and

$$T_{\mathrm{corr}} := \mathrm{id} + \sum_{\substack{A\subset\{1,\dots,n\}\\ 0<|A|<n}} \bigotimes_{k=1}^{n} S^{\iota_A(k)}. \tag{75}$$

The estimate (73) holds because $\tilde{T} - T_{\mathrm{corr}} = \mathcal{S}^{\otimes n}$. We note that this construction results in a quantum error-correcting code that corrects any $n-1$ errors. We can use similar reasoning to describe quantum codes that correct $k<n$ errors.

Constructing $\mathcal{H}_{\mathrm{ext}}$ as a tensor product of a number of copies of $\mathcal{H}$, the Hilbert space of the computer, evidently leads to the usual schemes for fault-tolerant quantum computation [36]. Other solutions, such as embedding the finite-dimensional Hilbert space $\mathcal{H}$ in a suitable infinite-dimensional Hilbert space (e.g., encoding a qubit in a harmonic oscillator [37]), can also be formulated in a manner consistent with our definition above.

Let us now address approximate correctability of strictly contractive errors. In Sec. IV B we have demonstrated that, in the absence of error correction, the sensitivity of quantum memories and computers to such errors grows exponentially with storage and computation time, respectively. Let T be a strictly contractive error channel. It is obvious that the appropriate approximate error-correction scheme must be such that the contraction rate of the ‘‘encoded’’ computer, where the errors are now modeled by the channel $\tilde{T}$, is effectively slowed down. In some cases, straightforward tensor-product realization may prove useful (e.g., when the product channel $T\otimes T$ is not strictly contractive). We must recall that, for any channel S, a necessary condition for correctability is $\kappa(S)=1$. Thus, if we can find a suitable approximate error-correcting scheme where $\tilde{T}$ would be well approximated by some channel T_{corr} with $\kappa(T_{\mathrm{corr}})=1$, we may effectively slow down the contraction rate by protecting the encoded computer against errors modeled by T_{corr}. A more ingenious approach may call for replacing circuit-based quantum computation with that in massively parallel arrays of interacting particles; several such implementations have already been proposed [38]. It is quite likely that the possible ‘‘encodings’’ of quantum computation in these massively parallel systems [39] may offer a more efficient implementation of approximate error correction.

Finally, we should mention that the idea of ‘‘approximate’’ noiseless subsystems has already been explored by Bacon, Lider, and Whaley [40]. In their work, it is argued that the symmetry, which is required of a channel in order for noiseless subsystems to exist, is generally broken by perturbing the channel. They show that, if the perturbations of the channel are ‘‘reasonable,’’ then the noiseless subsystem is stable to second order in time. We must reiterate that the negative results we have stated in the preceding section refer only to the nonexistence of ‘‘perfectly’’ noiseless subsystems; in the real world, we would have no choice but to settle for ‘‘almost perfect’’ anyway.

V. CONCLUSION

In this paper, we have offered an argument that errors in physically realizable quantum computers are naturally modeled by strictly contractive channels, i.e., channels that uniformly shrink, in the trace norm, the set of all density operators of the system under consideration. In particular, no two density operators in the image of a strictly contractive channel have orthogonal supports, which implies that any measurement designed to distinguish between these density operators will err with probability bounded away from zero. This implies, in turn, that there exists some precision threshold $\epsilon>0$ such that any two density operators ρ, σ with $\|\rho-\sigma\|_1<\epsilon$ cannot be distinguished by a particular experimentally available measuring apparatus.

We can turn this reasoning around by first postulating the existence of a precision threshold ϵ that would quantify resolving power of the least precise instrument employed in the experiment. As we have argued, the physical interpretation of the precision threshold boils down to limits on our ability to distinguish between density operators. A nonzero lower bound on the probability of error in optimum quantum hypothesis testing can thus be taken as an indication that the combined influence of the environmental noise and experimental imprecisions (which, in fact, are quite likely to be caused by indelible quantum-inechanical effects, such as vacuum fluctuations) can be economically captured by the concept of a strictly contractive channel.

