

**Minimal computational-space implementation of multi-round quantum protocols**

Alessandro Bisio, Giacomo Mauro D'Ariano, and Paolo Perinotti

*QUIT group, Dipartimento di Fisica "A. Volta", and INFN Sezione di Pavia, via Bassi 6, IT-27100 Pavia, Italy*

Giulio Chiribella

*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario N2L 2Y5, Canada*

(Received 9 June 2010; published 24 February 2011)

A single-party strategy in a multi-round quantum protocol can be implemented by sequential networks of quantum operations connected by internal memories. Here, we provide an efficient realization in terms of computational-space resources.

DOI: [10.1103/PhysRevA.83.022325](https://doi.org/10.1103/PhysRevA.83.022325)

PACS number(s): 03.67.Ac

**I. INTRODUCTION**

Many results in quantum-information [1] and quantum estimation theory [2,3] have been achieved through the general description of states and measurements in terms of density matrices and positive-operator-valued measures (POVMs), respectively. The advantages of this formalism are evident in optimization tasks, e.g., state discrimination, where one can look for the optimal measurement without considering the specific details of the apparatus. Furthermore, the optimization of preparation and measurement devices is reduced to the optimization of positive operators, for which many powerful techniques are known. Similar advantages are provided by the description of physical transformations as quantum channels (completely positive trace-preserving maps), which in turn can be represented by positive operators via the Choi-Jamiołkowski isomorphism [4].

The usage of the Choi-Jamiołkowski isomorphism is well established in quantum-information theory [5,6] since the early works on ancilla-assisted tomography [7,8]. Recently, the Choi-Jamiołkowski representation has been extended to more complex quantum devices, consisting of sequences of channels, quantum operations, and POVMs connected by internal wires [9–11]. In particular, Ref. [9] considered the application of these sequential networks to represent single-party strategies in multi-round quantum games, while Refs. [10,11] showed how these networks can implement a variety of higher-order quantum-information processing tasks, such as transforming states into channels, channels into channels, and even networks into networks. References [10,11] also coined the name *quantum combs* for the Choi-Jamiołkowski operators associated with sequential networks, and developed a simple set of rules to describe the interlinking of networks in terms of the corresponding operators. In this framework, once a specific task is fixed (e.g., cloning a channel [12] or estimating the POVM of a detector [13]), one can search for the quantum protocol that optimally realizes it. Having a simple description now becomes indispensable: since a quantum protocol is implemented by a complex network of devices, optimizing each device separately is not a viable approach. In the new framework, instead, the optimization of the protocol is reduced to the optimization of a single positive operator subject to linear constraints. In the simplest cases the search can be also implemented automatically through MATLAB routines [14,15].

Once the optimal Choi-Jamiołkowski operator has been found, however, one needs a way to unzip the information contained in it and to find a physical implementation of the network. In the present paper we solve this problem, providing an automatic procedure that, given the Choi-Jamiołkowski operator of a quantum network, allows one to construct a concrete implementation of it as a sequence of elementary devices. Among all possible implementations, the present one minimizes the computational space; that is, at each step it uses the smallest possible dimension of the Hilbert spaces. Our procedure can be fully automatized in the form of a computer software, accepting as an input the Choi-Jamiołkowski representation of the network and providing as an output the matrix representation of the operations that must be performed at each stage of the protocol. After the operations in the network have been determined, one can look for a further decomposition of them into elementary gates, using, e.g., the techniques of Refs. [16,17].

The paper is organized as follows. In Sec. II we review the general theory of quantum combs. In Sec. III we prove the theorem representing the main result of the paper, also providing a simpler proof of the realization theorem for quantum combs. In Sec. IV we consider the problem of optimal correction of a reversible unknown noise, and then we apply our results to reverse engineering of the optimal circuit. We conclude the paper with a summary and comments in Sec. V.

