PHYSICAL REVIEW A **85**, 032333 (2012)

Memory cost of quantum protocols

Alessandro Bisio,* Giacomo Mauro D'Ariano,† and Paolo Perinotti‡
QUIT Group, Dipartimento di Fisica, and INFN, via Bassi 6, 27100 Pavia, Italy§

Michal Sedlák‖
QUIT Group, Dipartimento di Fisica, via Bassi 6, 27100 Pavia, Italy§ *and*
Institute of Physics, Slovak Academy of Sciences, Dúbravská cesta 9, 845 11 Bratislava, Slovakia
(Received 16 December 2011; published 30 March 2012)

We consider the problem of minimizing the ancillary systems required to realize an arbitrary strategy of a quantum protocol, with the assistance of classical memory. For this purpose we introduce the notion of *memory cost* of a strategy to measure the resources required in terms of ancillary dimension. We provide a condition for the cost to be equal to a given value, and we use this result to evaluate the cost in some special cases. As an example, we show that any covariant protocol for the cloning of a unitary transformation requires at most one ancillary qubit. We also prove that the memory cost has to be determined globally and cannot be calculated by optimizing the resources independently at each step of the strategy.

DOI: 10.1103/PhysRevA.85.032333 PACS number(s): 03.67.Ac, 03.67.Lx

I. INTRODUCTION

Since the advent of quantum computation, the most important theoretical efforts in this field have aimed at proving a computational speedup in many information-processing tasks [1,2] with respect to their classical counterparts. For this reason, the optimization of algorithms is typically aimed at minimizing the number of computational steps, possibly at the expense of the computational space, i.e., the number of ancillary quantum systems (qubits) that are needed in the computation. This choice is dictated by the fact that time is the most valuable resource in computation. Moreover, compared with the classical case, in quantum computation, time optimization is even more important because of the detrimental effects of decoherence.

Besides time minimization, the next priority is optimization of the computational space. More precisely, the resource we need to minimize is quantum memory, that is, the number of ancillary systems that need to be kept coherent between subsequent steps. Since a classical memory has a negligible cost with respect to a quantum one, it would be very valuable to replace part of the quantum memory by a classical channel.

In Ref. [3] the minimization of quantum memory was carried out under the restrictive assumption that all the ancillary systems introduced during the computation are kept coherent until the very last step. In the present paper, we consider the same problem, taking into account the possibility of breaking the coherence of ancillary systems during the computation without affecting the overall strategy, by measuring and compressing the ancillary computational space at the expense of an extra classical memory that carries measurement outcome. In order to quantify the quantum memory cost of a strategy we introduce the notion of *memory cost*, which will be the logarithm of the maximum dimension of ancillary quantum systems required at all steps. For the special case of a strategy describing a single channel, our notion of memory cost coincides with the one of entanglement cost recently introduced in Ref. [4]. Indeed, a single channel can be interpreted as a quantum strategy made of two steps: (i) a quantum instrument followed by a compression conditional on the classical outcome and (ii) a conditional decompression. After providing a necessary and sufficient condition for a strategy to have a given memory cost, we show that its optimization cannot generally be carried out by minimizing the memory required at each step separately. The reason for this is that in the memory optimization of a strategy one can exploit different channel implementations of the same strategy. This fact implies that in general the optimization must be a global one. Finally, we investigate how the symmetry properties of a quantum strategy can lead to a nontrivial bound of its memory cost and we calculate it for simple classes of covariant channels.

The paper is organized as follows. In Sec. II we present some elementary results of linear algebra with special emphasis on the Choi isomorphism. In Sec. III we review the general theory of quantum combs [5–7], which provides a unified framework to treat quantum strategies. Section IV provides the definition of memory cost along with the main theorem. In Sec. V we provide some examples in which the application of the necessary and sufficient condition allows us to draw nontrivial conclusions about the cost of a strategy. We conclude the paper with Sec. VI, where we summarize the results and discuss some open problems.

II. PRELIMINARIES AND NOTATION

In this section we introduce the basic mathematical tools and the notation that will be used throughout the whole manuscript. If $\mathcal{H}$ denotes a finite-dimensional Hilbert space, $\mathcal{L}(\mathcal{H})$ denotes the set of linear operators on $\mathcal{H}$. Once we fixed an orthonormal basis $\{|n\rangle\}$ for $\mathcal{H}$ a one-to-one correspondence

*alessandro.bisio@unipv.it
†dariano@unipv.it
‡paolo.perinotti@unipv.it
§http://www.qubit.it
‖michal.sedlak@unipv.it

$A \leftrightarrow |A\rangle\rangle$ between $\mathcal{L}(\mathcal{H})$ and $\mathcal{H} \otimes \mathcal{H}$ is well defined, with

$$A = \sum_{nm} \langle n|A|m\rangle |n\rangle\langle m|,$$
$$|A\rangle\rangle := \sum_{nm} \langle n|A|m\rangle |n\rangle|m\rangle, \quad (1)$$

and the following identity is satisfied:

$$A \otimes B|C\rangle\rangle = |ACB^T\rangle\rangle, \quad (2)$$

where X^T denotes transposition of X with respect to the fixed basis (where X^* will denote complex conjugation). In the following we will denote $\mathrm{Supp}(A)$ as the support of A and $\mathrm{Rnk}(A)$ as the dimension of $\mathrm{Supp}(A)$, i.e., $\mathrm{Rnk}(A) := \dim[\mathrm{Supp}(A)]$. The set of linear maps from $\mathcal{L}(\mathcal{H}_1)$ to $\mathcal{L}(\mathcal{H}_2)$ will be denoted by $\mathcal{L}(\mathcal{L}(\mathcal{H}_1),\mathcal{L}(\mathcal{H}_2))$.

The following result, due to Choi [8], establishes a bijective correspondence between $\mathcal{L}(\mathcal{L}(\mathcal{H}_1),\mathcal{L}(\mathcal{H}_2))$ and $\mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$.

Theorem 1. Let $\mathcal{I}$ be the identity on $\mathcal{L}(\mathcal{H}_1)$. The linear map $\mathfrak{C} : \mathcal{L}(\mathcal{L}(\mathcal{H}_1),\mathcal{L}(\mathcal{H}_2)) \rightarrow \mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$, defined as

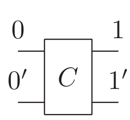
$$\mathfrak{C} : \mathcal{C} \mapsto C := \mathcal{C} \otimes \mathcal{I}(|I\rangle\rangle\langle\langle I|), \quad (3)$$

is invertible and its inverse $\mathfrak{C}^{-1}$ is given by

$$[\mathfrak{C}^{-1}(C)](A) = \mathrm{Tr}_1[(I_2 \otimes A^T)C] = \mathcal{C}(A), \quad (4)$$

where Tr_1 denotes the partial trace over $\mathcal{H}_1$ and I_2 is the identity on $\mathcal{H}_2$. The operator $C = \mathfrak{C}(\mathcal{C})$ is called the Choi operator of $\mathcal{C}$.

Throughout this paper we will use the calligraphic style $\mathcal{C}$ to denote the linear map and the italic C to denote the corresponding Choi operator. It is useful to give a diagrammatic representation of linear maps: we will sketch a map $\mathcal{C} \in \mathcal{L}(\mathcal{L}(\bigotimes_{i=1}^{N} \mathcal{H}_i),\mathcal{L}(\bigotimes_{j=1}^{M} \mathcal{H}_j))$ as a box with N *input wires* on the left and M *output wires* on the right. For example, if $\mathcal{C} \in \mathcal{L}(\mathcal{L}(\mathcal{H}_0 \otimes \mathcal{H}_{0'}),\mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_{1'}))$ we have

$C =$  (5)

We now show how some features of a linear map $\mathcal{C}$ translate in terms of the Choi operator C.