As we have shown, the set C_{sc} of all strictly contractive channels on a given system $\mathbf{Q}$ is dense in the set C of all channels on $\mathbf{Q}$. Since no finite-precision measurement will be able to distinguish between an arbitrary channel T and some strictly contractive channel T', it is reasonable to ascribe to strictly contractive channels the property of ‘‘experimental reality,’’ just as we would ascribe this property to elements of the set $[0,2\pi)\cap\mathbb{Q}$ (where $\mathbb{Q}$ is the set of rational numbers) in any experiment involving finite-precision measurements of angles.

In light of this interpretation, it is important to investigate the robustness of quantum memories and computers in the presence of strictly contractive errors. We have found that, in the absence of error correction, any state stored in a noisy quantum register converges exponentially fast to the fixed point of the error channel T, and the rate of convergence is independent of the dimension of the register Hilbert space. In other words, the sensitivity of quantum registers to strictly contractive noise is an intensive property, i.e., independent of the register's size. Similarly, computations performed on a noisy quantum computer with different initial states quickly yield indistinguishable results, again at a rate that does not depend on the computer's size (number of qubits). Furthermore, the property of strict contractivity turns out to be strong enough to proscribe the existence of noiseless subsystems of the computer affected by any strictly contractive error channel.

However, these results are more of a blessing than a curse for the future of quantum information processing: they certainly indicate that the successful solution of problems faced by researchers in this field will require models of computers far more ingenious than networks of one- and two-qubit gates. As we have mentioned above, systems of interacting particles (or quantum cellular automata) may well prove to be a viable medium for the experimental realization of large-scale quantum computers. In this respect, we would like to point out a possible connection between strictly contractive channels and ergodic quantum cellular automata [41]. A cellular automaton is ergodic if it possesses a unique invariant state, which it reaches irrespective of initial conditions, and this is exactly the property shared by quantum systems under the influence of strictly contractive errors. As an example, let us consider information storage in a quantum cellular automaton. It is essential that this automaton be nonergodic, for otherwise it would not be able to ‘‘remember’’ anything. Assuming that each cell (site) of the automation is under the influence of some strictly contractive error channel T, an interesting problem would be to devise such a transition rule that the automaton would not be ergodic. In this respect, we should mention that, while T is a strictly contractive channel, it is not at all obvious whether $T\otimes T$ is strictly contractive as well: it has a unique fixed point among the product density operators, namely, $\rho_T\otimes\rho_T$, but there may also be another fixed point of $T\otimes T$ that is not a product density operator.

Finally we mention one more point worth exploring. In our discussion of physically realizable quantum computers, we have implicitly assumed that the (im)precision of all experimentally available procedures can be traced back to the (im)precision of state preparation, quantified by some threshold value ϵ (i.e., when we say that state ρ has been prepared, we mean that any state σ with $\|\rho-\sigma\|_1<\epsilon$ may have emerged from our preparing apparatus), as well as the (im)precision of measurements (we would not be able to distinguish any two states ρ, σ with $\|\rho-\sigma\|_1<\epsilon$). This is suggestive of Ludwig’s axiomatics of quantum theory [42], and it would be theoretically rewarding to consider physically realizable quantum computers from this axiomatic perspective as well.

ACKNOWLEDGMENTS

The author would like to thank G. M. D’Ariano, M. Ozawa, and H. P. Yuen for enlightening discussions and constructive criticism and D.A. Lidar for interesting comments and pointers to useful references. This work was supported by the U.S. Army Research Office through MURI Grant No. DAAD19-00-1-0177.

[1] W. G. Unruh, Phys. Rev. A **51**, 992 (1995); G. M. Palma, K.-A. Suominen, and A. K. Ekert, Proc. R. Soc. London, Ser. A **452**, 567 (1996).

[2] From this point on, we will refer to quantum computers as simply ‘‘computers’’ for brevity.

[3] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).

[4] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).

[5] D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).

[6] E. Knill, R. Laflamme, and L. Viola, Phys. Rev. Lett. **84**, 2525 (2000).

[7] P. Zanardi, Phys. Rev. A **63**, 012301 (2001).

[8] Please note that we must be careful to distinguish *precision*, which is a figure of merit for individual operations, from *accuracy*, which is a term that refers to repeated operations of the same kind (cf., [11] for a thorough discussion). In our case, precision of a physically realizable computer is a measure of the closeness of its output state to that of the ideal computer, while accuracy quantifies the closeness of output states, generated by the computer on repeated runs, in terms of the closeness of the corresponding input states.

