JOURNAL OF MATHEMATICAL PHYSICS VOLUME 45, NUMBER 9 SEPTEMBER 2004

Extremal covariant quantum operations and positive operator valued measures

Giacomo Mauro D'Ariano[a)]

QUIT Group, Istituto Nazionale di Fisica della Materia, Unità di Pavia, Dipartimento di Fisica "A. Volta," via Bassi 6, I-27100 Pavia, Italy and Department of Electrical and Computer Engineering, Northwestern University, Evanston, Illinois 60208

(Received 19 March 2004; accepted 4 June 2004; published 16 August 2004)

We consider the convex sets of QO's (quantum operations) and POVM's (positive operator valued measures) which are covariant under a general finite-dimensional unitary representation of a group. We derive necessary and sufficient conditions for extremality, and give general bounds for ranks of the extremal POVM's and QO's. Results are illustrated on the basis of simple examples. © *2004 American Institute of Physics.* [DOI: 10.1063/1.1777813]

I. INTRODUCTION

The need for miniaturization and the new quantum information technology[1] has recently motivated a search for new quantum devices with maximum control at the quantum level. Among the many problems posed by the new technology there is the need of engineering quantum devices which perform specific measurements[2–5] or particular state transformations—the so-called *quantum operations*[6–8]—which are optimized with respect to some given criterion. In most cases such optimal quantum measurements/operations are *covariant*[9] with respect to a group of physical transformations. For the case of a quantum measurement, "group-covariant" means that there is an action of the group on the probability space which maps events into events, in such a way that when the quantum system is transformed according to a group transformation, the probability of the given event becomes the probability of the transformed event. This situation is very natural, and occurs in most practical applications. (See Refs. 10 and 11.) For example, the heterodyne measurement[12,13] is covariant under the group of displacements of the complex field, which means that if we displace the state of radiation by an additional complex averaged field, then the output photocurrent will be displaced by the same complex quantity.

In quantum mechanics the probabilities for a given apparatus for all possible states are described by positive operator valued measures (POVM),[3] and we will say that the measurement is covariant when its POVM is covariant under a unitary group representation.[2,10] For quantum operations (QO), on the other hand, covariance means that the output of a group-transformed input state is simply the transformed output state—a situation again quite common in practice. Typically covariance means that the apparatus is required to work equally well on a full set of states which is invariant under a group of transformations. For instance, if one wants to engineer an eavesdropping apparatus for a BB84 cryptographic scheme[14,15] that clones equally well all equatorial qubits, then the optimal cloning operation must be covariant under the group $\mathbf{G}=\mathbb{Z}_4$ of $\pi/2$ rotations of the Bloch sphere around its polar axis, which is a subgroup of the group of all axial rotations $\mathbf{G}=\mathbb{U}(1)$.[16] Similarly, if one wants to engineer a QO which works equally well on all pure states, then the operation must be covariant under the full $\mathbb{SU}(d)$ group, where d is the dimension of the Hilbert space of the quantum system.

It is easy to see that all POVM's covariant under some group representation make a convex set, which describes the complete class of possible covariant apparatuses. The same obviously

[a)]Electronic mail: dariano@unipv.it; http://www.qubit.it holds for group-covariant QO's. Typically in most applications the optimization resorts to minimize a concave function on the convex set of covariant machines (in quantum estimation theory[3] actually such function is generally linear), whence the optimal machine will correspond to an extremal element of the convex set. For such purpose it is convenient to classify all extremal covariant POVM's and QO's, and this is precisely the subject of the present paper.

For finite dimensional Hilbert space, a characterization of all noncovariant extremal QO's was given in Ref. 17, whereas a characterization of all extremal POVM's can be found in Refs. 18 and 19 for discrete finite probability space. On the other hand, no classification of the extremal QO's or POVM's is available yet under a covariance constraint, since, as we will see, this constraint makes the classification problem much harder. Coincidentally, in many applications the optimal QO/POVM is restricted to be rank-one from the special form of the optimization function (this is the case, for example, of optimal phase estimation for pure states,[2,3,20] or of phase covariant optimal cloning of pure states[16]), and this has lead to a widespread belief that optimality is synonym of rank-one. However, as we will see in this paper, for sufficiently large dimension the extremal QO's/POVM's can easily have rank larger than one: this can actually happen for optimization with mixed input states, such as in the case of optimal phase estimation with phase-coherent mixed states.[21]

In this paper we provide a classification for finite dimensions of all extremal POVM's and QO's that are covariant under a general unitary group representation. We will generally consider continuous Lie groups, since then all results will also apply to the case of discrete groups as well, with just a little change of notation. We provide necessary and sufficient conditions for extremality, along with simple necessary conditions, which allow to "sieve" the extremal QO's/POVM's. From these conditions general bounds for the rank of the extremal QO's/POVM's easily follow as corollaries.

The paper is organized as follows. In Sec. II we briefly review the concept of POVM and that of covariant POVM based on the Holevo's theorem.[2] In Sec. III we recall the necessary concepts about QO's, including their operator form introduced in Ref. 22, which allows to easily classify the covariant QO's as non-negative operators in the commutant of a suitable representation of the group. Section IV is entirely devoted to some technical lemmas which will be used in the classification of both POVM's and QO's. Finally Secs. V and VI contains the classification theorem of extremal group covariant POVM's and QO's, respectively, with some simple explicit examples, in particular with application to phase-covariant estimation and phase-covariant optimal cloning.

II. POSITIVE OPERATOR VALUED MEASURES

In the following we will denote by $\boldsymbol{B}(\mathcal{K},\mathcal{H})$ the linear space of bounded operators from the Hilbert space $\mathcal{K}$ to the Hilbert space $\mathcal{H}$, and by $\boldsymbol{B}(\mathcal{H}) \doteq \boldsymbol{B}(\mathcal{H},\mathcal{H})$ the algebra of bounded operators on $\mathcal{H}$. By $\boldsymbol{T}_1(\mathcal{H})$ we will denote the trace-class operators on $\mathcal{H}$, and by $\boldsymbol{T}_1^+(\mathcal{H})$ its positive elements.

A general measurement is described by a probability space $\mathfrak{X}$ equipped with a sigma-algebra structure $\sigma(\mathfrak{X})$ of measurable subsets $B \in \sigma(\mathfrak{X})$. The measurement returns a random outcome $x \in \mathfrak{X}$. In quantum mechanics the probability that the outcome belongs to a subset $B \in \sigma(\mathfrak{X})$ depends on the state $\rho \in \boldsymbol{T}_1^+(\mathcal{H})$ of the system in a way which is distinctive of the measuring apparatus according to the Born rule

$$p(B) = \mathrm{Tr}[P(B)\rho], \tag{1}$$

where P is a function on $\sigma(\mathfrak{X})$ which is positive-operator valued in $\boldsymbol{B}(\mathcal{H})$, with the normalization condition

$$P(\mathfrak{X}) = I_{\mathcal{H}}. \tag{2}$$

Positivity of P is needed for positivity of probabilities for every state ρ, whereas Eq. (2) guarantees normalization of probabilities. In synthesis, P is a positive operator valued measure (POVM) on the probability space $\mathfrak{X}$. In a sense the POVM P represents our knowledge of the measuring apparatus from which we can infer information on the state ρ from probabilities. The linearity of the Born rule (1) in both arguments ρ and P is consistent with the intrinsically statistical nature of the measurement, in which our partial knowledge of both the system and the apparatus reflects in convex structures for both states and POVM's. This means that not only states, but also POVM's can be "mixed," namely there are POVM's that give probability distributions that are equivalent to choose randomly among different apparatuses.

Group covariant POVM's: Let us consider now the general scenario in which a group of physical transformations $\mathbf{G}$ can act on the probability space $\mathfrak{X}$. We will write gx for the action of the group element $g\in\mathbf{G}$ on the point $x\in\mathfrak{X}$, and gB for the action of g on a whole subset $B\subseteq\mathfrak{X}$. We will always consider the case in which $\mathbf{G}$ acts transitively on $\mathfrak{X}$, namely for any two points on $\mathfrak{X}$ there is always a group element which connects them. A consequence of transitivity is that $\mathfrak{X}$ can be always regarded as the homogeneous factor space $\mathfrak{X}=\mathbf{G}/\mathbf{G}_x$, $\mathbf{G}_x$ denoting the stability group of any point $x\in\mathfrak{X}$.

A POVM P on $\mathcal{H}$ for the probability space $\mathfrak{X}$ is covariant under the unitary representation $g\to U_g$ of the group $\mathbf{G}$ when for every set $B\in\sigma(\mathfrak{X})$ one has

$$U_g^\dagger P(B) U_g = P(g^{-1}B). \tag{3}$$

The following general theorem by Holevo[2] classifies all group-covariant POVM's.

Theorem 1 (Holevo): *For square-integrable representations, a POVM P on the probability space $\mathfrak{X}$ is covariant with respect to the unitary representation $g\to U_g$ on $\mathcal{H}$ of the group $\mathbf{G}$ of transformations of $\mathfrak{X}$ if and only if it admits a density of the form*

$$\mathrm{d}P_x = U_{g_x}^\dagger \Xi U_{g_x}\mathrm{d}x, \quad g_x\in\mathbf{G}:g_x x_0 = x, \tag{4}$$

where $\mathrm{d}x$ is an invariant measure on $\mathfrak{X}$, with $\Xi\geqslant 0$ in the commutant $\mathbf{G}'_{x_0}$ of the isotropy group $\mathbf{G}_{x_0}$ of x_0, satisfying the constraint

$$\int_{\mathbf{G}} \mathrm{d}g\, U_g^\dagger \Xi U_g = I_{\mathcal{H}}, \tag{5}$$

with $\mathrm{d}g$ invariant measure on $\mathbf{G}$.

In the case in which the POVM is designed to estimate the group element itself $g\in\mathbf{G}$ corresponding to an unknown transformation U_g, then the stability group is the identity, whence $\mathfrak{X}=\mathbf{G}$ and the POVM P is covariant if and only if it admits a density of the form

$$\mathrm{d}P_g = U_g^\dagger \Xi U_g\, \mathrm{d}g, \quad g\in\mathbf{G} \tag{6}$$

for any $\Xi\geqslant 0$ satisfying the constraint (5). The possible *seed* operators $\Xi\geqslant 0$ satisfying the constraint (5) form a convex set. In Sec. V we will classify all extremal elements Ξ of such convex set.

