PHYSICAL REVIEW A **92**, 022355 (2015)

No-signaling bounds for quantum cloning and metrology

P. Sekatski, M. Skotiniotis, and W. Dür

Institut für Theoretische Physik, Universität Innsbruck, Technikerstr. 25, A-6020 Innsbruck, Austria

(Received 23 January 2015; revised manuscript received 5 May 2015; published 28 August 2015)

The impossibility of superluminal communication is a fundamental principle of physics. Here we show that this principle underpins the performance of several fundamental tasks in quantum information processing and quantum metrology. In particular, we derive tight no-signaling bounds for probabilistic cloning and superreplication that coincide with the corresponding optimal achievable fidelities and rates known. In the context of quantum metrology, we derive the Heisenberg limit from the no-signaling principle for certain scenarios including reference frame alignment and maximum likelihood state estimation. We elaborate on the equivalence of assymptotic phase-covariant cloning and phase estimation for different figures of merit.

DOI: 10.1103/PhysRevA.92.022355 PACS number(s): 03.67.Hk, 03.67.−a, 03.65.−w

I. INTRODUCTION

Nothing can travel faster than the speed of light. This is one of the pillars of modern physics and an explicit element of Einstein's theory of relativity. Any violation of this principle would lead to problems with local causality giving rise to logical contradictions. This principle not only applies to matter, but also to information, rendering superluminal communication impossible. While not explicitly contained in the postulates of quantum mechanics all attempts to construct or observe violations of this principle have failed, leading us to believe that this is indeed a basic ingredient of our description of nature. In fact, modifications of quantum mechanics, e.g., by allowing nonlinear dynamics, would lead to signaling and a violation of this fundamental principle [1–3]. It is therefore natural to assume that no-signaling holds and try to deduce what follows under such an assumption.

Indeed, the no-signaling principle has been used to derive bounds and limitations on several physical processes and tasks. These include the observation that a perfect quantum copying machine would allow for superluminal communication [4–6], limitations on universal quantum $1 \rightarrow 2$ cloning [7,8] and $1 \rightarrow M$ cloning [9], a security proof for quantum communication [10], optimal state discrimination [11], and bounds on the success probability of port-based teleportation [12]. However, no-signaling alone is not restrictive enough as it allows for stronger nonlocal correlations than possible within quantum mechanics [13], and several attempts have been made to further supplement the no-signaling principle in order to retrieve quantum mechanical correlations [14–17].

Here we derive limitations on optimal quantum strategies from fundamental principles. In particular we show the following:

(1) Tight no-signaling bound on probabilistic phase-covariant quantum cloning.

(2) Asymptotically tight no-signaling bound on unitary superreplication.

(3) A derivation of the Heisenberg limit for metrology from the no-signaling condition.

(4) Quantum protocols that achieve the bounds placed by no-signaling.

We assume the Hilbert space structure of pure states and show how the no-signaling principle directly leads to tight bounds on different fundamental tasks in quantum information processing and quantum metrology. We start by showing how the impossibility of faster-than-light communication between Alice and Bob can be used to provide upper bounds on Bob's ability to perform certain tasks, even if Bob has access to supraquantum resources. Not only does the no-signaling principle allow us to prove ultimate limits on these fundamentally important tasks, it also allows us to demonstrate the optimality of known protocols and shed light on the recently discovered possibility of probabilistic superreplication of states [18] and operations [19,20].

We derive a no-signaling bound on the global fidelity of $N \rightarrow M$ probabilistic phase-covariant cloning [18]. Our derivation is constructive, and we provide the optimal deterministic quantum protocol that achieves the bound [18]. In similar fashion, we derive a no-signaling bound on the replication of unitary operations [19], which is tight in the large M limit. Furthermore, we derive the Heisenberg limit of quantum metrology solely from the no-signaling principle, more specifically for phase reference alignment [21–23]. We find a tight no-signaling bound on the maximal likelihood and a bound with the correct scaling on the fidelity of reference frame alignment for phase both for the uniform prior as well as for a nonuniform prior probability distribution.

We show that the no-signaling condition can be used to establish bounds on the performance of quantum information tasks for which no bounds are known or for which the brute force optimization of the tasks is hard. This demonstrates an alternative approach to establish the possibilities and limitations of quantum information processing, which is based on fundamental principles rather than actual protocols. We emphasize that this approach is not limited to the specific tasks discussed here but is generally applicable.

We also discuss the correspondence between asymptotic phase-covariant quantum cloning and state estimation and establish the correspondence between different figures of merit for the two tasks. Finally we supplement our approach by a general argument, extending that of Ref. [3], showing that optimal quantum protocols are at the edge of no-signaling.

II. NO SIGNALING

In this section we describe the operational setting underpinning all three tasks we consider (cloning, replication of unitaries, and metrology), as well as the no-signaling condition. All three tasks we consider can be described in the following operationally generic setting. A party, Bob, possess an N-qubit state,

$$|\Phi^N\rangle_B = \sum_{\mathbf{v}} a_{\mathbf{v}} |\mathbf{v}\rangle_B = \sum_{n=0}^{N} p_n \underbrace{\sum_{|\mathbf{v}|=n} \frac{a_{\mathbf{v}}}{p_n} |\mathbf{v}\rangle_B}_{|\tilde{n}\rangle_B}, \tag{1}$$

where $\mathbf{v}$ runs over all N-bit strings and $|\tilde{n}\rangle_B$ is a superposition over all states with Hamming weight $|\mathbf{v}| = n$. Bob then receives, via a remote preparation scenario to be described shortly, the action of a unitary operator $U_\theta^{\otimes N}$ such that

$$|\Phi_\theta^N\rangle = U_\theta^{\otimes N} |\Phi^N\rangle, \tag{2}$$

where $U_\theta = e^{i\theta H}$ with H an arbitrary Hamiltonian acting on two-level systems (qubits) with *spectral radius* $\sigma(H)$, θ uniformly chosen from $(0,2\pi\sigma(H)]$.

Bob has to process $U_\theta^{\otimes N}$ for some quantum information task in an optimal way. In particular, we do not demand that Bob's processing be described by linear maps, nor do we demand that the mapping from valid quantum states to probability distributions be given by the Born rule. All that we require of Bob's processing outcomes is that they should be valid inputs for someone whose processing power is limited by quantum theory. We choose such a setting because our goal is rather pragmatic: we wish to derive upper bounds on *quantum* information tasks. Hence, throughout this work we shall assume that all of Bob's *static* resources, i.e., pure states of physical systems, ensembles of pure states, and probability distributions, are described within the framework of quantum theory, but Bob's *dynamical* resources, i.e., processing maps, are not. In fact imposing no-signaling condition for quantum static resources is equivalent to imposing quantum mechanics (see Sec. VI), but when a direct optimization over quantum strategies is unfeasible, the no-signaling argument can help to show that a known strategy is optimal.

What Bob has to output varies depending on which task he performs. For example, if the required task is the cloning of the state $|\psi(\theta)\rangle$, then Bob has to output an M-qubit state, ρ_θ^M, that is a close approximation to $|\psi(\theta)\rangle^{\otimes M}$. If the required task is the replication of the unitary operator U_θ then Bob has to output a quantum channel acting on the Hilbert space of M qubits that is a close approximation to $U_\theta^{\otimes M}$. Finally, if the required task is to estimate the parameter θ, then Bob must output a probability distribution corresponding to his updated knowledge about parameter θ. We denote the outcome of Bob's processing, be it a quantum state, channel, or probability distribution, by $\mathcal{P}(\theta)$.

To incorporate the no-signaling condition we consider that Bob holds one part of a suitably chosen entangled state

$$|\Psi\rangle_{AB} = \sum_{n=0}^{N} p_n |n\rangle_A |\tilde{n}\rangle_B \tag{3}$$

which he shares with Alice, where Alice keeps the $(N+1)$-level system spanned by $\{|n\rangle_A\}$ and Bob holds the 2^N-dimensional system spanned by $\{|\tilde{n}\rangle_B\}$. The state $|\Psi\rangle_{AB}$ can always be chosen such that Bob receives the action of $U_\theta^{\otimes N}$ on an arbitrary input state. This is achieved by Alice first performing $(U_\theta^{\otimes N} \otimes \mathbb{1})|\Psi\rangle_{AB}$, followed by a measurement in

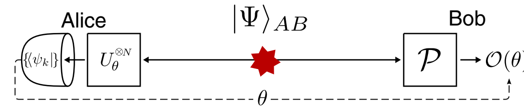

FIG. 1. (Color online) Generic setting for faster-than-light communication. Alice and Bob share an entangled state $|\Psi\rangle_{AB}$. By applying $U_\theta^{\otimes N}$ followed by a suitable measurement Alice can prepare any ensemble $\{p_k |\Phi_{\theta|k}\rangle\langle\Phi_{\theta|k}|\}$, which Bob processes into $\mathcal{O}(\theta) = \sum_k p_k \mathcal{P}(\theta|k)$. The no-signaling condition imposes that $\mathcal{O}(\theta)$ is independent of θ chosen by Alice.

the *Fourier basis* $\{|k\rangle \propto \sum_n e^{in\frac{2\pi k}{N+1}} |n\rangle_A\}$ with $k = 0,\dots,N$ (see Fig. 1). If Alice obtains outcome k, then Bob's state becomes

$$|\Phi^N_{\theta+\frac{2\pi k}{N+1}}\rangle = U^{\otimes N}_{\theta+\frac{2\pi k}{N+1}} |\Phi^N\rangle. \tag{4}$$

As all outcomes, $|k\rangle$, are equally likely, Bob ends up with a random state from the ensemble $\{|\Phi^N_{\theta+\frac{2\pi k}{N+1}}\rangle, k \in (0,\dots,N)\}$.

