Quantum measurement for a group-covariant state set

Kenji Nakahira[*]
Yokohama Research Laboratory, Hitachi, Ltd., Yokohama, Kanagawa 244-0817 and
Quantum Information Science Research Center, Quantum ICT Research Institute, Tamagawa University, Machida, Tokyo 194-8610, Japan

Tsuyoshi Sasaki Usuda
School of Information Science and Technology, Aichi Prefectural University, Nagakute, Aichi 480-1198 and
Quantum Information Science Research Center, Quantum ICT Research Institute, Tamagawa University, Machida, Tokyo 194-8610, Japan

(Received 2 November 2012; published 10 January 2013)

We consider a group covariant quantum state set with a group in which each element corresponds to a unitary or antiunitary operator. This type of quantum state set can express a broad class of quantum state sets, including geometrically uniform state sets and self-symmetric state sets. We derive that for any quantum measurement for a group-covariant state set (both with and without a certain fraction of inconclusive results), a group covariant quantum measurement exists with respect to the same group with the same performance, that is, the same probability of correct detection and the same rate of inconclusive results. We then show that a group covariant optimal measurement exists for any group-covariant state set. In some cases, we derive an optimal measurement for a group-covariant state set.

DOI: 10.1103/PhysRevA.87.012308 PACS number(s): 03.67.−a, 03.67.Hk

I. INTRODUCTION

One of the fundamental problems in quantum information is quantum state discrimination. The problem consists in identifying the quantum state that belongs to a given finite set of known states with given prior probabilities. In quantum mechanics, there is no way to discriminate perfectly between nonorthogonal states. Thus, it is of importance to obtain measurement strategies that can discriminate between them as accurately as possible.

The subject of quantum state discrimination was pioneered in the 1970s by Helstrom, Holevo, and Yuen *et al.* [1–3]. Necessary and sufficient conditions for obtaining an optimal measurement that minimizes the probability of a detection error, which we call a minimum error measurement, were formulated by Holevo and Yuen *et al.* [2,3]. However, it is generally very difficult to obtain a closed-form analytical solution for the optimal measurements that satisfy these conditions. Several works have been reported to tackle the problems of finding minimum error measurements (see, e.g., [4–7]).

In recent years, other types of optimal measurements have also been considered, such as a measurement that maximizes the probability of correct detection with zero probability of a detection error, which we refer to as an optimal unambiguous measurement [8,9], and a measurement that maximizes the probability of correct detection with a fixed rate of inconclusive results, which we call an optimal inconclusive measurement [10]. Minimum error measurements and optimal unambiguous measurements can be considered as the special cases of optimal inconclusive measurements.

Recently, many research efforts have been made to express optimal measurements for some state sets. There are some state sets in which analytical solutions for minimum error measurements are known, for example, cyclic pure state sets [4,5], three mirror-symmetric state sets [11], linear codes with binary letter states [6], and pseudocyclic codes with q-ary letter states [12]. In the case of a geometrically uniform (GU) state set, which is defined over a finite group of unitary operators, Eldar *et al.* derived that an optimal GU measurement exists [13]. In the special case of a GU state set, the square root measurement (SRM) is a minimum error measurement for a pure state set [7,13]. In some cases of mixed GU state sets, analytical solutions of an optimal measurement have been found [13–17]. For a GU state set, Eldar also derived that there exist both an optimal inconclusive measurement and an optimal unambiguous measurement that are GU [18,19]. A self-symmetric state set, in which each density operator is invariant over a certain regular normal operator, is another case of a symmetric state set. We showed that for a self-symmetric state set, a minimum error measurement with self-symmetry exists [20].

A GU state set and a self-symmetric state set have different types of symmetries. In addition, state sets having other types of symmetry exist such as three mirror-symmetric state sets [11]. These symmetries can be formulated as the invariance of the corresponding collection of quantum states under the action of a group. We call a state set with some of these symmetries a group covariant quantum state set. To the best of our knowledge, however, for group-covariant state sets there has been no attempt to systematically study the above optimal measurements.

In this paper, we consider a group covariant quantum state set with a group in which each element corresponds to unitary or antiunitary operators. First, we introduce a group covariant quantum state set and provide some examples in Sec. III. Next, in Sec. IV, we show that for any quantum measurement for a group-covariant state set both with and without a certain fraction of inconclusive results, a group covariant measurement exists with respect to the same group with the same performance. In particular, we show that a group covariant optimal measurement exists. We also show that there exists a Lagrange operator for an optimal measurement with

[*] kenji.nakahira.kp@hitachi.com

the same symmetry. Then we derive optimal measurements for several special cases, which are extensions of the results of Refs. [13,18,19]. Finally, in Sec. V, we illustrate group covariant optimal measurements for some group-covariant state sets.

II. QUANTUM MEASUREMENTS

Suppose that $\{\hat{\rho}'_m\}$ $(m \in \mathcal{I}_M)$ is a set of M density operators describing quantum states where $\mathcal{I}_k = \{0,1,\ldots,k-1\}$. Each density operator $\hat{\rho}'_m$ is positive (denoted $\hat{\rho}'_m \geqslant 0$) and has unit trace ($\mathrm{Tr}\hat{\rho}'_m = 1$). We refer to $\{\hat{\rho}_m = \xi_m \hat{\rho}'_m\}$ as a quantum state set with prior probabilities $\{\xi_m\}$, instead of $\{\hat{\rho}'_m\}$. $\{\hat{\rho}_m\}$ satisfies $\hat{\rho}_m \geqslant 0, \mathrm{Tr}\hat{\rho}_m > 0$, and $\sum_{m=0}^{M-1} \mathrm{Tr}\hat{\rho}_m = 1$. For given $\{\hat{\rho}_m\}$, $\{\xi_m\}$, and $\{\hat{\rho}'_m\}$ are uniquely determined as $\xi_m = \mathrm{Tr}\hat{\rho}_m$ and $\hat{\rho}'_m = \xi_m^{-1}\hat{\rho}_m$. Let us call the Hilbert space that is spanned by the supports of the operators $\hat{\rho}_0,\ldots,\hat{\rho}_{M-1}$ the state space $\mathcal{H}$.

A state with a rank 1 density operator is called a pure state; otherwise, it is a mixed state. A pure state set has only pure states. A mixed state set has at least one mixed state.

We consider a quantum measurement $\{\hat{\Pi}_m\}$ $(m \in \mathcal{I}_{M+1})$ defined in $\mathcal{H}$. The operator $\hat{\Pi}_m$ for each $m \in \mathcal{I}_M$ corresponds to detection of the state $\hat{\rho}_m$ and the operator $\hat{\Pi}_M$ corresponds to an inconclusive result. Let $\mathcal{M}$ be the entire set of quantum measurements, each of which consists of $M+1$ detection operators. Any measurement $\{\hat{\Pi}_m\} \in \mathcal{M}$ satisfies

$$\hat{\Pi}_m \geqslant 0, \quad \forall m \in \mathcal{I}_{M+1}, \quad \sum_{m=0}^{M} \hat{\Pi}_m = \hat{1}, \tag{1}$$

where $\hat{1}$ is the identity operator. $\{\hat{\Pi}_m\}$ is referred to as a positive operator-valued measure (POVM).

The probabilities of correct detection $P_{\mathrm{C}}(\{\hat{\Pi}_m\})$ and a detection error $P_{\mathrm{E}}(\{\hat{\Pi}_m\})$ are defined by

$$\begin{aligned} P_{\mathrm{C}}(\{\hat{\Pi}_m\}) &= \sum_{m=0}^{M-1} \mathrm{Tr}(\hat{\rho}_m \hat{\Pi}_m), \\ P_{\mathrm{E}}(\{\hat{\Pi}_m\}) &= \sum_{\substack{m=0 \\ (m \neq k)}}^{M-1} \sum_{k=0}^{M-1} \mathrm{Tr}(\hat{\rho}_m \hat{\Pi}_k). \end{aligned} \tag{2}$$

The probability of an inconclusive result $P_{\mathrm{I}}(\{\hat{\Pi}_m\})$ can be expressed as

$$P_{\mathrm{I}}(\{\hat{\Pi}_m\}) = 1 - P_{\mathrm{C}}(\{\hat{\Pi}_m\}) - P_{\mathrm{E}}(\{\hat{\Pi}_m\}). \tag{3}$$

$P_{\mathrm{I}}(\{\hat{\Pi}_m\})$ can also be expressed as $P_{\mathrm{I}}(\{\hat{\Pi}_m\}) = \mathrm{Tr}(\hat{G}\hat{\Pi}_M)$, where

$$\hat{G} = \sum_{m=0}^{M-1} \hat{\rho}_m. \tag{4}$$

Any measurement with $P_{\mathrm{I}}(\{\hat{\Pi}_m\}) = 0$ satisfies $\hat{\Pi}_M = 0$.

An optimal inconclusive measurement maximizes the probability of correct detection $P_{\mathrm{C}}(\{\hat{\Pi}_m\})$ given a fixed probability of an inconclusive result, $P_{\mathrm{I}}(\{\hat{\Pi}_m\}) = p \ \ (0 \leqslant p < 1)$. A minimum error measurement is a special case of an optimal inconclusive measurement, which satisfies $p = 0$. An optimal unambiguous measurement maximizes the probability of correct detection $P_{\mathrm{C}}(\{\hat{\Pi}_m\})$ and discriminates unambiguously between the states $\hat{\rho}_m$, i.e., satisfies $P_{\mathrm{E}}(\{\hat{\Pi}_m\}) = 0$, which is also a special case of an optimal inconclusive measurement with sufficiently large p. If $\sum_{m=0}^{M-1} \mathrm{rank}\hat{\rho}_m = \dim \mathcal{H}$ holds, then the minimum error measurement is a von Neumann measurement and uniquely determined as described in [21] (see also [1,22] in the pure state case), whereas an inconclusive measurement with $p > 0$ is in general not a von Neumann measurement and is not uniquely determined.