Proposition 1. Let $\mathcal{C} \in \mathcal{L}(\mathcal{L}(\mathcal{H}_0),\mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_A))$ and $\mathcal{D} \in \mathcal{L}(\mathcal{L}(\mathcal{H}_2 \otimes \mathcal{H}_A),\mathcal{L}(\mathcal{H}_3))$ be two linear maps and C, D be their Choi operators. Then we have

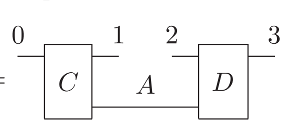
(a) *$\mathcal{C}$ is completely positive if and only if $C \geqslant 0$;*

(b) *$\mathcal{C}$ does not increase the trace if and only if $\mathrm{Tr}_{1A}[C] \leqslant I_0$; the equality holds when $\mathcal{C}$ is trace preserving;*

(c) *the Choi operator of the composition $(\mathcal{I}_1 \otimes \mathcal{D}) \circ (\mathcal{I}_2 \otimes \mathcal{C})$ is given by the* link product [5] *of C and D, that is. $\mathfrak{C}((\mathcal{I}_2 \otimes \mathcal{D}) \circ (\mathcal{I}_3 \otimes \mathcal{C})) = C * D$, where*

$$C * D := \mathrm{Tr}_A[(C \otimes I_{34})(I_{01} \otimes D)]. \quad (6)$$

The link $C * D$ in Eq. (6) can be visualized as follows:

$C * D =$  .

III. QUANTUM STRATEGIES

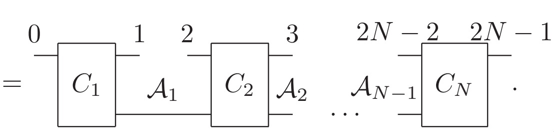
In the usual description of quantum mechanics each physical system is associated with a Hilbert space $\mathcal{H}$ and the states of the system are represented by positive semidefinite operators ρ with $\mathrm{Tr}[\rho] = 1$. A single use [9] of a physical device which performs a transformation of the system is represented by a linear map $\mathcal{C} \in \mathcal{L}(\mathcal{L}(\mathcal{H}_{\mathrm{in}}),\mathcal{L}(\mathcal{H}_{\mathrm{out}}))$ which is completely positive ($C \geqslant 0$) and trace nonincreasing ($\mathrm{Tr}_{\mathrm{out}} C \leqslant I_{\mathrm{in}}$). If the transformation is deterministic, $\mathcal{C}$ is trace preserving ($\mathrm{Tr}_{\mathrm{out}}[C] = I_{\mathrm{in}}$) and is called a *quantum channel*, while in the general probabilistic case it is called a *quantum operation*. A set of quantum operations $\boldsymbol{\mathcal{M}} \equiv \{\mathcal{M}_i\}$ such that $\mathcal{M}_\Omega := \sum_i \mathcal{M}_i$ is a quantum channel is called a *quantum instrument*. Physically, a quantum instrument describes a device that has both a classical and a quantum outcome. One can regard a demolishing measurement device as a special case of a quantum instrument where there is only a classical outcome. The mathematical description of a measurement is given in this case by a set of positive operators $\boldsymbol{P} := \{P_i\}$ which sum to the identity $\sum_i P_i = I$—a *positive operator valued measure* (POVM).

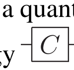
A general *quantum strategy* can be obtained by connecting the outputs of some transformations into the input of some others. If the transformations that we are connecting are deterministic, i.e., quantum channels, we have *deterministic quantum strategies*, and we talk about *probabilistic quantum strategies* otherwise. In a valid quantum strategy no closed loops are allowed [10]: this requirement ensures that causality is preserved, since a closed path would correspond to a time loop. Quantum strategies can be used to describe a huge variety of multistep quantum protocols, such as cryptographic protocols [11,12], standard quantum algorithms [1,2,13], and multiround quantum games [14].

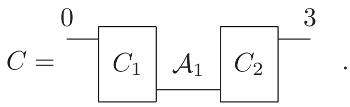
It is possible to prove that any deterministic quantum strategy is equivalent to a concatenation of N channels $\mathcal{C}_i \in \mathcal{L}(\mathcal{L}(\mathcal{H}_{2i-2} \otimes \mathcal{A}_{i-1}),\mathcal{L}(\mathcal{H}_{2i-1} \otimes \mathcal{A}_i))$ ($\mathcal{A}_0 = \mathcal{A}_N = \mathbb{C}$) and thus it is represented by a map $\mathcal{R}^{(N)}$ whose Choi operator is given by the link product of the C_i's, i.e.,

$$R^{(N)} = C_1 * \cdots * C_N. \quad (7)$$

This result allows us to represent each deterministic quantum strategy $\mathcal{R}^{(N)}$ as a sequence of N computational steps, each of them corresponding to a channel $\mathcal{C}_i$:

$R^{(N)} =$  . (8)

Equation (8) is our standard representation of a quantum strategy $\mathcal{R}^{(N)}$, where the apex (N) makes explicit the number of steps of the strategy. We chose to attach one free incoming and one free outgoing wire to each map $\mathcal{C}_i$ since strategies in which some input and output wires are missing correspond to the special cases in which $\dim(\mathcal{H}_j) = 1$ for some j. It is worth noticing that a quantum channel $\mathcal{C}$ can be seen either as a single-step strategy  or as a two-steps strategy in which both the output of the first step and the input of the second one are one dimensional:



(9)

The representation given by Eq. (9) will be useful when discussing the memory cost of a channel. In Eq. (8) we also chose to label the free input and output wires by integer numbers. In this way the Hilbert spaces of the input wires are labeled by even numbers while the output ones correspond to odd numbers. We define the overall input space of a quantum strategy $\mathcal{R}^{(N)}$ as $\mathcal{H}_{\text{in}} = \bigotimes_{i=1}^{N} \mathcal{H}_{2i-2}$ and the overall output space as $\mathcal{H}_{\text{out}} = \bigotimes_{j=1}^{N} \mathcal{H}_{2i-1}$.

The previous considerations can be summarized by the following definition.

Definition 1. A linear map $\mathcal{R}^{(N)} \in \mathcal{L}(\mathcal{L}(\mathcal{H}_{\text{in}}),\mathcal{L}(\mathcal{H}_{\text{out}}))$ *is a deterministic quantum strategy when there exists a set of channels* $\{\mathcal{C}_i \in \mathcal{L}(\mathcal{L}(\mathcal{H}_{2i-2} \otimes \mathcal{A}_{i-1}),\mathcal{L}(\mathcal{H}_{2i-1} \otimes \mathcal{A}_i))\}$ *such that* $C_1 * \cdots * C_N = R^{(N)}$. *The set* $\mathscr{C} := \{\mathcal{C}_i\}$ *is called a* realization of $\mathcal{R}^{(N)}$ *and the set* $\mathsf{S} := \{1,2,\ldots,N\}$ *is called* the set of steps *of the quantum strategy*.