The no-signaling condition now requires that Bob, who does not know which unitary $U_\theta, \theta \in (0,2\pi]$ was chosen by Alice, cannot learn θ from the above ensemble no matter what processing power, quantum or otherwise, Bob has at his disposal. If this were not the case, then Alice and Bob, who are spatially separated, can use the above construction to perform faster-than-light communication. Denoting the outcome of Bob's processing by $\mathcal{P}(\theta|k)$ the no-signaling condition requires that the mixture

$$\mathcal{O}(\theta) = \frac{1}{N+1} \sum_{k=0}^{N} \mathcal{P}(\theta|k) \tag{5}$$

is independent of θ chosen by Alice.

Note that the no-signaling bound derived above is based on a particular way to embed a quantum information processing task into a communication scenario. The bound turns out to be tight in the present context but is not in general. We will come back to this point from a more general perspective in Sec. VI.

III. PROBABILISTIC PHASE COVARIANT CLONING

We first apply the no-signaling condition to the case of phase-covariant quantum cloning (PCC). The latter task involves cloning an unknown state from the set $\{|\psi(\theta)\rangle = U(\theta)|\psi\rangle\}$ [18,24]. We focus on PCC of equatorial states, $|\psi(\theta)\rangle = 1/\sqrt{2}(|0\rangle + e^{i\theta}|1\rangle)$, which play a crucial role in proving the security of quantum key distribution [10]. Specifically, we provide a bound for the optimal PCC of N qubits into $M > N$ qubits and show that this bound is achievable by a deterministic quantum mechanical strategy, if one drops the restriction of separable N-qubit input states. The latter strategy involves the use of a suitable N-partite entangled input state on which $U_\theta^{\otimes N}$ is applied. We stress that this task does not correspond to the usual definition of cloning, as in the literature cloning always assumes separable N-copy input states. We then show how our deterministic strategy is equivalent to the probabilistic PCC of Ref. [18], by introducing a suitable filter operation that maps $|\psi(\theta)\rangle^{\otimes N}$ to the suitable N-partite entangled state.

A *deterministic*, phase-covariant quantum cloning machine is some transformation, $\mathcal{C}$, whose input is N copies of an unknown equatorial qubit state $|\psi(\theta)\rangle$ that outputs an M-qubit state $\rho^M(\theta)=\mathcal{C}((|\psi(\theta)\rangle\langle\psi(\theta)|)^{\otimes N})$. Optimal deterministic cloning machines, be it state-dependent [24,25] or state-independent [26–29], have been constructed, and tight bounds, for the case of $1\to 2$ cloning, based on the no-signaling condition have been derived [7,8]. A probabilistic cloning machine is more powerful in that it allows for a much higher number of copies at the cost of succeeding only some of the time. Indeed, probabilistic PCC, when successful, can output up to N^2 faithful copies of $|\psi(\theta)\rangle$. However, the probability of success is exponentially small [18].

If the input state to the probabilistic PCC machine is remotely prepared by Alice, as explained in Sec. II, then the no-signaling condition on the output of Bob's probabilistic PCC procedure has to be independent of θ, i.e.,

$$\rho^M=\rho^M(\theta)=\frac{1}{N+1}\sum_{k\geqslant 0}^{N}\rho^M_{\theta+\frac{2\pi k}{N+1}}. \tag{6}$$

Following Ref. [18], we quantify the success of the cloning procedure by the *worst case global cloning fidelity*

$$F_{wc}^{\mathcal{C}_{N\to M}}=\inf_\theta F_C\big(\rho_\theta^M,(|\psi(\theta)\rangle\langle\psi(\theta)|)^{\otimes M}\big), \tag{7}$$

where $F_C(\rho_\theta^M,(|\psi(\theta)\rangle\langle\psi(\theta)|)^{\otimes M})=\mathrm{Tr}[\rho_\theta^M(|\psi(\theta)\rangle\langle\psi(\theta)|)^{\otimes M}]$ is the *global* fidelity between the output of the cloner and M perfect copies of the input state.

Recalling that the Uhlmann fidelity, $F_U(\rho,\sigma)=\mathrm{tr}\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}$ it follows that $F_C(\rho_\theta^M,(|\psi(\theta)\rangle\langle\psi(\theta)|)^{\otimes M})=F_U(\rho_\theta^M,(|\psi(\theta)\rangle\langle\psi(\theta)|)^{\otimes M})^2$. Moreover, as the worst case fidelity is always smaller or equal than the mean fidelity, the following bound holds:

$$F_{wc}^{\mathcal{C}_{N\to M}}\leqslant\left(\int\frac{d\theta}{2\pi}F_U\big(\rho_\theta^M,(|\psi(\theta)\rangle\langle\psi(\theta)|)^{\otimes M}\big)\right)^2.$$

Thus an upper bound for the worst case global cloning fidelity can be obtained by obtaining an upper bound on the mean Uhlmann fidelity.

In order to upper bound the mean Uhlmann fidelity we first rewrite the latter as

$$\begin{aligned}&\int\frac{d\theta}{2\pi}F_U\big(\rho_\theta^M,(|\psi(\theta)\rangle\langle\psi(\theta)|)^{\otimes M}\big)\\&=\int_0^{2\pi}\sum_{k=0}^N\frac{d\theta}{2\pi(N+1)}\\&\quad\times F_U\big(\rho^M_{\theta+\frac{2\pi k}{N+1}},(U_{\frac{2\pi k}{N+1}}|\psi(\theta)\rangle\langle\psi(\theta)|U^\dagger_{\frac{2\pi k}{N+1}})^{\otimes M}\big)\\&\leqslant\int_0^{2\pi}\frac{d\theta}{2\pi}F_U\left(\rho^M,\sum_{k=0}^N\frac{(U_{\frac{2\pi k}{N+1}}|\psi(\theta)\rangle\langle\psi(\theta)|U^\dagger_{\frac{2\pi k}{N+1}})^{\otimes M}}{N+1}\right),\end{aligned} \tag{8}$$

where we have used the joint concavity of the Uhlmann fidelity, $F_U(\sum_i p_i\rho_i,\sum_i p_i\sigma_i)\geqslant\sum_i p_iF_U(\rho_i,\sigma_i)$ in the last line of Eq. (8). As $|\psi(\theta)\rangle=U_\theta|+\rangle$, and $[U_{\frac{2\pi k}{N+1}},U_\theta]=0$, unitary invariance of the fidelity, $F(\rho,U\sigma U^\dagger)=F(U^\dagger\rho U,\sigma)$, allows us to shift the action of $U(\theta)^{\otimes M}$ onto ρ^M, and the integrand of Eq. (8) reads

$$\int_0^{2\pi}\frac{d\theta}{2\pi}F_U\left(U_\theta^\dagger\rho^MU_\theta,\sum_{k=0}^N\frac{(U_{\frac{2\pi k}{N+1}}|+\rangle\langle+|U^\dagger_{\frac{2\pi k}{N+1}})^{\otimes M}}{N+1}\right). \tag{9}$$

Finally using the concavity of the Uhlmann fidelity, $F(\sum_i p_i\rho_i,\sigma)\geqslant\sum_i p_iF(\rho_i,\sigma)$, to move the integral over θ inside the argument for the Uhlmann fidelity, and defining the maps $\mathcal{G}_{\mathbb{Z}_{N+1}}[\cdot]\equiv\frac{1}{N+1}\sum_{k=0}^NU^{\otimes M}_{\frac{2\pi k}{N+1}}(\cdot)U^{\dagger\otimes M}_{\frac{2\pi k}{N+1}}$ and $\mathcal{G}^\dagger_{\mathbb{U}(1)}[\cdot]\equiv\frac{1}{2\pi}\int_0^{2\pi}\mathrm{d}\theta\,U_\theta^{\dagger\otimes M}(\cdot)U_\theta^{\otimes M}$, we obtain the desired upper bound for the worst case global cloning fidelity:

$$F_{wc}^{\mathcal{C}_{N\to M}}\leqslant F_U\big(\mathcal{G}^\dagger_{\mathbb{U}(1)}[\rho^M],\mathcal{G}_{\mathbb{Z}_{N+1}}[(|+\rangle\langle+|)^{\otimes M}]\big)^2. \tag{10}$$

We now proceed to give an explicit expression for the upper bound of Eq. (10). The maps $\mathcal{G}$ impose a *block-diagonal* structure on any density matrix on which they act, making it it easy to find ρ_M that maximizes Eq. (10). As the state $(|+\rangle\langle+|)^{\otimes M}$ is symmetric under permutations it suffices to maximize over all symmetric ρ^M. For any permutation symmetric ρ^M, $\mathcal{G}^\dagger_{\mathbb{U}(1)}[\rho^M]$ is diagonal and can be written as

$$\mathcal{G}^\dagger_{\mathbb{U}(1)}[\rho^M]=\bigoplus_{n=0}^Mp_n\,|n,M\rangle\langle n,M|\,, \tag{11}$$

where $\{|n,M\rangle\}_{n=0}^M$ is an orthonormal basis spanning the symmetric subspace of M qubits with n qubits in state $|1\rangle$ and $M-n$ qubits in state $|0\rangle$. Correspondingly, we may write

$$\mathcal{G}_{\mathbb{Z}_{N+1}}[(|+\rangle\langle+|)^{\otimes M}]=\bigoplus_{\lambda=0}^N|\phi^{(\lambda)}\rangle\langle\phi^{(\lambda)}|\,, \tag{12}$$

where $|\phi^{(\lambda)}\rangle=\sum_{n|n \mod (N+1)=\lambda}\sqrt{\frac{\binom{M}{n}}{2^M}}|n,M\rangle$ are unnormalized pure symmetric states with the sum running over all n that have a reminder λ after division by $N+1$. The states $|\phi^{(\lambda)}\rangle$ have nonzero overlap with the symmetric states $|n,M\rangle$ whenever $n \mod (N+1)=\lambda$.