III. QUANTUM OPERATIONS

The mathematical structure that describes the most general state change in quantum mechanics—such as the evolution of an open system or the state change due to a measurement—is the *quantum operation* (QO) of Kraus.[1,6] Such abstract theoretical evolution has a precise physical counterpart in its implementations as a unitary interaction between the system undergoing the QO and a part of the apparatus—the so-called *ancilla*—which after the interaction is read by means of a conventional quantum measurement. We can consider generally different input and output Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$, respectively, allowing the treatment of very general quantum machines, e.g., of the kind of quantum optimal cloners.[22,23] For example, in the cloning from one to n copies one has input space $\mathcal{H}$ and output space $\mathcal{K}=\mathcal{H}^{\otimes n}$, or its symmetric version $\mathcal{K}=(\mathcal{H}^{\otimes n})_+$ for symmetric cloning. Within the present paper we will only consider finite-dimensional Hilbert spaces. In the Heisenberg picture the QO evolves observables, and will be denoted by a map $\mathcal{M}$ from $\boldsymbol{B}(\mathcal{K})$ to

$\boldsymbol{B}(\mathcal{H})$. In the Schrödinger picture the QO evolves states, and it is given by the dual map $\mathcal{M}^\tau:\boldsymbol{T}_1(\mathcal{H})\to\boldsymbol{T}_1(\mathcal{K})$, the dualism being determined by the equivalence of the two pictures in terms of the trace inner product, namely $\mathrm{Tr}[\mathcal{M}(X)\rho]=\mathrm{Tr}[\mathcal{M}^\tau(\rho)X]$ for all $\rho\in\boldsymbol{T}_1(\mathcal{H})$ and for all $X\in\boldsymbol{B}(\mathcal{K})$. The maps $\mathcal{M}$ and $\mathcal{M}^\tau$ are linear *completely positive* (CP), namely they preserve positivity of the input operator for any trivial extension $\mathcal{M}\otimes\mathcal{I}$ on a larger Hilbert space that includes any possible additional quantum system, $\mathcal{I}$ denoting the identity map on the additional system. In the Schrödinger picture the CP property physically means that the map $\mathcal{M}^\tau$ from $\boldsymbol{T}_1(\mathcal{H})$ to $\boldsymbol{T}_1(\mathcal{K})$ preserves positivity of any input state of the quantum system (with Hilbert space $\mathcal{H}$) entangled with any possible additional quantum system. The map $\mathcal{M}^\tau$ of a QO must also be trace-not-increasing, with the trace $\mathrm{Tr}[\mathcal{M}^\tau(\rho)]\leqslant 1$ representing the probability that the transformation occurs, and the input and output states being connected as follows:

$$\rho\mapsto\rho'=\frac{\mathcal{M}^\tau(\rho)}{\mathrm{Tr}[\mathcal{M}^\tau(\rho)]}. \tag{7}$$

By denoting with $I_\mathcal{H}$ the identity operator on the Hilbert space $\mathcal{H}$, we see that the trace-not-increasing condition along with positivity of the map are equivalent to the constraint

$$\mathcal{M}(I_\mathcal{K})=K\in\boldsymbol{B}(\mathcal{H}),\quad 0\leqslant K\leqslant I_\mathcal{H}. \tag{8}$$

For finite-dimensional Hilbert spaces it is convenient to represent the maps $\mathcal{M}$ from $\boldsymbol{B}(\mathcal{K})$ to $\boldsymbol{B}(\mathcal{H})$ as operators $R_\mathcal{M}$ on $\mathcal{K}\otimes\mathcal{H}$ using the following one-to-one correspondence:

$$R_\mathcal{M}=\mathcal{M}^\tau\otimes\mathcal{I}(|I\rangle\langle I|),\quad \mathcal{M}^\tau(\rho)=\mathrm{Tr}_\mathcal{H}[(I_\mathcal{K}\otimes\rho^\tau)R_\mathcal{M}], \tag{9}$$

where $|I\rangle=\Sigma_n|n\rangle\otimes|n\rangle$ is a fixed vector in $\mathcal{H}\otimes\mathcal{H}$, $\{|n\rangle\otimes|m\rangle\}$ denotes an orthonormal basis for $\mathcal{H}\otimes\mathcal{H}$, and the transposition τ for operators is defined with respect to the orthonormal basis $|n\rangle\langle m|$ for $\boldsymbol{B}(\mathcal{H})$ taken as real. One can easily check the correspondence (9), and injectivity follows from linearity. In addition, the operator $R_\mathcal{M}$ is non-negative if and only if the map $\mathcal{M}$ is CP, and the constraint (8) in terms of the operator K rewrites as follows:

$$\mathrm{Tr}_\mathcal{K}[R_\mathcal{M}]=K,\quad 0\leqslant K\leqslant I_\mathcal{H}. \tag{10}$$

The positive operators $R_\mathcal{M}$ satisfying the constraint (10) make a convex set, which is the operator counterpart of the convex set of the corresponding QO's $\mathcal{M}$.

Group covariant CP-maps: We call the map $\mathcal{M}$ from $\boldsymbol{B}(\mathcal{K})$ to $\boldsymbol{B}(\mathcal{H})$ $\mathbf{G}$-covariant, when

$$\mathcal{M}(V_g^\dagger XV_g)=U_g^\dagger\mathcal{M}(X)U_g,\quad \forall\, g\in\mathbf{G}, \tag{11}$$

$\{U_g\}$ and $\{V_g\}$ denoting unitary representations of $\mathbf{G}$ over the input and output spaces $\mathcal{H}$ and $\mathcal{K}$, respectively. The Schrödinger picture version of identity (11) is

$$\mathcal{M}^\tau(U_g\rho U_g^\dagger)=V_g\mathcal{M}^\tau(\rho)V_g^\dagger,\quad \forall\, g\in\mathbf{G}, \tag{12}$$

where $\mathcal{M}^\tau$ goes from $\boldsymbol{T}_1(\mathcal{H})$ to $\boldsymbol{T}_1(\mathcal{K})$.

The operator form $R_\mathcal{M}$ for maps $\mathcal{M}$ simplifies the classification of QO's that are covariant under a group $\mathbf{G}$, resorting to the Wedderburn's decomposition of the commutant of the representation. It is easy to show that the map $\mathcal{M}$ is $\mathbf{G}$-covariant [i.e., it satisfies Eq. (11)] if and only if its corresponding operator $R_\mathcal{M}$ is invariant under the representation $V_g\otimes U_g^*$.[22] In fact, from Eq. (9) using invariance of partial trace under cyclic permutation of operators acting only on the traced space one has

$$0=\mathcal{M}^\tau(\rho)-V_g^\dagger\mathcal{M}^\tau(U_g\rho U_g^\dagger)V_g=\mathrm{Tr}_\mathcal{H}\{(I_\mathcal{K}\otimes\rho^\tau)[R_\mathcal{M}-(V_g^\dagger\otimes U_g{}^\tau)R_\mathcal{M}(V_g\otimes U_g^*)]\}, \tag{13}$$

and, since Eq. (9) is a one-to-one correspondence between maps and operators, one concludes that

$$[R_{\mathcal{M}}, V_g \otimes U_g^*] = 0, \quad \forall g \in \mathbf{G}. \tag{14}$$

Therefore, the problem of classifying covariant CP-maps resorts to that of classifying positive elements of the commutant of the representation $V_g \otimes U_g^*$ on $\mathcal{K} \otimes \mathcal{H}$. By labeling with k the generic equivalence class of the representation, with multiplicity m_k, the Wedderburn's decomposition of the representation space is written as follows:[24]

$$\mathcal{K} \otimes \mathcal{H} = \bigoplus_k (\mathcal{H}_k \otimes \mathbb{C}^{m_k}). \tag{15}$$

Then, since $R_{\mathcal{M}}$ must be a positive operator in the commutant of the representation it must have the general form

$$R_{\mathcal{M}} = \oplus_k (I_{\mathcal{H}_k} \otimes w_k^\dagger w_k) = W^\dagger W, \quad W \doteq \oplus_k (I_{\mathcal{H}_k} \otimes w_k), \tag{16}$$

where w_k is any operator on $\mathbb{C}^{m_k}$, i.e., a $m_k \times m_k$ matrix. Therefore, the classification of covariant trace-not-increasing QO's with $\mathcal{M}(I_{\mathcal{K}}) = \mathcal{K} \leqslant I_{\mathcal{H}}$ is equivalent to classify the operators $R_{\mathcal{M}}$ of the form (16) with the constraint

$$\sum_k \mathrm{Tr}_{\mathcal{K}}[(I_{\mathcal{H}_k} \otimes w_k^\dagger w_k)] = K \leqslant I_{\mathcal{H}}. \tag{17}$$

The constraint (17) is generally quite involved, due to the subspace mismatch between the tensor product $\mathcal{K} \otimes \mathcal{H}$ and the Wedderburn's decomposition: its simplification will be the main task of Sec. VI.

IV. TECHNICAL LEMMAS

This section will be entirely devoted to technical lemmas, which will be used for the classification of both extremal covariant POVM's and QO's. The lemmas connect conditions on the vanishing of partial traces with linear spannings.

In the following we will make use of the following simple fact for any linear space $\mathcal{L}$ and a subspace $\mathcal{S} \subseteq \mathcal{L}$: if the only vector of $\mathcal{L}$ that is orthogonal to the whole subspace $\mathcal{S}$ is the null vector, then one has $\mathcal{S} = \mathcal{L}$. Moreover, since orthogonality to a set s of vector implies orthogonality to its linear span $\mathsf{Span}(\mathsf{s})$, then the previous assertion holds also for subsets $\mathsf{s} \subseteq \mathcal{L}$ (not necessarily subspace), namely if the only vector orthogonal to the subset s is the null vector, than one has $\mathcal{L} \equiv \mathsf{Span}(\mathsf{s})$. From now we will also make use of the following natural notation

$$X(\boldsymbol{B}(\mathcal{A}) \otimes I_B) Y^\dagger \doteq \mathsf{Span}\{X(A \otimes I_B) Y^\dagger, A \in \boldsymbol{B}(\mathcal{A})\}, \tag{18}$$

for X, Y any operators with domain $\mathcal{A} \otimes \mathcal{B}$.