A necessary and sufficient condition for unambiguous measurements to exist for the state set $\{\hat{\rho}_m\}$ is that there exists $m \in \mathcal{I}_M$ such that the kernel of the state $\hat{\rho}_m$ does not contain the intersection of the kernels of the others, that is [23],

$$\mathrm{Ker}\hat{\rho}_m \not\supseteq \bigcap_{k \in \mathcal{I}_M, k \neq m} \mathrm{Ker}\hat{\rho}_k. \tag{5}$$

In particular, in the case in which $\{\hat{\rho}_m = |\psi_m\rangle\langle\psi_m|\}$ is a pure state set, unambiguous detection between $\{\hat{\rho}_m\}$ is possible if and only if $\{|\psi_m\rangle\}$ are linearly independent [24].

III. GROUP-COVARIANT STATE SET

We consider a quantum state set with group symmetry, that is, it is invariant under the action of a group in which each element corresponds to a unitary or antiunitary operator. This type of state set, which we call a group-covariant state set, generalizes a GU state set [13] and a self-symmetric state set [20]. Note that Davies derived a measurement maximizing the mutual information for a group-covariant state set with an irreducible representation [25]. Decker generalized Davies' result to reducible representations [26], but only in the case of unitary operators. In this paper, we assume that a group can be reducible and that each element of the group corresponds to a unitary or antiunitary operator.

First, we define a group-covariant state set. Let us consider the following operations from a positive operator $\hat{T}$ to another:

$$\pi_{\hat{U}}(\hat{T}) = \hat{U}\hat{T}\hat{U}^{\dagger}, \tag{6}$$

where $\hat{U}$ is a unitary or antiunitary operator and where denotes conjugate transpose. (The antiunitary operator is described in detail by Wigner [27].) Note that if $\hat{U}$ is an antiunitary operator, then $\pi_{\hat{U}}(\hat{T})$ is also expressed as $\pi_{\hat{U}}(\hat{T}) = \hat{U}_{\mathrm{uni}}\hat{T}^*\hat{U}_{\mathrm{uni}}^{\dagger}$ when using a unitary operator $\hat{U}_{\mathrm{uni}}$ corresponding to $\hat{U}$. $\hat{T}^*$ denotes

$$\hat{T}^* = \sum_{n=0}^{N-1}\sum_{n'=0}^{N-1} \{\langle\phi_n|\hat{T}|\phi_{n'}\rangle\}^* |\phi_n\rangle\langle\phi_{n'}|, \tag{7}$$

where $\{|\phi_n\rangle\}$ $(n \in \mathcal{I}_N, N = \dim\mathcal{H})$ is some complete orthonormal basis of $\mathcal{H}$ and where z^* denotes the complex conjugate of the complex number z. Let $\mathcal{F}$ be the entire set of operations $\pi_{\hat{U}}(\hat{T})$.

A group-covariant state set is defined as the following group action.

Definition 1. A state set $\mathcal{P} = \{\hat{\rho}_m\}$ $(m \in \mathcal{I}_M)$ is a group-covariant state set with respect to $\mathcal{G}$, which we refer to as a $\mathcal{G}$-symmetric state set, if there is a finite group $\mathcal{G}$ with $|\mathcal{G}| \geqslant 2$ ($|\mathcal{G}|$ is the number of elements in the group $\mathcal{G}$) that satisfies the

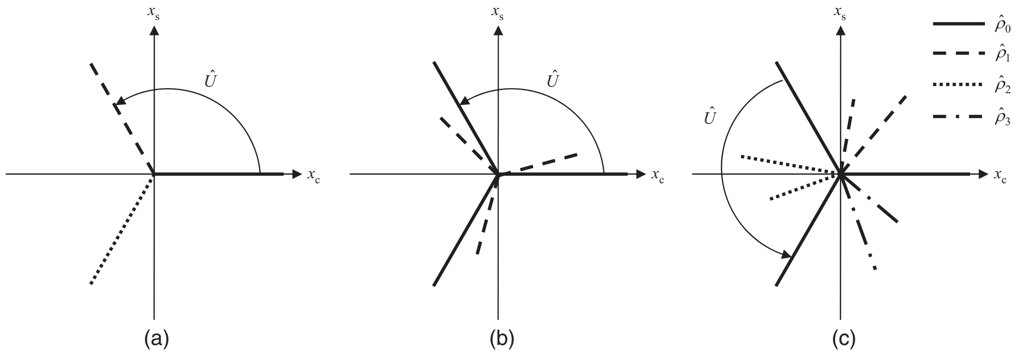

FIG. 1. Phase-space representation of examples of group-covariant state sets: (a) a GU state set; (b) a self-symmetric state set; (c) another type of state set. Each line segment represents a coherent state. A state expressed by multiple line segments is a mixed state in which the corresponding coherent states are uniformly mixed.

following properties:

(1) There is an operation $\pi_g \in \mathcal{F}$ for each $g \in \mathcal{G}$ such that $\pi_g \neq \pi_h$ for any $g,h \in \mathcal{G}$ $(g \neq h)$.

(2) $\pi_g(\hat{\rho}_m) \in \mathcal{P}$ for any $g \in \mathcal{G}$ and $m \in \mathcal{I}_M$.

(3) $\pi_e(\hat{\rho}_m) = \hat{\rho}_m$ for any $m \in \mathcal{I}_M$, where e is the identity element of $\mathcal{G}$.

(4) $\pi_{gh}(\hat{\rho}_m) = \pi_g(\pi_h(\hat{\rho}_m))$ for any $g,h \in \mathcal{G}$ and $m \in \mathcal{I}_M$.

The group $\mathcal{G}$ is said to act on $\mathcal{P}$.

Let $\tau_g(m) \in \mathcal{I}_M$ $(g \in \mathcal{G}, m \in \mathcal{I}_M)$ be a number that satisfies $\hat{\rho}_{\tau_g(m)} = \pi_g(\hat{\rho}_m)$. We denote $g \circ \hat{T} = \pi_g(\hat{T})$ and $g \circ m = \tau_g(m)$ to simplify the notation. Thus, if $\mathcal{P}$ is a $\mathcal{G}$-symmetric state set, then we have

$$g \circ \hat{\rho}_m = \hat{\rho}_{g \circ m}, \quad \forall g \in \mathcal{G}, \quad m \in \mathcal{I}_M. \tag{8}$$

Note that $\xi_{g \circ m} = \mathrm{Tr}\pi_g(\hat{\rho}_m) = \mathrm{Tr}\hat{\rho}_m = \xi_m$ for any $g \in \mathcal{G}$ and $m \in \mathcal{I}_M$.

Next, we show three examples of group-covariant state sets: GU or compound GU (CGU) state sets [13], self-symmetric state sets, and other state sets.

Example 1 (GU or CGU state set). Let us consider the unitary operators $\hat{U}_k$ that form a group $\mathcal{G} = \{\hat{U}_k\}$ $(k \in \mathcal{I}_S$, $S = |\mathcal{G}| \geqslant 2)$. A CGU state set is defined as a quantum state set $\mathcal{P} = \{\hat{\rho}_{k,j}\}$ $(k \in \mathcal{I}_S,\ j \in \mathcal{I}_J)$ satisfying

$$\pi_k(\hat{\rho}_{0,j}) = \hat{U}_k \hat{\rho}_{0,j} \hat{U}_k^\dagger = \hat{\rho}_{k,j}, \tag{9}$$

where J is a natural number [13]. It is easy to verify that a CGU state set is a $\mathcal{G}$-symmetric state set. A GU state set is a special class of CGU state sets in which $J = 1$.

The phase-space representation of an example of a GU state set $\{\hat{\rho}_0,\hat{\rho}_1,\hat{\rho}_2\}$ where $\hat{U}^3 = \hat{1}$ is shown in Fig. 1(a). $\hat{\rho}_m = |\alpha_m\rangle\langle\alpha_m|/3$ is a coherent state of light where $|\alpha_m\rangle$ is the eigenvector of the annihilation operator corresponding to the eigenvalue $\alpha_m = \alpha \exp(i2\pi m/3)$ $(\alpha \neq 0, i = \sqrt{-1})$.

The action of $\mathcal{G}$ on $\mathcal{P}$ is called free if, for all $m \in \mathcal{I}_M$, $g \circ m = m$ $(g \in \mathcal{G})$ implies $g = e$ [28]. The action of $\mathcal{G}$ is transitive if for any $m,n \in \mathcal{I}_M$, $g \in \mathcal{G}$ exists such that $g \circ m = n$ [28]. $\mathcal{P}$ is a CGU state set if and only if $\mathcal{G}$ exists such that the action of $\mathcal{G}$ on $\mathcal{P}$ is free. As a special case, $\mathcal{P}$ is a GU state set if and only if $\mathcal{G}$ exists such that the action of $\mathcal{G}$ on $\mathcal{P}$ is free and transitive.