Because of the block-diagonal structure we rewrite the mean Uhlmann fidelity as

$$\begin{aligned}&F_U\big(\mathcal{G}^\dagger_{\mathbb{U}(1)}[\rho^M],\mathcal{G}_{\mathbb{Z}_{N+1}}[(|+\rangle\langle+|)^{\otimes M}]\big)\\&\quad=\sum_{\lambda=0}^N\sqrt{\langle\phi^{(\lambda)}|\,\mathcal{G}_{\mathbb{U}(1)}[\rho^M]\,|\phi^{(\lambda)}\rangle}.\end{aligned} \tag{13}$$

Denoting by $p_\lambda=\sum_{\{n|n \mod (N+1)=\lambda\}}p_n$ the probability of projecting $\mathcal{G}^\dagger_{\mathbb{U}(1)}[\rho^M]$ on the sector with a given λ we can maximize the Uhlmann fidelity by optimizing each sector λ independently. This is achieved by finding the n in each sector λ such that the overlap $\langle\phi^{(\lambda)}|n,M\rangle$ is maximized. The maximum Uhlmann fidelity then reads

$$\begin{aligned}&\max_{p_n}F_U\Big(\bigoplus_{n=0}^Mp_n\,|n,M\rangle\langle n,M|\,,\bigoplus_{\lambda=0}^N|\phi^{(\lambda)}\rangle\langle\phi^{(\lambda)}|\Big)\\&\quad=\max_{p_\lambda}\sqrt{p_\lambda\max_n|\langle\phi^{(\lambda)}|n,M\rangle|^2}=\sqrt{\sum_\lambda\max_n|\langle\phi^{(\lambda)}|n,M\rangle|^2}.\end{aligned} \tag{14}$$

The probability $|\langle\phi^{(\lambda)}|n,M\rangle|^2 = \frac{1}{2^M}\binom{M}{n}$ is given by the binomial distribution if $n \mod (N+1) = \lambda$ and is zero otherwise. Thus, it is always optimal to choose $n \mod (N+1)$ closest to $\frac{M}{2}$. Doing so for all λ we find that the maximal fidelity is given by the square root of the sum of the $N+1$ largest terms of the binomial distribution $\frac{1}{2^M}\binom{M}{n}$. Hence, the upper bound for the worst case global cloning fidelity reads

$$F_{wc}^{\mathcal{C}_{N\to M}} \leqslant \frac{1}{2^M}\sum_{\lambda=0}^{N}\binom{M}{\lfloor\frac{M-N}{2}\rfloor+\lambda}, \tag{15}$$

where $\lfloor\cdot\rfloor$ denotes the floor function. Finally, noting that the binomial distribution, $\frac{1}{2^M}\binom{M}{n}$ can be approximated by a Gaussian $\mathcal{N}(\mu = M/2, \sigma = \sqrt{M}/2)$, the upper bound in Eq. (15) can be approximated, for $M \gg N$, by

$$F_{wc}^{\mathcal{C}_{N\to M}} \leqslant \operatorname{erf}\left(\frac{N+1}{\sqrt{2M}}\right). \tag{16}$$

We note that as long as $M = \mathcal{O}(N^2)$ the upper bound in (16) approaches unity in the limit $N \to \infty$. Indeed, one can make an even stronger claim. Any replication procedure that respects the no-signaling condition and produces a number of replicas $M = \mathcal{O}(N^{2+\alpha})$ does so with a cloning fidelity that tends to zero exponentially fast.

We now show how one can achieve the no-signaling bound of Eq. (16) using a deterministic quantum mechanical strategy, as depicted in Fig. 2. Instead of N copies of $|\psi(\theta)\rangle$, suppose Bob prepares the entangled state

$$|\Phi^N\rangle \propto \sum_{\lambda=0}^{N}\sqrt{\binom{M}{\lfloor\frac{M-N}{2}\rfloor+\lambda}}\,|N,\lambda\rangle\,. \tag{17}$$

Bob now applies the cloning map $\mathcal{C} : |N,\lambda\rangle \mapsto |M, \lfloor\frac{M-N}{2}\rfloor+\lambda\rangle$ that maps totally symmetric N-qubit states to totally symmetric M-qubit states. This strategy achieves the bound of Eq. (16) as the latter is valid for all input states. We pause to note that the above result does not contradict the well-known limits for deterministic cloning, as in the latter Bob is forced to input N copies of a qubit state.

The bound of Eq. (16) is the ultimate bound that can be achieved even by a probabilistic strategy. Indeed, the best probabilistic quantum mechanical PCC attains precisely the no-signaling bound of Eq. (16) [18]. In fact, there is an easy way to see how the probabilistic strategy of Ref. [18] and the deterministic strategy described above are related. Starting from N copies of the state $|\psi(\theta)\rangle$, the probabilistic PCC of Ref. [18] has Bob first apply the probabilistic filter that projects onto the state $|\Phi^N\rangle$ of Eq. (17) and succeeds with probability $p_{yes} = |\langle\Phi^N|+\rangle^{\otimes N}|^2$. As such a filter commutes with the unitary $U_\theta^{\otimes N}$ it can be seen as part of the overall state preparation. The advantage, then, of probabilistic PCC can be simply understood as a passage from the standard quantum limit in quantum metrology, achieved for separable input states, to the Heisenberg limit achieved by entangled input states. Notice that no probabilistic advantage exists for the case of $1 \to M$ cloning. For the latter, the fidelity of Eq. (16) takes the simple form $F^{\mathcal{C}_{1\to M}} = \frac{1}{2^{M-1}}\binom{M}{\frac{M-1}{2}}$ for M odd and $F^{\mathcal{C}_{1\to M}} = \frac{1}{2^M}\binom{M+1}{\frac{M}{2}+1}$ for M even and is known to be achievable by a deterministic strategy [23].

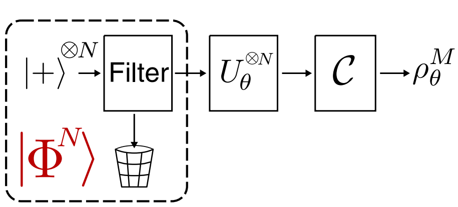

FIG. 2. (Color online) Equivalence between probabilistic PCC and deterministic PCC using arbitrary states. The filter in the probabilistic cloning can be viewed as part of a probabilistic preparation of a general state from a separable N-qubit state. Allowing for arbitrary input states makes the preparation process deterministic.

IV. REPLICATION OF UNITARIES

We now consider the task where Bob has to output an approximation, V_θ, of $U_\theta^{\otimes M}$ having received only N uses of the black box implementing the unitary transformation U_θ [19,30]. The figure of merit that one uses is the global Jamiołkowski fidelity (process fidelity) [31],

$$F\big(U_\theta^{\otimes M}, V_\theta\big) = \big\langle\psi_{U_\theta^{\otimes M}}\big|\,\rho_{V_\theta}\,\big|\psi_{U_\theta^{\otimes M}}\big\rangle, \tag{18}$$

averaged over all θ, where $|\psi_{U_\theta^{\otimes M}}\rangle = (\mathbb{1}\otimes U_\theta^{\otimes M})|\Phi^+\rangle$ and $\rho_{V_\theta} = \mathbb{1}\otimes V_\theta(|\Phi^+\rangle\langle\Phi^+|)$, with $|\Phi^+\rangle = 1/\sqrt{2^M}\sum_n |n\rangle\,|n\rangle$, where n are the M-qubit bit strings, are the corresponding Choi-Jamiołkowski states [32] for $U_\theta^{\otimes M}$ and V_θ, respectively. It was shown in Ref. [19] that when $M < N^2$ Bob can approximate $U_\theta^{\otimes M}$ almost perfectly, i.e., with process fidelity approaching unity in the large N limit. We now show that the protocol in Ref. [19] saturates the no-signaling bound.