Lemma 1: *Let $B \in \boldsymbol{B}(\mathcal{B}_2 \otimes \mathcal{B}_1, \mathcal{A})$, $\mathcal{A}$ and $\mathcal{B}_{1,2}$ denoting arbitrary finite-dimensional Hilbert spaces. Then, the injectivity of the linear CP map $\mathcal{W}(A) = \mathrm{Tr}_{B_1}[B^\dagger A B]$ on $\boldsymbol{B}(\mathcal{A})$ is equivalent to the spanning condition*

$$\boldsymbol{B}(\mathcal{A}) = B(\boldsymbol{B}(\mathcal{B}_2) \otimes I_{B_1}) B^\dagger. \tag{19}$$

Proof: The injectivity of the map $\mathcal{W}(A) = \mathrm{Tr}_{B_1}[B^\dagger A B]$ on $\boldsymbol{B}(\mathcal{A})$ means that

$$\forall A \in \boldsymbol{B}(\mathcal{A}), \quad \mathrm{Tr}_{B_1}[B^\dagger A B] = 0 \Rightarrow A = 0. \tag{20}$$

The condition $\mathrm{Tr}_{\mathcal{B}_1}[B^\dagger A B] = 0$ is equivalent to $\mathrm{Tr}[C\ \mathrm{Tr}_{B_1}[B^\dagger A B]] = 0\ \forall C \in \boldsymbol{B}(\mathcal{B}_2)$. Therefore, since one has

$$\mathrm{Tr}[C\ \mathrm{Tr}_{\mathcal{B}_1}[B^\dagger A B]] = \mathrm{Tr}[(C \otimes I_{B_1}) B^\dagger A B] = \mathrm{Tr}[B(C \otimes I_{B_1}) B^\dagger A] \tag{21}$$

condition (20) is then equivalent to

$$\forall A \in \boldsymbol{B}(\mathcal{A}), \quad \mathrm{Tr}[B(\boldsymbol{B}(\mathcal{B}_2) \otimes I_{B_1})B^\dagger A] = 0 \Rightarrow A = 0, \tag{22}$$

where we used notation (18). Equation (22) says that the only operator $A \in \boldsymbol{B}(\mathcal{A})$ orthogonal to the operator space $B(\boldsymbol{B}(\mathcal{B}_2)\otimes I_{B_1})B^\dagger \subseteq \boldsymbol{B}(\mathcal{A})$ is the null operator, which means that $B(\boldsymbol{B}(\mathcal{B}_2)\otimes I_{B_1})B^\dagger$ is actually the full linear space $\boldsymbol{B}(\mathcal{A})$, namely condition (22) is equivalent to condition (19). ■

The above theorem leads immediately to the following corollaries.

Corollary 1: A necessary condition for injectivity of the map $\mathcal{W}(A) = \mathrm{Tr}_{B_1}[B^\dagger AB]$ *on* $\boldsymbol{B}(\mathcal{A})$ *is*

$$\dim(\mathcal{A}) \leqslant \min\{\dim(\mathcal{B}_2), \mathrm{rank}(B)\}. \tag{23}$$

Corollary 2: The injectivity of the map $\mathcal{W}(A) = \mathrm{Tr}_{B_1}[B^\dagger AB]$ *on* $\boldsymbol{B}(\mathcal{A})$ *is equivalent to the existence of a linear injective map* $\mathcal{V}$ *from* $\boldsymbol{B}(\mathcal{A})$ *to* $\boldsymbol{B}(\mathcal{B})$ *such that*

$$\forall A \in \boldsymbol{B}(\mathcal{A}), \quad B(\mathcal{V}(A) \otimes I_{\mathcal{B}_1})B^\dagger = A. \tag{24}$$

The relation between the maps $\mathcal{W}$ *and* $\mathcal{V}$ *is given by*

$$\mathcal{W}(A) = \mathrm{Tr}_{\mathcal{B}_1}[B^\dagger B(\mathcal{V}(A) \otimes I_{\mathcal{B}_1})B^\dagger B]. \tag{25}$$

Proof: The spanning condition (19)—equivalent to the injectivity of the map $\mathcal{W}(A) = \mathrm{Tr}_{\mathcal{B}_1}[B^\dagger AB]$ on $\boldsymbol{B}(\mathcal{A})$—guarantees that for each $A \in \boldsymbol{B}(\mathcal{A})$ there exists an element, say V_A, of $\boldsymbol{B}(\mathcal{B})$ such that $B(V_A \otimes I_{\mathcal{B}_1})B^\dagger = A$. Consider now an orthonormal basis A_j for $\boldsymbol{B}(\mathcal{A})$, and denote by V_j any element of $\boldsymbol{B}(\mathcal{B})$ such that $B(V_j \otimes I_{\mathcal{B}_1})B^\dagger = A_j$. It is clear that the $\{V_j\}$ can be chosen as linearly independent. Now, for every element $A \in \boldsymbol{B}(\mathcal{A})$ define $\mathcal{V}(A) = \Sigma_j \mathrm{Tr}[A_j^\dagger A]V_j$. This map is clearly linear and injective. The map $\mathcal{V}(A)$ corresponds to a nonorthogonal change of basis (from $\{A_j\}$ to $\{V_j\}$) which compensates the nonorthogonal change of basis $B(V_j \otimes I_{\mathcal{B}_1})B^\dagger = A_j$. Equation (25) follows by substituting Eq. (24) into the map $\mathcal{W}$. ■

We have also the additional lemma.

Lemma 2: As in Lemma 1, *the injectivity of the map* $\mathcal{W}(A) = \mathrm{Tr}_{\mathcal{B}_1}[B^\dagger AB]$ *on* $\boldsymbol{B}(\mathcal{A})$ *is equivalent to the linear independence of the set of operators* $\{W_i^\dagger W_j\}$, *where* $W_i \in \boldsymbol{B}(\mathcal{B}_1, \mathcal{B}_2)$ *are defined from the singular value decomposition* $B = \Sigma_i |V_i\rangle\langle W_i|$ *through the identity* $|W_i\rangle = (W_i \otimes I_{\mathcal{B}_1})|I\rangle$, $|I\rangle \in \mathcal{B}_1^{\otimes 2}$ *denoting the fixed vector* $|I\rangle = \Sigma_l |l\rangle \otimes |l\rangle$, *for* $\{|l\rangle \otimes |m\rangle\}$ *arbitrary orthonormal basis of* $\mathcal{B}_1^{\otimes 2}$.

Proof: First, notice that the identity $|X\rangle = (X \otimes I_{\mathcal{B}_1})|I\rangle$ sets a bijection between vectors $|X\rangle \in \mathcal{B}_2 \otimes \mathcal{B}_1$ and operators $X \in \boldsymbol{B}(\mathcal{B}_1, \mathcal{B}_2)$. Then, using the singular value decomposition $B = \Sigma_i |V_i\rangle\langle W_i|$, with $|V_i\rangle \in \mathcal{A}$ and $|W_i\rangle \in \mathcal{B}_2 \otimes \mathcal{B}_1$, the partial trace in Eq. (20) becomes

$$\mathrm{Tr}_{\mathcal{B}_1}[B^\dagger AB] = \sum_{ij} \langle V_i|A|V_j\rangle \mathrm{Tr}_{\mathcal{B}_1}[|W_i\rangle\langle W_j|] = \sum_{ij} \langle V_i|A|V_j\rangle W_i^\tau W_j^*, \tag{26}$$

where τ denotes the transposition for which $(X \otimes I_{\mathcal{B}_1})|I\rangle = (I_{\mathcal{B}_1} \otimes X^\tau)|I\rangle$, and $*$ denotes complex conjugation, i.e., $X^\dagger = (X^\tau)^*$. By taking the complex conjugate of the last equation and introducing the matrix $A_{ij} \doteq \langle V_i|A|V_j\rangle^* \in \mathsf{M}_N(\mathbb{C})$ where $N = \mathrm{rank}(B)$ (N^2 is the cardinality of the set $\{W_i^\dagger W_j\}$), the statement (20) is equivalent to

$$\{A_{ij}\} \in \mathsf{M}_N(\mathbb{C}), \quad \sum_{ij} A_{ij} W_i^\dagger W_j = 0 \Rightarrow A_{ij} = 0, \quad \forall\, i,j, \tag{27}$$

namely the operators $\{W_i^\dagger W_j\}$ are linearly independent. ■

In the following we will need the following generalization of Lemma 1.

Lemma 3: Let $B \in \boldsymbol{B}(\oplus_k(\mathcal{B}_2^{(k)} \otimes \mathcal{B}_1^{(k)}), \mathcal{A})$, *and denote by* P_k *the orthogonal projector over* $\mathcal{B}_2^{(k)} \otimes \mathcal{B}_1^{(k)}$, $\mathcal{A}$ *and* $\mathcal{B}_{1,2}^{(k)}$ *being arbitrary finite-dimensional Hilbert spaces.*

The following implication,

$$A \in \boldsymbol{B}(\mathcal{A}), \quad \mathrm{Tr}_{\mathcal{B}_2^{(k)}}[P_k B^\dagger ABP_k] = 0\ \forall\, k \Rightarrow A = 0, \tag{28}$$

is equivalent to

$$\boldsymbol{B}(\mathcal{A}) = \mathrm{Span}\{B[\oplus_k(\boldsymbol{B}(\mathcal{B}_2^{(k)}) \otimes I_{\mathcal{B}_1^{(k)}})]B^\dagger\}, \tag{29}$$

and necessary conditions are

$$\dim(\mathcal{A})^2 \leqslant \sum_k \dim(\mathcal{B}_2^{(k)})^2, \tag{30}$$

$$\dim(\mathcal{A}) \leqslant \mathrm{rank}(B). \tag{31}$$

Proof: The condition $\mathrm{Tr}_{\mathcal{B}_1^{(k)}}[P_k B^\dagger A B P_k]=0\ \forall k$ is equivalent to say that for any $C_k \in \boldsymbol{B}(\mathcal{B}_2^{(k)})$ one has $\mathrm{Tr}[P_k C_k \mathrm{Tr}_{\mathcal{B}_1^{(k)}}[P_k B^\dagger A B P_k]]=0\ \forall k$. Since one has

$$\mathrm{Tr}[C_k \mathrm{Tr}_{\mathcal{B}_1^{(k)}}[P_k B^\dagger A B P_k]] = \mathrm{Tr}[(C_k \otimes I_{\mathcal{B}_1^{(k)}})P_k B^\dagger A B P_k] = \mathrm{Tr}[BP_k(C_k \otimes I_{\mathcal{B}_1^{(k)}})P_k B^\dagger A], \tag{32}$$

and, therefore, condition (28) is equivalent to

$$A \in \boldsymbol{B}(\mathcal{A}), \quad \mathrm{Tr}[BP_k(\boldsymbol{B}(\mathcal{B}_2^{(k)}) \otimes I_{\mathcal{B}_1^{(k)}})P_k B^\dagger A] = 0\ \forall\, k \Rightarrow A = 0. \tag{33}$$

The last condition says that the only operator in $\boldsymbol{B}(\mathcal{A})$ which is orthogonal to the set $BP_k(\boldsymbol{B}(\mathcal{B}_2^{(k)})\otimes I_{\mathcal{B}_1^{(k)}})P_k B^\dagger\ \forall k$ is the null operator, or, in other words that the set spans the full operator space $\boldsymbol{B}(\mathcal{A})$, namely Eq. (29). The necessary conditions then follow trivially. ■

We are now ready to classify the extremal group covariant POVM's and QO's in the following sections. In order to classify extremal elements of convex sets, we will use the method of perturbations. We will call a non-null operator B a *perturbation* for an operator A in a convex set if both $A \pm tB$ are still in the convex set for some (sufficiently small) $t > 0$. Then, clearly A is not extremal in the convex set if and only if it has a perturbation.