Example 2 (self-symmetric state set). A self-symmetric state set $\mathcal{P} = \{\hat{\rho}_m\}$ $(m \in \mathcal{I}_M)$ is defined as a quantum state set such that there exists a regular normal operator $\hat{A}$ of the space $\mathcal{H}$ satisfying

$$\hat{A}\hat{\rho}_m\hat{A}^{-1} = \hat{\rho}_m, \quad \forall m \in \mathcal{I}_M. \tag{10}$$

We exclude the trivial case where $\hat{A}$ is expressed by $\hat{A} = c\hat{1}$ $(c \neq 0$ is a complex number).

Here we show that a self-symmetric state set is also a group-covariant state set. Let $\{\hat{P}_l\}$ $(l \in \mathcal{I}_L)$ be the entire set of orthogonal projection operators onto the eigenspaces of $\hat{A}$. We consider the following unitary operator:

$$\hat{U} = \sum_{l=0}^{L-1} \exp\left(i\frac{2\pi l}{L}\right)\hat{P}_l. \tag{11}$$

$\hat{U}$ has the same eigenspaces as $\hat{A}$ and satisfies $\hat{U}\hat{\rho}_m\hat{U}^{-1} = \hat{\rho}_m$ for any $m \in \mathcal{I}_M$ and $\hat{U}^L = \hat{1}$. Since $\mathcal{G} = \{\hat{U}^l\}$ $(l \in \mathcal{I}_L)$ is a group and $\pi_{\hat{U}^l}(\hat{\rho}_m) = \hat{U}^l\hat{\rho}_m\hat{U}^{-l} = \hat{\rho}_m$, a state set $\mathcal{P}$ satisfying Eq. (10) is a $\{\hat{U}^l\}$-symmetric state set.

The phase-space representation of an example of a self-symmetric state set is shown in Fig. 1(b). $\hat{\rho}_m$ is a mixed state of coherent light expressed as $\hat{\rho}_m = \xi_m(|\alpha_m\rangle\langle\alpha_m| + \hat{U}|\alpha_m\rangle\langle\alpha_m|\hat{U}^{-1} + \hat{U}^2|\alpha_m\rangle\langle\alpha_m|\hat{U}^{-2})/3$, where $\hat{U}|\alpha_m\rangle = |\exp(i2\pi m/3)\alpha_m\rangle$. Equation (10) holds with $\hat{A} = \hat{U}$.

The action of $\mathcal{G}$ on $\mathcal{P}$ is called faithful if for any $g,h \in \mathcal{G}$ $(g \neq h)$ there exists $m \in \mathcal{I}_M$ such that $g \circ m \neq h \circ m$ [28]. When π_g is a unitary operation for any $g \in \mathcal{G}$, $\mathcal{P}$ is a self-symmetric state set if and only if $\mathcal{G}$ exists such that the action of $\mathcal{G}$ on $\mathcal{P}$ is not faithful.

Example 3 (another type of state set). An example of a group-covariant state set $\mathcal{P}$ that is neither a CGU state set nor a self-symmetric state set is shown in Fig. 1(c). It is easy to verify that the action is faithful but not free. In this example a unitary operator $\hat{U}$ exists such that $\hat{U}^3 = \hat{1}$ and a group $\mathcal{G} = \{\hat{1},\hat{U},\hat{U}^2\}$ acts on $\mathcal{P}$ as reported in Table I.

TABLE I. The group action of $\mathcal{G}$ on $\mathcal{P}$ with respect to the state set in Fig. 1(c).

$g \in \mathcal{G}$	$g \circ 0$	$g \circ 1$	$g \circ 2$	$g \circ 3$
$\hat{1}$	0	1	2	3
$\hat{U}$	0	2	3	1
$\hat{U}^2$	0	3	1	2

IV. QUANTUM MEASUREMENTS FOR GROUP-COVARIANT STATE SETS

A. Optimal measurements

Definition 2. A POVM $\{\hat{\Pi}_m\} \in \mathcal{M}$ satisfying

$$g \circ \hat{\Pi}_m = \hat{\Pi}_{g\circ m}, \quad \forall g \in \mathcal{G}, \quad m \in \mathcal{I}_M \tag{12}$$

is group covariant with respect to $\mathcal{G}$, which we call $\mathcal{G}$ symmetric. $\mathcal{M}^{(\mathcal{G})}$ is the entire set of $\mathcal{G}$-symmetric POVMs, each of which consists of $M+1$ detection operators.

First, we introduce the following lemma.

Lemma 3. For any positive operators $\hat{S},\hat{T}$, any $c \in \mathbf{R}_0$ ($\mathbf{R}_0$ is the entire set of non-negative real numbers), and any $g \in \mathcal{G}$, any operation $\pi_g \in \mathcal{F}$ expressed by Eq. (6) satisfies

$$g \circ (\hat{S}\hat{T}) = (g \circ \hat{S})(g \circ \hat{T}), \tag{13}$$

$$g \circ (\hat{S} + \hat{T}) = g \circ \hat{S} + g \circ \hat{T}, \tag{14}$$

$$g \circ (c\hat{T}) = c(g \circ \hat{T}), \tag{15}$$

$$g \circ 0 = 0, \tag{16}$$

$$g \circ \hat{1} = \hat{1}, \tag{17}$$

$$\mathrm{Tr}(g \circ \hat{T}) = \mathrm{Tr}\hat{T}, \tag{18}$$

$$g \circ (\hat{T}^+) = (g \circ \hat{T})^+, \tag{19}$$

where $\hat{T}^+$ denotes the Moore-Penrose inverse operator of $\hat{T}$. Moreover, we have that for any positive regular operator $\hat{T}$ and any $c \in \mathbf{R}$ ($\mathbf{R}$ is the entire set of real numbers),

$$g \circ (\hat{T}^c) = (g \circ \hat{T})^c. \tag{20}$$

It is easy to prove Lemma 3 from Eq. (6) (proof omitted). It follows that if $\{\hat{\Pi}_m\} \in \mathcal{M}^{(\mathcal{G})}$, then $g \circ \hat{\Pi}_M = g \circ (\hat{1} - \sum_{m=0}^{M-1} \hat{\Pi}_m) = \hat{1} - \sum_{m=0}^{M-1} \hat{\Pi}_{g\circ m} = \hat{\Pi}_M$ holds since $\{g \circ 0, g \circ 1, \ldots, g \circ (M-1)\} = \mathcal{I}_M$. For simplicity, let $g \circ M = \tau_g(M) = M$. By using Lemma 3, we obtain the following theorem.

Theorem 4. We consider a $\mathcal{G}$-symmetric state set $\mathcal{P} = \{\hat{\rho}_m\}$ ($m \in \mathcal{I}_M$). For any POVM $\{\hat{X}_m\} \in \mathcal{M}$, a $\mathcal{G}$-symmetric POVM $\{\hat{\Pi}_m\} \in \mathcal{M}^{(\mathcal{G})}$ exists such that $P_{\mathrm{C}}(\{\hat{\Pi}_m\}) = P_{\mathrm{C}}(\{\hat{X}_m\})$ and $P_{\mathrm{E}}(\{\hat{\Pi}_m\}) = P_{\mathrm{E}}(\{\hat{X}_m\})$.

Proof. We consider the operators $\{\hat{X}_m^{(g)}\}$ ($m \in \mathcal{I}_{M+1}$) defined as

$$\hat{X}_m^{(g)} = g^{-1} \circ \hat{X}_{g\circ m}. \tag{21}$$

It follows that $\{\hat{X}_m^{(g)}\} \in \mathcal{M}$ for any $g \in \mathcal{G}$. Indeed, from Eq. (21), $\hat{X}_m^{(g)} \geqslant 0$ and

$$\begin{aligned}\sum_{m=0}^{M} \hat{X}_m^{(g)} &= \sum_{m=0}^{M} (g^{-1} \circ \hat{X}_{g\circ m}) = g^{-1} \circ \left(\sum_{m=0}^{M} \hat{X}_{g\circ m}\right) \\ &= g^{-1} \circ \hat{1} = \hat{1}.\end{aligned} \tag{22}$$

Moreover, we have that for any $m \in \mathcal{I}_M$ and $k \in \mathcal{I}_{M+1}$,

$$\begin{aligned}\mathrm{Tr}(\hat{\rho}_m \hat{X}_k^{(g)}) &= \mathrm{Tr}[\hat{\rho}_m (g^{-1} \circ \hat{X}_{g\circ k})] = \mathrm{Tr}\{g^{-1} \circ [(g \circ \hat{\rho}_m)\hat{X}_{g\circ k}]\} \\ &= \mathrm{Tr}(\hat{\rho}_{g\circ m} \hat{X}_{g\circ k}).\end{aligned} \tag{23}$$

Thus, $P_{\mathrm{C}}(\{\hat{X}_m^{(g)}\}) = P_{\mathrm{C}}(\{\hat{X}_m\})$ and $P_{\mathrm{E}}(\{\hat{X}_m^{(g)}\}) = P_{\mathrm{E}}(\{\hat{X}_m\})$ hold.