In order to apply the no-signaling condition for the case of unitary replication in an easy way we consider the following communication scenario. Alice prepares the Choi-Jamiołkowski state corresponding to $U_\theta^{\otimes N}$, $|\psi_{U_\theta^{\otimes N}}\rangle$, at Bob's side, which he can then use to probabilistically implement $U_\theta^{\otimes N}$ on an arbitrary input state [33]. Consequently, the protocol for which we shall derive a no-signaling bound is inherently probabilistic. We note that a bound for a probabilistic protocol is automatically a bound for a deterministic protocol as well, as the former are less restrictive than the latter.

The no-signaling constraint for unitary replication takes the form

$$\mathcal{R}_N^M = \frac{1}{N+1}\sum_{k=0}^{N}\mathbb{1}\otimes V_{\theta+\frac{2\pi k}{N+1}}(|\Phi^+\rangle\langle\Phi^+|) \tag{19}$$

and is independent of θ. As the worst case process fidelity [Eq. (18)] is identical to the worst case global cloning fidelity used for PCC [Eq. (7)] the no-signaling bound for probabilistic replication of unitaries reads

$$F_{wc}\big(U_\theta^{\otimes M}, V_\theta\big) \leqslant \frac{1}{2^M}\sum_{\lambda=0}^{N}\binom{M}{\lfloor\frac{M-N}{2}\rfloor+\lambda}. \tag{20}$$

This bound is achieved, in the limit of large M, by the deterministic strategy in Ref. [19], for which the fidelity is independent of θ. This implies that probabilistic processes offer no advantage in this case. Thus, the optimal deterministic replication of unitary operations allowed by quantum mechanics is at the edge of no-signaling.

V. QUANTUM METROLOGY

We now apply the no-signaling condition to provide bounds for quantum metrology. The latter task involves the use of N systems, known as the probes, prepared in a suitable state $|\psi\rangle \in \mathcal{H}^{\otimes N}$, and subjected to a dynamical evolution described by a completely positive map, $\mathcal{E}_\theta$, that imprints the value of θ onto their state, i.e., $\rho_\theta = \mathcal{E}_\theta(|\psi\rangle\langle\psi|)$. Information about the value of θ is retrieved by a suitable measurement of the N probes. The goal in quantum metrology is to choose the initial state $|\psi\rangle$ and final measurement such that the value of θ can be inferred as precisely as possible.

If the N quantum probes are prepared in a separable quantum state, i.e., $|\psi\rangle = |\phi\rangle^{\otimes N}$, then the mean square error with which θ can be estimated, optimizing over all allowable measurements, scales inversely proportional with N [34]. This limit is known as the *standard quantum limit*. If, however, the N probes are prepared in a suitably entangled state, then the mean square error with which θ can be estimated scales inversely proportional with N^2 [34]. This limit is known as the *Heisenberg limit*. By allowing for a probabilistic strategy, the Heisenberg limit in precision can be obtained even with separable states [35,36]. Recently, it was shown that both the standard and Heisenberg limits are related with the maximum replication rates corresponding to deterministic and probabilistic PCC strategies, respectively [18,37].

We now show how the no-signaling condition implies that the ultimate bound in precision for metrology is the Heisenberg limit, even if supraquantum processing is allowed. We shall consider two particular examples of Bayesian quantum metrology: phase alignment, where the relevant parameter to be estimated is the phase of a local oscillator, $\theta \in (0,2\pi]$, which is initially completely unknown [38] (Sec. V A), and phase diffusion, where our prior knowledge of the parameter, initially described by a delta function around some value θ_0, diffuses over time [39] (Sec. V C). We stress that whereas analytical bounds for phase alignment are known, for phase diffusion bounds are known only for a small number of probes [39]. This is due to the fact that the optimal strategy is difficult to compute, even numerically. Nevertheless, our no-signaling constraint allows us to place an upper bound on the optimal fidelity of estimation for asymptotically many probe systems. We emphasize that a similar strategy can be applied to a variety of quantum information processing tasks, where limitations of the processes can be gauged by fundamental principles.

In Sec. V B we establish the relationship between optimal quantum cloning protocols and measure and prepare strategies. In particular, we show that a measure and prepare strategy that maximizes the alignment fidelity is asymptotically equivalent to a quantum cloning machine that maximizes the *per copy* fidelity, whereas a measure and prepare strategy that optimizes the maximum likelihood of estimation is asymptotically equivalent to a quantum cloning machine that maximizes the global fidelity.

A. Metrology with uniform prior

Consider the problem of phase alignment, i.e., estimating a completely unknown phase, θ. We will utilize two different ways of quantifying the precision of estimation of θ: the *maximum likelihood* of a correct guess, $\mu = p(\theta|\theta)$ [23], and the *fidelity* of alignment, given by the payoff function $f = \cos^2(\frac{\theta-\theta'}{2})$ [22]. For the case of phase alignment the no-signaling condition [Eq. (5)] takes the form

$$p(\theta'|\theta) = \frac{1}{N+1}\sum_{k=0}^{N} p\left(\theta'|\theta + \frac{2\pi k}{N+1}\right) \tag{21}$$

and is independent of θ (the same holds for a measurement with discrete outcomes). Note that we make no assumptions on how Bob obtains the probability distribution of Eq. (21). In particular we do not restrict Bob's processing to be quantum mechanical. We require only that the inputs and outputs to Bob's processing apparatus be valid quantum states and probability distributions, respectively.

1. Maximal likelihood

For the case where the precision is quantified by the maximum likelihood the no-signaling bound [Eq. (21)] gives $p(\theta|\theta) \leqslant (N+1)p(\theta)$. If the estimate θ' is unbiased, all outcomes are equally likely and the no-signaling bound takes the simple form $p(\theta|\theta) \leqslant N+1$. The bound is known to be achievable using the state [23]

$$\left|\Phi^N_{m.l.}\right\rangle = \frac{1}{\sqrt{N+1}}\sum_n |n\rangle . \tag{22}$$

2. Alignment fidelity

For the case where the precision is quantified by the fidelity of alignment, for each choice of θ,θ' the fidelity must be properly weighted by the *joint probability distribution*, $p(\theta',\theta) = p(\theta'|\theta)p(\theta)$. The average fidelity of alignment is thus

$$\bar{f} = \int \frac{d\theta}{2\pi}\int \mathrm{d}\theta' \cos^2\left(\frac{\theta-\theta'}{2}\right)p(\theta'|\theta). \tag{23}$$

The probability distribution that both maximizes the average fidelity and is compatible with no-signaling is

$$p(\theta'|\theta) = \begin{cases} \frac{N+1}{2\pi} & \text{if} \quad |\theta'-\theta| \leqslant \frac{\pi}{N+1} \\ 0 & \text{otherwise} \end{cases} \tag{24}$$

as we now show.

Our aim is to distribute the probability distribution of Eq. (21) among $N+1$ terms subject to the constraint that $\int d\theta' p(\theta') = 1$ such that the average fidelity of Eq. (23) is maximized. Without loss of generality assume that $\theta \in (0,\frac{2\pi}{N+1})$. If this is not the case we can always relabel the measurement outcomes $k \in (0,\ldots,N)$ such that θ lies in $(0,\frac{2\pi}{N+1})$. As $\cos^2(\frac{\theta'-\theta}{2})$ is largest when $\theta-\theta' = 0$ the average fidelity is optimized by setting $p(\theta'|\theta + \frac{2\pi k}{N+1}) = 0$ for $k \neq 0$. As this is true for all randomly chosen θ, and using the constraint $\int d\theta'\, p(\theta') = 1$, it follows that $p(\theta'|\theta) = \frac{N+1}{2\pi}$ for $|\theta'-\theta| \leqslant \frac{\pi}{N+1}$ and zero everywhere else.

We now derive the maximum average fidelity [Eq. (23)] compatible with no-signaling. As the conditional probability distribution $p(\theta'|\theta)$ of Eq. (24) depends only on the difference $\theta'-\theta$ we may write the average fidelity as

$$\bar{f} = 1 - \int_{-\pi}^{\pi}\frac{d\theta}{2\pi}\int_{-\pi}^{\pi} d\theta' p(\theta'-\theta)\sin^2\left(\frac{\theta-\theta'}{2}\right), \tag{25}$$

where we have used the identity $\cos^2(x) = 1 - \sin^2(x)$. As the integrand in Eq. (25) depends only on the difference $\theta' - \theta$ we may define $\phi = \theta' - \theta$ and $d\phi = d\theta'$ so that

$$\bar{f} = 1 - \int_{-\pi}^{\pi} d\phi\, p(\phi) \sin^2\left(\frac{\phi}{2}\right). \quad (26)$$

Substituting the no-signaling probability distribution of Eq. (24) in place of $p(\phi)$ in Eq. (26) one obtains

$$\bar{f} = 1 - \frac{N+1}{2\pi} \int_{\frac{-\pi}{N+1}}^{\frac{\pi}{N+1}} \sin^2\left(\frac{\phi}{2}\right). \quad (27)$$

In the limit of large N the limits of integration in Eq. (27) become narrower, and we can use the small angle approximation to write $\sin(\phi/2) \approx \phi/2$. Substituting the latter into Eq. (27) and evaluating the integral one obtains the average fidelity $\bar{f} \approx 1 - \frac{\pi^2}{12N^2}$. The maximum average fidelity achievable by a quantum mechanical strategy is $\bar{f} \approx 1 - \frac{\pi^2}{4N^2}$ [22] achieved by the input state

$$\left|\Phi^N_{a.f.}\right\rangle \propto \sum_n \sin\left(\frac{n+1}{(N+2)\pi}\right) |n\rangle\,. \quad (28)$$

This fidelity is strictly smaller than the bound achieved by no-signaling. Nevertheless, the no-signaling bound gives rise to the right scaling with respect to N.