V. EXTREMAL COVARIANT POVM'S

We have seen that the covariant POVM for the estimation of a group element g of an unknown unitary transformation U_g is of the general form

$$\mathrm{d}P_g = \mathrm{d}g\ U_g^\dagger \Xi U_g^\dagger, \tag{34}$$

with probability space $\mathfrak{X} = \mathbf{G}$, and with

$$\int_{\mathbf{G}} \mathrm{d}_g\ U_g^\dagger \Xi U_g = I_{\mathcal{H}}. \tag{35}$$

The Wedderburn's decomposition (15) of the representation space here rewrites as follows:

$$\mathcal{H} = \bigoplus_k (\mathcal{H}_k \otimes \mathbb{C}^{m_k}), \tag{36}$$

where we remind that k labels the equivalence class of irreducible components, and m_k denotes its multiplicity. The integral in the normalization condition (35) belongs to the commutant of the representation, whence it can be rewritten as follows:

$$\int_{\mathbf{G}} \mathrm{d}g\ U_g^\dagger \Xi U_g = \bigoplus_k d_{\mathcal{H}_k}^{-1}[I_{\mathcal{H}_k} \otimes \mathrm{Tr}_{\mathcal{H}_k}(P_k \Xi P_k)] = I_{\mathcal{H}}, \tag{37}$$

P_k denoting the orthogonal projector on the subspace $\mathcal{H}_k \otimes \mathbb{C}^{m_k}$. Equation (37) follows from the simple fact that for an irreducible representation on the space say $\mathcal{L}$, one has $\int_{\mathbf{G}} \mathrm{d}g\ U_g^\dagger Z U_g = d_{\mathcal{L}}^{-1}\ \mathrm{Tr}[Z] I_{\mathcal{L}}$ for measure $\mathrm{d}g$ normalized to unit on $\mathbf{G}$. Equation (37) allows to split the constraint (35) into the following set of constraints:

$$\mathrm{Tr}_{\mathcal{H}_k}(P_k \Xi P_k) = d_{\mathcal{H}_k} I_{m_k}, \quad \forall\, k, \tag{38}$$

where by I_{m_k} we denote the identity matrix over $\mathbb{C}^{m_k}$. We then conclude that the classification of extremal **G**-covariant POVM's is equivalent to find the extremal Ξ within the convex set of operators $\Xi \geqslant 0$ satisfying the constraints (38). For such purpose we have the following theorem.

Theorem 2: Let Ξ be an element of the convex set of positive operators on $\mathcal{H}$ satisfying the constraints

$$\mathrm{Tr}_{\mathcal{H}_k}(P_k \Xi P_k) = d_{\mathcal{H}_k} I_{m_k}, \quad \forall\, k \in \mathsf{S}, \tag{39}$$

where S denotes the set of equivalence classes of irreducible components in the representation. Write Ξ in the form $\Xi = X^\dagger A X$ with $A \geqslant 0$, choosing $\mathsf{Rng}(X) = \mathsf{Supp}(A) \doteq \mathsf{Ker}(A)^\perp$. Then

(1) *Θ is a perturbation of Ξ if and only if Θ is Hermitian, with $\mathrm{Tr}_{\mathcal{H}_k}(P_k \Theta P_k) = 0\ \forall k \in \mathrm{S}$, and $\Theta = X^\dagger B X$ for some nonzero Hermitian B with $\mathsf{Supp}(B) \subseteq \mathsf{Supp}(A)$.*
(2) *For the specific choice of the form of A* as *$A = \oplus_k A_k$, with $A_k \in B(\mathcal{H}_k \otimes \mathbb{C}^{m_k})$, one has $B = \oplus_k B_k$, $B_k \in \boldsymbol{B}(\mathcal{H}_k \otimes \mathbb{C}^{m_k})$ and $\mathsf{Supp}(B_k) \subseteq \mathsf{Supp}(A_k)$, $\forall k \in \mathsf{S}$;*
(3) *$\Xi = X^\dagger X$ is extremal if and only if*

$$\boldsymbol{B}(\mathsf{Rng}(X)) = \mathsf{Span}\{X[\oplus_k (I_{\mathcal{H}^{(k)}} \otimes \boldsymbol{B}(\mathbb{C}^{m_k}))]X^\dagger\}. \tag{40}$$

Proof:

(1) Let Θ Hermitian, with $\mathrm{Tr}_{\mathcal{H}_k}(P_k \Theta P_k) = 0$, and $\Theta = X^\dagger B X$ for some nonzero Hermitian $B \in \boldsymbol{B}(\mathcal{H})$ and with $\mathsf{Supp}(B) \subseteq \mathsf{Supp}(A)$. Then for $\mathrm{rank}(B) > 0$ Θ is necessarily nonzero, and since $A \geqslant 0$, both constraints $A \pm tB \geqslant 0$ and $\mathrm{Tr}_{\mathcal{H}_k}(P_k(\Xi \pm t\Theta)P_k) = d_{\mathcal{H}_k} I_{m_k}\, \forall k$ are satisfied for some $t > 0$, whence Θ is a perturbation for Ξ. Conversely, suppose $\Theta \in \boldsymbol{B}(\mathcal{H})$ is a perturbation for Ξ. Since we must have $\Xi \pm t\Theta \geqslant 0$ and $Tr_{\mathcal{H}_k}[P_k(\Xi \pm t\Theta)P_k] = d_{\mathcal{H}_k} I_{m_k}$ for some $t > 0$, then Θ is Hermitian with $\mathrm{Tr}_{\mathcal{H}_k}(P_k \Theta P_k) = 0\ \forall k \in \mathsf{S}$. Moreover, if we write Ξ in the form $\Xi = X^\dagger A X$ with nonnegative $A \in \boldsymbol{B}(\mathcal{H})$, and $\mathsf{Rng}(X) = \mathsf{Supp}(A)$, then also Θ can be written in the same form $\Theta = X^\dagger B X$ for some nonzero Hermitian $B \in \boldsymbol{B}(\mathcal{H})$ and $\mathrm{Tr}_{\mathcal{H}_k}[P_k(\Xi \pm t\Theta)P_k] = d_{\mathcal{H}_k} I_{m_k}$. In fact, if X is not invertible, it can be always completed to an invertible operator $Z = X + Y$ by adding an operator Y with $\mathsf{Rng}(Y) = \mathsf{Ker}(A)$, and one can equivalently write $\Xi = Z^\dagger A Z$. Now we can write also the perturbation operator in the form $\Theta = Z^\dagger B Z$. However, since $A \pm tB \geqslant 0$ for some t, then necessarily B must have $\mathsf{Supp}(B) \subseteq \mathsf{Supp}(A) = \mathsf{Rng}(X)$, whence $Z^\dagger B Z = X^\dagger B X$.
(2) First it is obvious that a choice of the form $A = \oplus_k A_k$, with $A_k \in \boldsymbol{B}(\mathcal{H}_k \otimes \mathbb{C}^{m_k})$ is always possible. Then, in order to have $A \pm tB \geqslant 0$ for some $t > 0$, one must have $B = \oplus_k B_k$, each B_k Hermitian, with $\mathsf{Supp}(B_k) \subseteq \mathsf{Supp}(A_k)$, $\forall k \in \mathsf{S}$.
(3) Since $\mathsf{Supp}(A) \subseteq \mathsf{Rng}(X)$ and $A \geqslant 0$, we can always merge $\sqrt{A}$ into X by substituting $X \to \sqrt{A} X$. Then, since Ξ is not extremal iff it has a perturbation, by part (1) one sees that Ξ is extremal iff for Hermitian $B \in \boldsymbol{B}(\mathcal{H})$ with $\mathsf{Supp}(B) \subseteq \mathsf{Rng}(X)$, one has

$$\mathrm{Tr}_{\mathcal{H}_k}(P_k X^\dagger B X P_k) = 0\ \forall\, k \in \mathsf{S} \quad \Rightarrow \quad B = 0, \tag{41}$$

whence via Cartesian decomposition of B we have the equivalent statement

$$B \in \boldsymbol{B}(\mathsf{Rng}(X)), \quad \mathrm{Tr}_{\mathcal{H}_k}(P_k X^\dagger B X P_k) = 0\ \forall\, k \in \mathsf{S} \quad \Rightarrow \quad B = 0. \tag{42}$$

Then, by Lemma 3 this is equivalent to condition (40). ■

Corollary 3: A necessary condition for extremality of the seed Ξ of a group covariant representation as in Theorem 2 is

$$\mathrm{rank}(\Xi)^2 \leqslant \sum_k m_k^2. \tag{43}$$

Proof: Equation (43) is a trivial consequence of the necessary condition (40). ■

Corollary 4: Every rank-one POVM is extremal.

Proof: For $\mathrm{rank}(X)=1$ the iff condition (40) is trivially satisfied. ■

Theorem 3: *For* S *containing only a single equivalence class, say* h, *with multiplicity* $m_h \geqslant 1$, *the extremality of a covariant POVM on the Hilbert space* $\mathcal{H}=\mathcal{H}_h\otimes\mathbb{C}^{m_h}$ *is equivalent to the linear independence of the set of operators* $\{W_i^\dagger W_j\}$, *where* $W_i\in\boldsymbol{B}(\mathbb{C}^{m_h},\mathcal{H}_h)$ *are defined from the spectral decomposition* $\Xi=\Sigma_i|W_i\rangle\langle W_i|$ *of the seed* Ξ *of the POVM through the identity* $|W_i\rangle=(W_i\otimes I_{m_h})|I\rangle$, $|I\rangle\in(\mathbb{C}^{m_h})^{\otimes 2}$ *denoting the fixed vector* $|i\rangle=\Sigma_l|l\rangle\otimes|l\rangle$, *for* $\{|l\rangle\otimes|m\rangle\}$ *arbitrary orthonormal basis of* $(\mathbb{C}^{m_h})^{\otimes 2}$. *Extremal POVM's with any rank* $\mathrm{rank}(\Xi)\leqslant m_h$ *are admissible.*

