# Minimal covariant observables identifying all pure states

Claudio Carmeli*
*D.I.M.E., Università di Genova, Via Cadorna 2, I-17100 Savona, Italy,*
*and I.N.F.N., Sezione di Genova, Via Dodecaneso, 33, I-16146 Genova, Italy*

Teiko Heinosaari†
*Turku Centre for Quantum Physics, Department of Physics and Astronomy, University of Turku, Finland*

Alessandro Toigo‡
*Dipartimento di Matematica, Politecnico di Milano,*
*Piazza Leonardo da Vinci 32, I-20133 Milano, Italy, and I.N.F.N.,*
*Sezione di Milano, Via Celoria 16, I-20133 Milano, Italy*

It has been recently shown that an observable that identifies all pure states of a $d$-dimensional quantum system has minimally $4d-4$ outcomes or slightly less (the exact number depending on the dimension $d$) [1]. However, no simple construction of this type of observable with minimal number of outcomes is known. In this work we investigate the possibility to have a covariant observable that identifies all pure states and has minimal number of outcomes for this purpose. It is shown that the existence of these kind of observables depends on the dimension of the Hilbert space. The fact that these kind of observables fail to exist in some dimensions indicates that the dual pair of observables – pure states lacks the symmetry that the dual pair of observables – states has.

PACS numbers: 03.65.Aa, 03.65.Wj, 03.65.Fd

## I. INTRODUCTION

An observable is called *informationally complete* if it identifies all states [2]. An informationally complete observable acting on a finite dimensional Hilbert space of dimension $d$ is called *minimal* if it has as small number of outcomes as possible, and this smallest number is known to be $d^2$ [3].

Often, it is enough to concentrate on pure states. For instance, we may have a prior knowledge that the otherwise unknown state is pure and we want to identify it. A measurement that identifies all pure states may not be able to identify all states. In particular, this kind of measurement can have have less outcomes than $d^2$ whenever $d \geq 3$. The minimal number of outcomes is roughly $4d-4$ and always less or equal to this [1]. In spite of the quite precise knowledge about the minimal number of outcomes, a simple or instructive construction of an observable that identifies all pure states and has minimal number of outcomes for this purpose is not known.

The present paper concentrates on minimal *covariant* observables identifying all pure states. To explain the problem, we start by recalling the standard construction of a minimal covariant observable identifying all states. First, fix an orthonormal basis $\{h_0, \ldots, h_{d-1}\}$ for a $d$-dimensional Hilbert space $\mathcal{H}_d$ and let $U$ be the shift operator in this basis, i.e., $Uh_\ell = h_{\ell+1}$, with summation modulo $d$. Then $j \mapsto U^j$ is a unitary representation of the cyclic group $\mathbb{Z}_d$. We then define $V$ to be the unitary operator $Vh_\ell = e^{2\pi i \ell/d} h_\ell$, hence giving another unitary representation $k \mapsto V^k$ of the group $\mathbb{Z}_d$. The operators $U$ and $V$ commute up to a scalar factor, $VU = e^{2\pi i/d} UV$, thus the combined map $W(j,k) := U^j V^k$ is a projective unitary representation of the product group $\mathbb{Z}_d \times \mathbb{Z}_d$. By fixing a positive operator $M$ satisfying $\mathrm{tr}\,[M] = 1/d$ and setting

$$\mathsf{M}(j,k) := W(j,k) M W(j,k)^* \,, \qquad j,k \in \mathbb{Z}_d \tag{1}$$

we obtain an observable $\mathsf{M}$ with $d^2$ outcomes. This construction also guarantees that $\mathsf{M}$ is *covariant*, i.e.,

$$W(j',k') \mathsf{M}(j,k) W(j',k')^* = \mathsf{M}(j+j', k+k') \tag{2}$$

for all $(j,k), (j',k') \in \mathbb{Z}_d \times \mathbb{Z}_d$. In order to obtain informationally complete observable one has to choose $M$ such that $\mathrm{tr}\,[MW(j,k)] \neq 0$ for all $j,k \in \mathbb{Z}_d$; see e.g. [4], [5].