B. Correspondence between asymptotic cloning and phase estimation

Every estimation strategy can be used in a measure and prepare cloning protocol (henceforth referred to as M&P), where Bob first estimates the N-copy input state and, based on his estimate, prepares an M-qubit state. There are two free choices in every M&P protocol: (a) what is the optimal estimation strategy, i.e., which figure of merit to chose, and (b) which output state should we prepare, i.e., do we prepare M-copies of $|\psi(\theta)\rangle$ or some suitable M-partite entangled state. Similarly, there are two figures used in the literature thus far, to quantify the quality of a quantum cloning machine: (a) the *global fidelity* [18] defined by the overlap of the M-qubit output of the cloning machine, ρ^M, with the the ideal M-copy state $|\psi\rangle^{\otimes M}$ (this is the figure of merit that we considered in the previous section) and (b) the *per copy fidelity* [7,8,24,26–29], which is the average of the overlap of the reduced single qubit output state $\rho^M|_n = \mathrm{tr}_{\mathrm{all}\setminus n}\rho^M$ with a perfect single-qubit state $|\psi\rangle$.

In this subsection we discuss how the optimal M&P strategies compare with optimal cloning when the number of copies M goes to infinity. In particular, we will show that the optimal M&P strategy based on the *alignment fidelity* is equivalent to an asymptotic quantum cloning machine which optimizes the *per copy fidelity* of the clones, whereas the optimal M&P strategy based on the maximum likelihood is equivalent to an asymptotic quantum cloning machine which optimizes the *global fidelity*. The equivalence between asymptotic phase-covariant cloning and M&P protocols was known for both deterministic cloning for *per copy fidelity* [40] and *global fidelity* [41], as well as probabilistic cloning [37], but we believe it is still interesting to show the exact correspondence between the different figures of merit for cloning and phase estimation.

1. Per copy cloning fidelity and alignment fidelity

We begin by discussing the equivalence between a M&P strategy based on the alignment fidelity and an asymptotically optimal cloning machine that maximizes the *per copy* fidelity. The asymptotic equivalence between deterministic optimal quantum cloning for *per copy fidelity* and state discrimination was proven in Ref. [40] for the general case (any input state alphabet). Obviously this also holds for the particular case of phase-covariant cloning and phase estimation that we are discussing here. For the probabilistic phase-covariant cloning it was also shown recently [37] that for any cloning strategy with a given success probability there exists a M&P protocol with the same success probability that leads to the same *per copy fidelity* in the asymptotic limit [42]. But what does the *per copy fidelity* mean for the phase estimation part of the M&P strategy? In particular what is the estimation strategy that leads to the asymptotic equivalence with optimal cloning?

For this case it is quite easy to see, as the *per copy fidelity* directly translates into the alignment fidelity of the estimation strategy as the optimal output state simply consists of preparing copies of $|\psi(\theta')\rangle$, where θ' is Bob's estimate of θ. Consequently, the best M&P average per copy cloning fidelity, given by $\int p(\theta)p(\theta'|\theta)\mathrm{tr}\,|\psi(\theta')\rangle\langle\psi(\theta')|\,|\psi(\theta)\rangle\langle\psi(\theta)|\,d\theta\,d\theta'$, equals the alignment fidelity $\int p(\theta)p(\theta'|\theta)\cos^2(\frac{\theta-\theta'}{2})d\theta\,d\theta'$. Hence, the optimal phase alignment protocol [22], achieved for the input state Eq. (28), directly translates into the optimal probabilistic M&P cloning with per copy fidelity $\bar{f} = 1 - \frac{\pi^2}{4N^2}$. Again this probabilistic strategy provides a drastic improvement over the optimal deterministic cloning strategy, where the average per copy fidelity is $f = 1 - \frac{1}{N}$ in the large N limit [23].

2. Global cloning fidelity and maximal likelihood

Let us now turn to the global fidelity. The naive M&P strategy consists in preparing M copies $|\psi(\theta')\rangle^{\otimes M}$ all pointing in the estimated direction θ'. In this case the output state is

$$\rho^M = \frac{1}{2\pi} \int d\theta\, d\theta'\, p(\theta'|\theta)\, |\psi(\theta)\rangle\langle\psi(\theta)|^{\otimes M}\, d\theta. \quad (29)$$

The cloning fidelity is now given by

$$F^{N\to M}_{M\&P} = \left| \frac{1}{2\pi} \int d\theta\, d\theta'\; p(\theta'|\theta) |\langle\psi(\theta')|\psi(\theta)\rangle|^{2M} \right|. \quad (30)$$

Now in the limit $M \to \infty$ the overlap $|\langle\psi(\theta')|\psi(\theta)\rangle|^{2M} \to \frac{2\sqrt{\pi}}{\sqrt{M}}\delta(\theta - \theta')$ where the constant of proportionality is obtained by integrating over the entire range of either θ or θ'. Inserting this expression back into Eq. (30) yields the global fidelity for this M&P protocol of

$$F^{N\to M}_{M\&P} = \sqrt{\frac{1}{\pi M}}\, p(\theta|\theta). \quad (31)$$

The global fidelity of this M&P protocol is directly proportional to the maximum likelihood for phase estimation. However, we note that when one substitutes the optimal maximal likelihood $p(\theta|\theta) = N + 1$, achieved by the input state in Eq. (22), Eq. (31) is smaller than the global fidelity [Eq. (16)], which we proved to be the optimal fidelity achievable by the no-signaling condition, by a factor of $\sqrt{2}$. A similar discrepancy was already noted in Ref. [43] for deterministic cloning, and in Ref. [41] the same authors showed how to build M&P strategies that attain the optimal asymptotic global fidelity. This was done by allowing Bob to output more general states.

In the following we derive the optimal probabilistic M&P strategy that attains the asymptomatic global fidelity of the probabilistic phase-covariant cloner [Eq. (16)] for an arbitrary number of input copies N, this result was shown in Ref. [37], but our construction allows us to establish the correspondence between the global cloning fidelity and the maximal likelihood for phase estimation. We consider a M&P protocol based on maximum likelihood estimation (we shall discuss its optimality in the end of the section) but allow Bob to output a general state $U_\theta^{\otimes M}|\Psi^M\rangle$.

Without loss of generality let us assume that $\theta = 0$. The strategy discussed above would let Bob output the state

$$\rho_0^{M\&P} = \int p(\theta|0) U_\theta^M |\Psi^M\rangle\langle\Psi^M| U_\theta^{M\dagger} d\theta, \tag{32}$$

where the probability distribution $p(\theta|0) = \mathrm{tr}\,|\Phi_{m.l.}^N\rangle\langle\Phi_{m.l.}^N| E(\theta) = \frac{1}{(N+1)2\pi}\sum_{n,\bar{n}=0}^N e^{i\theta(n-\bar{n})}$. Here the optimal POVM elements are known to be covariant [23] and are given by $E(\theta) = \sum_{n,m=0}^N e^{i\theta(n-m)}|n\rangle\langle m|$. The corresponding M&P cloning fidelity is $F_{M\&P}^{N\to M} = \mathrm{tr}\rho_0^{M\&P}|\psi(0)\rangle\langle\psi(0)|^{\otimes M}$. Using the cyclic property of the trace to shift the action of the unitaries U_θ^M onto $|\psi(0)\rangle\langle\psi(0)|^{\otimes M}$ and carrying out the integration the global cloning fidelity reads

$$F_{M\&P}^{N\to M} = \mathrm{tr}\,|\Psi^M\rangle\langle\Psi^M|\,\mathcal{O}_M^N, \tag{33}$$

where

$$\mathcal{O}_M^N = \frac{1}{2^M}\sum_{m,\bar{m}=0}^M \sqrt{\binom{M}{m}\binom{M}{\bar{m}}}\,|m\rangle\langle\bar{m}|\,\Delta_N(m-\bar{m}) \tag{34}$$

with the coherence decay term $\Delta_N(m-\bar{m})$ given by

$$\begin{aligned}\Delta_N(m-\bar{m}) &= \int e^{i\theta(m-\bar{m})}\langle\Phi_{m.l}^N|\,E(\theta)\,|\Phi_{m.l}^N\rangle\frac{d\theta}{2\pi}\\ &= \int\sum_{n,\bar{n}=0}^N e^{i\theta(n+m-\bar{n}-\bar{m})}\frac{d\theta}{2\pi(N+1)}\\ &= \max\left\{1-\frac{|m-\bar{m}|}{N+1},0\right\}.\end{aligned} \tag{35}$$