**II. QUANTUM COMBS**

In this section we review the basic concepts and results of the general theory of quantum networks as presented in Refs. [10,11]. The most general quantum device is a quantum circuit board, namely, a network of quantum devices with open slots to which variable sub-circuits can be linked. By stretching and rearranging the internal wires of the network, we can give to each quantum circuit board the shape of a comb, like in Fig. 1. The empty slots of the circuit board become the empty spaces between two teeth of the comb. Referring to Fig. 1, each wire is labeled with a natural number, which is even for the input wires and odd for the output ones; the corresponding Hilbert spaces are labeled in the same fashion (that is, the Hilbert space of the system represented by the wire  $i$  is denoted by  $\mathcal{H}_i$ ). The ordering of the slots results from the causal ordering defined by the flow of quantum information

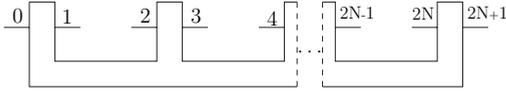


FIG. 1. A quantum comb with  $N$  slots. Information flows from left to right. The causal structure of the comb implies that the input system  $m$  cannot influence the output system  $n$  if  $m > n$ .

from input to output; with our notation we have that input system in wire  $i$  can influence the output system in a wire  $j > i$  but not in a wire  $k < i$ . Two circuit boards  $\mathcal{C}_1$  and  $\mathcal{C}_2$  can be connected by linking some outputs of  $\mathcal{C}_1$  with inputs of  $\mathcal{C}_2$ , thus forming a new board  $\mathcal{C}_3 := \mathcal{C}_1 * \mathcal{C}_2$ . We adopt the convention that wires that are connected are identified by the same label (see Fig. 2).

In the following we will often use the isomorphism between linear operators in  $\text{Lin}(\mathcal{H})$  and states in  $\mathcal{H} \otimes \mathcal{H}$ :

$$A = \sum_{nm} \langle n|A|m\rangle |n\rangle\langle m| \leftrightarrow |A\rangle = \sum_{nm} \langle n|A|m\rangle |n\rangle|m\rangle,$$

where  $\{|n\rangle\}$  is a fixed orthonormal basis.

The *quantum comb*  $\mathcal{C}$  associated with a circuit board  $\mathcal{C}$  with  $N$  input-output systems is the Choi-Jamiołkowski operator of the multipartite channel representing the input-output transformation that the board performs from states on  $\mathcal{H}_{\text{in}} := \bigotimes_{j=0}^{N-1} \mathcal{H}_{2j}$  to states on  $\mathcal{H}_{\text{out}} := \bigotimes_{j=0}^{N-1} \mathcal{H}_{2j+1}$ ,  $\mathcal{H}_n$  being the Hilbert space of the  $n$ th system. A quantum comb is then a positive operator acting on  $\mathcal{H}_{\text{out}} \otimes \mathcal{H}_{\text{in}}$  and it is defined as follows:

$$\mathcal{C}_{\text{out in}} := (\mathcal{C} \otimes \mathcal{I}_{\text{in}})(|I\rangle\langle\langle I|_{\text{in in}}). \quad (1)$$

[For clarity here we use the notation  $\mathcal{H}_{ab} \equiv \mathcal{H}_a \otimes \mathcal{H}_b$ ,  $A_{ab}$  to mean  $A \in \text{Lin}(\mathcal{H}_{ab})$ ,  $|\psi\rangle_b$  to mean  $|\psi\rangle \in \mathcal{H}_b$ , and  $|A\rangle_{ab}$  to mean  $|A\rangle \in \mathcal{H}_{ab}$ .] It can be proved that the causal structure is equivalent to the recursive normalization condition

$$\text{Tr}_{2k-1}[\mathcal{C}^{(k)}] = I_{2k-2} \otimes \mathcal{C}^{(k-1)} \quad k = 1, \dots, N, \quad (2)$$