[9] R. Durrett, *Probability: Theory and Examples*, 2nd ed. (Wadsworth, Belmont, 1996).

[10] E. Bernstein and U. Vazirani, SIAM J. Comput. **26**, 1411 (1997).

[11] T. Brody, *The Philosophy Behind Physics* (Springer-Verlag, Berlin, 1993), pp. 139–156.

[12] D. A. Meyer, Phys. Rev. Lett. **83**, 3751 (1999).

[13] O. Bratteli and D. W. Robinson, *Operator Algebras and Quantum Statistical Mechanics*, 2nd ed. (Springer-Verlag, New York, 1987), Vol. 1, pp. 42–64.

[14] D. P. Zhelobenko, *Compact Lie Groups and Their Representations* (American Mathematical Society, Providence, 1978).

[15] R. Bhatia, *Matrix Analysis* (Springer-Verlag, New York, 1997), Chap. IV.

[16] A. Yu. Kitaev, Russ. Math. Surveys **52**, 1191 (1997).

[17] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982), p. 28.

[18] K. Kraus, *States, Effects, and Operations* (Springer-Verlag, Berlin, 1983).

[19] V. I. Paulsen, *Completely Bounded Maps and Dilations* (Longman, Harlow, UK, 1986).

[20] D. Aharonov, A. Yu. Kitaev, and N. Nisan, in *Proceedings of the 30th ACM Symposium on Theory of Computing* (ACM Press, New York, 1998), p. 20.

[21] G. Giedke, H. J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 2641 (1999).

[22] A. S. Holevo and R. F. Werner, Phys. Rev. A **63**, 032312 (2001).

[23] M. Raginsky, Phys. Lett. A **290**, 11 (2001).

[24] G. M. D’ariano, P. Lo Presti, and M. G. A. Paris, Phys. Rev. Lett. **87**, 270404 (2001).

[25] M. Reed and B. Simon, *Methods of Modern Mathematical Physics I: Functional Analysis* (Academic, San Diego, 1980), Chap. V.

[26] I. Stakgold, *Green’s Functions and Boundary Value Problems*, 2nd ed. (Wiley, New York, 1998), Chap. 4.

[27] G. Mahler and V. Weberruss, *Quantum Networks*, 2nd ed. (Springer-Verlag, 1998), Chap. 2.

[28] D. Bruss, L. Faoro, C. Macchiavello, and G. M. Palma, J. Mod. Opt. **47**, 325 (2000).

[29] M. B. Ruskai, S. Szarek, and E. Werner, LANL e-print quant-ph/0101003.

[30] G. G. Amosov, A. S. Holevo, and R. F. Werner, Probl. Inf. Transm. **36**, 25 (2000).

[31] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976), Chap. IV.

[32] H. P. Yuen, LANL e-print quant-ph/0006109 v7 (Appendix A).

[33] Our definition of a quantum circuit differs from the conven-

tional one. See, e.g., A. C.-C. Yao, in Proceedings of the 34th IEEE Symposium on Foundations of Computer Science, IEEE Computer Society, Palo Alto, CA (1993), p. 352.

[34] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[35] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[36] J. Preskill, Proc. R. Soc. London, Ser. A **454**, 385 (1998).

[37] D. Gottesman, A. Yu. Kitaev, and J. Preskill, Phys. Rev. A **64**, 012310 (2001).

[38] P. Zanardi and F. Rossi, Phys. Rev. B **59**, 8170 (1999); H. J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001); R. Raussendorf and H. J. Briegel, *ibid.* **86**, 5188 (2001).

[39] The term ‘‘massively parallel’’ here refers to the symmetrical nature of quantum arrays of interacting particles. This usage is different from the usual connotation of massive parallelism, intrinsic in the mathematical structure of quantum theory.

[40] D. Bacon, D. A. Lidar, and K. B. Whaley, Phys. Rev. A **60**, 1944 (1999).

[41] S. Richter and R. F. Werner, J. Stat. Phys. **82**, 963 (1996).

[42] G. Ludwig, *An Axiomatic Basis for Quantum Mechanics* (Springer-Verlag, Berlin, 1985), Vols. 1 and 2.