It is important to notice that the same $R^{(N)}$ can have different realizations. As long as one is not interested in the inner structure of a quantum strategy but just in its properties as a linear map from $\mathcal{H}_{\text{in}}$ to $\mathcal{H}_{\text{out}}$, the description provided by $R^{(N)}$ is exhaustive and there is no need to specify a realization. On the other hand, if we fix a realization $\mathscr{C}$ of $\mathcal{R}^{(N)}$ we specify some details about the physical implementation of the quantum strategy. For example, the dimensions of the spaces $\mathcal{A}_i$ determine the amount of memory used in the physical implementation of the strategy.

Definition 1 identifies the set of the Choi operators of deterministic quantum strategies with the set of linear maps $\mathcal{R}^{(N)}$ for which there exists a realization $\mathscr{C}$. The following theorem recasts this characterization in terms of linear constraints which $R^{(N)}$ has to fulfill.

Theorem 2. A positive operator $R^{(N)} \in \mathcal{L}(\mathcal{H}_{\text{in}} \otimes \mathcal{H}_{\text{out}})$ *is the Choi operator of a deterministic quantum strategy if and only if it satisfies the normalization*

$$\mathrm{Tr}_{2k-1}[R^{(k)}] = I_{2k-2} \otimes R^{(k-1)}, \qquad k = 1,\ldots,N, \quad (10)$$

where $R^{(k)} \in \mathcal{L}(\bigotimes_{n=0}^{2k-1} \mathcal{H}_n)$ *is the Choi operator of the quantum strategy corresponding to the first* k *steps and* $R^{(0)} = 1$. *The Choi operator of a deterministic quantum strategy is called a* deterministic quantum comb *[5]* .

Theorem 2 can be understood as a generalization of Theorem 1 to quantum strategies. It provides a one-to-one correspondence between the set of deterministic quantum strategies and the set of positive semidefinite operators satisfying Eq. (10).

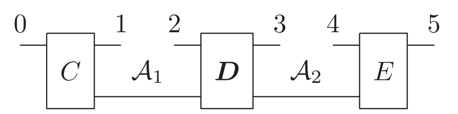
We now extend the previous discussion to the probabilistic case. It is possible to prove a probabilistic counterpart of Theorem 2, which states that a linear map $\mathcal{S}^{(N)}$ is a probabilistic quantum strategy if and only if its Choi operator $S^{(N)}$ satisfies the following constraint:

$$0 \leqslant S^{(N)} \leqslant R^{(N)}, \quad (11)$$

where $R^{(N)}$ is a deterministic comb. The Choi operator of a probabilistic quantum strategy is called a probabilistic quantum comb. The quantum strategy generalization of a quantum instrument is called a *generalized instrument* and it is a set of probabilistic quantum strategies $\boldsymbol{\mathcal{R}}^{(N)} := \{\mathcal{R}_i^{(N)}\}$ such that the set $\boldsymbol{R}^{(N)} := \{R_i^{(N)}\}$ of the corresponding probabilistic quantum combs satisfies

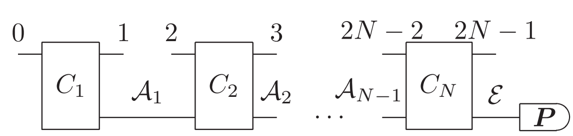
$$\sum_i R_i^{(N)} = R_\Omega^{(N)}, \quad (12)$$

where $R_\Omega^{(N)}$ is a deterministic quantum comb. A generalized instrument is the mathematical representation of a strategy that produces both the classical outcome i and the quantum outcome $\mathcal{R}_i^{(N)}(\rho) \in \mathcal{L}(\mathcal{H}_{\text{out}})$ with probability $\mathrm{Tr}[\mathcal{R}_i^{(N)}(\rho)]$ when the state $\rho \in \mathcal{L}(\mathcal{H}_{\text{in}})$ is fed into the free inputs of the strategy. A typical example of a generalized instrument is a quantum network in which at least one of the devices is a quantum instrument:



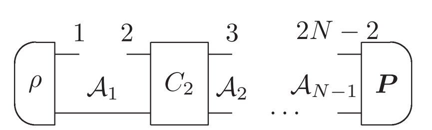
(13)

In Eq. (13) the two channels C and E are connected through wires $\mathcal{A}_1$ and $\mathcal{A}_2$ to the quantum instrument $\boldsymbol{\mathcal{D}}$. If $\boldsymbol{\mathcal{R}}^{(N)} := \{\mathcal{R}_i^{(N)}\}$ is a generalized instrument, one can verify that $\sum_i R_i^{(N)} \otimes |i\rangle\langle i|_E$, where $\{|i\rangle_E\}$ is an orthonormal basis for an ancillary Hilbert space $\mathcal{E}$, is a deterministic comb. If we apply the von Neumann measurement $\boldsymbol{P} := \{|i\rangle\langle i|\}$ on the ancilla $\mathcal{E}$, depending on the outcome i the Choi operator of the strategy will be $R_i^{(N)}$. This proves that every generalized instrument can be realized as a deterministic quantum strategy followed by a POVM on an ancillary Hilbert space, i.e.,



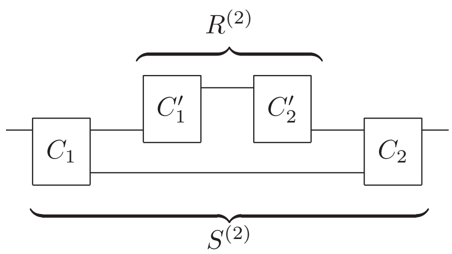
(14)

A generalized instrument such that $\dim(\mathcal{H}_0) = \dim(\mathcal{H}_{2N+1}) = 1$ is called a *tester* and can be interpreted as the quantum strategy analog of a POVM. Specializing Eq. (14), we have that a tester can be realized as a quantum strategy whose first step is a state preparation and whose last step is a POVM:



(15)

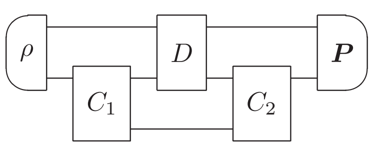
Since a quantum strategy is a map from multiple input spaces to multiple output spaces, we can imagine connecting two quantum strategies $\mathcal{R}^{(N)}$ and $\mathcal{S}^{(M)}$ by linking some outputs of $\mathcal{R}^{(N)}$ ($\mathcal{S}^{(M)}$) with some inputs of $\mathcal{S}^{(M)}$ ($\mathcal{R}^{(N)}$), for example,

$R^{(2)} * S^{(2)} =$ 

.

We adopt the convention that if wire $i \in \mathcal{R}^{(N)}$ is connected with wire $j \in \mathcal{S}^{(M)}$ they are identified by the same label, i.e., $i = j$. Again, if we want such a composition to form a valid quantum strategy $\mathcal{R}_3^{(L)}$ we need to require that the graph of the connections in the composite strategy does not contain closed loops. By applying Proposition Proposition 1, it is possible to prove that the comb of the composite network is given by the link product of $R^{(N)}$ and $S^{(M)}$, i.e., $T^{(L)} = R^{(N)} * S^{(M)}$.