where  $\mathcal{C}^{(N)} = \mathcal{C}$ ,  $\mathcal{C}^{(0)} = 1$ ,  $\mathcal{C}^{(k)} \in \mathcal{L}(\mathcal{H}_{\text{out}_k} \otimes \mathcal{H}_{\text{in}_k})$  with  $\mathcal{H}_{\text{in}_k} = \bigotimes_{j=0}^{k-1} \mathcal{H}_{2j}$  and  $\mathcal{H}_{\text{out}_k} = \bigotimes_{j=0}^{k-1} \mathcal{H}_{2j+1}$ , is the comb of the reduced circuit  $\mathcal{C}^{(k)}$  obtained by discarding the last  $N - k$  teeth.

One can prove that the connection of two circuit boards is represented by the *link product* of the corresponding combs  $\mathcal{C}_1$  and  $\mathcal{C}_2$ , which is defined as [11]  $\mathcal{C}_1 * \mathcal{C}_2 = \text{Tr}_{\mathcal{K}}[\mathcal{C}_1^{\theta_{\mathcal{K}}} \mathcal{C}_2]$ ,  $\theta_{\mathcal{K}}$  denoting partial transposition over the Hilbert space  $\mathcal{K}$  of the connected systems (we identify with the same labels the Hilbert spaces of connected systems).

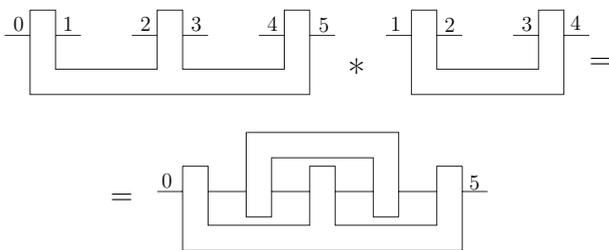


FIG. 2. Linking of two combs. We identify the wires with the same label.

### III. REALIZATION ALGORITHM

One can wonder whether each positive operator which satisfies Eq. (2) corresponds to a sequential network of quantum channels. The answer is indeed positive, as shown in Refs. [9–11] with the following Stinespring dilation theorem:

*Theorem 1.* Let  $\mathcal{C}^{(N)}$  be a positive operator on  $\mathcal{H}_{\text{out}} \otimes \mathcal{H}_{\text{in}}$ , with  $\mathcal{H}_{\text{in}} := \bigotimes_{j=0}^{N-1} \mathcal{H}_{2j}$  and  $\mathcal{H}_{\text{out}} := \bigotimes_{j=0}^{N-1} \mathcal{H}_{2j+1}$ . If  $\mathcal{C}^{(N)}$  satisfies Eq. (2), then it is the Choi-Jamiołkowski operator of a sequential network given by the concatenation of  $N$  isometries: for every state  $\rho \in \text{Lin}(\mathcal{H}_{\text{in}})$  one has

$$\mathcal{C}^{(N)}(\rho) = \text{Tr}_{A_N}[V^{(N)} \dots V^{(1)} \rho V^{(1)\dagger} \dots V^{(N)\dagger}], \quad (3)$$

where  $V^{(k)}$  is an isometry from  $\mathcal{H}_{2k-2} \otimes \mathcal{H}_{A_{k-1}}$  to  $\mathcal{H}_{2k-1} \otimes \mathcal{H}_{A_k}$ , and  $\mathcal{H}_{A_k}$  is an ancillary space,  $\mathcal{H}_{A_0} = \mathbb{C}$  [in Eq. (3) we omitted the identity operators on the Hilbert spaces where the isometries do not act].