Proof: For S containing a single equivalence class h with multiplicity $m_h\geqslant 1$ the seed Ξ of the POVM must satisfy the single constraint

$$\mathrm{Tr}_{\mathcal{H}_h}(\Xi)=d_{\mathcal{H}_h}I_{m_h}. \tag{44}$$

Now, write Ξ in the form $\Xi=X^\dagger AX$ with $X\in\boldsymbol{B}(\mathcal{H}_h\otimes\mathbb{C}^{m_h},\mathcal{A})$, and $\mathsf{Rng}(X)=\mathsf{Supp}(A)$, A being a Hilbert space such that $\mathsf{Supp}(A)\subseteq\mathcal{A}\subseteq\mathcal{H}_h\otimes\mathbb{C}^{m_h}$, and which can be chosen as $\mathcal{A}\simeq\mathsf{Rng}(X)$. Then, according to Theorem 2 Θ is a perturbation for Ξ iff it is of the form $\Theta=X^\dagger BX$, with B Hermitian, $\mathsf{Supp}(B)\subseteq\mathsf{Supp}(A)$, and $\mathrm{Tr}_{\mathcal{H}_h}(X^\dagger BX)=0$. This means that the extremality of Ξ is equivalent to the injectivity of the map $\mathcal{W}(B)=\mathrm{Tr}_{\mathcal{H}_h}(X^\dagger BX)$ over the set of Hermitian operators B with $\mathsf{Supp}(B)\subseteq\mathsf{Supp}(A)$, which is equivalent to injectivity of the same map on $\boldsymbol{B}(\mathsf{Rng}(X))$. We are thus in the situation of Lemma 2, with $\mathcal{A}=\mathsf{Rng}(X)$, $\mathcal{B}_1=\mathbb{C}^{m_h}$ and $\mathcal{B}_2=\mathcal{H}_h$. Therefore, by writing the singular value decomposition of $X=\Sigma_i|V_i\rangle\langle W_i|$, with $\mathsf{Span}\{|V_i\rangle\}=\mathsf{Rng}(X)=\mathsf{Supp}(A)$ the injectivity of the map $\mathcal{W}(B)=\mathrm{Tr}_{\mathcal{H}_h}[X^\dagger BX]$ on $\boldsymbol{B}(\mathsf{Rng}(\mathcal{X}))$ is equivalent to the linear independence of the set of operators $\{W_i^\dagger W_j\}$, where $W_i\in\boldsymbol{B}(\mathbb{C}^{m_h},\mathcal{H}_h)$ are defined through the identity $|W_i\rangle=(W_i\otimes I_{m_h})|I_i\rangle$, $|I\rangle\in(\mathbb{C}^{m_h})^{\otimes 2}$ denoting the fixed vector $|I\rangle=\Sigma_l|l\rangle\otimes|l\rangle$, with $\{|l\rangle\otimes|m\rangle\}$ arbitrary orthonormal basis of $(\mathbb{C}^{m_h})^{\otimes 2}$. Now, the maximum rank of the POVM is given by the maximum number of operators W_i such that the set of operators $\{W_i^\dagger W_j\}$ in $\boldsymbol{B}(\mathbb{C}^{m_h})$ is linearly independent. Since we can have at most m_h^2 linearly independent operators in $\boldsymbol{B}(\mathbb{C}^{m_h})$, the maximum cardinality of the set $\{W_i\}$ is m_h. ■

Corollary 5: A POVM which is covariant under an irreducible representation is extremal: *If and only if iff it is rank one*.

Proof: For S containing a single equivalence class h with multiplicity $m_h=1$ the iff condition (40) rewrites

$$\boldsymbol{B}(\mathsf{Rng}(X))=\mathsf{Span}\{X(I_{\mathcal{H}^{(h)}}\otimes\mathbb{C}^1)X^\dagger\}=\mathsf{Span}\{XX^\dagger\}, \tag{45}$$

which is satisfied iff $\mathrm{rank}(X)=1$. As an alternative proof, the present corollary corresponds to the situation of Theorem 3 for multiplicity $m_h=1$. ■

A. Example

Consider a POVM on $\mathcal{H}$ with $\dim(\mathcal{H})=d$ covariant under $\mathbf{G}=\mathbb{U}(1)$, with

$$U_\phi=\exp(i\phi N),\quad N=\sum_{n=0}^{d-1}n|n\rangle\langle n|. \tag{46}$$

Here we have d one-dimensional irreducible representations with characters $\chi_k(\phi)=\exp(ik\phi)$, $k=0,\ldots,d-1$, namely they are all inequivalent, whence with unit multiplicity. Therefore, the necessary condition (43) bounds the rank of the POVM as follows:

$$\mathrm{rank}(\Xi)^2\leqslant\dim(\mathcal{H}), \tag{47}$$

and in order to have $\mathrm{rank}(\Xi)=2$ one must have $\dim(\mathcal{H})\geqslant 4$. According to Theorem 2 the extremal POVM's have seed of the form $\Xi=X^\dagger X$ satisfying the identity

$$\boldsymbol{B}(\mathsf{Rng}(X)) = \mathsf{Span}\{|X_k\rangle\langle X_k|:0 \leqslant k \leqslant \dim(\mathcal{H})\}, \tag{48}$$

where $|X_k\rangle = X|k\rangle$, $\{|k\rangle\}$ denoting any orthonormal basis for $\mathcal{H}$. Notice that in the present example the operator Ξ corresponds to a so-called *correlation matrix*, namely a positive matrix with all ones on the diagonal. This follows from the constraint (38), which in our case is simply $\langle k|\Xi|k\rangle = 1, \forall k$. Therefore, the present classification of extremal POVM's coincides with the classification of extremal correlation matrices given in Ref. 25.

B. Example

Consider a POVM for n qubits on the Hilbert space $\mathcal{H}=(\mathbb{C}^2)^{\otimes n}$ covariant under the tensor representation $U_\phi^{\otimes n}$ of $\mathbf{G}=\mathbb{U}(1)$, with

$$U_\phi = \exp(i\phi|1\rangle\langle 1|), \tag{49}$$

where $\{|0\rangle,|1\rangle\}$ is a orthonormal basis for $\mathbb{C}^2$. Here we have $n+1$ one-dimensional irreducible representations with characters $\chi_k(\phi)=\exp(ik\phi)$, $k=0,\ldots,n$, and with multiplicity $m_k=\binom{n}{k}$. An orthonormal basis of each subspace $\mathbb{C}^{m_k}$ of $\mathcal{H}=\oplus_k \mathbb{C}^{m_k}$ is given by

$$\{|j\rangle_k\} = \{P_j^{(n,k)}|\underbrace{00\cdots 0}_{n-k}\underbrace{11\cdots 1}_{k}\rangle\}, \tag{50}$$

where $P_j^{(n,k)}$ denotes the jth permutation of k qubits in the state $|1\rangle$ in the tensor product of n qubits in total, with all other qubits in the state $|0\rangle$. In the present example, the iff condition for extremality (40) requires that $\Xi = X^\dagger X$ satisfies the identity

$$\boldsymbol{B}(\mathsf{Rng}(X)) = \mathsf{Span}\{X|i\rangle_{kk}\langle j|X^\dagger, k \in \mathsf{S}, i,j=1,\ldots,m_k\}, \tag{51}$$

where now $\{|i\rangle_k\}$ denotes any orthonormal basis for $\mathbb{C}^{m_k}$. The necessary condition (43) bounds the rank of the POVM as follows:

$$\mathrm{rank}(\Xi)^2 \leqslant \sum_{k=0}^{n}\binom{n}{k}^2 = \binom{2n}{n}. \tag{52}$$

Here, in order to have $\mathrm{rank}(\Xi)\geqslant 2$ one needs $n\geqslant 2$ qubits. For $n=2$ according to the previous example, one necessarily must have at least two inequivalent classes, since each of the irreducible components has less than four dimensions (the same is true also for $n=3$). The previous example is also recovered by considering the special case in which $\mathsf{Rng}(X)\subseteq ((\mathbb{C}^2)^{\otimes n})_+$, i.e., containing only the subrepresentation of $U_\phi^{\otimes n}$ on the symmetric subspace $((\mathbb{C}^2)^{\otimes n})_+$, with multiplicity 1.

C. Example

Consider a POVM on $\mathcal{H}^{\otimes 2}$ which is covariant under the group representation $U_g\otimes I_{\mathcal{H}}$, where U_g is an irreducible representation of $\mathbf{G}$ on $\mathcal{H}$. Here, we trivially have a single equivalence class, say h, (corresponding to the irreducible representation U_g) with multiplicity $m_h=\dim(\mathcal{H})$, i.e., the Hilbert space $\mathcal{H}$ coincides with the multiplicity space $\mathcal{H}\simeq\mathbb{C}^{m_h}$. This is exactly the case considered in Theorem 3. Therefore, the extremality of the POVM is equivalent to the linear independence of the set of operators $\{W_i^\dagger W_j\}$, where $W_i\in\boldsymbol{B}(\mathcal{H})$ are defined from the spectral decomposition $\Xi = \Sigma_i |W_i\rangle\langle W_i|$ of the seed Ξ of the POVM through the identity $|W_i\rangle = (W_i\otimes I_{\mathcal{H}})|I\rangle$, as in Theorem 3. Therefore, we can have extremal POVM's with any $\mathrm{rank}(\Xi)\leqslant\dim(\mathcal{H})$. Notice that there cannot be more than a single maximally entangled vector $|W_i\rangle$ in the decomposition of Ξ, since, otherwise, at least two operators W_i would be proportional to unitary operators, and then the set $\{W_i^\dagger W_j\}$ would be necessarily linearly dependent (two products would be both proportional to the identity). The rank-one case with a single maximally entangled projector corresponds to a so-called *Bell POVM*.

VI. EXTREMAL COVARIANT QUANTUM OPERATIONS

In the following we will denote shortly by $\boldsymbol{A}_{\mathbf{G}}$ the operator algebra generated by the group representation $V_g\otimes U_g^*$, by $\boldsymbol{A}'_{\mathbf{G}}$ its commutant, and finally by $\boldsymbol{H}'_{\mathbf{G}}$ the Hermitian operators in the commutant. The following theorem classifies all extremal $\mathbf{G}$-covariant maps $\mathcal{M}$ in the convex set given by Eq. (17).