Consider now the problem of discriminating between two deterministic quantum strategies $\mathcal{R}_0^{(N)}$ and $\mathcal{R}_1^{(N)}$ given with prior probability $\frac{1}{2}$. A possible way could be to (i) prepare a multipartite input state, possibly entangled with some ancillary degrees of freedom, (ii) send it as input through the free input wires of the unknown strategy, and, eventually, (iii) perform a two-outcome POVM on the output state. However, it is possible to exploit the causal order of the quantum strategy so that the input at step k can depend on the previous outputs at steps $j < k$, i.e.,



. (16)

The most general way for the discrimination of two deterministic quantum strategies $\mathcal{R}_0^{(N)}$ and $\mathcal{R}_1^{(N)}$ is then described by a two-outcome tester $\boldsymbol{\mathcal{T}}^{(N+1)} = \{\mathcal{T}_0^{(N+1)}, \mathcal{T}_1^{(N+1)}\}$ and the probability of error p_e as a function of $\mathcal{R}_0^{(N)}$, $\mathcal{R}_1^{(N)}$, and $\boldsymbol{\mathcal{T}}^{(N+1)}$ is given by

$$p_e\big(\mathcal{R}_1^{(N)}, \mathcal{R}_0^{(N)}, \boldsymbol{\mathcal{T}}^{(N+1)}\big) = \tfrac{1}{2}\big(R_1^{(N)} * T_0^{(N+1)} + R_0^{(N)} * T_1^{(N+1)}\big). \tag{17}$$

This leads to an operational notion of distance between quantum strategies [15].

Definition 2. Let $\mathcal{R}_0^{(N)}$ and $\mathcal{R}_1^{(N)}$ be two deterministic quantum strategies. The distance between $\mathcal{R}_0^{(N)}$ and $\mathcal{R}_1^{(N)}$ is given by

$$\big\|\mathcal{R}_0^{(N)} - \mathcal{R}_1^{(N)}\big\|_{op} := 1 - 2 \max_{\mathcal{T}^{(N+1)}} p_e\big(\mathcal{R}_1^{(N)}, \mathcal{R}_0^{(N)}, \boldsymbol{\mathcal{T}}^{(N+1)}\big), \tag{18}$$

where $\boldsymbol{\mathcal{T}}^{(N+1)} = \{\mathcal{T}_0^{(N+1)}, \mathcal{T}_1^{(N+1)}\}$ is a tester and p_e is defined according to Eq. (17).

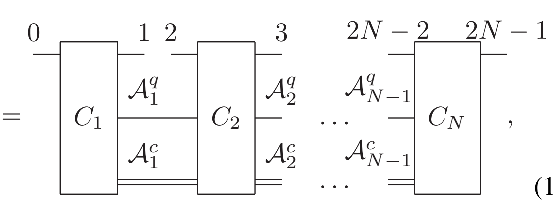
It is easy to prove that when $\mathcal{R}_0^{(N)}$ and $\mathcal{R}_1^{(N)}$ are channels, Eq. (18) leads to the usual distance of the norm of the complete boundedness.

IV. MEMORY COST OF QUANTUM STRATEGIES

The main achievement of the general theory of quantum combs is that arbitrarily complex quantum strategies can always be represented by positive operators subjected to linear constraints. This result is extremely relevant for applications. Suppose we fix an information-processing task and we look for the quantum strategy that achieves the best performances allowed by quantum theory. Thanks to Theorem 2 this search is reduced to an optimization problem over a (convex) set of suitably normalized positive operators. Such a procedure is much more efficient than separately optimizing each element of the strategy.

However, once the optimal Choi operator has been found, one has to find an actual realization of the quantum strategy. Since a single quantum strategy can be realized in many different ways one could be interested in finding the one that best fits some requirements. For example, a reasonable request is to minimize the usage of some resource, such as the number of controlled-NOT gates. Another resource which is valuable and hard to realize in present-day quantum technology is quantum memory. One would benefit a lot from knowing how much quantum memory is needed in order to realize a given quantum strategy and whether it is possible to replace some quantum memory with classical memory.

In this section we provide an algebraic characterization of the amount of quantum memory which is employed in the realization of a given quantum strategy. As we pointed out in the previous section, if $\mathscr{C}$ is a realization of a deterministic quantum strategy $\mathcal{R}^{(N)}$, the amount of memory which one has to preserve from step i to step $i+1$ can be quantified by the dimension of the Hilbert space $\mathcal{A}_i$. Since we are interested in quantifying the amount of quantum memory, we need to introduce a formalism that enables a distinction between quantum memory and classical memory. To this end, it is convenient to model a classical memory as quantum system whose states must stay diagonal with respect to a fixed orthonormal basis $\{|i\rangle\}$. We then suppose that each $\mathcal{A}_i$ is split as $\mathcal{A}_i := \mathcal{A}_i^{(c)} \otimes \mathcal{A}_i^{(q)}$, where $\mathcal{A}_i^{(q)}$ is the quantum memory and $\mathcal{A}_i^{(c)}$ is the Hilbert space that can carry only classical information [16]. With this definition, Eq. (8) becomes

$R^{(N)} =$ 

, (19)

where the classical memories are denoted by double wires.

For the purpose of introducing the next two definitions, let $\mathcal{R}^{(N)}$ be a deterministic quantum network, $\mathsf{S} = \{1, \ldots, N\}$ be its set of steps, and J be a subset of S. We say that $\mathcal{R}^{(N)}$ can be realized with $\boldsymbol{d} := \{d_k\}$-dimensional quantum memories at steps J if and only if there exists a realization $\mathscr{C}$ of $\mathcal{R}^{(N)}$ such that $\dim(\mathcal{A}_k^{(q)}) \leqslant d_k$ for all $k \in \mathsf{J}$.

Definition 3. The zero-error memory cost at steps J of a deterministic quantum strategy $\mathcal{R}^{(N)}$ is defined as

$$\mathsf{M}_{\mathsf{J}}(\mathcal{R}^{(N)}, 0) := \min_{\mathscr{C}} \max_{k \in \mathsf{J}} \log_2\big[\dim\big(\mathcal{A}_k^q\big)\big], \tag{20}$$

where the minimum is taken over all the possible realizations $\mathscr{C}$ of $\mathcal{R}^{(N)}$.

For any $\epsilon \geqslant 0$ it is possible to introduce the following notion.

Definition 4. The ϵ*-tolerant memory cost at steps* J *of* $\mathcal{R}^{(N)}$ *is defined as*

$$\mathsf{M}_{\mathsf{J}}(\mathcal{R}^{(N)},\epsilon) := \min_{\mathcal{S}^{(N)} \in B_{\text{op}}(\mathcal{R}^{(N)},\epsilon)} \mathsf{M}_{\mathsf{I}}(\mathcal{S}^{(N)},0), \tag{21}$$

where $B_{\text{op}}(\mathcal{R}^{(N)},\epsilon)$ *is the set of quantum strategies that are* ϵ*-close to* $\mathcal{R}^{(N)}$ *in the operational norm, i.e.,*

$$B_{\text{op}}(\mathcal{R}^{(N)},\epsilon) := \{\mathcal{S}^{(N)} s.t \|\mathcal{S}^{(N)} - \mathcal{R}^{(N)}\|_{\text{op}} \leqslant \epsilon\},$$

where $\mathcal{S}^{(N)}$ *is a deterministic quantum strategy.*

Equation (20) quantifies the minimum amount of quantum memory that one needs in order to realize a given a quantum strategy $\mathcal{R}^{(N)}$. In the case of a two-step deterministic quantum strategy whose entanglement cost is zero we recover the notion of one-way local operations and classical communication (LOCC). More generally, one could wonder how much quantum memory is needed in the realization of a strategy $\mathcal{S}^{(N)}$ which is similar to a target one $\mathcal{R}^{(N)}$: this intuition is formalized by Eq. (21).

The following result [3] provides the least upper bound to the amount of quantum memory which is required in the realization of any deterministic quantum strategy where coherence is preserved until the last step.