This result, however, provides little insight on how to construct the isometries. We now give the explicit construction in terms of the Choi-Jamiołkowski operator in a way that can be automatically evaluated by a computer routine:

*Theorem 2.* The minimal dimension of the ancilla space  $\mathcal{H}_{A_k}$  in Theorem 1 is the dimension of the support of  $\mathcal{C}^{(k)}$ . A choice of isometries  $V^{(k)} : \mathcal{H}_{2k-2} \otimes \mathcal{H}_{A_{k-1}} \rightarrow \mathcal{H}_{2k-1} \otimes \mathcal{H}_{A_k}$  with minimal ancilla space is obtained by taking  $\mathcal{H}_{A_k} = \text{Supp}(\mathcal{C}^{(k)*})$ , where  $*$  denotes the complex conjugation in the canonical basis, and

$$V^{(k)} = I_{2k-1} \otimes \mathcal{C}^{(k)\frac{1}{2}*} \mathcal{C}^{(k-1)-\frac{1}{2}*} \times |I\rangle_{(2k-1)(2k-1)'} T_{(2k-2) \rightarrow (2k-2)'}, \quad (4)$$

where  $T_{n \rightarrow m} = \sum_i |i\rangle_m \langle i|_n$ .

*Proof.* One has  $V^{(k)\dagger} V^{(k)} = (\mathcal{C}^{(k-1)*})^{-\frac{1}{2}} \text{Tr}_{2k-1}[\mathcal{C}^{(k)*}] (\mathcal{C}^{(k-1)*})^{-\frac{1}{2}}$ , and Eq. (2) yields  $V^{(k)\dagger} V^{(k)} = I_{2k-2} \otimes I_{\text{Supp}(\mathcal{C}^{(k-1)*})} = I_{2k-2} \otimes I_{A_{k-1}}$ . Therefore,  $V^{(k)}$  is an isometry. Now, define the isometry  $W^{(k)} = V^{(k)} \dots V^{(1)}$ , from  $\mathcal{H}_{\text{in}_k}$  to  $\mathcal{H}_{\text{out}_k} \otimes \mathcal{H}_{A_k}$ . By definition one has  $W^{(k)} = [I_{\text{out}_k} \otimes (\mathcal{C}^{(k)*})^{\frac{1}{2}}][|I\rangle_{(\text{out}_k)(\text{out}_k)'} \otimes T_{\text{in}_k \rightarrow (\text{in}_k)'}]$ . However, according to Ref. [18], this is the minimal isometry of the channel  $\mathcal{C}^{(k)}$ . Since the isometry is minimal, it is not possible to choose an ancillary space smaller than  $\mathcal{H}_{A_k}$ . Finally, since  $\mathcal{C}^{(N)}$  is just the channel associated with the network, Eq. (3) follows. ■

Theorem 2 implies Theorem 1, and provides a recipe for the concrete realization of the quantum network with minimal dimension of the ancillas at each step. The dimension of the ancilla is the quantum “space” of the computational network. Note that sometimes the isometries  $V^{(k)}$  can act trivially on some subsystem, resulting in further simplifications of the physical implementation.

### IV. OPTIMAL INVERSION OF A UNITARY

As an application of the methods outlined above we now consider the problem of finding the quantum network that realizes the optimal inversion of a unitary operation. Such a network consists of a circuit board  $\mathcal{C}$  with an empty slot to be linked to the unitary channel  $\mathcal{U}(\rho) = U\rho U^\dagger$  sending states on  $\mathcal{H}_1$  to states on  $\mathcal{H}_2$ . The resulting circuit  $\mathcal{C} * \mathcal{U}$  has to be as similar as possible to the channel  $\mathcal{U}^{-1}$  [see Fig. (3)]. The quantum comb of  $\mathcal{C}$  is  $\mathcal{C} \in \text{Lin}(\mathcal{H}_{3210})$ ,

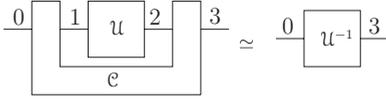


FIG. 3. The quantum circuit  $\mathcal{C}$ , when linked with the unitary channel  $\mathcal{U} : \text{Lin}(\mathcal{H}_1) \rightarrow \text{Lin}(\mathcal{H}_2)$ , tries to reproduce the action of  $\mathcal{U}^{-1}$  from input  $\mathcal{H}_0$  to output  $\mathcal{H}_3$ .