Theorem 4: *Let R be an element of the convex set of positive operators in the commutant $\boldsymbol{A}'_{\mathbf{G}}$ of the operator algebra $\boldsymbol{A}_{\mathbf{G}}$ generated by the group representation $V_g\otimes U_g^*$ on $\mathcal{K}\otimes\mathcal{H}$, i.e., of the form*

$$R=\oplus_k(I_{\mathcal{H}_k}\otimes w_k^\dagger w_k)=W^\dagger W,\quad W\doteq\oplus_k(I_{\mathcal{H}_k}\otimes w_k), \tag{53}$$

satisfying the constraint

$$\sum_k \mathrm{Tr}_{\mathcal{K}}[(I_{\mathcal{H}_k}\otimes w_k^\dagger w_k)]=K\leqslant I_{\mathcal{H}}, \tag{54}$$

where

$$\mathcal{H}\otimes\mathcal{K}=\bigoplus_k(\mathcal{H}_k\otimes\mathbb{C}^{m_k}) \tag{55}$$

is the Wedderburn's decomposition of the representation space, k labeling the equivalence class of representations, with multiplicity m_k. Denote by P_k the orthogonal projector over the space $\mathcal{H}_k\otimes\mathbb{C}^{m_k}$ of the equivalence class. Write R in the form $R=X^\dagger QX$ with $Q,X\in\boldsymbol{A}'_{\mathbf{G}}$ and $\mathsf{Rng}(X)=\mathsf{Supp}(Q)$. Then:

(1) *S is a perturbation of R if and only if $S\in\boldsymbol{H}'_{\mathbf{G}}$, with $\mathrm{Tr}_{\mathcal{K}}[S]=0$, and $S=X^\dagger OX$ for some nonzero $O\in\boldsymbol{H}'_{\mathbf{G}}$ with $\mathsf{Supp}(O)\subseteq\mathsf{Rng}(X)$. Specifically, writing $Q=\oplus_k(I_{\mathcal{H}_k}\otimes Q_k)$ and $X=\oplus_k(I_{\mathcal{H}_k}\otimes X_k)$, one has $O=\oplus_k(I_{\mathcal{H}_k}\otimes O_k)$ with $\mathsf{Supp}(O_k)\subseteq\mathsf{Rng}(X_k)$ $\forall k$.*

(2) *One can always write R in the form $R=X^\dagger X$, with $X\in\boldsymbol{A}'_{\mathbf{G}}$ of the form $X=\oplus_k(I_{\mathcal{H}_k}\otimes X_k)$. Denote by S the set of equivalence classes k for which $X_k\neq 0$. Then, a necessary and sufficient condition for extremality of $R=X^\dagger X$ with $\mathrm{Tr}_{\mathcal{K}}[R]=K$ is the injectivity of the map $\mathcal{T}(O)=\mathrm{Tr}_{\mathcal{K}}[X^\dagger OX]$ on $\boldsymbol{A}'_{\mathbf{G}}\cap\boldsymbol{B}(\mathsf{Rng}(X))$, namely*

$$O\in\boldsymbol{A}'_{\mathbf{G}}\cap\boldsymbol{B}(\mathsf{Rng}(X)),\quad \mathrm{Tr}_{\mathcal{K}}[X^\dagger OX]=0\Rightarrow O=0, \tag{56}$$

which is equivalent to

$$\oplus_{k\in\mathsf{S}}\boldsymbol{B}(\mathsf{Rng}(X_k))=\oplus_{k\in\mathsf{S}}X_k\mathrm{Tr}_{\mathcal{H}_k}[P_k(I_{\mathcal{K}}\otimes\boldsymbol{B}(\mathcal{H}))P_k]X_k^\dagger. \tag{57}$$

Proof:

(1) Let $S\in\boldsymbol{H}'_{\mathbf{G}}$, with $\mathrm{Tr}_{\mathcal{K}}[S]=0$, and $S=X^\dagger OX$ for some nonzero Hermitian O with $\mathsf{Supp}(O)\subseteq\mathsf{Supp}(Q)$. Then for $\mathrm{rank}(O)>0$ $S\in\boldsymbol{H}'_{\mathbf{G}}$ is necessarily nonzero, and since $\boldsymbol{H}'_{\mathbf{G}}\in Q\geqslant 0$, all constraints: $Q\pm tO\in\boldsymbol{H}'_{\mathbf{G}}$, $Q\pm tO\geqslant 0$, and $\mathrm{Tr}_{\mathcal{K}}[R\pm tS]=K$ are satisfied for some $t>0$, whence S is a perturbation for R. Conversely, suppose that $S\in\mathcal{K}\otimes\mathcal{H}$ is a perturbation for R. Since we must have $\boldsymbol{H}'_{\mathbf{G}}\ni R\pm tS\geqslant 0$ and $\mathrm{Tr}_{\mathcal{K}}[R\pm tS]=K$ for some $t>0$, then $S\in\boldsymbol{H}'_{\mathbf{G}}$ with $\mathrm{Tr}_{\mathcal{K}}[S]=0$. Moreover, if we write R in the form $R=X^\dagger QX$ with $\mathsf{Rng}(X)=\mathsf{Supp}(Q)$, then also S can be written in the form $S=X^\dagger OX$ for some nonzero Hermitian $O\in\boldsymbol{H}'_{\mathbf{G}}$. In fact, if X is not invertible, it can be always completed to an invertible operator $Z=X+Y$ by adding an operator $Y\in\boldsymbol{A}'_{\mathbf{G}}$ of the form $Y=\oplus_k(I_{\mathcal{H}_k}\otimes Y_k)$ with $\mathsf{Rng}(Y_k)=\mathsf{Ker}(Q_k)$ [where $Q=\oplus_k(I_{\mathcal{H}_k}\otimes Q_k)$], and one can equivalently write $R=Z^\dagger QZ$ with $Q\in\boldsymbol{H}'_{\mathbf{G}}$ and $Z\in\boldsymbol{A}'_{\mathbf{G}}$. Now we can write also the perturbation operator in the form $S=Z^\dagger OZ$. However, since for some t the operator $Q\pm tO\geqslant 0$ must belong to the commutant $\boldsymbol{A}'_{\mathbf{G}}$, then necessarily $O\in\boldsymbol{H}'_{\mathbf{G}}$ and $\mathsf{Supp}(O)\subseteq\mathsf{Supp}(Q)=\mathsf{Rng}(X)$, with $Z^\dagger OZ=X^\dagger OX$. Specifically, writing $Q=\oplus_k(I_{\mathcal{H}_k}\otimes Q_k)$, one has $O=\oplus_k(I_{\mathcal{H}_k}\otimes O_k)$ with $\mathsf{Supp}(O_k)\subseteq\mathsf{Supp}(Q_k)=\mathsf{Rng}(X_k)\,\forall k$.

(2) As in part (1) we can always take Q as the identity, and redefine $X\to\sqrt{Q}X$, since $Q\geqslant 0$, keeping X of the form $X=\oplus_k(I_{\mathcal{H}_k}\otimes X_k)$, since both operators in the product $\sqrt{Q}X$ belong to the algebra $\boldsymbol{A}'_{\mathbf{G}}$. From part (1) we then see that $R=X^\dagger X$ with $X\in\boldsymbol{A}'_{\mathbf{G}}$ is extremal if and only if

$$O\in\boldsymbol{H}'_{\mathbf{G}}\cap\boldsymbol{B}(\mathsf{Rng}(X)),\quad \mathrm{Tr}_{\mathcal{K}}[X^\dagger OX]=0\Rightarrow O=0, \tag{58}$$

and via Cartesian decomposition this is equivalent to

$$O\in\boldsymbol{A}'_{\mathbf{G}}\cap\boldsymbol{B}(\mathsf{Rng}(X)),\quad \mathrm{Tr}_{\mathcal{K}}[X^\dagger OX]=0\Rightarrow O=0. \tag{59}$$

Since $O\in\boldsymbol{A}'_{\mathbf{G}}\cap\boldsymbol{B}(\mathsf{Rng}(X))$ can be decomposed as $O=\oplus_k(I_{\mathcal{H}_k}\otimes O_k)$ with $O_k\in\boldsymbol{B}(\mathsf{Rng}(X_k))$ $\forall k\in\mathsf{S}$, then the statement (59) is equivalent to

$$\forall k\in\mathsf{S}\ O_k\in\boldsymbol{B}(\mathsf{Rng}(X_k)),$$

$$\sum_{k\in\mathsf{S}}\mathrm{Tr}_{\mathcal{K}}[(I_{\mathcal{H}_k}\otimes X_k)^\dagger(I_{\mathcal{H}_k}\otimes O_k)(I_{\mathcal{H}_k}\otimes X_k)]=0\Rightarrow O_k=0\ \forall\ k\in\mathsf{S}, \tag{60}$$

or else

$$\forall k\in\mathsf{S}\quad O_k\in\boldsymbol{B}(\mathsf{Rng}(X_k)),$$

$$\mathrm{Tr}_{\mathcal{K}}[\oplus_{k\in\mathsf{S}}(I_{\mathcal{H}_k}\otimes X_k)^\dagger(I_{\mathcal{H}_k}\otimes O_k)(I_{\mathcal{H}_k}\otimes X_k)]=0\Rightarrow O_k=0\ \forall\ k\in\mathsf{S}, \tag{61}$$

The vanishing of the partial trace can be written as the vanishing of the trace $\mathrm{Tr}[\oplus_{k\in\mathsf{S}}(I_{\mathcal{H}_k}\otimes X_k)^\dagger(I_{\mathcal{H}_k}\otimes O_k)(I_{\mathcal{H}_k}\otimes X_k)(I_{\mathcal{K}}\otimes C)]$ for any $C\in\boldsymbol{B}(\mathcal{H})$, namely the vanishing of $\mathrm{Tr}\{\oplus_{k\in\mathsf{S}}O_kX_k\,\mathrm{Tr}_{\mathcal{H}_k}[P_k(I_{\mathcal{K}}\otimes C)P_k]X_k^\dagger\}$ for any $C\in\boldsymbol{B}(\mathcal{H})$, and upon defining $S=\oplus_{k\in\mathsf{S}}O_k$, the statement (61) rewrites

$$S\in\oplus_{k\in\mathsf{S}}\boldsymbol{B}(\mathsf{Rng}(X_k)),\quad \mathrm{Tr}\{S\oplus_{k\in\mathsf{S}}X_k\,\mathrm{Tr}_{\mathcal{H}_k}[P_k(I_{\mathcal{K}}\otimes\boldsymbol{B}(\mathcal{H}))P_k]X_k^\dagger\}=0\Rightarrow S=0, \tag{62}$$

namely, since the only operator in the linear space $\oplus_{k\in\mathsf{S}}\boldsymbol{B}(\mathsf{Rng}(X_k))$ orthogonal to the subspace $\oplus_{k\in\mathsf{S}}X_k\,\mathrm{Tr}_{\mathcal{H}_k}[P_k(I_{\mathcal{K}}\otimes\boldsymbol{B}(\mathcal{H}))P_k]X_k^\dagger$ is the null operator, one has

$$\oplus_{k\in\mathsf{S}}\boldsymbol{B}(\mathsf{Rng}(X_k))=\oplus_{k\in\mathsf{S}}X_k\,\mathrm{Tr}_{\mathcal{H}_k}[P_k(I_{\mathcal{K}}\otimes\boldsymbol{B}(\mathcal{H}))P_k]X_k^\dagger. \tag{63}$$

■

Corollary 6: As in Theorem 4, a necessary condition for extremality is

$$\sum_{k\in\mathsf{S}}\mathrm{rank}(X_k)^2\leqslant\dim(\mathcal{H})^2. \tag{64}$$

Corollary 7: Any rank-one covariant QO is extremal.