Consider the operators $\{\hat{\Pi}_m\}$ ($m \in \mathcal{I}_{M+1}$) expressed as

$$\hat{\Pi}_m = \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} \hat{X}_m^{(g)}. \tag{24}$$

$\{\hat{\Pi}_m\}$ is obviously a POVM with $P_{\mathrm{C}}(\{\hat{\Pi}_m\}) = P_{\mathrm{C}}(\{\hat{X}_m\})$ and $P_{\mathrm{E}}(\{\hat{\Pi}_m\}) = P_{\mathrm{E}}(\{\hat{X}_m\})$. We have that for any $g \in \mathcal{G}$ and $m \in \mathcal{I}_{M+1}$,

$$\begin{aligned}g \circ \hat{\Pi}_m &= \frac{1}{|\mathcal{G}|} \sum_{h \in \mathcal{G}} g \circ \hat{X}_m^{(h)} = \frac{1}{|\mathcal{G}|} \sum_{h \in \mathcal{G}} g \circ h^{-1} \circ \hat{X}_{h\circ m} \\ &= \frac{1}{|\mathcal{G}|} \sum_{k \in \mathcal{G}} k^{-1} \circ \hat{X}_{k\circ g\circ m} = \frac{1}{|\mathcal{G}|} \sum_{k \in \mathcal{G}} \hat{X}_{g\circ m}^{(k)} = \hat{\Pi}_{g\circ m},\end{aligned} \tag{25}$$

where $k = h \circ g^{-1}$. Therefore, $\{\hat{\Pi}_m\} \in \mathcal{M}^{(\mathcal{G})}$. ■

Corollary 5. We consider a $\mathcal{G}$-symmetric state set $\mathcal{P} = \{\hat{\rho}_m\}$ ($m \in \mathcal{I}_M$). A $\mathcal{G}$-symmetric minimum error measurement and a $\mathcal{G}$-symmetric optimal inconclusive measurement exist. Moreover, if $\mathcal{P}$ satisfies Eq. (5), then a $\mathcal{G}$-symmetric optimal unambiguous measurement exists.

Proof. Let $\{\hat{X}_m\} \in \mathcal{M}$ be an optimal measurement, i.e., a minimum error measurement or an optimal inconclusive measurement or an optimal unambiguous measurement. From Theorem 4, $\{\hat{\Pi}_m\} \in \mathcal{M}^{(\mathcal{G})}$ exists such that $P_{\mathrm{C}}(\{\hat{\Pi}_m\}) = P_{\mathrm{C}}(\{\hat{X}_m\})$ and $P_{\mathrm{E}}(\{\hat{\Pi}_m\}) = P_{\mathrm{E}}(\{\hat{X}_m\})$. Thus, $\{\hat{\Pi}_m\}$ is also optimal. ■

Theorem 6. We consider a $\mathcal{G}$-symmetric state set $\mathcal{P} = \{\hat{\rho}_m\}$ ($m \in \mathcal{I}_M$). Let $\mathcal{Q}$ be a set whose elements are pairs of the probabilities of correct detection and a detection error ($P_{\mathrm{C}}, P_{\mathrm{E}}$). Assume that $\mathcal{Q}$ is convex, that is, for any two pairs $(P_{\mathrm{C1}}, P_{\mathrm{E1}})$, $(P_{\mathrm{C2}}, P_{\mathrm{E2}}) \in \mathcal{Q}$, and any $t \in \mathbf{R}$ satisfying $0 \leqslant t \leqslant 1$, $(tP_{\mathrm{C1}} + (1-t)P_{\mathrm{C2}}, tP_{\mathrm{E1}} + (1-t)P_{\mathrm{E2}}) \in \mathcal{Q}$. Let $\mathcal{M}_{\mathcal{Q}}^{(\mathcal{G})}$ be the entire set of $\mathcal{G}$-symmetric POVMs $\{\hat{\Pi}_m\}$ that satisfy $(P_{\mathrm{C}}(\{\hat{\Pi}_m\}), P_{\mathrm{E}}(\{\hat{\Pi}_m\})) \in \mathcal{Q}$. Then $\mathcal{M}_{\mathcal{Q}}^{(\mathcal{G})}$ is a convex set (possibly empty). That is, for any POVMs $\{\hat{\Pi}_m\}, \{\hat{\Pi}'_m\} \in \mathcal{M}_{\mathcal{Q}}^{(\mathcal{G})}$ and any $t \in \mathbf{R}$ satisfying $0 \leqslant t \leqslant 1$, we have

$$\{t\hat{\Pi}_m + (1-t)\hat{\Pi}'_m\} \in \mathcal{M}_{\mathcal{Q}}^{(\mathcal{G})}. \tag{26}$$

Let $\mathcal{Q}_{\mathrm{i}} = \{(P_{\mathrm{C}}, P_{\mathrm{E}}) : P_{\mathrm{C}} \geqslant 0, P_{\mathrm{E}} \geqslant 0, P_{\mathrm{C}} + P_{\mathrm{E}} = 1 - p\}$ and $\mathcal{Q}_{\mathrm{u}} = \{(P_{\mathrm{C}}, 0) : 0 \leqslant P_{\mathrm{C}} \leqslant 1\}$. It is easy to verify that both $\mathcal{Q}_{\mathrm{i}}$ and $\mathcal{Q}_{\mathrm{u}}$ are convex. Thus, the problem of obtaining an optimal measurement clearly remains in convex programming even if we restrict the solution domain from $\mathcal{M}$ to $\mathcal{M}_{\mathcal{Q}_{\mathrm{i}}}^{(\mathcal{G})}$ or $\mathcal{M}_{\mathcal{Q}_{\mathrm{u}}}^{(\mathcal{G})}$.

Proof. Suppose that $\{\hat{\Pi}_m\}$ and $\{\hat{\Pi}'_m\}$ are in $\mathcal{M}_{\mathcal{Q}}^{(\mathcal{G})}$. Both $(P_{\mathrm{C}}(\{\hat{\Pi}_m\}), P_{\mathrm{E}}(\{\hat{\Pi}_m\}))$ and $(P_{\mathrm{C}}(\{\hat{\Pi}'_m\}), P_{\mathrm{E}}(\{\hat{\Pi}'_m\}))$ are elements of the set $\mathcal{Q}$. Consider $\{\hat{\Pi}''_m = t\hat{\Pi}_m + (1-t)\hat{\Pi}'_m\} \in \mathcal{M}$. From Eq. (2), $P_{\mathrm{C}}(\{\hat{\Pi}''_m\}) = tP_{\mathrm{C}}(\{\hat{\Pi}_m\}) + (1-t)P_{\mathrm{C}}(\{\hat{\Pi}'_m\})$ and $P_{\mathrm{E}}(\{\hat{\Pi}''_m\}) = tP_{\mathrm{E}}(\{\hat{\Pi}_m\}) + (1-t)P_{\mathrm{E}}(\{\hat{\Pi}'_m\})$ hold. Thus, $(P_{\mathrm{C}}(\{\hat{\Pi}''_m\}), P_{\mathrm{E}}(\{\hat{\Pi}''_m\})) \in \mathcal{Q}$. Moreover, we have that for any $g \in \mathcal{G}$ and $m \in \mathcal{I}_{M+1}$,

$$\begin{aligned}g \circ \hat{\Pi}''_m &= g \circ (t\hat{\Pi}_m + (1-t)\hat{\Pi}'_m) \\ &= t(g \circ \hat{\Pi}_m) + (1-t)(g \circ \hat{\Pi}'_m) \\ &= t\hat{\Pi}_{g\circ m} + (1-t)\hat{\Pi}'_{g\circ m} = \hat{\Pi}''_{g\circ m}.\end{aligned} \tag{27}$$

Therefore, $\{\hat{\Pi}''_m\} \in \mathcal{M}_{\mathcal{Q}}^{(\mathcal{G})}$. ■

B. Dual problems

It was shown in Ref. [18] that necessary and sufficient conditions for an optimal inconclusive measurement $\{\hat{\Pi}_m\}$ are that a positive operator $\hat{\Gamma}$, which is called a Lagrange operator, and $\lambda \in \mathbf{R}$ exist satisfying

$$\hat{\Gamma} - \hat{\rho}_m \geqslant 0, \quad \forall m \in \mathcal{I}_{M+1}, \tag{28}$$

$$(\hat{\Gamma} - \hat{\rho}_m)\hat{\Pi}_m = 0, \quad \forall m \in \mathcal{I}_{M+1}, \tag{29}$$

where $\hat{\rho}_M = \lambda \hat{G}$. Summing Eq. (29) over $m = 0, \ldots, M$ gives [29]

$$\hat{\Gamma} = \sum_{k=0}^{M} \hat{\rho}_k \hat{\Pi}_k. \tag{30}$$

Necessary and sufficient conditions for a minimum error measurement, which have been derived in Refs. [2,3], can be interpreted as that $\hat{\Gamma} \geqslant 0$ exists such that Eqs. (28) and (29) hold for $\lambda = 0$ and $\hat{\Pi}_M = 0$. It is known that only Eqs. (28) and (30) are also necessary and sufficient conditions for a minimum error measurement [30]. [Note that if Eq. (28) holds, then $\hat{\Gamma}$ is a Hermitian operator since $\hat{\Gamma} \geqslant 0$.] The following remark shows that an optimal inconclusive measurement has similar properties.

Remark 7. Necessary and sufficient conditions for an optimal inconclusive measurement $\{\hat{\Pi}_m\} \in \mathcal{M}$ for a quantum state set $\{\hat{\rho}_m\}$ $(m \in \mathcal{I}_M)$ are that $\lambda \in \mathbf{R}$ exists such that Eqs. (28) and (30) hold where $\hat{\rho}_M = \lambda \hat{G}$.