with  $\mathcal{H}_3 \simeq \mathcal{H}_2 \simeq \mathcal{H}_1 \simeq \mathcal{H}_0 \simeq \mathbb{C}^d$ , and, according to Eq. (2), satisfies the normalization

$$\text{Tr}_3[C] = I_2 \otimes C^{(1)}, \quad \text{Tr}_1[C^{(1)}] = I_0. \quad (5)$$

Choi operator of the unitary channel is  $|U\rangle\langle U|_{21}$  and the link  $\mathcal{C} * \mathcal{U}$  gives the operator  $\langle\langle U^*|_{21} \mathcal{C} |U^*\rangle\rangle_{21} \in \text{Lin}(\mathcal{H}_{30})$ . To quantify the similarity between the channel  $\mathcal{C} * \mathcal{U}$  and the target  $\mathcal{U}^{-1}$  we use the channel fidelity [19]: if  $\mathcal{A}$  and  $\mathcal{B}$  are two channels and  $A$  and  $B$  are their Choi-Jamiołkowski operators the channel fidelity  $\mathcal{F}(\mathcal{A}, \mathcal{B})$  is defined as  $f(d^{-1}A, d^{-1}B)$  where  $f$  is the state fidelity  $f(\rho, \sigma) = |\text{Tr}\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}|^2$ . In our case we have

$$\begin{aligned} F(\mathcal{C}, \mathcal{U}) &= f(d^{-1}(\mathcal{C} * |U\rangle\langle U|) \langle\langle U|_{21}, d^{-1}|U^\dagger\rangle\rangle \langle\langle U^\dagger|_{30}) \\ &= \frac{1}{d^2} \langle\langle U^\dagger|_{30} \langle\langle U^*|_{21} \mathcal{C} |U^\dagger\rangle\rangle_{30} |U^*\rangle_{21}. \end{aligned} \quad (6)$$

We assume the unknown unitary  $U$  randomly distributed according to the Haar measure of  $\text{SU}(d)$ , and, as a figure of merit, we adopt the average of the gate fidelity:

$$\begin{aligned} \bar{F} &= \int_{\text{SU}(d)} dU F(\mathcal{C}, \mathcal{U}) \\ &= \frac{1}{d^2} \int_{\text{SU}(d)} dU \langle\langle U^\dagger|_{30} \langle\langle U^*|_{21} \mathcal{C} |U^\dagger\rangle\rangle_{30} |U^*\rangle_{21}, \end{aligned} \quad (7)$$

where  $dU$  denotes the invariant Haar measure. The following lemma holds:

*Lemma.* The operator  $C$  maximizing the fidelity (7) can be assumed without loss of generality to satisfy the commutation relation

$$[C, U_3 \otimes W_2 \otimes U_1 \otimes W_0] = 0 \quad \forall V, W \in \text{SU}(d). \quad (8)$$

The proof consists in the standard averaging argument: Let  $C$  be optimal. Then take its average  $\bar{C} = \int dU dW (U_3 \otimes W_2 \otimes U_1 \otimes W_0) C (U_3 \otimes W_2 \otimes U_1 \otimes W_0)^\dagger$ : it is immediate to see that  $\bar{C}$  satisfies Eqs. (8) and (5) and has the same fidelity as  $C$ .

As an elementary consequence of Schur's lemmas, we have the following identities:

$$\begin{aligned} \int_{\text{SU}(d)} dU U X U^\dagger &= \frac{1}{d} \text{Tr}[X] I, \\ \int_{\text{SU}(d)} dU (U \otimes U) X (U^\dagger \otimes U^\dagger) \\ &= \text{Tr}[P^+ X] \frac{P^+}{d_+} + \text{Tr}[P^- X] \frac{P^-}{d_-}, \end{aligned} \quad (9)$$

