

## Efficient Universal Programmable Quantum Measurements

Giacomo Mauro D'Ariano\* and Paolo Perinotti†

*QUIT Group, Dipartimento di Fisica "A. Volta," via Bassi 6, I-27100 Pavia, Italy*

(Received 21 October 2004; published 8 March 2005)

A universal programmable detector is a device that can be tuned to perform any desired measurement on a given quantum system, by changing the state of an ancilla. With a finite dimension  $d$  for the ancilla only approximate universal programmability is possible, with size  $d = f(\varepsilon^{-1})$  increasing the function of the "accuracy"  $\varepsilon^{-1}$ . In this Letter we show that, much better than the exponential size known in the literature, one can achieve polynomial size. An explicit example with linear size is also presented. Finally, we show that for covariant measurements exact programmability is feasible.

DOI: 10.1103/PhysRevLett.94.090401

PACS numbers: 03.65.Ta, 03.67.-a

A concrete problem in quantum information processing [1] is to experimentally achieve any theoretically designed quantum measurement, and possibly be able to change the measured observable dynamically on the fly, as it would be needed, e.g., when trying to eavesdrop quantum-encrypted information. For such a purpose, a programmable measurement apparatus, which could be tuned to perform any desired measurement, would be an invaluable resource. However, as first noticed in Refs. [2,3], with a finite-dimensional ancilla, exact universal programmability of measurement is impossible, as a consequence of the no-go theorem for programmability of unitary transformations [4]. One can still achieve measurement programmability probabilistically, or even deterministically, though within some accuracy. Since different measurements within some classes can be mapped to each other via quantum channels (e.g., all observables are connected to each other by a unitary transformation), then the problem of measurement programmability clearly carries relations with that of channels programming [5]. Because of the correspondence between channels and bipartite states [6,7], quantum channels can be easily programmed probabilistically by using a teleportation scheme with the channel stored in the state of the shared bipartite resource [1]. This and other methods can then be used to program channels and measurements probabilistically [8,9], and recently optical implementations for polarization-encoded qubits have been proposed [10]. However, one should emphasize that, different from the case of programmability of quantum channels or operations—where a series of many of them in sequence amplifies errors—in the case of a quantum measurement, being the last quantum processing stage it is certainly more efficient to consider deterministic programmability at the expense of small bounded systematic errors, rather than achieving the exact measurement probabilistically. In Ref. [3] a measurement for qubits that can be approximately programmed to achieve any observable has been presented, which needs an ancilla with dimension growing exponentially versus the accuracy  $\varepsilon^{-1}$ . In this Letter we show that actually it is possible to design the programmable measurement much more efficiently, with dimen-

sion  $d$  of the ancilla growing only polynomially versus the accuracy  $\varepsilon^{-1}$ . We also provide a specific example for such efficient programmability for qubits, with dimension  $d$  linear in  $\varepsilon^{-1}$ . We also show that in some cases, e.g., when the programmability is restricted to covariant measurements, even exact deterministic programmability is possible.

In quantum mechanics the statistics of a generic measurement apparatus is described by a positive operator-valued measure (POVM). For simplicity in this Letter we consider the case of discrete sampling space  $\mathcal{X}$  of possible outcomes for the measurement, in which case a POVM  $\mathbf{P}$  is just a set of positive operators  $P_i \geq 0$  on the Hilbert space  $\mathcal{H}$  of the system, each corresponding to an elementary outcome  $i \in \mathcal{X}$ , and satisfying the normalization condition  $\sum_{i \in \mathcal{X}} P_i = I$ . In the following to simplify notation, we write simply  $\sum_i$  for  $\sum_{i \in \mathcal{X}}$ , and do not specify the sampling space  $\mathcal{X}$  anymore.