Proof. It was shown in Refs. [18] and [29] that Eqs. (28) and (30) are necessary conditions for optimality. Now we prove that these equations are also sufficient conditions. Assume that $\lambda \in \mathbf{R}$ exists satisfying Eqs. (28) and (30). Consider another POVM, $\{\hat{\Pi}'_m\} \in \mathcal{M}$, with the probability of an inconclusive result, $\mathrm{Tr}(\hat{G}\hat{\Pi}'_M) = p = \mathrm{Tr}(\hat{G}\hat{\Pi}_M)$. We have

$$\begin{aligned} &P_{\mathrm{C}}(\{\hat{\Pi}_m\}) - P_{\mathrm{C}}(\{\hat{\Pi}'_m\}) \\ &= [P_{\mathrm{C}}(\{\hat{\Pi}_m\}) + \lambda p] - [P_{\mathrm{C}}(\{\hat{\Pi}'_m\}) + \lambda p] \\ &= \sum_{k=0}^{M} \mathrm{Tr}(\hat{\rho}_k \hat{\Pi}_k) - \sum_{m=0}^{M} \mathrm{Tr}(\hat{\rho}_m \hat{\Pi}'_m) \\ &= \sum_{m=0}^{M} \mathrm{Tr}\{(\hat{\Gamma} - \hat{\rho}_m)\hat{\Pi}'_m\} \geqslant 0, \end{aligned} \tag{31}$$

where the inequality follows from $\hat{\Gamma} - \hat{\rho}_m \geqslant 0$ and $\hat{\Pi}'_m \geqslant 0$. Thus, the POVM $\{\hat{\Pi}_m\}$ is an optimal inconclusive measurement. ■

The following theorem shows that a symmetric Lagrange operator associated with an optimal inconclusive measurement for a $\mathcal{G}$-symmetric state set exists.

Theorem 8. We consider a $\mathcal{G}$-symmetric state set $\mathcal{P} = \{\hat{\rho}_m\}$ $(m \in \mathcal{I}_M)$. A Lagrange operator $\hat{\Gamma}$ associated with an optimal inconclusive measurement satisfying $g \circ \hat{\Gamma} = \hat{\Gamma}$ $(g \in \mathcal{G})$ exists.

Thus, $\hat{\Gamma}$ is obtained by minimizing $\mathrm{Tr}\hat{\Gamma}$ subject to the constraints $\hat{\Gamma} \geqslant \hat{\rho}_m$ and $g \circ \hat{\Gamma} = \hat{\Gamma}$, which is also a convex programming problem. Assalini *et al.* showed that the symmetry of a Lagrange operator $\hat{\Gamma}$ permits computationally efficient calculation of a minimum error measurement in the cyclic case [31]. Theorem 8 can also be used to obtain a minimum error measurement and an optimal inconclusive measurement efficiently.

Proof. Let $\{\hat{\Pi}_m\}$ be a $\mathcal{G}$-symmetric optimal inconclusive measurement, which always exists from Corollary 5. Since $g \circ \hat{\rho}_M = \hat{\rho}_M$ and $g \circ \hat{\Pi}_M = \hat{\Pi}_M$,

$$\begin{aligned} g \circ \hat{\Gamma} &= g \circ \sum_{m=0}^{M} \hat{\rho}_m \hat{\Pi}_m = \sum_{m=0}^{M} (g \circ \hat{\rho}_m)(g \circ \hat{\Pi}_m) \\ &= \sum_{m=0}^{M} \hat{\rho}_{g\circ m} \hat{\Pi}_{g\circ m} = \hat{\Gamma}. \end{aligned} \tag{32}$$

■

Now we consider an optimal unambiguous measurement. Suppose that Eq. (5) holds. Let $\hat{\Phi}_m$ $(m \in \mathcal{I}_M)$ be the orthogonal projection operator onto $\cap_{j\neq m}\mathrm{Ker}\hat{\rho}_j = \mathrm{Ker}\hat{\sigma}_m$ where $\hat{\sigma}_m = \hat{G} - \hat{\rho}_m$. [Note that $\mathrm{Ker}\hat{A} \cap \mathrm{Ker}\hat{B} = \mathrm{Ker}(\hat{A} + \hat{B})$ for positive operators $\hat{A}$ and $\hat{B}$.] In Ref. [23], necessary and sufficient conditions for an optimal unambiguous measurement are that there exists a Lagrange operator $\hat{Z} \geqslant 0$ satisfying $\hat{\Phi}_m(\hat{Z} - \hat{\rho}_m)\hat{\Phi}_m \geqslant 0$ $(m \in \mathcal{I}_M)$ and $\mathrm{Tr}\hat{Z} = P_{\mathrm{C}}(\{\hat{\Pi}_m\})$. It can be shown that a Lagrange operator $\hat{Z}$ associated with an optimal unambiguous measurement for a $\mathcal{G}$-symmetric state set exists such that $g \circ \hat{Z} = \hat{Z}$ $(g \in \mathcal{G})$ as the following theorem.

Theorem 9. We consider a $\mathcal{G}$-symmetric state set $\mathcal{P} = \{\hat{\rho}_m\}$ $(m \in \mathcal{I}_M)$ satisfying Eq. (5). A Lagrange operator $\hat{Z}$ associated with an optimal unambiguous measurement satisfying $g \circ \hat{Z} = \hat{Z}$ $(g \in \mathcal{G})$ exists.

Proof. Let $\{\hat{\Pi}_m\}$ be a $\mathcal{G}$-symmetric optimal unambiguous measurement (which always exists). Let $\hat{Z}' \geqslant 0$ be a Lagrange operator associated with $\{\hat{\Pi}_m\}$. $\hat{Z}$ is defined by

$$\hat{Z} = \frac{1}{|\mathcal{G}|} \sum_{g\in\mathcal{G}} g \circ \hat{Z}'. \tag{33}$$

It is easy to verify that $\hat{Z} \geqslant 0$, $\mathrm{Tr}\hat{Z} = |\mathcal{G}|^{-1} \sum_{g\in\mathcal{G}} \mathrm{Tr}\hat{Z}' = \mathrm{Tr}\hat{Z}' = P_{\mathrm{C}}(\{\hat{\Pi}_m\})$, and $g \circ \hat{Z} = \hat{Z}$. Now we show that $\hat{\Phi}_m(\hat{Z} - \hat{\rho}_m)\hat{\Phi}_m \geqslant 0$. $\hat{\Phi}_m$ is expressed by $\hat{\Phi}_m = \hat{1} - \hat{\sigma}_m \hat{\sigma}_m^+$. We have

$$g \circ \hat{\Phi}_m = \hat{1} - (g \circ \hat{\sigma}_m)(g \circ \hat{\sigma}_m^+) = \hat{1} - \hat{\sigma}_{g\circ m} \hat{\sigma}_{g\circ m}^+ = \hat{\Phi}_{g\circ m}, \tag{34}$$

since $g \circ \hat{\sigma}_m = G - g \circ \hat{\rho}_m = \hat{\sigma}_{g\circ m}$. Thus,

$$\begin{aligned} \hat{\Phi}_m(\hat{Z} - \hat{\rho}_m)\hat{\Phi}_m &= \frac{1}{|\mathcal{G}|} \sum_{g\in\mathcal{G}} \hat{\Phi}_m(g \circ \hat{Z}' - \hat{\rho}_m)\hat{\Phi}_m \\ &= \frac{1}{|\mathcal{G}|} \sum_{g\in\mathcal{G}} g \circ [\hat{\Phi}_{g^{-1}\circ m}(\hat{Z}' - \hat{\rho}_{g^{-1}\circ m})\hat{\Phi}_{g^{-1}\circ m}] \\ &\geqslant 0, \end{aligned} \tag{35}$$

where the inequality follows from $\hat{\Phi}_m(\hat{Z}' - \hat{\rho}_m)\hat{\Phi}_m \geqslant 0$ for any $m \in \mathcal{I}_M$. ■

C. Decomposing into the direct sum of measurements

Suppose that a group $\mathcal{G}$ does not act faithfully on $\mathcal{P}$. It is known that a subgroup $\mathcal{G}'$ of $\mathcal{G}$ that acts faithfully on $\mathcal{P}$ can be obtained [28]. Consider $\mathcal{K} = \{h \in \mathcal{G} : h\circ m = m (\forall m \in \mathcal{I}_M)\}$. $\mathcal{K}$ is a normal subgroup of $\mathcal{G}$ $(|\mathcal{K}| \geqslant 2)$, and the action of the quotient group $\mathcal{G}' = \mathcal{G}/\mathcal{K}$ is faithful. Since a $\mathcal{G}$-symmetric state set $\mathcal{P}$ is also $\mathcal{K}$ symmetric and $\mathcal{G}'$ symmetric, any POVM $\{\hat{\Pi}_m\} \in \mathcal{M}^{(\mathcal{G})}$ satisfies

$$h\circ\hat{\Pi}_m = \hat{\Pi}_m, \quad \forall h \in \mathcal{K}, \quad m \in \mathcal{I}_{M+1}, \tag{36}$$

$$g\circ\hat{\Pi}_m = \hat{\Pi}_{g\circ m}, \quad \forall g \in \mathcal{G}', \quad m \in \mathcal{I}_{M+1}. \tag{37}$$

In some cases, a $\mathcal{G}$-symmetric POVM may be easily analyzed by dividing the group $\mathcal{G}$ into subgroups $\mathcal{K}$ and $\mathcal{G}'$. In particular, if the group $\mathcal{K}$ has an element h in which $\pi_h(\hat{T})$ is represented as $\pi_h(\hat{T}) = \hat{U}\hat{T}\hat{U}^\dagger$ ($\hat{U}$ is a unitary operator), then each state $\hat{\rho}_m$ can be expressed as the following direct sum of operators defined in the eigenspaces $\{\mathcal{X}_l\}$ ($l \in \mathcal{I}_L$) of $\hat{U}$:

$$\hat{\rho}_m = \bigoplus_{l=0}^{L-1} W_l\hat{\rho}_{m;l}, \quad \hat{\rho}_{m;l} = \hat{P}_l\hat{\rho}_m\hat{P}_l/W_l, \tag{38}$$

where $\hat{P}_l$ is the orthogonal projection operator onto the space $\mathcal{X}_l$ and $W_l = \sum_m \mathrm{Tr}(\hat{P}_l\hat{\rho}_m\hat{P}_l)$ is the normalizing constant such that $\sum_m \mathrm{Tr}\hat{\rho}_{m;l} = 1$.