Having established the form of the M&P fidelity [Eq. (33)] we can now proceed to optimize this expression and obtain the corresponding optimal state $|\Psi^M\rangle$. First, we note that the optimal state should have maximal support over those values of m that lie in the interval $(\frac{M}{2}\pm\sqrt{\frac{M}{4}})$ since for this range of values the binomial coefficients in O_M^N are large. Second, $|\Psi^M\rangle$ should be roughly constant in the range $[m, m+N+1]$ such that that all the coherence terms, $|m\rangle\langle\bar{m}|$, add up constructively, i.e., $\sum_{\bar{m}-m}\Delta_N(m-\bar{m}) = N+1$. In the limit $M\to\infty$ both of these requirements can be satisfied simultaneously. In particular, choosing $|\langle m|\Psi^M\rangle|^2 = \frac{1}{\sqrt{2\pi}\sigma}e^{\frac{-(m-M/2)}{2\sigma^2}}$ leads to a M&P fidelity of

$$F_{M\&P}^{N\to M} = \frac{(N+1)\sqrt{2}}{\sqrt{\pi M}}\left[1+O\left(\frac{N+1}{\sigma}\right)^2+O\left(\frac{\sigma}{\sqrt{M}}\right)^2\right]. \tag{36}$$

We note that Eq. (36) corresponds to the asymptotic expansion of the optimal cloning fidelity of Eq. (16). Choosing $\sigma = M^{\frac{1}{2}-\epsilon}$, for $0\leqslant\epsilon<\frac{1}{2}$ yields the optimal M&P fidelity that is equivalent to the asymptotically optimal cloning machine whose performance is quantified by the global fidelity.

Note that the entire argument above is applicable even if one considers a different estimation strategy, i.e., a different figure of merit. Indeed, the only thing that changes if one changes the estimation strategy (going to a general input state $|\Phi^N\rangle$) is the coherence decay $\Delta_N(m-\bar{m})$ in Eq. (35). However, its contribution of the coherence terms to the cloning fidelity $\sum_m\Delta_N(m) = p_{|\Phi^N\rangle}(0|0)$ is given by the maximal likelihood, which establishes a correspondence between the asymptotic global fidelity of the M&P cloner and the maximal likelihood of the estimation [remark also that the optimal input state Eq. (22) and Eq. (17) match for $M\to\infty$]. Of course, the same correspondence holds for deterministic cloning, for which the maximal likelyhood for N-copies state $|\psi(\theta)\rangle^{\otimes N}$ is simply obtained as $\langle\psi(\theta)|^{\otimes N}E(\theta)|\psi(\theta)\rangle^{\otimes N} = \frac{1}{2^N}[\sum_{j=0}^N\sqrt{\binom{N}{j}}]^2$ and the optimal global fidelity is known to be $\frac{1}{2^{N+M}}\binom{M}{M/2}[\sum_{j=0}^N\sqrt{\binom{N}{j}}]^2$ [23].

To summarize (see the table below), for phase-covariant cloning the M&P strategy based on maximal likelihood estimation (Sec. VA1) is optimal with respect to the *global* cloning fidelity, whereas the M&P strategy based on the alignment fidelity of estimation (Sec. VA2) is optimal with respect to the per copy fidelity of cloning. Both M&P strategies attain the optimal cloning for any fixed N and $M\to\infty$, and this is true both for optimal deterministic as well as probabilistic cloning. We believe that same correspondence should hold for universal cloning; however, this is beyond the scope of this paper. The correspondence between the different M&P strategies and optimal cloning machines is summarized in the following table:

Estimation scenario for M&P cloning		Optimal asymptotic cloning (probabilistic or deterministic
Maximal likelihood	→	Global fidelity
Alignment fidelity	→	Per copy fidelity

C. Metrology with general prior

Let us now consider a more general metrological scenario where Bob has some prior knowledge, $p(\theta)$, of the parameter θ. Following Ref. [39] we consider the prior, $p(\theta;t) = \frac{1}{2\pi}[1 + 2\sum_{n=1}^\infty\cos(n\theta)e^{-n^2t}]$, that arises from a diffusive evolution of $p(\theta) = \delta(\theta)$. The mean fidelity [Eq. (23)] now reads

$$\bar{f}_t = 1-\int d\theta'\int p(\theta'|\theta)p(\theta;t)\sin^2\left(\frac{\theta-\theta'}{2}\right)d\theta. \tag{37}$$

An efficient algorithm optimizing $\bar{f}_t$ for moderate N was derived in Ref. [39]. However, the optimization becomes intractable, even numerically, when N increases. Indeed, optimizing $\bar{f}_t$ for large N is in general a hard task. Nevertheless the no-signaling constraint allows us to derive an upper bound for $\bar{f}_t$ for large enough N as we now show.

Our goal is to minimize the integrand of Eq. (37) under the no-signaling constraint of Eq. (21). For a fixed value of t the product

$$g(\theta;\theta',t) = p(\theta;t)\sin^2\left(\frac{\theta-\theta'}{2}\right) \tag{38}$$

in Eq. (37) obtains its minimum value when $\theta-\theta'=0$. In addition $g(\theta;\theta',t)$ is monotonically increasing so long as the derivative of $g(\theta;\theta',t)$ around $\theta'=\theta$ is greater than zero. This is true so long as

$$\tan^2\left(\frac{\theta-\theta'}{2}\right) < \left(\frac{m}{M}\right)^2 := \tan^2\left(\frac{\Delta}{2}\right), \tag{39}$$

where $m \equiv \min_\theta p(\theta;t)$ and $M = \max_\theta |\partial_\theta p(\theta;t)|$. Outside the interval $[\theta'-\Delta,\theta'+\Delta]$ the function $g(\theta;\theta',t)$ is larger than $m\sin^2(\Delta/2)$. Therefore, $g(\theta;\theta',t)$ attains its global minimum in the finite interval satisfying the condition

$$\sin^2\left(\frac{\theta-\theta'}{2}\right) < m\sin^2\left(\frac{\Delta}{2}\right) = \frac{m^3}{M^2+m^2}. \tag{40}$$

Now consider the narrowest probability distribution compatible with no-signaling given by $\frac{N+1}{2\pi}p(\theta')$, where $p(\theta')$ is the probability distribution given in Eq. (21), for $|\hat{\theta}_\ell-\theta| < \frac{\pi}{N+1}$ and zero elsewhere. For large enough N this probability distribution is contained entirely in the interval $[\theta'-\Delta,\theta'+\Delta]$ where $g(\theta;\theta',t)$ attains its minimum and therefore minimizes the integrant of Eq. (37). Plugging this probability into Eq. (37) and using the condition $\int d\theta' p(\theta')=1$ leads to

$$\bar{f}_t \approx 1 - \frac{\pi^2}{12N^2}\vartheta_4(0,e^{-t}), \tag{41}$$

where $\vartheta_4(0,e^{-t}) = 1+2\sum_{n=1}^{\infty}(-1)^n e^{-n^2 t} = m$ is the Jacobi theta function ranging from 0, when $p(\theta;0)=\delta(\theta)$, to 1, when $p(\theta;\infty)=1/2\pi$ (see Fig. 3). Again we discover that the ultimate bound in precision scales inversely proportional to N^2.

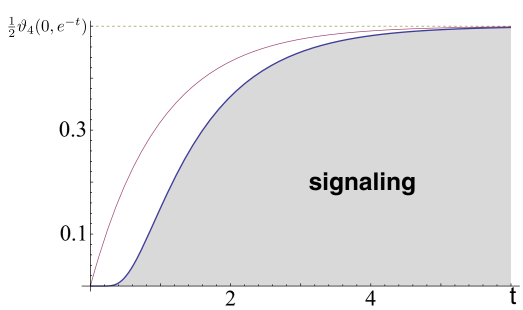

FIG. 3. (Color online) The lower bound on the asymptotically achievable error $\frac{1}{2}\vartheta_4(0,e^{-t}) = \frac{6N^2}{\pi^2}(1-\bar{f}_t)$ (bottom curve) and the error of the prior $\int p(\theta;t)\sin^2(\theta/2)\,d\theta$ (top curve) as functions of t.

VI. DISCUSSION

A. Tightness of bounds

We have shown that the no-signaling condition can set upper bounds on several important quantum information tasks, such as cloning, unitary replication, and metrology. In the case of PCC and unitary replication we have shown that the no-signaling bound coincides with the optimal quantum mechanical strategy, implying that quantum mechanical strategies for PCC cloning and unitary replication are at the edge of no-signaling. However, for the case of metrology, and in particular for the average fidelity of estimation, we see that there is a gap between the no-signaling bound and the optimal quantum strategy. Could this gap be an indication of the existence of a supraquantum strategy, compatible with no-signaling, that outperforms the best quantum mechanical strategy? The answer is no, as we now explain.

In deriving the no-signaling constraint of Eq. (5) we considered only one particular way for Alice and Bob to attempt for faster-than-light communication, using a suitably entangled state $|\Psi\rangle_{AB}$. This, in turn, led to the sharp probability distribution of Eq. (24). However, one can construct a communication scenario where the probability distribution of Eq. (24) can lead to signaling as we now show.