The POVM of a measuring apparatus gives the probability distribution of the outcomes for each input state  $\rho$  via the Born rule

$$p(i|\rho) \doteq \text{Tr}[\rho P_i]. \quad (1)$$

The usual case of the customary observable corresponds to  $\{P_i\}$  being the orthogonal projectors on the eigenspaces of a self-adjoint operator.

We now want to build up a detector which is "programmable," namely, such that we can tune its POVM by changing the state of an ancillary unit in the detector. Clearly, the most general programmable detector would have its ancilla interacting with the measured system via a unitary transformation  $U$ , which is then followed by an observable  $\{E_i\}$  jointly measured on the system and ancilla,  $U$  and  $\{E_i\}$  being fixed constituents of the apparatus (due to the Naimark theorem, considering a POVM in place of the observable  $\{E_i\}$  would simply be equivalent to having a higher dimensional ancilla and another fixed operator  $U$ ). If such a detector could be programmed to achieve a given POVM  $\mathbf{P} = \{P_i\}$  ideally, this means that there would exist a "program state"  $\sigma_{\mathbf{P}}$  of the ancilla such that the following identity holds:

$$p(i|\rho) = \text{Tr}[\rho P_i] = \text{Tr}[U(\rho \otimes \sigma_{\mathbf{P}})U^\dagger E_i], \quad \forall i, \quad \forall \rho. \quad (2)$$

Clearly, the unitary interaction can be included in the definition itself of the joint observable  $\{E_i\}$  by defining  $F_i \doteq U^\dagger E_i U$  for all  $i \in \mathcal{X}$ . By taking the partial trace in Eq. (2) over the ancilla and using the polarization identity [Eq. (2) holds for all states], one obtains

$$P_i = \text{Tr}_A[(I \otimes \sigma_{\mathbf{P}})F_i]. \quad (3)$$

Therefore, a programmable detector is completely specified by the joint POVM  $\mathbf{F} = \{F_i\}$  on the system plus ancilla; therefore in the following the detector is identified with  $\mathbf{F}$ . Notice that from Eq. (3) it follows that the convex set of states  $\mathcal{A}$  of the ancilla is in correspondence via the map  $\mathcal{M}_{\mathbf{F}}(\sigma) \doteq [(I \otimes \sigma)\mathbf{F}]$  with a convex subset  $\mathcal{P}_{\mathbf{F}}$  of the convex set  $\mathcal{P}_n$  of the system POVM's with the same number  $n \leq \infty$  of outcomes of  $\mathbf{F}$  ( $\mathcal{P}_{\mathbf{F}}$  is the convex set of POVM's that can be achieved with the fixed programmable detector  $\mathbf{F}$ ). Therefore, if the POVM  $\mathbf{P}$  is extremal (e.g., it is an observable [11]), and if there exists a state of the ancilla  $\sigma_{\mathbf{P}}$  that satisfies identity (2), then there also exists a pure state  $\sigma_{\mathbf{P}}$  satisfying the same identity: we use this observation in the following.

The problem of measurement programmability can be restated in mathematical terms by asking whether  $\mathcal{P}_{\mathbf{F}} \doteq \mathcal{M}_{\mathbf{F}}(\mathcal{A}) \equiv \mathcal{P}_n$  for some  $\mathbf{F}$ . In words: there exists a POVM  $\mathbf{F}$  such that by varying the state  $\sigma \in \mathcal{A}$  in Eq. (3) one obtains the full convex set of POVM's  $\mathcal{P}_n$  on  $\mathcal{H}$ ? We will show now that this is impossible, and we will use for this purpose a generalization of the argument of Ref. [3].