Note that Theorem 4 and Corollary 5 hold if the operation π_g satisfies Equations (13)–(15), even if π_g cannot be described by Eq. (6). [Eqs. (16)–(20) can be derived from Eqs. (13)–(15).] For example, if each $\hat{\rho}_m$ satisfies Eq. (10), i.e., $\hat{\rho}_m$ commutes with a regular normal operator $\hat{A}$, then an operation expressed as

$$\pi_{\hat{P},\hat{U}}(\hat{T}) = \hat{U}\{\hat{P}\hat{T}\hat{P} + (\hat{1}-\hat{P})\hat{T}^*(\hat{1}-\hat{P})\}\hat{U}^\dagger \tag{39}$$

also satisfies Eqs. (13)–(15) for any positive operator $\hat{T}$ commuting with $\hat{A}$, where $\hat{P}$ and $\hat{U}$ are, respectively, an orthogonal projection operator and a unitary operator satisfying $\hat{P}\hat{A} = \hat{A}\hat{P}$ and $\hat{U}\hat{A} = \hat{A}\hat{U}$. $\pi_{\hat{P},\hat{U}}(\hat{T})$ of Eq. (39) indicates a unitary operation in the support space of $\hat{P}$ and an antiunitary operation in the kernel space of $\hat{P}$. Such a $\hat{\rho}_m$ can even be easily analyzed by expressing it as the direct sum in Eq. (38).

We explained in our previous paper [20] that the problem of finding a minimum error measurement for a self-symmetric state set can be replaced by the equivalent problem of finding a minimum error measurement for the state set $\{\hat{\rho}_{m;l}\}$ for each l. A similar proposition can be obtained for an optimal unambiguous measurement as follows.

Proposition 10. Suppose that $\{\hat{\rho}_m\}$ ($m \in \mathcal{I}_M$) satisfies Eq. (5) and can be expressed as Eq. (38). For each $l \in \mathcal{I}_L$, let $\{\hat{\Pi}_{m;l}\}$ ($m \in \mathcal{I}_{M+1}$) be an optimal unambiguous measurement for $\{\hat{\rho}_{m;l}\}$ in its state space $\mathcal{X}_l$. (If unambiguous detection between $\{\hat{\rho}_{m;l}\}$ is not possible, then let $\hat{\Pi}_{m;l} = \hat{0}$ for all $m \in \mathcal{I}_M$ and $\hat{\Pi}_{M;l} = \hat{P}_l$.) Then the following POVM $\{\hat{\Pi}_m\} \in \mathcal{M}$ is an optimal unambiguous measurement for $\{\hat{\rho}_m\}$:

$$\hat{\Pi}_m = \bigoplus_{l=0}^{L-1} \hat{\Pi}_{m;l}. \tag{40}$$

Proof. From Theorem 4, there exists an unambiguous measurement $\{\hat{X}_m\}$ that is expressed as $\{\hat{X}_m = \bigoplus_{l=0}^{L-1} \hat{X}_{m;l}\}$, with $\hat{X}_{m;l}$ defined in $\mathcal{X}_l$. For each $l \in \mathcal{I}_L$, let $P_{\mathrm{C};l}(\{\hat{Y}_{m;l}\})$ be the probability of correct detection of the POVM $\{\hat{Y}_{m;l}\}$ for $\{\hat{\rho}_{m;l}\}$. We have

$$P_{\mathrm{C}}\left(\left\{\bigoplus_{l=0}^{L-1} \hat{Y}_{m;l}\right\}\right) = \sum_{l=0}^{L-1} W_l P_{\mathrm{C};l}(\{\hat{Y}_{m;l}\}). \tag{41}$$

Since $\{\hat{\Pi}_{m;l}\}$ is an optimal unambiguous measurement for $\{\hat{\rho}_{m;l}\}$, $P_{\mathrm{C};l}(\{\hat{\Pi}_{m;l}\}) \geqslant P_{\mathrm{C};l}(\{\hat{X}_{m;l}\})$. Therefore, from Eq. (41), $P_{\mathrm{C}}(\{\hat{\Pi}_m\}) \geqslant P_{\mathrm{C}}(\{\hat{X}_m\})$. Since $\{\hat{X}_m\}$ is an optimal unambiguous measurement, $P_{\mathrm{C};l}(\{\hat{\Pi}_{m;l}\}) = P_{\mathrm{C};l}(\{\hat{X}_{m;l}\})$ holds. Thus, $\{\hat{\Pi}_m\}$ is also an optimal unambiguous measurement. ■

D. SRM, SIM, and EPM

Here we consider some suboptimal measurements, that is, the SRM, the scaled inverse measurement (SIM), and the equal probability measurement (EPM). Eldar *et al.* derived that the SRM, the SIM, and the EPM for a GU (CGU) state set are also GU (CGU) and that these measurements are optimal under certain constraints [13,18,19]. Here we extend these results to a group-covariant state set.

The SRM $\{\hat{\Pi}_m^{(\mathrm{SRM})}\} \in \mathcal{M}$ is defined by

$$\hat{\Pi}_m^{(\mathrm{SRM})} = \hat{G}^{-\frac{1}{2}}\hat{\rho}_m\hat{G}^{-\frac{1}{2}}, \quad m \in \mathcal{I}_M, \quad \hat{\Pi}_M^{(\mathrm{SRM})} = 0. \tag{42}$$

A sufficient condition for the SRM to be a minimum error measurement is given in Ref. [13].

The SIM $\{\hat{\Pi}_m^{(\mathrm{SIM})}\} \in \mathcal{M}$ is defined by

$$\begin{aligned} \hat{\Pi}_m^{(\mathrm{SIM})} &= \frac{1-p}{N}\hat{G}^{-1}\hat{\rho}_m\hat{G}^{-1}, \quad m \in \mathcal{I}_M, \\ \hat{\Pi}_M^{(\mathrm{SIM})} &= \hat{1} - \sum_{m=0}^{M-1} \hat{\Pi}_m^{(\mathrm{SIM})}. \end{aligned} \tag{43}$$

It follows that $P_{\mathrm{I}}(\{\hat{\Pi}_m^{(\mathrm{SIM})}\}) = p$ holds. To satisfy Eq. (1), $p \geqslant p_{\min} = 1 - N\lambda_{\min}$ is required, where $\lambda_{\min}$ is the smallest eigenvalue of $\hat{G}$. Eldar showed a sufficient condition for the SIM to be an optimal inconclusive measurement [18].

The SIM with $p = p_{\min}$, which is called the EPM, is known to be an optimal unambiguous measurement for any GU linearly independent pure state set [19].

Proposition 11. Let $\mathcal{P} = \{\hat{\rho}_m\}$ ($m \in \mathcal{I}_M$) be a $\mathcal{G}$-symmetric state set. The SRM and the SIM for $\mathcal{P}$ are both $\mathcal{G}$ symmetric.

According to Proposition IV D, the EPM, which is a special case of the SIM, is also $\mathcal{G}$ symmetric.

Proof. From Eq. (20) and $g\circ G = G$, we obtain $g\circ(\hat{G}^{-1/2}) = (g\circ\hat{G})^{-1/2} = \hat{G}^{-1/2}$ and $g\circ(\hat{G}^{-1}) = \hat{G}^{-1}$. Therefore, the SRM $\{\hat{\Pi}_m^{(\mathrm{SRM})}\}$ and the SIM $\{\hat{\Pi}_m^{(\mathrm{SIM})}\}$ satisfy, for any $m \in \mathcal{I}_M$,

$$g\circ\hat{\Pi}_m^{(\mathrm{SRM})} = \hat{G}^{-\frac{1}{2}}\hat{\rho}_{g\circ m}\hat{G}^{-\frac{1}{2}} = \hat{\Pi}_{g\circ m}^{(\mathrm{SRM})}, \tag{44}$$

$$g\circ\hat{\Pi}_m^{(\mathrm{SIM})} = \frac{1-p}{N}\hat{G}^{-1}\hat{\rho}_{g\circ m}\hat{G}^{-1} = \hat{\Pi}_{g\circ m}^{(\mathrm{SIM})}. \tag{45}$$

Thus, $\{\hat{\Pi}_m^{(\mathrm{SRM})}\}$ and $\{\hat{\Pi}_m^{(\mathrm{SIM})}\}$ are both $\mathcal{G}$ symmetric. ■

Consider a $\mathcal{G}$-symmetric state set $\mathcal{P} = \{\hat{\rho}_m\}$ ($m \in \mathcal{I}_M$). $\{g\circ\hat{\rho}_m : \forall g \in \mathcal{G}\}$ is called the orbit of $\hat{\rho}_m \in \mathcal{P}$ under $\mathcal{G}$. Let $\{\mathcal{O}_k\}$ ($k \in \mathcal{I}_O$) be the entire set of orbits of $\hat{\rho}_m$ under $\mathcal{G}$, where O is the number of orbits. Note that $\mathcal{G}$ is transitive if and only if $O = 1$.