Let us first consider the qubit case ($N=1$). Let Alice and Bob share the entangled state $|\Psi\rangle_{AB} = \cos(\varepsilon)|00\rangle + \sin(\varepsilon)|11\rangle$. Alice can chose to measure her system in either the computational basis $\{|0\rangle,|1\rangle\}$ or the x basis $\{|\pm\rangle = \frac{|0\rangle\pm|1\rangle}{\sqrt{2}}\}$ steering Bob's state into the ensembles $\mathcal{E}^{(1)} = \{\cos^2(\varepsilon)|0\rangle\langle 0|, \sin^2(\varepsilon)|1\rangle\langle 1|\}$ and $\mathcal{E}^{(2)} = \{\frac{1}{2}|\varepsilon\rangle\langle\varepsilon|, \frac{1}{2}|-\varepsilon\rangle\langle-\varepsilon|\}$, respectively, where $|\pm\varepsilon\rangle = \cos(\varepsilon)|0\rangle \pm \sin(\varepsilon)|1\rangle$, as shown in Fig. 4.

This construction obviously holds if all the states are rotated by the same angle. In particular, we can always set this angle such that the probability distribution in Eq. (24) yields $p(\theta'||0\rangle) = p(\theta'||-\varepsilon\rangle) = 0$ and $p(\theta'||1\rangle) = p(\theta'||\varepsilon\rangle) = \frac{1}{\pi}$. In this case the two ensembles give a different probability to observe the outcome θ', $p(\theta'|\mathcal{E}^{(1)}) = \frac{\sin^2(\varepsilon)}{\pi}$ and $p(\theta'|\mathcal{E}^{(2)}) = \frac{1}{2\pi}$. Hence, Bob can distinguish the two ensembles with nonzero probability and infer Alice's choice of measurement instantaneously.

Let us now consider the general case. Any probability distribution $p(\theta)$ defines a continuous ensemble $\mathcal{E}^{(p)} = \{p(\theta)|\Phi_\theta^N\rangle\langle\Phi_\theta^N|\}$, where $|\Phi_\theta^N\rangle = \sum_{n=0}^{N}\psi_n e^{i\theta n}|n\rangle$ are the

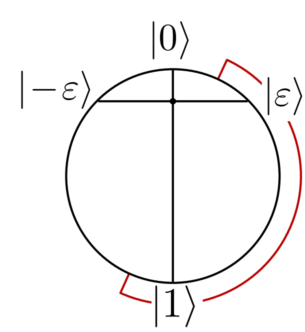

FIG. 4. (Color online) The two ensemble decompositions of ρ_ε for a qubit, leading to faster-than-light communication for the probability distribution Eq. (24) (represented by the red semicircle).

N-qubit states of Eq. (2). Without loss of generality we consider $p(\theta)$ such that

$$p(\theta) = \frac{1}{2\pi}\left[1 + 2\sum_{k=1}^{\infty} p_k \cos(k\theta)\right]. \tag{42}$$

The density matrix for the ensemble $\mathcal{E}^{(p)}$ is given by $\rho = \sum_{n,m=0}^{N} \psi_n \psi_m^* |n\rangle\langle m|\, p_{|n-m|}$, in such a way that it only depends on the first N coefficients, p_k, of the Fourier series in Eq. (42). For any two distributions $p_1(\theta)$ and $p_2(\theta)$ that are identical in the first N components of the Fourier series the ensembles $\mathcal{E}^{(p_1)}$ and $\mathcal{E}^{(p_2)}$ give rise to the same density matrix ρ, and therefore cannot be distinguished by Bob.

In particular, the ensemble given by the probability distributions $p_1(\theta) = \frac{1}{2\pi}$ and $p_2(\theta) = \frac{1}{2\pi}[1 + \cos(M\theta)]$, for $M > N$, correspond to the same density matrix (see Fig. 4). However, with the outcome probability distribution of Eq. (24) Bob can distinguish the two probability distributions with nonzero probability as $p(\theta'|\mathcal{E}^{(p_2)}) - p(\theta'|\mathcal{E}^{(p_1)}) = \frac{N+1}{2\pi}\int_{-\frac{\pi}{N+1}}^{\frac{\pi}{N+1}}[p_2(\theta) - p_1(\theta)]\, d\theta = \mathrm{sinc}(\frac{M\pi}{N+1}) \neq 0$. Therefore, the probability distribution of Eq. (24) leads to signaling when Alice can chose to prepare $\mathcal{E}^{(p_1)}$ or $\mathcal{E}^{(p_2)}$.

More generally the above argument implies that any outcome probability $p(\theta'|\theta)$ compatible with no-signaling has to satisfy $\int p(\theta'|\theta)\cos(M\theta)d\theta = 0$ for $M > N$; i.e., the Fourier components p_k of $p(\theta'|\theta)$ are necessarily zero for $k > N$. Therefore, for finite N, probability distributions with sharp edges such as the one in Eq. (24) are ruled out.

A tighter no-signaling bound can be obtained if we optimize over all possible no-signaling scenarios, i.e., over all possible bipartite entangled states $|\Psi\rangle_{AB}$. In fact any ensemble $\{p_k,\rho_k\}$ corresponding to a density matrix, $\rho_B = \sum_k p_k\rho_k$, at Bob's side can be remotely prepared by Alice, if they initially share a suitable entangled state $|\Psi\rangle_{AB}$ (that depends only on ρ_B) and Alice does an appropriate measurement [1,44].

B. Quantum mechanics at the edge of no-signaling

The above argument shows that the probability distribution of Eq. (24) is valid only for one possible no-signaling scenario, and that in order to obtain a tighter bound we should consider all possible states shared between Alice and Bob and all possible measurements at Alice's side that steer Bob's partial state into different ensembles of pure states that correspond to the same density matrix. Would such an optimization close the gap between our no-signaling bound and the optimal quantum strategy?

Following Ref. [3], we now show that such an optimization is not even necessary, as the only processing compatible with no-signaling is given by the Born rule, i.e., the probability of some measurement outcome ℓ for the input state ρ is given by $P_\ell = \mathrm{tr}\rho E_\ell$ for some positive operator E_ℓ.

Indeed, any ensemble leading to the same density matrix for Bob can be remotely prepared by Alice [1,44]. This together with the no-signaling condition implies the linearity of Bob's processing, $\mathcal{P}$. The latter states that for any two ensembles $\{p_k,\rho_k\}$ and $\{q_k,\sigma_k\}$, corresponding to the same ρ_B, the ensembles after the processing $\{p_k,\mathcal{P}(\rho_k)\}$ and $\{q_k,\mathcal{P}(\sigma_k)\}$ cannot be distinguished with a nonzero probability. Adding the assumption that probabilities are attributed to quantum states via the Born rule (as it is done in Ref. [3]) the condition above implies equality on the density matrices corresponding to the processed ensembles:

$$\sum_k p_k\mathcal{P}(\rho_k) = \sum_k q_k\mathcal{P}(\sigma_k) \equiv \mathcal{P}(\rho_B). \tag{43}$$

This shows that any dynamical evolution of quantum states that respects no-signaling is necessarily described by a completely positive (CP) map [3]. The results of Ref. [3] are concerned with situations where the outputs of Bob's processing are quantum mechanical states. In this case Ref. [3] implies that the optimal quantum mechanical strategies are at the edge of no-signaling.

However, in the case of quantum metrology the outputs are probability distributions. We remark than in Ref. [3] the validity of the Born rule was assumed and used to derive the possibility for remote state preparation of any ensemble and to get the linearity constraint of Eq. (43) from the indistinguishably of processed ensembles. In this case supraquantum metrology is ruled out. However, if we make no assumptions on how probabilities are assigned to measurement outcomes of quantum states but take only remote state preparation as an experimental fact, the no-signaling constraint implies the Born rule already. In this case no-signaling again implies the indistinguishably of two ensembles $\{p_k,\rho_k\}$ and $\{q_k,\sigma_k\}$ corresponding to the same density matrix ρ_B, which in turn implies the linearity of the probability assignment rule. The probability P_ℓ to observe some outcome ℓ has to satisfy

$$\sum_k p_k P_\ell(\rho_k) = \sum_k q_k P_\ell(\sigma_k) \equiv P_\ell(\rho_B); \tag{44}$$

i.e., outcome probabilities *depend only on the density matrix* but not on a particular ensemble. Note that one can easily construct probability assignment rules for pure states that do not satisfy Eq. (44) (see the example from the previous section), so it is not something one has to impose *a priori.* However, as we just saw assuming no-signaling together with the practical possibility for steering enforces linearity.

It is well known that the only probability assignment rule compatible with linearity is the Born rule: $P_\ell(\rho_B) = \mathrm{tr}\rho_B E_\ell$ for some positive operator E_ℓ [45]. For systems of dimension $d > 2$ this can also be seen as a consequence of Gleason's theorem (it suffices to consider all ensembles of pure states forming an orthonormal basis). Moreover, similar result for the equivalence of CP dynamics and the Born rule being enforced by linearity are known to hold in a more general context of probabilistic theories with purification [46]. In summary, we have shown that also in the case of quantum metrology the optimal quantum mechanical strategies are at the edge of no-signaling.