Let us consider a two level system  $\mathcal{H} \simeq \mathbb{C}^2$ , and suppose that we want to program at least all possible observables by means of a single programmable detector with finite-dimensional ancilla. Each observable on  $\mathcal{H} \simeq \mathbb{C}^2$  is simply a two-outcome orthogonal POVM  $\{P, I - P\}$ , with  $P = |\psi\rangle\langle\psi|$  and  $I - P = |\psi^\perp\rangle\langle\psi^\perp|$ ,  $|\psi\rangle$  being a unit vector in  $\mathcal{H}$ . In other words, the observables on  $\mathcal{H} \simeq \mathbb{C}^2$  are in correspondence with the pure states of the system. As previously noticed, without loss of generality we can take the program state  $\sigma_\psi$  as pure, and we denote it as  $\sigma_\psi = |\Phi(\psi)\rangle\langle\Phi(\psi)|$ . The POVM  $\mathbf{F}$  of the programmable detector would then be a two-value POVM—so-called *effect*— $\{F, I - F\}$ , and exact programmability for all observables would imply

$$|\psi\rangle\langle\psi| = \text{Tr}_A\{[I \otimes |\Phi(\psi)\rangle\langle\Phi(\psi)|]F\}, \quad (4)$$

namely,

$$\begin{aligned} \langle\psi| \otimes \langle\Phi(\psi)|]F[|\psi\rangle \otimes |\Phi(\psi)\rangle] &= 1, \\ \langle\psi| \otimes \langle\Phi(\psi)|]F[|\psi^\perp\rangle \otimes |\Phi(\psi)\rangle] &= 0, \\ = \langle\psi^\perp| \otimes \langle\Phi(\psi)|]F[|\psi^\perp\rangle \otimes |\Phi(\psi)\rangle] &= 0. \end{aligned} \quad (5)$$

Equations (5) imply that for all  $\psi \in \mathcal{H}$  one has

$$F|\psi\rangle|\Phi(\psi)\rangle = |\psi\rangle|\Phi(\psi)\rangle, \quad F|\psi^\perp\rangle|\Phi(\psi)\rangle = 0, \quad (6)$$

namely, for all  $\psi \neq \psi' \in \mathcal{H}$  one has

$$\langle\psi^\perp| \langle\Phi(\psi)|F|\psi'\rangle|\Phi(\psi')\rangle = \langle\psi^\perp|\psi'\rangle\langle\Phi(\psi)|\Phi(\psi')\rangle = 0, \quad (7)$$

which implies that  $\langle\Phi(\psi)|\Phi(\psi')\rangle = 0$ . This means that the ancillary system must have a continuum of orthonormal states, which cannot happen in a separable Hilbert space. Suppose now that a perfect programmable detector can be devised for observables of higher dimensional systems. Then one could single out a bidimensional subspace in which observables can be perfectly programmed, which is absurd as we just proved. This implies that exact deterministic universal programmability of observables is impossible.

One can then ask if it is possible to approximate all possible observables  $\mathbf{P}$  within some accuracy  $\varepsilon^{-1}$  using a single finite-dimensional ancilla: here we answer this question with a general lower bound for the optimal accuracy  $\varepsilon^{-1}$  achievable by a programmable detector versus the dimension of its ancilla.

The first step is to give a precise definition of the accuracy of the approximation. For this purpose, we consider the usual distance between two probability distributions  $\{p_i\}$  and  $\{q_i\}$

$$\delta(\mathbf{p}, \mathbf{q}) = \sum_i |p_i - q_i|, \quad (8)$$

and define accordingly the distance between two POVM's as the distance between their respective probabilities, maximized over all possible states, namely,

$$\delta(\mathbf{P}, \mathbf{Q}) = \max_\rho \sum_i |\text{Tr}[\rho(P_i - Q_i)]|. \quad (9)$$

Then, we say that the POVM  $\mathbf{P}$  approximates within  $\varepsilon$  the POVM  $\mathbf{Q}$  if their distance is less than  $\varepsilon$ , namely,

$$\delta(\mathbf{P}, \mathbf{Q}) \leq \varepsilon. \quad (10)$$

We then rate the performance of a programmable detector  $\mathbf{F}$  saying that it achieves accuracy  $\varepsilon^{-1}$ —shortly, it is  *$\varepsilon$  programmable*—when

$$\max_{\mathbf{P} \in \mathcal{P}_n} \min_{\mathbf{Q} \in \mathcal{P}_{\mathbf{F}}} \delta(\mathbf{P}, \mathbf{Q}) \leq \varepsilon. \quad (11)$$