Theorem 12. Consider a $\mathcal{G}$-symmetric state set $\mathcal{P} = \{\hat{\rho}_m\}$ ($m \in \mathcal{I}_M$). Let $s_k \in \mathcal{I}_M$ ($k \in \mathcal{I}_O$) be a number such that $\hat{\rho}_{s_k}$ is an element of the orbit $\mathcal{O}_k$. Let $r_m = \mathrm{rank}\hat{\rho}_m$. ψ_m denotes the $N \times r_m$ matrix such that $\hat{\rho}_m = \psi_m\psi_m^\dagger$ via the eigendecomposition of $\hat{\rho}_m$. The following properties are satisfied.

(1) If, for any $k \in \mathcal{I}_O$,

$$\psi_{s_k}^\dagger \hat{G}^{-1/2} \psi_{s_k} = \alpha \hat{1}, \tag{46}$$

where $\alpha \in \mathbf{R}_0$ is a constant independent of m, then the SRM is a minimum error measurement.

(2) If, for any $k \in \mathcal{I}_O$,

$$\psi_{s_k}^\dagger \hat{G}^{-1} \psi_{s_k} = \beta \hat{1}, \tag{47}$$

where $\beta \in \mathbf{R}_0$ is a constant independent of m and $p \geqslant p_{\min} = 1 - N\lambda_{\min}$, then the SIM is an optimal inconclusive measurement.

(3) Let q be the number of distinct singular values of the matrix of columns $\psi_0, \ldots, \psi_{M-1}$. Suppose that $\mathcal{P}$ is a linearly independent pure state set. If, for any $k \in \mathcal{I}_O$ and any natural number t satisfying $t \leqslant q$,

$$\psi_{s_k}^\dagger \hat{G}^{t/2-1} \psi_{s_k} = \gamma_t, \tag{48}$$

where $\gamma_1, \ldots, \gamma_q \in \mathbf{R}_0$ are constants independent of m, then the EPM is an optimal unambiguous measurement.

(4) If $\mathcal{P}$ is a pure state set and $\mathcal{G}$ is transitive, then the SRM and the SIM are a minimum error measurement and an optimal inconclusive measurement with $p \geqslant p_{\min}$, respectively. Moreover, if $\mathcal{P}$ is linearly independent, then the EPM is an optimal unambiguous measurement.

Proof. According to Theorem 1 of Ref. [13], the fact that Eq. (46) is satisfied for any $m \in \mathcal{I}_M$, not only $m \in \{s_k\}$ ($k \in \mathcal{I}_O$), means that the SRM is a minimum error measurement. In a similar fashion, according to Theorem 3 of Ref. [18] and also Theorem 3 of Ref. [19], if Eq. (47) is satisfied for any $m \in \mathcal{I}_M$ then the SIM is an inconclusive measurement, and if Eq. (48) is satisfied for any $m \in \mathcal{I}_M$ then the EPM is an unambiguous measurement.

Now suppose that for some $u \in \mathbf{R}$, we have that, for any $k \in \mathcal{I}_O$,

$$\psi_{s_k}^\dagger \hat{G}^{u} \psi_{s_k} = c_u \hat{1}, \tag{49}$$

where $c_u \in \mathbf{R}_0$ is a constant independent of m. To prove that properties 1–3 of Theorem 12 hold, it is sufficient to show that $\psi_m^\dagger \hat{G}^u \psi_m = c_u \hat{1}$ for any $m \in \mathcal{I}_M$. Premultiplying by ψ_{s_k} and postmultiplying by $\psi_{s_k}^\dagger$ on both sides of Eq. (49) gives $\hat{\rho}_{s_k} \hat{G}^u \hat{\rho}_{s_k} = c_u \hat{\rho}_{s_k}$. Since $m \in \mathcal{I}_M$ can be expressed by $m = g \circ s_k$ ($g \in \mathcal{G}$) by using $k \in \mathcal{I}_O$ such that $\hat{\rho}_m \in \mathcal{O}_k$, we have

$$\begin{aligned} \hat{\rho}_m \hat{G}^u \hat{\rho}_m &= \hat{\rho}_{g \circ s_k} \hat{G}^u \hat{\rho}_{g \circ s_k} = g \circ \left(\hat{\rho}_{s_k} \hat{G}^u \hat{\rho}_{s_k}\right) \\ &= g \circ \left(c_u \hat{\rho}_{s_k}\right) = c_u \hat{\rho}_m. \end{aligned} \tag{50}$$

Let $\phi_m = \psi_m (\psi_m^\dagger \psi_m)^{-1}$. Since $\psi_m^\dagger \phi_m = \hat{1}$ and Eq. (50),

$$\psi_m^\dagger \hat{G}^u \psi_m = \phi_m^\dagger \hat{\rho}_m \hat{G}^u \hat{\rho}_m \phi_m = c_u \phi_m^\dagger \hat{\rho}_m \phi_m = c_u \hat{1}. \tag{51}$$

We finally show that property 4 of Theorem 12 holds. Suppose that $\mathcal{P}$ is a pure state set and $\mathcal{G}$ is transitive, i.e., $O = 1$. Equations (46)–(48) are satisfied, since $\psi_m^\dagger \hat{G}^u \psi_m$ is scalar and $\{s_k\}$ contains only one element. ■

V. EXAMPLES

We now consider two examples of group-covariant state sets.

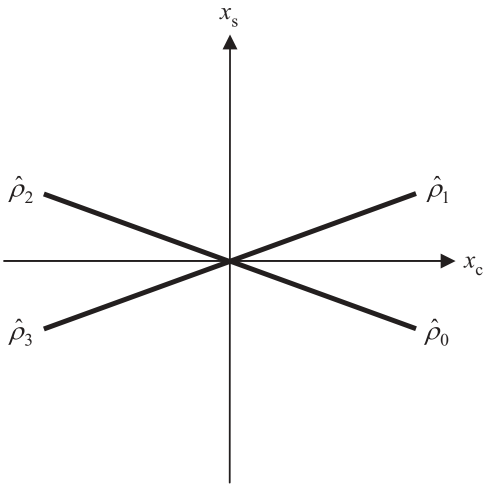

FIG. 2. Phase-space representation of an example of a group-covariant state set with respect to a transitive group $\mathcal{G} = \{e, g_1, g_2, g_3\}$. $\{\hat{\rho}_m\}$ is the set of the coherent states of light expressed by Eq. (52). Each element in $\mathcal{G}$ corresponds to one of the operations of Eq. (53).

A. Generalized GU state set

Consider a group-covariant state set consisting of four coherent states of light $\mathcal{P} = \{\hat{\rho}_m\}$ ($m \in \mathcal{I}_4$) expressed by

$$\begin{aligned} &\hat{\rho}_0 = |\alpha\rangle\langle\alpha|/4, \quad \hat{\rho}_1 = |\alpha^*\rangle\langle\alpha^*|/4, \\ &\hat{\rho}_2 = |-\alpha\rangle\langle-\alpha|/4, \quad \hat{\rho}_3 = |-\alpha^*\rangle\langle-\alpha^*|/4, \end{aligned} \tag{52}$$

where $|\alpha\rangle$ is the eigenvector of the annihilation operator corresponding to the eigenvalue $\alpha \notin \mathbf{R}$. The phase-space representation of an example of the state set $\mathcal{P}$ is illustrated in Fig. 2.

$\mathcal{P}$ is a $\mathcal{G}$-symmetric state set where $\mathcal{G} = \{e, g_1, g_2, g_3\}$. The corresponding operations in $\mathcal{F}$ are

$$\begin{aligned} &\pi_e(\hat{T}) = \hat{T}, \quad \pi_{g_1}(\hat{T}) = \hat{T}^*, \\ &\pi_{g_2}(\hat{T}) = \hat{U}\hat{T}\hat{U}^\dagger, \quad \pi_{g_3}(\hat{T}) = \hat{U}\hat{T}^*\hat{U}^\dagger, \end{aligned} \tag{53}$$

where the asterisk indicates the operation satisfying $(|\alpha\rangle\langle\alpha|)^* = |\alpha^*\rangle\langle\alpha^*|$ and where $\hat{U}$ is the unitary operator satisfying $\hat{U}|\beta\rangle = |-\beta\rangle$ for any coherent state $|\beta\rangle$. The group action of $\mathcal{G}$, $g \circ m$ ($g \in \mathcal{G}, m \in \mathcal{I}_M$), is reported in Table II.

Since the action of $\mathcal{G}$ on $\mathcal{P}$ is free and transitive, $\mathcal{P}$ can be regarded as a generalized GU state set in Ref. [13] (or a GU state set with respect to unitary and antiunitary operators). According to Theorem 12, the SRM and the SIM are a minimum error measurement and an optimal inconclusive measurement with $p \geqslant p_{\min}$, respectively. Moreover, since $\mathcal{P}$ is linearly independent, the EPM is an optimal unambiguous

TABLE II. The group action of $\mathcal{G}$ on the generalized GU state set expressed by Eq. (52).

$g \in \mathcal{G}$	$g \circ 0$	$g \circ 1$	$g \circ 2$	$g \circ 3$
e	0	1	2	3
g_1	1	0	3	2
g_2	2	3	0	1
g_3	3	2	1	0

TABLE III. The group action of $\mathcal{G}'$ on the three mirror-symmetric state set expressed by Eq. (54).