Proposition 2. Any deterministic quantum strategy $\mathcal{R}^N$ *can be realized with* $\boldsymbol{d} := \{d_k\}$*-dimensional quantum memories at steps* S*, where* $d_k = \text{Rnk}(R^{(k)})$.

The main result of this section is a necessary and sufficient condition for a deterministic quantum strategy to be realized with $\boldsymbol{d} := \{d_k\}$-dimensional quantum memories at steps J. We first consider the case in which the set $\mathsf{J} = \{k\}$ contains just a single step k, and then we generalize the result to arbitrary sets. Let us start with the following technical definition.

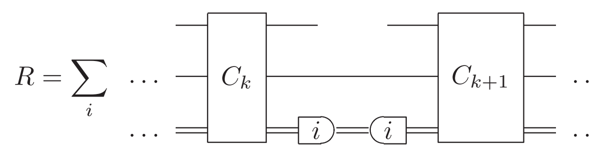
Definition 5. A quantum strategy $\mathcal{Q}^{(N)} \in \mathcal{L}(\mathcal{L}(\mathcal{H}_{\text{in}}),\mathcal{L}(\mathcal{H}_{\text{out}}))$ *is deterministic after the kth step if* $Q^{(N)}$ *satisfies*

$$\text{Tr}_{2l-1}[Q^{(l)}] = I_{2l-2} \otimes Q^{(l-1)}, \qquad l = k+1,\ldots,N,$$
$$Q^{(k)} \leqslant R^{(k)}, \tag{22}$$

where $R \in \mathcal{L}(\bigotimes_{i=0}^{2k-1} \mathcal{H}_i)$ *is a deterministic quantum comb.* Notice that Eq. (22) has the following simple operational interpretation: A quantum strategy $\mathcal{Q}^{(N)}$ that is deterministic after the kth step can be viewed as an element of a generalized instrument $\{\mathcal{Q}^{(N)},\mathcal{R}^{(N)} - \mathcal{Q}^{(N)}\}$, where also $\mathcal{R}^{(N)} - \mathcal{Q}^{(N)}$ is deterministic after the kth step. The deterministic strategy $\mathcal{R}^{(N)}$ is not unique, and it can be represented, e.g., by any deterministic comb of the form $R^{(N)} := Q^{(N)} + S \otimes (R^{(k)} - Q^{(k)})$, where $S \in \mathcal{L}(\bigotimes_{i=2k}^{2N-1} \mathcal{H}_i)$ is any deterministic quantum comb. The generalized instrument $\{\mathcal{Q}^{(N)},\mathcal{R}^{(N)} - \mathcal{Q}^{(N)}\}$ can be realized by a generalized instrument with k steps followed by a conditional deterministic comb with $N - k$ steps for each of the two outcomes. In particular, the conditional comb for the outcome corresponding to $\mathcal{Q}^{(N)}$ is $Q^{(k)-\frac{1}{2}} Q^{(N)} Q^{(k)-\frac{1}{2}}$. We are now ready to prove the following proposition.

Proposition 3. A deterministic quantum strategy $\mathcal{R}^{(N)} \in \mathcal{L}(\mathcal{L}(\mathcal{H}_{\text{in}}),\mathcal{L}(\mathcal{H}_{\text{out}}))$ *can be realized with a d-dimensional quantum memory at step k if and only if there exists a set* $\{\mathcal{Q}_j^{(N)}\}$ *of quantum strategies deterministic after the kth step such that* $R^{(N)} = \sum_j Q_j^{(N)}$ *and* $\text{Rnk}(Q_j^{(k)}) \leqslant d$.

Proof. First we suppose that $R^{(N)}$ is realizable with a d-dimensional quantum memory at step k. Then there exists a set of channels $\{\mathcal{C}_i | \mathcal{C}_i : \mathcal{L}(\mathcal{H}_{2i-2} \otimes \mathcal{A}_{i-1}) \to \mathcal{L}(\mathcal{H}_{2i-1} \otimes \mathcal{A}_i)\}$ such that $C_1 * \cdots * C_k * C_{k+1} * \cdots * C_N = R^{(N)}$ and $\mathcal{A}_k := \mathcal{A}_k^{(q)} \otimes \mathcal{A}_k^{(c)}$ with $\dim(\mathcal{A}_k^{(q)}) = d$. If we introduce the notation $S := C_1 * \cdots * C_k$ $[S \in \mathcal{L}(\bigotimes_{i=0}^{2k-1} \mathcal{H}_i \otimes \mathcal{A}_k)]$, $T := C_{k+1} * \cdots * C_N$ $[T \in \mathcal{L}(\bigotimes_{i=2k}^{N} \mathcal{H}_i \otimes \mathcal{A}_k)]$ we have $S * T = R^{(N)}$. Let now $\mathcal{D} : \mathcal{L}(\mathcal{A}_k^{(c)}) \to \mathcal{L}(\mathcal{A}_k^{(c)})$ be the measure-and-reprepare channel on the classical system, whose Choi operator is $D = \sum_i |i\rangle\langle i| \otimes |i\rangle\langle i|$. Since the classical information is not affected by the action of $\mathcal{D}$ we have



$$R^{(N)} = S * T = S * D * T = S * \sum_i |i\rangle\langle i| \otimes |i\rangle\langle i| * T$$
$$= \sum_i S_i * T_i, \tag{23}$$

where $S_i = S * |i\rangle\langle i|$ and $T_i = T * |i\rangle\langle i|$. We have that the set $\{S_i\}$ defines a generalized instrument while T_i defines a deterministic quantum strategy for each i. Let us now consider the spectral decompositions of the operators S_i,

$$S_i = \sum_{j \in J_i} X_{j,i}, \qquad X_{j,i} := |\psi_{j,i}\rangle\langle\psi_{j,i}|, \tag{24}$$

where J_i are disjoint sets. Notice that the set $\{X_{j,i}\}$ defines a generalized instrument from which $\{S_i\}$ can be obtained by coarse graining. Let us now define $Q_{j,i}^{(N)} := X_{j,i} * T_i$. One can verify that $Q_{j,i}^{(N)}$ is deterministic after the kth step for all j,i. Since $Q_{j,i}^{(k)} = \text{Tr}_{\mathcal{A}_k^{(q)}}(X_{j,i}) = \text{Tr}_{\mathcal{A}_k^{(q)}}(|\psi_{j,i}\rangle\langle\psi_{j,i}|)$ the dimension of $\mathcal{A}_k^{(q)}$ is an upper bound for the Schmidt rank of $|\psi_{j,i}\rangle$ with respect the bipartition $(\bigotimes_{i=0}^{2k-1} \mathcal{H}_i) \otimes \mathcal{A}_k^{(q)}$, which consequently implies that the rank of $Q_{j,i}^{(k)}$ is at most d. Combining Eqs. (23) and (24) we have $\sum_{ij} Q_{i,j}^{(N)} = \sum_i (\sum_j X_{j,i}) * T_i = \sum_i S_i * T_i = R^{(N)}$ and the thesis is proved.