We now derive an upper bound for the function  $d = f(\varepsilon)$  that gives the minimal needed dimension of the ancilla to achieve accuracy  $\varepsilon^{-1}$ . We can restrict attention to programmability of observables only, namely, with  $n = \dim(\mathcal{H})$  and  $\mathcal{P}_n$  is substituted with the set of observables  $\mathcal{O}_n$  in Eq. (11). In fact, the generalization to nonorthogonal POVM's is just equivalent to program observables in the larger dimension  $n^2$ . Clearly the function  $d = f(\varepsilon^{-1})$  must be increasing, since the higher the accuracy  $\varepsilon^{-1}$  is, the larger the minimal dimension  $d$  needed for the ancilla, namely, the “size” of the programmable detector.

The distance defined in Eq. (11) is hard to handle analytically; hence we bound it as follows:

$$\delta(\mathbf{P}, \mathbf{Q}) \leq \sum_i \|P_i - Q_i\| \leq \sum_i \|P_i - Q_i\|_2, \quad (12)$$

where  $\|A\|$  is the usual operator norm of  $A$ , and  $\|A\|_2 \doteq \sqrt{\text{Tr}[A^\dagger A]}$  is the Frobenius norm. Consider now a  $d$ -dimensional ancilla and a system-ancilla interaction  $U$  of the following *controlled-unitary* form:

$$U = \sum_{k=1}^d W_k \otimes |\phi_k\rangle\langle\phi_k|, \quad (13)$$

where  $\{\phi_k\}$  is an orthonormal complete set of vectors for the ancilla and  $W_k$  are generic unitary operators on  $\mathcal{H}$ . Consider then a POVM  $\mathbf{E} = U\mathbf{F}U^\dagger$  of the form

$$E_i = |\psi_i\rangle\langle\psi_i| \otimes I_A, \quad (14)$$

where  $I_A$  denotes the identity operator on the ancilla space, and  $\{\psi_k\}$  is a complete orthonormal set for the system. The observable to be approximated is then written as follows:

$$P_i = W^\dagger |\psi_i\rangle\langle\psi_i| W, \quad (15)$$

$W$  being a unitary operator on  $\mathcal{H}$ , and we scan all possible observables by varying  $W$ . For the program state of the ancilla we use one of the states  $\phi_k$ , which give the POVM's

$$Q_i = W_k^\dagger |\psi_i\rangle\langle\psi_i| W_k. \quad (16)$$

This special form simplifies the calculation of the bound in Eq. (12), which becomes

$$\begin{aligned} \delta(\mathbf{P}, \mathbf{Q}) &\leq \sum_i \sqrt{2(1 - |\langle\psi_i|W^\dagger W_k|\psi_i\rangle|^2)} \\ &\leq \sqrt{2} \sum_i \sqrt{2 - \langle\psi_i|(W^\dagger W_k - W_k^\dagger W)|\psi_i\rangle}, \end{aligned} \quad (17)$$