$g \in \mathcal{G}$	$g \circ 0$	$g \circ 1$	$g \circ 2$
K	0	1	2
$g_2 K$	1	0	2

measurement. Note that a closed-form analytical expression for an optimal inconclusive measurement for a generalized pure GU state set with arbitrary p was derived [32].

B. Three mirror-symmetric state set

We give an example of a mirror-symmetric state set consisting of three states $\mathcal{P} = \{\hat{\rho}_m = \xi_m |\nu_m\rangle\langle\nu_m|\}$ $(m \in \mathcal{I}_3)$ expressed as

$$\begin{aligned} |\nu_0\rangle &= \cos\theta\,|+\rangle + \sin\theta\,|-\rangle\,, \\ |\nu_1\rangle &= \cos\theta\,|+\rangle - \sin\theta\,|-\rangle\,, \quad |\nu_2\rangle = |+\rangle\,, \end{aligned} \tag{54}$$

where $0 < \theta < \pi/2$, $\xi_0 = \xi_1 = \xi$, and $\xi_2 = 1 - 2\xi$ $(0 < \xi < 1/2)$. $\{|+\rangle, |-\rangle\}$ are orthonormal basis. A minimum error measurement of the mirror-symmetric state set is derived by Andersson *et al.* [11].

Let $\mathcal{G} = \{e, g_1, g_2, g_3\}$. $\mathcal{P}$ is a $\mathcal{G}$-symmetric state set in which the corresponding operations in $\mathcal{F}$ are given by the same expression as Eq. (53), except that $U = |+\rangle\langle+| - |-\rangle\langle-|$ and that the operation denoted by the asterisk satisfies $(|+\rangle\langle+|)^* = |+\rangle\langle+|$ and $(|-\rangle\langle-|)^* = |-\rangle\langle-|$. The action of $\mathcal{G}$ on $\mathcal{P}$ is not faithful since any state is invariant under the action of the group $\mathcal{K} = \{e, g_1\}$. As described in Sec. IV C, the action of the quotient group $\mathcal{G}' = \mathcal{G}/\mathcal{K} = \{K, g_2 K\}$ is faithful. The group action of $\mathcal{G}'$, $g \circ m$ $(g \in \mathcal{G}', m \in \mathcal{I}_3)$, is reported in Table III.

Let us consider group covariant optimal measurements for the state set. Since $\mathcal{P}$ is a pure state set that is not linearly independent, unambiguous detection between the states is not possible. Eldar showed that an optimal inconclusive measurement, $\{\hat{\Pi}^{(i)}_m\}$, satisfies $\mathrm{rank}\,\hat{\Pi}^{(i)}_m \leqslant \mathrm{rank}\,\hat{\rho}_m$ $(m \in \mathcal{I}_3)$ [18]. Thus, $\hat{\Pi}^{(i)}_m$ can be expressed as $\hat{\Pi}^{(i)}_m = |\pi_m\rangle\langle\pi_m|$ $(m \in \mathcal{I}_3)$. Since every $\hat{\Pi}^{(i)}_m$ is invariant under the action of the group $\mathcal{K}$, we have $\hat{\Pi}^{(i)*}_m = \hat{\Pi}^{(i)}_m$ for any $m \in \mathcal{I}_4$. Since $\{\hat{\Pi}^{(i)}_m\} \in \mathcal{M}^{(\mathcal{G}')}$, it follows that $\hat{U}\hat{\Pi}^{(i)}_0\hat{U}^\dagger = \hat{\Pi}^{(i)}_1$ and $\hat{U}\hat{\Pi}^{(i)}_2\hat{U}^\dagger = \hat{\Pi}^{(i)}_2$ are satisfied. Therefore, $|\pi_m\rangle$ is expressed as

$$\begin{aligned} |\pi_0\rangle &= a_1\,|+\rangle + a_2\,|-\rangle\,, \\ |\pi_1\rangle &= a_1\,|+\rangle - a_2\,|-\rangle\,, \quad |\pi_2\rangle = a_3\,|+\rangle\,, \end{aligned} \tag{55}$$

where $a_1 \in \mathbf{R}$ and $a_2, a_3 \in \mathbf{R}_0$. (Note that whereas $|\pi_2\rangle = a_4\,|-\rangle$ $(a_4 \in \mathbf{R})$ also satisfies the above symmetry conditions, no optimal inconclusive measurement satisfies $|\pi_2\rangle = a_4\,|-\rangle$ since $\langle\nu_2|-\rangle = 0$.] From Eq. (1) we obtain $a_2 \leqslant 1/\sqrt{2}$ and $a_3 \leqslant \sqrt{1 - 2a_1^2}$.

A minimum error measurement, $\{\hat{\Pi}^{(e)}_m\}$, can be considered as a special case of an optimal inconclusive measurement with $p = 0$. Thus, $\hat{\Pi}^{(e)}_m$ $(m \in \mathcal{I}_3)$ can also be expressed as $\hat{\Pi}^{(e)}_m = |\pi_m\rangle\langle\pi_m|$, satisfying Eq. (55). Moreover, since $\sum_{m=0}^{2} \hat{\Pi}^{(e)}_m = \hat{1}$, we obtain $a_2 = 1/\sqrt{2}$ and $a_3 = \sqrt{1 - 2a_1^2}$. These results are the same as those found by Andersson *et al.* [11].

VI. CONCLUSION

In this paper we have considered a group covariant quantum state set where each element in a group corresponds to the operation represented by a unitary or antiunitary operator. This class of quantum state sets includes the GU state sets and the self-symmetric state sets. We have shown that for any quantum measurement for a group-covariant state set with a certain fraction of inconclusive results, a group covariant quantum measurement exists with respect to the same group with the same probabilities of correct detection and a detection error.

We have also shown that for any group-covariant state set, there exists a minimum error measurement, an optimal inconclusive measurement, and an optimal unambiguous measurement, all of which are group covariant. We then derived that, for a group-covariant state set, a Lagrange operator having the same symmetry associated with an optimal measurement exists. We have described sufficient conditions under which the SRM, SIM, or EPM is optimal, which are extensions of the results of Eldar *et al.* [13,18,19].

ACKNOWLEDGMENT

T.S.U. was supported (in part) by JSPS Kakenhi Grant No. 24360151.

[1] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).

[2] A. S. Holevo, J. Multivar. Anal. **3**, 337 (1973).

[3] H. P. Yuen, R. S. Kennedy, and M. Lax, IEEE Trans. Inf. Theory **21**, 125 (1975).

[4] V. P. Belavkin, Radio Eng. Electron. Phys. **20**, 39 (1975).

[5] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, Int. J. Theor. Phys. **36**, 1269 (1997).

[6] T. S. Usuda, I. Takumi, M. Hata, and O. Hirota, Phys. Lett. A **256**, 104 (1999).

[7] Y. C. Eldar and G. D. Forney Jr., IEEE Trans. Inf. Theory **47**, 858 (2001).

[8] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).

[9] A. Chefles and S. M. Barnett, Phys. Lett. A **250**, 223 (1998).

[10] A. Chefles and S. M. Barnett, J. Mod. Opt. **45**, 1295 (1998).

[11] E. Andersson, S. M. Barnett, C. R. Gilson, and K. Hunter, Phys. Rev. A **65**, 052308 (2002).

[12] T. S. Usuda, S. Usami, I. Takumi, and M. Hata, Phys. Lett. A **305**, 125 (2002).

[13] Y. C. Eldar, A. Megretski, and G. C. Verghese, IEEE Trans. Inf. Theory **50**, 1198 (2004).

[14] K. Kato and O. Hirota, IEEE Trans. Inf. Theory **49**, 3312 (2003).

[15] C. L. Chou and L. Y. Hsu, Phys. Rev. A **68**, 042305 (2003).

[16] T. Sawada, T. Tsuchimoto, and T. S. Usuda, Proc. QCMC **2007**, 405 (2007).

[17] G. Cariolaro and A. Vigato, in *IEEE Information Theory Workshop, ITW'11*, Paraty, Brazil, October 18 (IEEE, New York, 2011), pp. 242–246.

[18] Y. C. Eldar, Phys. Rev. A **67**, 042309 (2003).

[19] Y. C. Eldar, IEEE Trans. Inf. Theory **49**, 446 (2003).

[20] K. Nakahira and T. S. Usuda, IEEE Trans. Inf. Theory **58**, 1215 (2012).

[21] A. S. Holevo, Probab. Math. Stat. **3**, 113 (1982).

[22] R. S. Kennedy, MIT Res. Lab. Electron. Quarter. Progr. Rep. **110**, 142 (1973).

[23] Y. C. Eldar, M. Stojnic, and B. Hassibi, Phys. Rev. A **69**, 062318 (2004).

[24] A. Chefles, Phys. Lett. A **239**, 339 (1998).

[25] E. B. Davies, IEEE Trans. Inf. Theory **24**, 596 (1978).

[26] T. Decker, IEEE Trans. Inf. Theory **55**, 2375 (2009).

[27] E. P. Wigner, J. Math. Phys. **1**, 409 (1960).

[28] I. M. Isaacs, *Finite Group Theory* (American Mathematical Society, Providence, RI, 2008).

[29] J. Fiurášek and M. Ježek, Phys. Rev. A **67**, 012321 (2003).

[30] A. S. Holevo, Probl. Inf. Transm. **10**, 317 (1974).

[31] A. Assalini, G. Cariolaro, and G. Pierobon, Phys. Rev. A **81**, 012315 (2010).

[32] K. Nakahira, T. S. Usuda, and K. Kato, Phys. Rev. A **86**, 032316 (2012).