where  $P^\pm = 1/2(I \pm E)$  ( $E$  representing the swap operator  $E|\phi\rangle|\psi\rangle = |\psi\rangle|\phi\rangle$ ) are the projections on the symmetric and antisymmetric subspaces of  $\mathcal{H} \otimes \mathcal{H}$ . By the invariance of the Haar measure  $dU$ , Eqs. (9) allow us to write the following

expression for  $C$ , which is equivalent to the conditions in Eq. (8):

$$C = \sum_{\mu, \nu \in \mathbf{S}} a^{\mu\nu} P_{31}^{\mu} \otimes P_{20}^{\nu}, \quad (10)$$

where  $\mathbf{S} = \{+, -\}$ ,  $P_{ij}^\pm$  are the projections onto the symmetric and antisymmetric subspaces of  $\mathcal{H}_i \otimes \mathcal{H}_j$ , while by positivity of  $C$  necessarily  $a^{\mu\nu} \geq 0 \forall \mu, \nu$ . Moreover, using Eqs. (8) and (10), the fidelity (7) becomes

$$\begin{aligned} \bar{F} &= \frac{1}{d^2} \langle\langle I|_{30} \langle\langle I|_{21} \mathcal{C} |I\rangle\rangle_{30} |I\rangle\rangle_{21} \\ &= \frac{1}{d^2} \sum_{\nu \in \mathbf{S}} a^{\nu\nu} d_\nu, \quad d_\nu = \text{Tr}[P^\nu], \end{aligned} \quad (11)$$

while using the identities

$$\text{Tr}_i[P_{ij}^\pm] = \frac{d_\pm}{d} I_j, \quad (12)$$

the normalization (5) becomes  $\sum_{\mu \in \mathbf{S}} a^{\mu\nu} d_\mu = 1, \forall \nu \in \mathbf{S}$ . The last equality implies the bound  $\bar{F} = \frac{1}{d^2} \sum_{\mu \in \mathbf{S}} a^{\mu\mu} d_\mu \leq 2/d^2$ , which is saturated if and only if  $a^{\mu\nu} = \frac{\delta_{\mu\nu}}{d_\mu}$ , that is, if and only if

$$\begin{aligned} C &= \frac{P_{31}^+ \otimes P_{20}^+}{d_+} + \frac{P_{31}^- \otimes P_{20}^-}{d_-} \\ &= \int_{\text{SU}(d)} d\hat{U} |\hat{U}^\dagger\rangle\langle\langle \hat{U}^\dagger|_{30} \otimes |\hat{U}^*\rangle\rangle \langle\langle \hat{U}^*|_{21}. \end{aligned} \quad (13)$$

We now use Theorem 2 to construct the optimal network from the quantum comb  $C$ . Since  $C^{(1)} = d^{-1}I_{10}$  the first isometry is given by

$$V^{(1)} = (I_1 \otimes C^{(1)*\frac{1}{2}}) |I\rangle\rangle_{11'} \otimes T_{0 \rightarrow 0'} = \frac{1}{\sqrt{d}} |I\rangle\rangle_{11'} \otimes T_{0 \rightarrow 0'},$$

namely, it consists of the preparation of the maximally entangled state  $\frac{1}{\sqrt{d}} |I\rangle\rangle_{11'}$ , while the input state is stored in a subsystem of the ancilla space  $\mathcal{H}_{A_1} \subset \mathcal{H}_{1'0'}$ .

The second isometry  $V^{(2)} : \mathcal{H}_2 \otimes \mathcal{H}_{A_1} \rightarrow \mathcal{H}_3 \otimes \mathcal{H}_{A_2}$  is given by

$$V^{(2)} = (\sqrt{d} I_3 \otimes C^{*\frac{1}{2}}) |I\rangle\rangle_{33'} \otimes T_{2 \rightarrow 2'}. \quad (14)$$