and using the Jensen's inequality for the square root function we have

$$\delta(\mathbf{P}, \mathbf{Q}) \leq \sqrt{2n} \|W - W_k\|_2. \quad (18)$$

Now we can always take  $d$  sufficiently large such that we can choose the  $d$  operators  $\{W_k\}$  in the unitary transformation  $U$  in Eq. (13) in such a way that for each given  $W$  there is always a unitary operator  $W_k$  in the set for which  $\sqrt{2n} \|W - W_k\|_2$  is bounded by  $\varepsilon$ . This guarantees that for the given observable  $\mathbf{P}$  corresponding to  $W$  there is a program state for the ancilla such that the POVM  $\mathbf{Q}$  achieved by the programmable detector is close to the desired  $\mathbf{P}$  less than  $\varepsilon$ . The set of all possible unitary operators  $W$  is a compact manifold of dimension  $h = n^2 - n$ . We now consider a covering of the manifold with balls of radius  $r = \frac{\varepsilon}{\sqrt{2n}}$  centered at the operators  $W_k$ . This guarantees that any  $W$  would be within a distance  $\frac{\varepsilon}{\sqrt{2n}}$  from an operator  $W_k$ , which in turns implies that the accuracy of the

programmable device is bounded by  $\varepsilon$  via Eq. (18). Using the volume  $V = \frac{\pi^{h/2} r^h}{\Gamma(\frac{h}{2}+1)}$  of the  $h$ -dimensional sphere of radius  $r$ , we obtain the number of balls needed for the covering (for sufficiently small  $\varepsilon$ ) corresponding to the upper bound for the minimal dimension of the ancilla

$$d \leq \kappa(n) \left(\frac{1}{\varepsilon}\right)^{n(n-1)}, \quad (19)$$

where  $\kappa(n)$  is a constant that depends on  $n$ . Equation (19) gives an upper bound for the dimension  $d$  which is polynomial versus the accuracy  $\varepsilon^{-1}$ .

For qubits, the observable has only two elements,  $P_0 = |\psi\rangle\langle\psi|$  and  $P_1 = |\psi_\perp\rangle\langle\psi_\perp| = I - P_0$ , and the distance in Eq. (9) can be evaluated analytically as follows:

$$\delta(\mathbf{P}, \mathbf{Q}) = \max_\rho 2|\text{Tr}[\rho(P_0 - Q_0)]|. \quad (20)$$

The best device known [3] for programming qubit observables has a dimension of the ancilla which grows exponentially versus  $\varepsilon^{-1}$ . The programmable detector uses  $N$  qubits in the state  $|\psi\rangle^{\otimes N}$ , and the POVM  $\mathbf{F} = \{F_0, I - F_0\}$  is given by

$$F_0 = Z_+^{(N+1)}, \quad (21)$$

with  $Z_+^{(N+1)}$  denoting the orthogonal projector over the totally symmetric Hilbert space  $(\mathcal{H}^{\otimes(N+1)})_+$ , where  $\mathcal{H} \simeq \mathbb{C}^2$ . With this choice one can easily evaluate the POVM programmed in the detector in Eq. (3), obtaining

$$\begin{aligned} Q_0 &= \text{Tr}_A[(I \otimes |\psi\rangle\langle\psi|^{\otimes N}) Z_+^{(N+1)}] \\ &= |\psi\rangle\langle\psi| + \frac{1}{N+1}(I - |\psi\rangle\langle\psi|). \end{aligned} \quad (22)$$

Then, upon substituting  $Q_0 - P_0 = \frac{1}{N+1}(I - |\psi\rangle\langle\psi|)$  in Eq. (20) one obtains  $\varepsilon \doteq \delta(\mathbf{P}, \mathbf{Q}) = \frac{2}{N+1}$ , corresponding to

$$d = \frac{1}{2} 4^{\varepsilon^{-1}}, \quad (23)$$

which must be compared with the polynomial growth in Eq. (19).

As regards now the programmability of all POVM's (i.e., including the nonorthogonal ones), notice that one just needs to be able to program only the extremal POVM's in  $\mathcal{P}_n$ , since their convex combinations correspond to mixing the program state or to randomly choosing among different detectors. Then, since their maximum number of outcomes is  $n^2$ , the extremal POVM's have Naimark's extension to observables in dimension  $n^2$ , when we are reduced to the case of programmability of observables in dimension  $n^2$ .