We now prove sufficiency of the condition. By hypothesis we have $R^{(N)} = \sum_j Q_j^{(N)}$, where the $\{Q_j^{(N)}\}$ are deterministic after the kth step. Let us introduce the operators $|Q_j^{(k)\frac{1}{2}}\rangle\rangle\langle\langle Q_j^{(k)\frac{1}{2}}| \otimes |j\rangle\langle j| \in \mathcal{L}(\bigotimes_{i=0}^{2k-1} \mathcal{H}_i \otimes \mathcal{A}_{k,j}^{(q)} \otimes \mathcal{A}_k^{(c)})$, where $\mathcal{A}_{k,j}^{(q)} := \text{Supp}(Q_j^{(k)})$ and $\mathcal{A}_k^{(c)}$ is an Hilbert space carrying classical information encoded into the orthonormal basis $|j\rangle$. Since $\text{Rnk}(Q_j^{(k)}) \leqslant d$ for each j we can without loss of generality consider an isometric embedding of each $\mathcal{A}_{k,j}^{(q)}$ into a d-dimensional Hilbert space $\mathcal{A}_k^{(q)}$. One can easily check that $S := \sum_j |Q_j^{(k)\frac{1}{2}}\rangle\rangle\langle\langle Q_j^{(k)\frac{1}{2}}| \otimes |j\rangle\langle j|$ satisfies the normalization (10) and then Theorem 2 implies that there exists a realization $S = C_1 * \cdots * C_k$, where $C_k \in \mathcal{L}(\mathcal{A}_{k-1} \otimes \mathcal{H}_{2k-2} \otimes \mathcal{A}_k \otimes \mathcal{H}_{2k-1})$.

We now introduce the operator $T := \sum_j |j\rangle\langle j| \otimes Q_j^{(k)-\frac{1}{2}} Q_j^{(N)} Q_j^{(k)-\frac{1}{2}} \in \mathcal{L}(\mathcal{A}_k^{(c)} \otimes \mathcal{A}_k^{(q)} \otimes \bigotimes_{i=2k}^{2N-1} \mathcal{H}_i)$ (where also in this case we assumed the embedding $\mathcal{A}_{k,j}^{(q)} \hookrightarrow \mathcal{A}_k^{(q)}$). One can prove that T is a well-defined deterministic quantum comb. There exists then a realization $T = C_{k+1} * \ldots * C_N$, where $C_{k+1} \in \mathcal{L}(\mathcal{A}_k \otimes \mathcal{H}_{2k} \otimes \mathcal{A}_{k+1} \otimes \mathcal{H}_{2k+1})$. It is easy to verify that $S * T = R^{(N)}$, which in turns implies that $C_1 * \ldots * C_k * C_{k+1} * \ldots * C_N$ is a realization of $R^{(N)}$ with $\dim \mathcal{A}_k^{(q)} = d$. ■

The result of Proposition 3 can be extended to the case of multiple steps.

Theorem 3. *Let $\mathcal{R}^{(N)}$ be a deterministic quantum strategy and let J be a set of steps. For each $k \in \mathsf{J}$ we introduce an index i_k. The following two statements are equivalent:*

(a) *$\mathcal{R}^{(N)}$ is realizable with $\boldsymbol{d} := \{d_k\}$-dimensional quantum memories at steps J.*

(b) *There exists a set $Q_{\mathbf{i}}^{(N)}$, $\boldsymbol{i} = i_{k_{\min}}, \ldots, i_{k_{\max}}$, such that*

$$R^{(N)} = \sum_{\boldsymbol{i}} Q_{\boldsymbol{i}}^{(N)}, \qquad \mathrm{Rnk}\big(Q^{(k)}_{i_{k_{\min}},\ldots,i_k}\big) \leqslant d_k,$$

$$Q^{(N)}_{i_{k_{\min}},\ldots,i_k} \text{ are deterministic after the } k\text{th step,}$$

where we defined

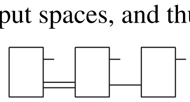
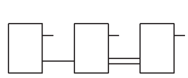
$$Q^{(N)}_{i_{k_{\min}},\ldots,i_k} := \sum_{i_{k'}} Q^{(N)}_{i_{k_{\min}},\ldots,i_{k'}}.$$

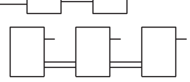
with k' denoting the element following k in J.

Proof. The result follows by iterating the proof of Proposition 3. ■

One could wonder whether the existence of a realization of a quantum strategy $\mathcal{R}^{(N)}$ with memory d_k at step k and of a realization with memory d_l at step l implies that there exists a realization of $\mathcal{R}^{(N)}$ with $\{d_k,d_l\}$-dimensional quantum memories at steps $\{k,l\}$. This would imply the equality $\mathsf{M}_{\mathsf{J}\cup\mathsf{I}}(\mathcal{R}^{(N)},0) = \max\{\mathsf{M}_{\mathsf{J}}(\mathcal{R}^{(N)},0),\mathsf{M}_{\mathsf{I}}(\mathcal{R}^{(N)},0)\}$ for any two sets of steps $\mathsf{J},\mathsf{I} \subseteq \mathsf{S}$. If this were true, a global minimization of the quantum memory would reduce to $N-1$ independent minimizations, one at each step. Unfortunately, this is not the case, as shown by the following counterexample.

Bennett *et al.* [17] introduced a state $\rho \in \mathcal{L}(\mathcal{H}_0 \otimes \mathcal{H}_1 \otimes \mathcal{H}_2)$ which is two-way separable but not three-way separable; i.e., we have $\rho = \sum_i \sigma_i^{[01]} \otimes \tau_i^{[2]} = \sum_j \tilde{\rho}_j^{[0]} \otimes \tilde{\tau}_j^{[12]}$ for some choice of unnormalized states $\sigma_i^{[01]}$, $\tau_i^{[2]}$, $\tilde{\rho}_j^{[0]}$, and $\tilde{\tau}_j^{[12]}$, but we cannot have $\rho = \sum_i \alpha_i^{[0]} \otimes \beta_i^{[1]} \otimes \gamma_i^{[2]}$ for any choice of unnormalized states $\alpha_i^{[0]}$, $\beta_i^{[1]}$, and $\gamma_i^{[2]}$ [18]. Every normalized quantum state can be interpreted as a quantum strategy with trivial input spaces, and thus we have

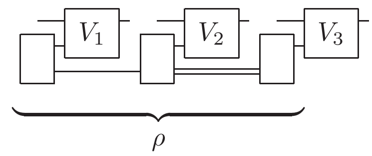
$\rho =$  or $\rho =$  ,

but $\rho \neq$  .

The fact that ρ is two-way separable but not three-way separable means that the three-step quantum strategy ρ is realizable with one-dimensional quantum memory either at step 1 or at step 2 but it cannot be realized with one-dimensional quantum memory at both steps, i.e.,

$$\mathsf{M}_{\{1,2\}}(\rho,0) > \max\{\mathsf{M}_{\{1\}}(\rho,0),\mathsf{M}_{\{2\}}(\rho,0)\}. \tag{25}$$

Moreover, we notice that it is possible to build a whole class of *three*-step quantum strategies with the property (25) by linking an isometric channel to each subsystem of ρ, i.e.,

$\mathcal{S}^{(3)} =$ 

$$\mathsf{M}_{\{1,2\}}(\mathcal{S}^{(3)},0) = 1, \quad \mathsf{M}_{\{1\}}(\mathcal{S}^{(3)},0) = \mathsf{M}_{\{2\}}(\mathcal{S}^{(3)},0) = 0.$$

V. EXAMPLES AND APPLICATIONS

It is in general a hard task to verify whether a deterministic quantum strategy can be realized with a given amount of quantum memory and to calculate its memory cost. Nevertheless, some properties of the quantum comb may imply nontrivial bounds on the quantum memory which is needed in the realization.

A. Memory requirements in the presence of symmetry

In this section we show that if a quantum strategy enjoys some symmetries, then the amount of quantum memory needed in the realization can be efficiently bounded. The following proposition provides the main tool we will use to prove such a bound.