Proof: For $\mathrm{rank}(X)=1$ the set S must contain only one equivalence class, and the iff condition (57) of Theorem 4 is then trivially satisfied. ■

Corollary 8: For an irreducible representation any extremal covariant QO must be rank-one.

Corollary 9 (Choi): In the noncovariant case, a QO $\mathcal{M}$ from $\mathbf{B}(\mathcal{K})$ to $\mathbf{B}(\mathcal{H})$ is extremal iff it can be written in the form $\mathcal{M}(O)=\Sigma_i\,W_i^\dagger OW_i$, with $W_i\in\boldsymbol{B}(\mathcal{H},\mathcal{K})$ and the set of operators $\{W_i^\dagger W_j\}$ linearly independent.

Proof: The noncovariant case corresponds to the trivial covariance group $\mathbf{G}=\mathbf{I}$, i.e., the group containing only the identity element. This corresponds to have just a single equivalence class, with multiplicity equal to $\dim(\mathcal{H}\otimes\mathcal{K})$. Then, as in the proof of point (2) of Theorem 4 the extremality of $R=X^\dagger X\in\boldsymbol{B}(\mathcal{H}\otimes\mathcal{K})$ is equivalent to the injectivity of the map $\mathcal{W}(A)=\mathrm{Tr}_{\mathcal{K}}[X^\dagger AX]$ on $\boldsymbol{B}(\mathsf{Rng}(X))$. According to Lemma 2, using the singular value decomposition $X=\Sigma_i\,|V_i\rangle\langle W_i|$, with $|V_i\rangle$ orthonormal basis for $\mathsf{Rng}(X)$ and $|W_i\rangle\in\mathcal{K}\otimes\mathcal{H}$, one has $\mathcal{M}(O)=\Sigma_i\,W_i^\dagger OW_i$ for $O\in\boldsymbol{B}(\mathcal{K})$, and $\mathcal{W}(A)=\Sigma_{ij}\,\langle V_i|A|V_j\rangle W_i^\tau W_j^*$ for $A\in\boldsymbol{B}(\mathsf{Rng}(X))$, and injectivity of $\mathcal{W}$ is equivalent to linear

TABLE I. Orthonormal bases for the supporting spaces $\mathcal{H}_k \otimes \mathbb{C}^{m_k} \equiv \mathbb{C}^{m_k}$ of the kth equivalence class of irreducible representations for 1 to 2 phase-covariant cloning. The orthonormal basis are chosen as subsets of an orthonormal basis for the tensor product $\mathcal{K}\otimes\mathcal{H}$.

k	$\lvert k_i\rangle \otimes \lvert h_j\rangle$
-1	$\lvert 001\rangle$
0	$\lvert 101\rangle, \lvert 011\rangle, \lvert 000\rangle$
1	$\lvert 100\rangle, \lvert 010\rangle, \lvert 111\rangle$
2	$\lvert 110\rangle$

independence of the set of operators $\{W_i^\dagger W_j\}$. ∎

Corollary 9 is the same as Choi theorem.[17] Notice that differently from the case of QO's, for POVM's the noncovariant case cannot be recovered as a special case of the covariant classification, since the group itself (or, more generally, the homogeneous factor space) coincides with the probability space $\mathfrak{X}$ of the POVM, whence trivializing $\mathbf{G}$ also trivializes $\mathfrak{X}$.

A. Example

Consider the phase-covariant cloning[16,22] for equatorial qubits from 1 to 2 copies. This corresponds to $\mathbf{G}=\mathbb{U}(1)$, with representations $U_\phi = e^{i\phi|1\rangle\langle 1|_0}$ and $V_\phi = e^{i\phi\Sigma_{s=1}^2 |1\rangle\langle 1|_s}$ where $s=0$ denotes the input qubit and $s=1,2$ the output ones. Here $\mathcal{H}=\mathbb{C}^2$ and $\mathcal{K}=\mathcal{H}^{\otimes 2}$. We first need to decompose the representation $V_\phi \otimes U_\phi^*$. This is made of one-dimensional representations, with characters $e^{ik\phi}$, with $k=-1,0,1,2$ and multiplicities $m_{-1}=1$, $m_0=3$, $m_1=3$, and $m_2=1$. The necessary condition (64) in the present case becomes $\Sigma_{k\in\mathsf{S}} \operatorname{rank}(X_k)^2 \leqslant \dim(\mathcal{H})^2=4$, which means that we can have either a single equivalence class with $\operatorname{rank}(X_k)\leqslant 2$, or two equivalence classes with $\operatorname{rank}(X_k)=1$ each. Orthonormal bases for the supporting spaces $\mathcal{H}_k \otimes \mathbb{C}^{m_k} \equiv \mathbb{C}^{m_k}$ of the kth equivalence class of irreducible representations are reported in Table I as subset of an orthonormal basis for the tensor product $\mathcal{K}\otimes\mathcal{H}$.

The operators $R=\Sigma_{k\in\mathsf{S}} R_k = \Sigma_{k\in\mathsf{S}}\Sigma_l \lvert\psi_l^{(k)}\rangle\langle\psi_l^{(k)}\rvert$ satisfying the necessary conditions and the trace-preserving condition are reported in Table II. It is easy to check that the case of $\operatorname{rank}(X_k)=2$, which would be possible only for $k=0$ or $k=1$, does not satisfy the iff condition (56). Therefore it is possible to have only rank-one operators X_k.

As a specific optimization problem, let us consider the maximization of the fidelity averaged over the two outputs

TABLE II. Cloning from 1 to 2 copies: classification of operators $R=\Sigma_{k\in\mathsf{S}} R_k = \Sigma_{k\in\mathsf{S}}\Sigma_l \lvert\psi_l^{(k)}\rangle\langle\psi_l^{(k)}\rvert$ satisfying the necessary condition.

$\mathsf{S}\doteq\{k\}$	$\{\lvert\psi_l^{(k)}\rangle\}$	$\{\lvert\psi_l^{(k')}\rangle\}$	
$\{-1,2\}$	$\lvert 001\rangle$	$\lvert 110\rangle$	
$\{0,1\}$	$a\lvert 000\rangle + b\lvert 011\rangle + c\lvert 101\rangle$	$a'\lvert 111\rangle + b'\lvert 100\rangle + c'\lvert 010\rangle$	$\lvert a\rvert^2+\lvert b'\rvert^2+\lvert c'\rvert^2=1$
			$\lvert a'\rvert^2+\lvert b\rvert^2+\lvert c\rvert^2=1$
$\{0,-1\}$	$\lvert 000\rangle + a\lvert 011\rangle + b\lvert 101\rangle$	$c\lvert 001\rangle$	$\lvert a\rvert^2+\lvert b\rvert^2+\lvert c\rvert^2=1$
$\{1,-1\}$	$a\lvert 100\rangle + b\lvert 010\rangle + c\lvert 111\rangle$	$d\lvert 001\rangle$	$\lvert a\rvert^2+\lvert b\rvert^2=1$
			$\lvert c\rvert^2+\lvert d\rvert^2=1$
$\{1,2\}$	$a\lvert 100\rangle + b\lvert 010\rangle + \lvert 111\rangle$	$d\lvert 110\rangle$	$\lvert a\rvert^2+\lvert b\rvert^2+\lvert d\rvert^2=1$
$\{0,2\}$	$a\lvert 000\rangle + b\lvert 011\rangle + c\lvert 101\rangle$	$d\lvert 110\rangle$	$\lvert a\rvert^2+\lvert d\rvert^2=1$
			$\lvert b\rvert^2+\lvert c\rvert^2=1$
$\{0\}$	$1/\sqrt{2}\lvert 101\rangle + 1/\sqrt{2}\lvert 011\rangle, \lvert 000\rangle$		
$\{1\}$	$1/\sqrt{2}\lvert 010\rangle + 1/\sqrt{2}\lvert 100\rangle, \lvert 111\rangle$		

TABLE III. Orthonormal bases for the supporting spaces $\mathcal{H}_k \otimes \mathbb{C}^{m_k} \equiv \mathbb{C}^{m_k}$ of the kth equivalence class of irreducible representations for 1 to 3 phase-covariant cloning. The orthonormal basis are chosen as subsets of an orthonormal basis for the tensor product $\mathcal{K} \otimes \mathcal{H}$.

k	$\lvert k_i\rangle \otimes \lvert h_j\rangle$
−1	$\lvert 0001\rangle$
0	$\lvert 1001\rangle, \lvert 0101\rangle, \lvert 0011\rangle, \lvert 0000\rangle$
1	$\lvert 1000\rangle, \lvert 0100\rangle, \lvert 0010\rangle, \lvert 1101\rangle, \lvert 1011\rangle, \lvert 0111\rangle$
2	$\lvert 1100\rangle, \lvert 1010\rangle, \lvert 0110\rangle, \lvert 1111\rangle$
3	$\lvert 1110\rangle$

$$F = \langle\psi| \tfrac{1}{2}\{\mathrm{Tr}_1[\mathcal{M}^{\tau}(|\psi\rangle\langle\psi|)] + \mathrm{Tr}_2[\mathcal{M}^{\tau}(|\psi\rangle\langle\psi|)]\}|\psi\rangle = \mathrm{Tr}\Big[\tfrac{1}{2}(I \otimes |\psi\rangle\langle\psi| + |\psi\rangle\langle\psi| \otimes I)\mathcal{M}^{\tau}(|\psi\rangle\langle\psi|)\Big] \tag{65}$$

and for equatorial qubits we can choose $|\psi\rangle = |+\rangle$, where $|\pm\rangle \doteq (1/\sqrt{2})(|0\rangle \pm |1\rangle)$. Then the fidelity rewrites as

$$F = \mathrm{Tr}[W R_{\mathcal{M}}], \tag{66}$$

$$W = |+\rangle\langle+|^{\otimes 3} + \tfrac{1}{2}(|-\rangle\langle-| \otimes |+\rangle\langle+| + |+\rangle\langle+| \otimes |-\rangle\langle-|) \otimes |+\rangle\langle+|. \tag{67}$$

One can see that W is invariant for permutations over the output copies, and, by construction, also all vectors in Table II have the same symmetry. Due to the special form of the fidelity, the optimal map [satisfying $\mathcal{M}(I_{\mathcal{K}}) = I_{\mathcal{H}}$] is obtained for $\mathsf{S} = \{0,1\}$ with corresponding rank-two operator $R_{\mathcal{M}}$ given by

$$R_{\mathcal{M}} = |\psi^{(0)}\rangle\langle\psi^{(0)}| + |\psi^{(1)}\rangle\langle\psi^{(1)}|,$$

$$|\psi^{(0)}\rangle - = \frac{1}{\sqrt{2}}\left(|000\rangle + \frac{1}{\sqrt{2}}|011\rangle + \frac{1}{\sqrt{2}}|101\rangle\right),$$

$$|\psi^{(1)}\rangle - = \frac{1}{\sqrt{2}}\left(|111\rangle + \frac{1}{\sqrt{2}}|100\rangle + \frac{1}{\sqrt{2}}|010\rangle\right), \tag{68}$$