Remarkably, this is the Stinespring isometry of a measure-and-prepare channel. Indeed, consider the channel  $\mathcal{E}(\rho) = \text{Tr}_{A_2}[V^{(2)} \rho V^{(2)\dagger}]$  and the POVM

$$Q_{\hat{U}} = (C^*)^{-\frac{1}{2}} |\hat{U}^T\rangle\rangle \langle\langle \hat{U}^T|_{3'0'} \otimes |\hat{U}\rangle\rangle \langle\langle \hat{U}|_{2'1'} (C^*)^{-\frac{1}{2}}, \quad (15)$$

which provides a resolution of the identity in  $\mathcal{H}_{A_2} = \text{Supp}(C^*)$  due to Eq. (13). We then have

$$\begin{aligned} \mathcal{E}(\rho) &= \int_{\text{SU}(d)} d\hat{U} \text{Tr}_{A_2}[V^{(2)} \rho V^{(2)\dagger} Q_{\hat{U}}] \\ &= d \int_{\text{SU}(d)} d\hat{U} \hat{U}^\dagger \langle\langle \hat{U}|_{2'1'} \rho |\hat{U}\rangle\rangle_{2'1'} \hat{U}, \end{aligned} \quad (16)$$

namely, the channel  $\mathcal{E}$  can be implemented by measuring the POVM  $P_{\hat{U}} = d |\hat{U}\rangle\rangle \langle\langle \hat{U}|_{2'1'}$  on the Hilbert space  $\mathcal{H}_{2'1'}$  and subsequently performing the unitary  $\hat{U}^\dagger$  on  $\mathcal{H}_0$ . Therefore, the optimal network for the inversion of an unknown unitary channel corresponds to an “estimate and re-prepare” strategy:

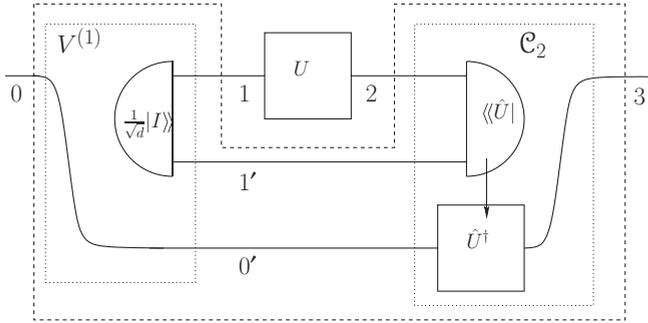


FIG. 4. Optimal circuit for the inversion of a unitary transformation. The input state in wire 0 is stored in a quantum memory. The unitary  $U$  to be inverted is estimated and the inverted estimated unitary is applied to the input.

first the isometry  $V^{(1)}$  provides the optimal input for the estimation of  $U$  (that is, the maximally entangled state  $d^{-\frac{1}{2}}|I\rangle\rangle_{11'}$ ), then, after the unknown unitary has been applied, the second channel  $\mathcal{E}$  performs the optimal POVM on the state  $d^{-\frac{1}{2}}|U\rangle\rangle_{11'}$  and, depending on the estimate  $\hat{U}$ , applies the unitary  $\hat{U}^\dagger$  on the input state stored in wire  $0'$  (see Fig. 4). The physical implementation involving measurement and classical feed-forward is an alternative to the coherent, fully quantum processing corresponding to the isometry  $V^{(2)}$ .

## V. CONCLUSION

In conclusion, we provided a general method for recovering all the isometries of a network from its Choi-Jamiołkowski operator minimizing the computational space. This result allows us to formulate an algorithm for designing optimal quantum networks for any desired task (e.g., cloning, discrimination, estimation):

- (i) Choose a suitable figure of merit  $F$  for the task of interest.
- (ii) Find the positive operator  $C$  satisfying constraint in Eq. (2) and maximizing  $F$ .