Proposition 4. Let $\mathcal{R}^{(N)} \in \mathcal{L}(\mathcal{L}(\mathcal{H}_{\text{in}}),\mathcal{L}(\mathcal{H}_{\text{out}}))$ *be a deterministic quantum strategy and* $\{P_i, P_i \in \mathcal{L}(\bigotimes_{i=0}^{2k-1} \mathcal{H}_i)\}$ *be a set of orthogonal projectors such that* $\sum_i P_i = I_{0,\ldots,2k-1}$, *where* $I_{0,\ldots,2k-1}$ *is the identity on* $\bigotimes_{i=0}^{2k-1} \mathcal{H}_i$. *Suppose that* $R^{(N)} = \sum_i P_i R^{(N)} P_i$. *Then* $\mathcal{R}^{(N)}$ *is realizable with* d_k*-dimensional memory at step* k, *where* $d_k := \max_i \mathrm{Tr}[P_i]$. *Moreover, if* $\mathcal{R}^{(N)}$ *is realizable with* d_l*-dimensional memory at step* l *with* $l > k$, *then* $\mathcal{R}^{(N)}$ *is also realizable with* $\{d_k,d_l\}$ *-dimensional memories at steps* $\{k,l\}$.

Proof. Let us define $Q_i^{(N)} := P_i R^{(N)} P_i$. They satisfy the hypothesis of Proposition 3 with $\mathrm{Rnk}(Q_i^{(k)}) \leqslant d_k$.

Consider now the case in which $\mathcal{R}^{(N)}$ is realizable with d_l memory at step $l > k$. Then there exists a set of operators $\tilde{Q}_j^{(N)}$ satisfying the hypothesis of Proposition 3 with $\mathrm{Rnk}(\tilde{Q}_j^{(l)}) \leqslant d_l$. Let us now define $Q_{i,j}^{(N)} := P_i \tilde{Q}_j^{(l)} P_i$. One can verify that they satisfy the hypothesis of Theorem 3 with $\mathrm{Rnk}(Q_i^{(N)}) \leqslant d_k$ (where we recall that $Q_i^{(N)} := \sum_j Q_{i,j}^{(N)}$). ■

Before considering the case of quantum strategies with symmetries let us now introduce some preliminary notions of group representation theory. If $U(g) \in \mathcal{L}(\mathcal{H})$ is a unitary representation of a compact Lie group, then it is decomposable into a direct sum of irreducible representations $U(g) = \bigoplus_\nu U_\nu(g) \otimes I_{m_\nu}$, where $U_\nu(g) \in \mathcal{L}(\mathcal{H}_\nu)$ and $\mathcal{H} = \bigoplus_\nu \mathcal{H}_\nu \otimes \mathbb{C}^{m_\nu}$. The spaces $\mathcal{H}_\nu$ are customarily called representation spaces while the $\mathbb{C}^{m_\nu}$'s are called multiplicity spaces. We are now ready to prove the main result of this section.

Proposition 5. Let $\mathcal{R}^{(N)} \in \mathcal{L}(\bigotimes_{i=0}^{N} \mathcal{H}_i)$ *be a deterministic quantum strategy and let* $U(g) \in \mathcal{L}(\bigotimes_{i=0}^{2k-1} \mathcal{H}_i), U(g) = \bigoplus_\nu U_\nu(g) \otimes I_{m_\nu}$, *be a unitary representation of a compact*

Lie group G. If the commutation

$$[R^{(N)}, I_{2N-1\ldots 2k} \otimes U(g)] = 0 \quad \forall\, g \in G \tag{26}$$

holds, then $\mathcal{R}^{(N)}$ is realizable with d_k-dimensional quantum memory at step k, where d_k is the dimension of the largest multiplicity space, i.e., $d_k := \max_\nu m_\nu$.

Proof. Equation (26) and Schur's lemmas imply the decomposition

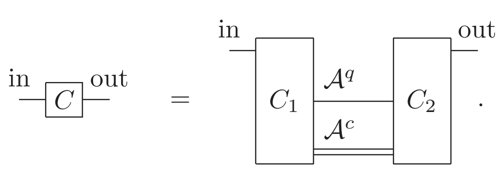
$$R^{(N)} = \sum_\nu P_\nu \otimes r_\nu. \tag{27}$$

Let $\{|\psi_\nu^j\rangle\}$ be an orthonormal basis for $\mathcal{H}_\nu$ and let P_{m_ν} denote the projectors on the multiplicity spaces $\mathbb{C}^{m_\nu}$. We now define the projectors $P_{\nu,j} := |\psi_\nu^j\rangle\langle\psi_\nu^j| \otimes P_{m_\nu}$. Since we have $\sum_{\nu,j} P_{\nu,j} = I_{0\ldots 2k-1}$ and Eq. (27) implies $R^{(N)} := \sum_{\nu,j} P_{\nu,j} R^{(N)} P_{\nu,j}$, the conditions of Proposition 4 are satisfied with $d_k := \max_{\nu,j} \mathrm{Tr}[P_{\nu,j}] = \max_\nu m_\nu$. ■

The optimal cloning of a unitary transformation for any dimension $d \geqslant 2$ [19] provides an example of a quantum strategy $\mathcal{R}^{(2)}$ that enjoys the property (26), with $\max_\nu m_\nu = 2$. We therefore conclude that any covariant protocol for cloning unitary channels has a memory cost of one qubit, independently of the dimension.

B. Memory cost of quantum channels

The aim of this section is to specialize the notion of memory cost to the case of channels and to provide examples that allow for an easy calculation. From Eq. (9), we have that a quantum channel $\mathcal{C} : \mathcal{L}(\mathcal{L}(\mathcal{H}_{\mathrm{in}}), \mathcal{L}(\mathcal{H}_{\mathrm{out}}))$ can be represented as a two-step deterministic quantum comb. This corresponds to interpreting $\mathcal{C}$ as if it was decomposed into an encoding channel $\mathcal{C}_1 : \mathcal{L}(\mathcal{L}(\mathcal{H}_{\mathrm{in}}), \mathcal{L}(\mathcal{A}^q \otimes \mathcal{A}^c))$ and a decoding channel $\mathcal{C}_2 : \mathcal{L}(\mathcal{L}(\mathcal{A}^q \otimes \mathcal{A}^c), \mathcal{L}(\mathcal{H}_{\mathrm{out}}))$:



(28)

Applying Definition 3, we say that a quantum channel $\mathcal{C}$ is realizable with d-dimensional quantum memory when there exist an encoding channel channel $\mathcal{C}_1 : \mathcal{L}(\mathcal{L}(\mathcal{H}_{\mathrm{in}}), \mathcal{L}(\mathcal{A}^q \otimes \mathcal{A}^c))$ and a decoding channel $\mathcal{C}_2 : \mathcal{L}(\mathcal{L}(\mathcal{A}^q \otimes \mathcal{A}^c), \mathcal{L}(\mathcal{H}_{\mathrm{out}}))$ such that $\dim(\mathcal{A}^q) \leqslant d$ and $C = C_1 * C_2$. Thanks to Proposition 3, this holds true if and only if there exists a set of operators $\{Q_i\}$ such that $C = \sum_i Q_i$ and $\mathrm{Rnk}(\mathrm{Tr}_{\mathrm{out}}[Q_i]) \leqslant d$. It is easy to verify that there is no loss of generality if we assume $\mathrm{Rnk}(Q_i) = 1$. We have then that a quantum channel $\mathcal{C}$ is realizable with d-dimensional quantum memory when there exists a decomposition $C = \sum_i |K_i\rangle\!\rangle\langle\!\langle K_i|$ such that $\mathrm{Rnk}(K_i^\dagger K_i) \leqslant d$. Equivalently, a quantum channel $\mathcal{C}$ is realizable with d-dimensional quantum memory when there exists a Kraus representation $\mathcal{C}(\rho) = \sum_i K_i \rho K_i^\dagger$ such that $\mathrm{Rnk}(K_i^\dagger K_i) \leqslant d$. The zero-error memory cost $\mathsf{M}(\mathcal{C},0)$ is equivalent to the zero-error entanglement cost of the quantum state $d_{\mathrm{in}}^{-1} C$ [20].