In this paper we address the following question: Is it possible to construct a covariant observable that identifies all pure states and has the minimal number of outcomes for this purpose? For dimension 2 the answer is positive since a qubit observable identifies all pure states only if it identifies all states [1], thus the previous construction gives an observable with the desired properties. One could presume that a similar construction should be possible in all dimensions, perhaps using a different symmetry group. However, we prove that the answer to the existence question depends on the dimension of the Hilbert space. More precisely, we construct a class of observables with the required properties in dimension 3 using the group of unit quaternions, but we show that they do not exist in dimension 7 (and certain other dimensions).

*Electronic address: claudio.carmeli@gmail.com
†Electronic address: teiko.heinosaari@utu.fi
‡Electronic address: alessandro.toigo@polimi.it

An interesting additional fact is that while the previously sketched general construction uses an irreducible projective representation of an abelian group, the analogous construction for a pure-state informationally complete observable in dimension 3 is forced to use a reducible unitary representation of a non-abelian group.

Our investigation is organized as follows. Sections II and III give some essential background information on pure-state informationally complete observables and covariant observables, respectively. In Section IV we derive some general conditions for the existence of covariant pure-state informationally complete observables. Then, in Section V we add the requirement of minimal number of outcomes and prove the main results. Finally, in Section VI we outline our conclusions and sketch some further developments and generalizations.

## II. PURE-STATE INFORMATIONALLY COMPLETE OBSERVABLES

Throughout this paper, by a *Hilbert space* we will always mean a finite dimensional complex Hilbert space. If $\mathcal{H}$ is a Hilbert space, we denote by $\mathcal{L}(\mathcal{H})$ the vector space of all linear operators on $\mathcal{H}$. It is a Hilbert space itself when equipped with the Hilbert-Schmidt inner product,

$$\langle L_1 \,|\, L_2 \rangle_{HS} = \mathrm{tr}\,[L_1^* L_2] \ .$$

A quantum state is described by a positive operator $\varrho \in \mathcal{L}(\mathcal{H})$ satisfying $\mathrm{tr}\,[\varrho] = 1$; it is a pure state if $\varrho$ is a 1-dimensional projection.

Quantum observables are described and identified with positive operator valued measures (POVMs). A POVM with finite number of outcomes is a mapping $\mathsf{M}$ from a finite set $\Omega$ into positive operators on $\mathcal{H}$, which is required to satisfy the normalization $\sum_x \mathsf{M}(x) = \mathbb{1}$; here $\mathbb{1}$ is the identity operator on $\mathcal{H}$. The probability of obtaining an outcome $x$ when the system is in a state $\varrho$ is $\mathrm{tr}\,[\varrho \mathsf{M}(x)]$.

We will be interested on the following two properties.

**Definition 1.** An observable $\mathsf{M}$ is called

(a) *informationally complete (IC)* if for any two different states $\varrho_1, \varrho_2$, there is at least one outcome $x \in \Omega$ such that $\mathrm{tr}\,[\varrho_1 \mathsf{M}(x)] \neq \mathrm{tr}\,[\varrho_2 \mathsf{M}(x)]$.

(b) *pure-state informationally complete (PIC)* if for any two different pure states $\varrho_1, \varrho_2$, there is at least one outcome $x \in \Omega$ such that $\mathrm{tr}\,[\varrho_1 \mathsf{M}(x)] \neq \mathrm{tr}\,[\varrho_2 \mathsf{M}(x)]$.

To be able to write down mathematical criteria for the above properties, we introduce some additional notation. For each observable $\mathsf{M}$, we denote by $\mathcal{S}_\mathsf{M}$ the linear span of the range of $\mathsf{M}$, i.e.,

$$\mathcal{S}_\mathsf{M} := \mathrm{span}\,\{\mathsf{M}(x) : x \in \Omega\} = \{\Sigma_x c_x \mathsf{M}(x) : c_x \in \mathbb{C}\}\,.$$

It is well-known that an observable $\mathsf{M}$ is informationally complete if and only if $\mathcal{S}_\mathsf{M} = \mathcal{L}(\mathcal{H})$ [6].