- (iii) Set  $C^{(0)} = 1$  and  $I_{A_0} = 1$ .
- (iv) For  $k = 1$  to  $k = N$  do the following: (a) Calculate  $I_{\text{in}_k} \otimes C^{(k)} = \text{Tr}_{\text{out}_k}[C]$ , where  $I_{\mathcal{H}}$  ( $\text{Tr}_{\mathcal{H}}$ ) denotes the identity (partial trace) over all Hilbert spaces but  $\mathcal{H}$ . (b) Define  $V^{(k)}$  as in Theorem 2.
- (v) The optimal network is given by the concatenation of the  $V^{(k)}$  in Eq. (3).

We applied the algorithm to design the optimal circuit for the inversion of a unitary transformation. It is worth noting that in general the numerical optimization of step (ii) can be challenging, and that it is typically convenient to exploit the symmetries of the problem to reduce the number of parameters, as we did here in our example. On the other hand, the remaining steps (iii)–(v), which represent the original result of the present paper, can be easily programmed on a computer.

Finally, we want to stress that minimality of the computational space provided by our procedure holds when one wants to keep all ancillary systems coherent until the last computational step. However, if one considers a nonminimal dilation it is possible that some ancillas can be discarded at some intermediate step, which would in principle allow for an even more economic implementation. Moreover, a further minimization of resources would be possible if the quantum memories could be replaced by classical memories at any step. However, a general analysis of these further optimization steps looks very hard, and presently only a specific case-by-case analysis is viable. As a direction for future research, it is very important to provide general algebraic conditions for the possibility of any of these two simplifications.

## ACKNOWLEDGMENTS

This work is supported by the Italian Ministry of Education through Grant PRIN 2008 and the EC through Project CO-QUIT. Research at Perimeter Institute for Theoretical Physics is supported in part by the Government of Canada through NSERC and by the Province of Ontario through MRI.

- 
- [1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University, Cambridge, UK, 2000).
  - [2] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North Holland, Amsterdam, 1982).
  - [3] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
  - [4] M.-D. Choi, *Lin. Alg. Appl.* **10**, 285 (1975); A. Jamiołkowski, *Rep. Math. Phys.* **3**, 275 (1972).
  - [5] B. Schumacher, *Phys. Rev. A* **54**, 2614 (1996).
  - [6] J. F. Poyatos, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **78**, 390 (1997).
  - [7] G. M. D'Ariano and P. Lo Presti, *Phys. Rev. Lett.* **86**, 4195 (2001).
  - [8] D. Leung, Ph.D. thesis, Stanford University, e-print arXiv:cs/0012017.
  - [9] G. Gutoski and J. Watrous, in *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing* (ACM, New York, NY, 2007), pp. 565–574.
  - [10] G. Chiribella, G. M. D'Ariano, and P. Perinotti, *Phys. Rev. Lett.* **101**, 060401 (2008).
  - [11] G. Chiribella, G. M. D'Ariano, and P. Perinotti, *Phys. Rev. A* **80**, 022339 (2009).
  - [12] G. Chiribella, G. M. D'Ariano, and P. Perinotti, *Phys. Rev. Lett.* **101**, 180504 (2008).
  - [13] J. S. Lundeen, A. Feito, H. Coldenstrodt-Ronge, K. L. Pregnell, C. Silberhorn, T. C. Ralph, J. Eisert, M. B. Plenio, and I. A. Walmsley, *Nature Phys.* **5**, 27 (2009).
  - [14] See the codes for convex optimization by M. Grant and S. Boyd at [<http://cvxr.com/cvx/>].
  - [15] J. Watrous (private communication).
  - [16] J. J. Vartiainen, M. Mottonen, and M. M. Salomaa, *Phys. Rev. Lett.* **92**, 177902 (2004).
  - [17] V. V. Shende, S. S. Bullock, and I. L. Markov, *IEEE Trans. Computer-Aided Design* **25**, 1000 (2006).
  - [18] G. Chiribella, G. M. D'Ariano, and P. Perinotti, *J. Math. Phys.* **50**, 042101 (2009).
  - [19] M. Raginsky, *Phys. Lett. A* **290**, 11 (2001).