A similar notion of memory cost of a quantum channel, $\mathscr{E}(\mathcal{C})$, has been recently introduced in Ref. [4] and can be rephrased within our framework as follows

$$\mathscr{E}(\mathcal{C}) = \lim_{\epsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\mathsf{M}(\mathcal{C}^{\otimes n},\epsilon). \tag{29}$$

In Ref. [4] the authors proved that the quantity $\mathscr{E}(\mathcal{C})$ can be expressed in terms of the entanglement of formation and they discuss the relation between $\mathscr{E}(\mathcal{C})$ and the quantum channel capacity of $\mathcal{C}$.

In the previous section we discussed the relation between symmetry properties and quantum memory. We now consider two particular classes of covariant channels which allow for an easy calculation of the zero-error memory cost. This is the case of covariant channels $\mathcal{C} \in \mathcal{L}(\mathcal{L}(\mathcal{H}), \mathcal{L}(\mathcal{H}))$ satisfying the constraints

$$\mathcal{C}(U\rho U^\dagger) = U\mathcal{C}(\rho)U^\dagger, \tag{30}$$

$$\mathcal{C}(U^*\rho U^T) = U\mathcal{C}(\rho)U^\dagger. \tag{31}$$

One can prove that condition (30) implies the following form for the Choi operator:

$$C_\alpha : = \alpha\frac{1}{d}|I\rangle\!\rangle\langle\!\langle I| + \beta\left(I - \frac{1}{d}|I\rangle\!\rangle\langle\!\langle I|\right), \tag{32}$$

where $\alpha + (d^2-1)\beta = d$. On the other hand, Eq. (31) implies

$$C_\gamma := \gamma P_+ + \delta P_-, \tag{33}$$

where $P_\pm = \frac{1}{2}(I \pm E)$ are the projections on the symmetric and antisymmetric space of $\mathcal{H}\otimes\mathcal{H}$, respectively, E is the swap operator, $E|\varphi\rangle|\psi\rangle = |\psi\rangle|\varphi\rangle$, and $(d+1)\gamma + (d-1)\delta = 2$.

In the case of a symmetry as in Eq. (32), the zero-error entanglement cost of states $1/dC_\alpha$ was evaluated in Ref. [21]. This result implies that $\mathsf{M}(C_\alpha,0) = \log_2(\lceil\alpha\rceil)$, where $\lceil\alpha\rceil$ denotes the ceiling of α.

As regards the case of Eq. (33), one realizes that the C_γ are rescaled Werner states [22] by a factor d. Thus, for $1/(d+1) \leqslant \gamma \leqslant 2/(d+1)$, C_γ is a separable operator and consequently $\mathsf{M}(C_\gamma,0) = 0$. Since $P_\pm$ can be decomposed as the sum of rank-one projections on the states $|m\rangle|m\rangle$ and $(1/\sqrt{2})(|m\rangle|n\rangle \pm |n\rangle|m\rangle)$, whose partial trace $\frac{1}{2}(|m\rangle\langle m| + |n\rangle\langle n|)$ has rank 2, we always have $\mathsf{M}(C_\alpha,0) = 1$, when $0 \leqslant \gamma \leqslant 1/(d+1)$, irrespective of the dimension d.

VI. CONCLUSIONS

In conclusion, we defined the notion of memory cost for a quantum strategy that captures the minimal dimension of ancillary systems that need to be kept coherent during an algorithm specified by the comb representing the strategy. The realization of the strategy using minimal global ancillary dimension can be algebraically characterized by Theorem 3, representing our main result.

We also showed by an example that the optimization of the memory required between two steps of the computation is in general not compatible with the optimization of the memory required between two different steps.

We notice that the algebraic condition provided by Theorem 3 does not allow for an easy evaluation of the memory cost for a given strategy. For this reason, providing a nontrivial bound on the memory requirement is a hard problem. In this paper we showed that symmetry arguments can help to calculate the memory cost of some particular channels and strategies, such as, e.g., the covariant cloning of unitary transformation.

A natural extension of this line of research consists in looking for new conditions under which similar bounds for the memory cost can be provided.

ACKNOWLEDGMENTS

This work has been supported by the EU FP7 programme through the STREP project COQUIT and by the Italian Ministry of Education through PRIN 2008.

[1] L. K. Grover, in Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, 212 (1996).
[2] P. Shor, SIAM Rev. **41**, 303 (1999).
[3] A. Bisio, G. M. D'Ariano, P. Perinotti, and G. Chiribella, Phys. Rev. A **83**, 022325 (2011).
[4] M. Berta, F. Brandao, M. Christandl, and S. Wehner, e-print arXiv:1108.5357.
[5] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. Lett. **101**, 060401 (2008).
[6] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. A **80**, 022339 (2009).
[7] A. Bisio, G. Chiribella, G. M. D'Ariano, and P. Perinotti, Acta Phys. Slovaca **61**, 273 (2011).
[8] M.-D. Choi, Lin. Alg. Appl. **10**, 285 (1975).
[9] If a device is used more than once we represent each different use with a linear map so that different uses of the same device are actually different linear maps.
[10] Within our formalism a physical closed loop in the laboratory, which is taking the output of a device and then sending it as an input to the same device, corresponds to many subsequent uses of the same transformation.
[11] G. M. D'Ariano, D. Kretschmann, D. M. Schlingemann, and R. F. Werner, Phys. Rev. A **76**, 032328 (2007).
[12] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Nat. Phys. **4**, 726 (2008).
[13] D. Deutsch and R. Jozsa, Proc. R. Soc. London A **439**, 553 (1992).
[14] G. Gutoski and J. Watrous, in Proceedings of the 39th Annual ACM Symposium on Theory of Computation, 565 (2007).
[15] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. Lett. **101**, 180501 (2008).
[16] This formalism is equivalent to the usage of a direct sum over the classical label $\mathcal{A} = \bigoplus_i \mathcal{A}^{(i)}$ with the prescription that each Hilbert space $\mathcal{A}^{(i)}$ is embedded into an Hilbert space $\tilde{\mathcal{A}}^{(i)}$ with $\dim(\tilde{\mathcal{A}}^{(i)}) = \max_j \dim(\mathcal{A}^{(j)})$.
[17] C. H. Bennett, D. P. Di Vincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).
[18] The superscript $[ij]$ denotes that $\xi^{[ij]} \in \mathcal{L}(\mathcal{H}_i \otimes \mathcal{H}_j)$.
[19] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. Lett. **101**, 180504 (2008).
[20] F. Buscemi and N. Datta, Phys. Rev. Lett. **106**, 130503 (2011).
[21] B. M. Terhal and P. Horodecki, Phys. Rev. A **61**, 040301 (2000).
[22] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).