We now give a programmable detector for qubits that achieves an accuracy that is linear in  $d$ . For the ancilla we use a generic  $d$ -dimensional quantum system, and relabel the dimension in the angular momentum fashion  $d \doteq 2j + 1$ . The idea is now to design a programmable detector in which the unitary transformation corresponding to the observable  $\{P_i\}$  in Eq. (17) is programmed by covariantly

changing the program state of the ancilla. By labeling unitary transformations by a group element  $g \in \mathbb{S}\mathbb{U}(2)$ , we write the observable to be programmed as  $P_0 \doteq V_g |\frac{1}{2}\rangle\langle\frac{1}{2}| V_g^\dagger$  where  $\{V_g\} \equiv (\frac{1}{2})$  is a unitary irreducible representation of  $\mathbb{S}\mathbb{U}(2)$  with angular momentum  $\frac{1}{2}$ , whereas the program state is written as  $W_g \sigma W_g^\dagger$ , with  $\{W_g\} \equiv (j)$  a unitary irreducible representation of  $\mathbb{S}\mathbb{U}(2)$  on the ancilla space with angular momentum  $j$ . As already noticed, without loss of generality we can always choose the state  $\sigma$  as pure. We now show that a good choice for the program state is  $\sigma = |j, j\rangle\langle j, j|$ ,  $\{|j, m\rangle\}$  denoting an orthonormal basis of eigenstates of  $J_z$  in the irreducible representation with angular momentum  $j$ . The tensor representation  $\{V_g \otimes W_g\} \equiv \frac{1}{2} \otimes j$  can be decomposed into the direct sum of two irreducible representations  $\frac{1}{2} \otimes j = j_+ \oplus j_-$ , where  $j_\pm = j \pm \frac{1}{2}$ . For the POVM  $\mathbf{F}$  of the programmable detector we use  $F_0 = Z_+$  and  $F_1 = Z_-$ ,  $Z_\pm$  denoting the orthogonal projector on the invariant space for angular momentum  $j_\pm$

$$F_0 = \sum_{m=-j_+}^{j_+} |j_+, m\rangle\langle j_+, m|. \quad (24)$$

Using the invariance  $(V_g \otimes W_g) F_0 (V_g^\dagger \otimes W_g^\dagger) = F_0$ , we can write the programmed POVM as follows:

$$\begin{aligned} Q_0 &= \text{Tr}_A[(I \otimes W_g^\dagger |j, j\rangle\langle j, j| W_g) F_0] \\ &= V_g^\dagger \text{Tr}_A[(I \otimes |j, j\rangle\langle j, j|) F_0] V_g \\ &= V_g \left( \frac{1}{2} |\frac{1}{2}\rangle\langle\frac{1}{2}| + \frac{1}{2j+1} |\frac{1}{2}, -\frac{1}{2}\rangle\langle\frac{1}{2}, -\frac{1}{2}| \right) V_g^\dagger, \end{aligned} \quad (25)$$

where we used the only nonvanishing Clebsch-Gordan coefficients  $|\langle j_+, j_+ | \frac{1}{2}, \frac{1}{2} | j, j \rangle|^2 = 1$  and  $|\langle j_+, j_+ | \frac{1}{2}, -\frac{1}{2} | j, j \rangle|^2 = \frac{1}{2j+1}$ . Clearly,  $Q_0 - P_0 = \frac{1}{2j+1} V_g |\frac{1}{2}, -\frac{1}{2}\rangle\langle\frac{1}{2}, -\frac{1}{2}| V_g^\dagger$ , where according to Eq. (20) the accuracy is given by  $\delta(\mathbf{P}, \mathbf{Q}) = 2/d$ . The scaling of the dimension with the accuracy is then linear

$$d = 2\varepsilon^{-1}, \quad (26)$$

whereas the bound (19) is quadratic  $d \propto \varepsilon^{-2}$ . Sublinear growth of  $d$  versus  $\varepsilon^{-1}$  is not excluded in general, but is not possible for the present model.