C. Probabilistic versus deterministic bounds

Notice that all the no-signaling bounds derived here are concerned with probabilistic strategies. This is most transparent in our derivation of a no-signaling bound for unitary replication. In some cases, the optimal deterministic strategy coincides with the optimal probabilistic one as is the case with replication of unitaries. In other cases the optimal probabilistic strategy can be made deterministic if one drops some restrictions on the input alphabet, as is the case for the cloning of states when one allows for entangled input states $U_\theta^{\otimes N}|\Phi^N\rangle$ instead of separable input states $|\psi(\theta)\rangle^{\otimes N}$. How does one decide if a deterministic bound still holds when one allows for probabilistic tasks? If this is not the case, can one achieve the probabilistic performance deterministically by allowing for more general input states?

It is known that, in general, any probabilistic strategy can be decomposed into a filter, F, acting on the input state and mapping it to an output state in the same Hilbert space, followed by a deterministic transformation [18]. Moreover, one is usually interested in probabilistic strategies where all states from the input alphabet $\{|\Phi_i\rangle\}$ have the same probability of success $p_s = \mathrm{tr} F\,|\Phi_i\rangle\langle\Phi_i|\,F^\dagger$. In this case what the probabilistic advantage has to offer is the possibility to modify the alphabet to any other alphabet reachable by a filter $\{|\Phi_i^F\rangle = \frac{1}{\sqrt{p_s}} F\,|\Phi_i^F\rangle\}$ [47]. So the question about the strength of the deterministic bound is actually whether the input alphabet $\{|\Phi_i\rangle\}$ is the best among alphabets $\{|\Phi_i^F\rangle\}$ for the particular task.

If this is not the case, then the probabilistic strategy can always be made deterministic by starting with the optimal alphabet. As we saw in Sec. III for the case of PCC the N-copy input states are not optimal leaving room for probabilistic improvement, whereas in the case of universal cloning no probabilistic advantage exists as the symmetry group of the input alphabet, $SU(2)$, forces the filter to be the identity. In fact, there is a substantial improvement in cloning fidelity if one allows entangled N-qubit states as inputs into the cloning machine, but such states are not reachable by any filter [18]. The entangled states that yield such a substantial improvement are exactly those states that maximize the average fidelity of alignment for a Cartesian frame of Ref. [48].

VII. CONCLUSION

In this paper we derived no-signaling bounds for various quantum information processing tasks. These include phase covariant cloning of states and unitary operations, as well as quantum metrology. In the latter case we showed the validity of the Heisenberg limit purely from the no-signaling condition. In general, following Ref. [3], we have shown that the optimal probabilistic quantum mechanical strategy is at the edge of no-signaling also for the case of metrology. Furthermore, we have found that for some tasks, such as PCC of states and unitaries, the optimal probabilistic and deterministic strategies coincide. These results show a direct connection between the no-signaling principle and the ultimate limits on quantum cloning and metrology. This connection provides a new insight into the *physical* origin of these limits, in contrast to the previously known limits based on optimization, using, e.g., semidefinte programs.

On the one hand it is clear that a bound for probabilistic strategies is also a bound for deterministic ones. However, it might be possible to derive tighter no-signaling bounds for deterministic strategies. It is an interesting open question how to incorporate the requirement that the protocol be deterministic in a no-signaling scenario.

On the other hand, there are several tasks for which the optimal quantum strategy is not known. In such cases the techniques and methods we provide here can be particularly useful in deriving limitations to these tasks based on no-signaling. We have demonstrated one such example for Bayesian metrology for arbitrary prior; however, the methods we introduce are applicable in a broader context. This provides an alternative approach to study the possibilities and limitations of quantum information processing.

ACKNOWLEDGMENTS

We thank Giulio Chiribella, Nicolas Gisin, and Christoph Simon for valuable remarks and comments. This work was supported by the Austrian Science Fund (FWF), Grant No. P24273-N16, and the Swiss National Science Foundation, Grant No. P2GEP2_151964.

[1] N. Gisin, Helv. Phys. Acta **62**, 363 (1989); Phys. Lett. A **143**, 1 (1990).
[2] J. Polchinski, Phys. Rev. Lett. **66**, 397 (1991).
[3] C. Simon, V. Bužek, and N. Gisin, Phys. Rev. Lett. **87**, 170405 (2001).
[4] N. Herbert, Found. Phys. **12**, 1171 (1982).
[5] G. Ghiradi and T. Weber, Lettere Al Nuovo Cimento Series 2 **26**, 599 (1979).
[6] C. Simon, G. Weihs, and A. Zeilinger, Acta Physica Slovaca **49**, 755 (1999).
[7] N. Gisin, Phys. Lett. A **242**, 1 (1998).
[8] S. Ghosh, G. Kar, and A. Roy, Phys. Lett. A **261**, 17 (1999).
[9] Z. Gedik and B. Çakmak, Phys. Rev. A **87**, 042314 (2013).
[10] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[11] J. Bae, W.-Y. Hwang, and Y.-D. Han, Phys. Rev. Lett. **107**, 170403 (2011).
[12] D. Pitalúa-García, Quantum information, Bell inequalities and the no-signalling principle, Ph.D. thesis, University of Cambridge 2013.
[13] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[14] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger, Phys. Rev. Lett. **96**, 250401 (2006); N. Linden, S. Popescu, A. J. Short, and A. Winter, *ibid.* **99**, 180502 (2007). P. Skrzypczyk, N. Brunner, and S. Popescu, *ibid.* **102**, 110402 (2009).
[15] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, Nature (London) **461**, 1101 (2009).
[16] M. Navascués and H. Wunderlich, P. R. Soc. A Math. Phys. **466**, 881 (2010).
[17] T. Fritz, A. B. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, and A. Acín, Nat. Commun. **4**, 2263 (2013).

[18] G. Chiribella, Y. Yang, and A. C.-C. Yao, Nat. Commun. **4**, 2915 (2013).
[19] W. Dür, P. Sekatski, and M. Skotiniotis, Phys. Rev. Lett. **114**, 120503 (2015).
[20] G. Chiribella, Y. Yang, and C. Huang, Phys. Rev. Lett. **114**, 120504 (2015).
[21] V. Bužek, R. Derka, and S. Massar, Phys. Rev. Lett. **82**, 2207 (1999).
[22] D. W. Berry and H. M. Wiseman, Phys. Rev. Lett. **85**, 5098 (2000).
[23] G. Chiribella, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, Phys. Rev. A **70**, 062105 (2004).
[24] D. Bruß, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, Phys. Rev. A **62**, 012302 (2000); G. M. D'Ariano and C. Macchiavello, *ibid.* **67**, 042306 (2003).
[25] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[26] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[27] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
[28] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, Phys. Rev. A **57**, 2368 (1998).
[29] R. F. Werner, Phys. Rev. A **58**, 1827 (1998).
[30] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. Lett. **101**, 180504 (2008).
[31] A. Gilchrist, N. K. Langford, and M. A. Nielsen, Phys. Rev. A **71**, 062310 (2005); W. Dür, M. Hein, J. I. Cirac, and H.-J. Briegel, *ibid.* **72**, 052326 (2005).
[32] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972); M.-D. Choi, Can. J. Math. **24**, 520 (1972).
[33] W. Dür and J. I. Cirac, Phys. Rev. A **64**, 012317 (2001).
[34] V. Giovannetti, S. Lloyd, and L. Maccone, Science **306**, 1330 (2004).
[35] J. Fiurášek, New J. Phys. **8**, 192 (2006).
[36] B. Gendra, E. Ronco-Bonvehi, J. Calsamiglia, R. Muñoz-Tapia, and E. Bagan, Phys. Rev. Lett. **110**, 100501 (2013); Phys. Rev. A **88**, 012128 (2013).
[37] B. Gendra, J. Calsamiglia, R. Muñoz-Tapia, E. Bagan, and G. Chiribella, Phys. Rev. Lett. **113**, 260402 (2014).
[38] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Rev. Mod. Phys. **79**, 555 (2007).
[39] R. Demkowicz-Dobrzański, Phys. Rev. A **83**, 061802(R) (2011).
[40] J. Bae and A. Acín, Phys. Rev. Lett. **97**, 030402 (2006).
[41] G. Chiribella and Y. Yang, New J. Phys. **16**, 063005 (2014).
[42] Actually, they show it more generally for any m-copy fidelity with a fixed m.
[43] Y. Yang and G. Chiribella, in *8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 22, edited by S. Severini and F. Brandao (Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2013), pp. 220–234.
[44] L. P. Hughston, R. Jozsa, and W. K. Wootters, Phys. Lett. A **183**, 14 (1993).
[45] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland Series in Statistics and Probability, Amsterdam, 1980).
[46] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. A **84**, 012311 (2011).
[47] If the input alphabet is generated by the action of a unitary on a fixed seed state $|\Psi_i = U_i|\Psi$, then the filter commutes with the unitary and modifies the seed state to $|\Psi^F = \frac{1}{\sqrt{p_s}} F|\Psi$.
[48] G. Chiribella, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, Phys. Rev. Lett. **93**, 180503 (2004).