B. Example

Consider the phase-covariant cloning[16,22] for equatorial qubits from 1 to 3 copies. This correspond to $\mathbf{G} = \mathbb{U}(1)$, with representations $U_\phi = e^{i\phi|1\rangle\langle 1|_0}$ and $V_\phi = e^{i\phi\Sigma_{s=1}^{3}|1\rangle\langle 1|_k}$ where $s=0$ denotes the input qubit and $s=1,2,3$ the output ones. Here $\mathcal{H} = \mathbb{C}^2$ and $\mathcal{K} = \mathcal{H}^{\otimes 3}$. We first need to decompose the representation $V_\phi \otimes U_\phi^*$. This is made of one-dimensional representations, with characters $e^{ik\phi}$, with $k = -1,0,1,2,3$ and multiplicities $m_{-1} = 1$, $m_0 = 4$, $m_1 = 6$, $m_2 = 4$, and $m_3 = 1$. Orthonormal bases for the supporting spaces $\mathcal{H}_k \otimes \mathbb{C}^{m_k} \equiv \mathbb{C}^{m_k}$ of the kth equivalence class of irreducible representations are reported in Table III as subset of an orthonormal basis for the tensor product $\mathcal{K} \otimes \mathcal{H}$. Again, since $\dim(\mathcal{H}) = 2$, the necessary condition (64) says that we can have only one equivalence class k with $\mathrm{rank}(X_k) \leqslant 2$, or two equivalence classes both with $\mathrm{rank}(X_k) = 1$. In Ref. 22 it is shown that the map which optimizes the averaged equatorial fidelity is actually given by the rank-one map for $\mathsf{S} = \{1\}$ with corresponding operator $R_{\mathcal{M}}$ given by

$$R_{\mathcal{M}} = |\psi^{(1)}\rangle\langle\psi^{(1)}|,$$

$$|\psi^{(1)}\rangle=\frac{1}{\sqrt{3}}(|1000\rangle+|0100\rangle+|0010\rangle+|1101\rangle+|1011\rangle+|0111\rangle). \tag{69}$$

Notice that, as a consequence of the specific symmetric form of the chosen fidelity criterion, the cloning maps of the examples in Secs. VI A and VI B are both symmetrical, namely the output Hilbert space is indeed restricted to the symmetric tensor space $(\mathcal{H}^{\otimes n})_+$. Clearly, with the same method also nonsymmetric types of cloning can be analyzed well.

C. Example

Consider a generic covariant QO with $\mathcal{K}\simeq\mathcal{H}$, $V_g=U_g$, and $\mathbf{G}=\mathrm{SU}(d)$, where $d=\dim(\mathcal{H})$. In this case the representation $U_g\otimes U_g^*$ has two irreducible components, one which is one dimensional, corresponding to the invariant vector $|I\rangle\in\mathcal{H}^{\otimes 2}$, and one on the orthogonal complement, and the two components will be denoted by $k=0$ and $k=1$, respectively. Since both the irreducible components of the representation have unit multiplicity, the operator $R=X^\dagger X$ must have $X=\sum_{k\in\mathsf{S}} c_kP_k$, $c_k\in\mathbb{C}$, P_k denoting the orthogonal projector on the invariant space of the irreducible component k, and the necessary condition (64) is trivially satisfied. On the other hand, one can see that the iff condition (56) is satisfied for the irreducible representations $\mathsf{S}=\{0\}$ and $\mathsf{S}=\{1\}$, whereas for the reducible one $\mathsf{S}=\{0,1\}$ the map $\mathcal{T}(O)=\mathrm{Tr}_{\mathcal{K}}[X^\dagger OX]$ is never injective on $\boldsymbol{A}'_{\mathbf{G}}\cap\boldsymbol{B}(\mathsf{Rng}(X))$ [one has $\mathrm{Tr}_{\mathcal{K}}[X^\dagger OX]=(1/d)[|c_0|^2a_0+(d^2-1)|c_1|^2a_1]I_{\mathcal{H}}$ for $O=a_0P_0+a_1P_1$, $a_0,a_1\in\mathbb{C}$]. Therefore, the only trace-preserving optimal maps are those corresponding to the operators $R=|I\rangle\langle I|$ and $R=[d/(d^2-1)](I^{\otimes 2}-(1/d)|I\rangle\langle I|)$, corresponding to the trivial map $\mathcal{M}=\mathcal{J}$ and to the so-called isotropic depolarizing channel $\mathcal{M}(O)=[d/(d^2-1)]\mathrm{Tr}[O]I_{\mathcal{H}}-[1/(d^2-1)]\rho$. Finally, notice that in the present example the optimal covariant maps are compatible only with (multiple of) the trace-preserving condition, since both partial traces $\mathrm{Tr}_{\mathcal{K}}[P_k]$ are proportional to the identity.

D. Example

We consider now the same problem as in the previous example, but now with $V_g=U_g^*$. In this case we need to consider the positive operators R which are invariant under $U_g^*\otimes U_g^*$. It will be easier to consider the representation $U_g\otimes U_g$ and then take the complex conjugate of R at the end. Now we have again two irreducible inequivalent components, say $k=\pm$ with invariant spaces $(\mathcal{H}^{\otimes 2})_\pm$, the symmetric and the antisymmetric spaces. As in the previous example, the general form of $R=X^\dagger X$ is $X=\sum_{k\in\mathsf{S}} c_kP_k$, $c_k\in\mathbb{C}$, and $P_\pm=\frac{1}{2}(I_{\mathcal{H}}^{\otimes 2}\pm E)$, where E is the swap operator on the tensor product. However, the map $\mathcal{T}(O)=\mathrm{Tr}_{\mathcal{K}}[X^\dagger OX]$ is injective on $\boldsymbol{A}'_{\mathbf{G}}\cap\boldsymbol{B}(\mathsf{Rng}(X))$ only for representations with a single irreducible component. One can see that $\mathrm{Tr}_{\mathcal{H}}[P_\pm]=\frac{1}{2}(d\pm 1)I_{\mathcal{H}}$, and only trace-preserving (or multiplying by a constant) QO's are compatible with the present covariance. In conclusion, the only extremal covariant operators are $R_\pm=(d\pm 1)^{-1}(I^{\otimes 2}\pm E)$, corresponding to the channels $\mathcal{M}_\pm(O)=(d\pm 1)^{-1}[\mathrm{Tr}(O)I_{\mathcal{H}}\pm O^\tau]$. The map $\mathcal{M}_+$ is the optimal transposition map of Ref. 26.

ACKNOWLEDGMENTS

The author is grateful to Koenraad Audenaert for having pointed attention to the work of Li and Tam which inspired the present work. The author is also very grateful to Giulio Chiribella for having pointed out an error in a preliminary version, and for a careful reading of the present paper. A substantial part of this work has been worked out during the *Benasque Session on Quantum Information and Communication 2003*. It has been sponsored by INFM through the project PRA-2002-CLON, and by EEC and MIUR through the cosponsored ATESIT project IST-2000-29681 and Cofinanziamento 2003. Partial support is also acknowledged from the MURI program administered by the Army Research Office under Grant No. DAAD19-00-1-0177.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[2] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, Series in Statistics and Probability (North-Holland, Amsterdam, 1982).
[3] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
[4] E. B. Davies, *Quantum Theory of Open Systems* (Academic, London, 1976).
[5] P. Busch, P. J. Lahti, and P. Mittelstaedt, *The Quantum Theory of Measurement*, Lecture Notes in Physics Vol. 2 (Springer, Berlin, 1991).
[6] K. Kraus, *States, Effects, and Operations* (Springer-Verlag, Berlin, 1983).
[7] E. B. Davies, *Quantum Theory of Open Systems* (Academic, London, 1976).
[8] W. F. Stinespring, Proc. Am. Math. Soc. **6**, 211 (1955).
[9] E. B. Davies, J. Funct. Anal. **6**, 318 (1970).
[10] It must be noticed that in the present paper we are focusing only on the statistical description of the measurement process—not on the change of state due to the measurement, nor on its realization scheme—and for this reason we identify the measurement covariance with the covariance of the POVM. The state change due to the measurement is described by the so-called "instrument" (Ref. 11), and the measuring scheme is given in terms of a unitary interaction with an ancilla and an orthogonal measurement on it. Clearly, the POVM covariance does not imply the covariance of all of its instruments, and the covarance of an instrument does not imply the covariance of all of the measurement realizations of the instrument.
[11] E. B. Davies and J. T. Lewis, Commun. Math. Phys. **17**, 239 (1970).
[12] H. P. Yuen and J. H. Shapiro, IEEE Trans. Inf. Theory **24**, 657 (1978); **25**, 179 (1979); **26**, 78 (1980).
[13] G. M. D'Ariano, "Quantum estimation theory and optical detection," in *Concepts and Advances in Quantum Optics and Spectroscopy of Solids*, edited by T. Hakioglu and A. S. Shumovsky (Kluwer Academic, Amsterdam, 1997), pp. 139–174.
[14] C. H. Bennett and G. Brassard, Proceedings of the IEEE International conference on computers, systems, and signal processing, Bangalore, India, 1984, pp. 175–179.
[15] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[16] G. M. D'Ariano and C. Macchiavello, Phys. Rev. A **67**, 042306 (2003).
[17] M.-D. Choi, Linear Algebr. Appl. **10**, 285 (1975).
[18] K. R. Parthasaraty, Infinite Dimen. Anal., Quantum Probab., Relat. Top. **2**, 557 (1999).
[19] G. M. D'Ariano and P. Lo Presti, quant-ph/0301110.
[20] G. M. D'Ariano, C. Macchiavello, and M. F. Sacchi, Phys. Lett. A **248**, 103 (1998).
[21] G. M. D'Ariano, C. Macchiavello, P. Perinotti, and M. F. Sacchi, Phys. Lett. A **268**, 241 (2000).
[22] G. M. D'Ariano and P. Lo Presti, Phys. Rev. A **64**, 042308 (2001).
[23] R. F. Werner, Phys. Rev. A **58**, 1827 (1998).
[24] D. P. Zhelobenko, *Compact Lie Groups and Their Representations* (American Mathematical Society, Providence, 1973).
[25] C.-K. Li and B.-S. Tam, SIAM J. Matrix Anal. Appl. **15**, 903 (1994).
[26] F. Buscemi, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, Phys. Lett. A **314**, 374 (2003).