We emphasize that the no-go theorem holds only for universal programmability. Indeed, if, for example, we restrict programmability to covariant POVM's, then exact deterministic programmability is possible. In fact, according to the Holevo theorem [12] a general group-covariant POVM density has the form  $P(dg) = V_g \nu V_g^\dagger \mu(dg)$ , with a  $\mu$  invariant measure on the group (for simplicity we restrict to a compact group and a trivial stability group: a more general analysis can be found in Refs. [13,14]). Then, it is easy to see that a necessary and sufficient condition in order to have  $P(dg)$  positive and normalized is that the operator  $\nu$  is positive and unit trace, namely, a state. The POVM can then be programmed exactly using an ancilla

with the same dimension as the system and with program state  $\nu^\tau$ , and using for the POVM  $\mathbf{F}$  the covariant Bell POVM  $\{|V_g\rangle\rangle\langle\langle V_g|\}$  as one can easily check that  $V_g \nu V_g^\dagger = \text{Tr}_A[(I \otimes \nu^\tau) |V_g\rangle\rangle\langle\langle V_g|]$  [we used the notation  $|V_g\rangle\rangle \doteq \sum_{mn} (\langle m | V_g | n \rangle) |m\rangle \otimes |n\rangle \in \mathcal{H}^{\otimes 2}$ , and  $\nu^\tau$  as the transposed of  $\nu$  with respect to the same basis used to define  $|V_g\rangle\rangle$ ].

In conclusion, we have shown how it is possible to achieve deterministically a programmable measurement with size polynomial versus the accuracy. For qubits one can program observables with size linear versus the accuracy, and for this we have provided an explicit example. Finally, we have noticed that for covariant measurements exact programmability is feasible. The actual minimal size of the programmable detector for a given accuracy is still an open problem.

This work has been cofounded by the EC under the program ATESIT (Contract No. IST-2000-29681) and the MIUR cofinanziamento 2003. P.P. acknowledges support from the INFN under Project No. PRA-2002-CLON. G.M.D. acknowledges partial support by the MURI program administered by the U.S. Army Research Office under Grant No. DAAD19-00-1-0177.

---

\*Also at Center for Photonic Communication and Computing, Department of Electrical and Computer Engineering, Northwestern University, Evanston, IL 60208, USA.

Electronic address: [dariano@unipv.it](mailto:dariano@unipv.it)

†Electronic address: [perinotti@fisicavolta.unipv.it](mailto:perinotti@fisicavolta.unipv.it)

- [1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
- [2] M. Dušek and V. Bužek, Phys. Rev. A **66**, 022112 (2002).
- [3] J. Fiurásek, M. Dušek, and R. Filip, Phys. Rev. Lett. **89**, 190401 (2002).
- [4] M. A. Nielsen and I. L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).
- [5] G. Vidal and J. I. Cirac, quant-ph/0012067.
- [6] M.-D. Choi, Linear Algebra Appl. **10**, 285 (1975).
- [7] G. M. D'Ariano, and P. Lo Presti, Phys. Rev. A **64**, 042308 (2001).
- [8] M. Hillery, V. Bužek, and M. Ziman, Phys. Rev. A **65**, 022301 (2002).
- [9] J. Fiurásek and M. Dušek, Phys. Rev. A **69**, 032302 (2004).
- [10] J. Soubusta, A. Černoč, J. Fiurásek, and M. Dušek, Phys. Rev. A **69**, 052321 (2004).
- [11] G. M. D'Ariano, P. Perinotti, and P. Lo Presti, quant-ph/0408115.
- [12] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, Series in Statistics and Probability (North-Holland, Amsterdam, New York, Oxford, 1982).
- [13] G. M. D'Ariano, J. Math. Phys. (N.Y.) **45**, 3620 (2004).
- [14] G. Chiribella and G. M. D'Ariano, J. Math. Phys. (N.Y.) **45**, 4435 (2004).