For any subset $\mathcal{S} \subseteq \mathcal{L}(\mathcal{H})$, we denote by $\mathcal{S}^\perp$ the orthogonal complement of $\mathcal{S}$ in the Hilbert-Schmidt inner product. In particular, for each observable $\mathsf{M}$ we have

$$\begin{aligned}\mathcal{S}_\mathsf{M}^\perp =& \{T \in \mathcal{L}(\mathcal{H}) : \mathrm{tr}\,[T^* S] = 0 \quad \forall S \in \mathcal{S}_\mathsf{M}\} \\ =& \{T \in \mathcal{L}(\mathcal{H}) : \mathrm{tr}\,[T \mathsf{M}(x)] = 0 \quad \forall x \in \Omega\}\,.\end{aligned}$$

Clearly, $\mathcal{S}_\mathsf{M}^\perp$ is a linear subspace of $\mathcal{L}(\mathcal{H})$ and $\mathrm{tr}\,[T] = 0$ for every $T \in \mathcal{S}_\mathsf{M}^\perp$ because

$$\mathrm{tr}\,[T] = \mathrm{tr}\,[T\mathbb{1}] = \sum_x \mathrm{tr}\,[T\mathsf{M}(x)] = 0\,.$$

If $\mathcal{H}$ is $d$-dimensional, then $\mathcal{L}(\mathcal{H})$ has dimension $d^2$. Since $\mathcal{L}(\mathcal{H})$ can be written as $\mathcal{L}(\mathcal{H}) = \mathcal{S}_\mathsf{M} \oplus \mathcal{S}_\mathsf{M}^\perp$, we obtain

$$\dim(\mathcal{S}_\mathsf{M}) + \dim(\mathcal{S}_\mathsf{M}^\perp) = d^2\,.$$

Notice that if $\mathsf{M}$ is injective and the set $\{\mathsf{M}(x) : x \in \Omega\}$ is linearly independent, then $\dim(\mathcal{S}_\mathsf{M})$ is just the number of outcomes of $\mathsf{M}$.

We recall the following result from [1].

**Proposition 1.** *An observable $\mathsf{M}$ is pure-state informationally complete if and only if every nonzero selfadjoint operator in $\mathcal{S}_\mathsf{M}^\perp$ has rank 3 or more.*

If $\mathcal{S}_\mathsf{M}^\perp = \{0\}$ (equivalently $\mathcal{S}_\mathsf{M} = \mathcal{L}(\mathcal{H})$), then the condition in Proposition 1 is satisfied. But then $\mathsf{M}$ is actually informationally complete with respect to all states and must have at least $d^2$ outcomes.

To obtain an observable $\mathsf{M}$ that is pure-state informationally complete and has as few outcomes as possible, we obviously need to choose $\mathcal{S}_\mathsf{M}$ to have as small dimension as possible while assuring that the condition stated in Proposition 1 holds. The first basic question then arises:

> If a linear subspace $\mathcal{S} \subseteq \mathcal{L}(\mathcal{H})$ is given, is it possible to find an observable $\mathsf{M}$ such that $\mathcal{S} = \mathcal{S}_\mathsf{M}$?

An easy construction [1] shows that the question has an affirmative answer if and only if

$$\mathbb{1} \in \mathcal{S} \qquad \text{and} \qquad \mathcal{S}^* = \mathcal{S}\,, \tag{3}$$

where the last condition means that $L^* \in \mathcal{S}$ whenever $L \in \mathcal{S}$. Moreover, in this case there exists $\mathsf{M}$ with exactly $\dim(\mathcal{S})$ outcomes such that $\mathcal{S} = \mathcal{S}_\mathsf{M}$, but not with less.

A more complicated task is to deduce the smallest possible dimension of a subspace $\mathcal{S} \subseteq \mathcal{L}(\mathcal{H})$ satisfying (3) and the criterion of Proposition 1, hence giving the minimal number of outcomes for a PIC observable. It was proved in [1] that the minimal number of outcomes for a PIC observable in $d$-dimensional Hilbert space is $4d - 4 - \delta(d)$, where $0 \leq \delta(d) \leq 2\log_2(d)$. The minimal numbers for the dimensions $2 - 15$ are listed in Table I.

TABLE I: The minimal number of outcomes for a PIC observable in the dimensions $2-15$. The exact value is not known in every dimension, but the uncertainty is at most $2\log_2(d)$.

| dimension | min # of outcomes |
|---|---|
| 2 | 4 |
| 3 | 8 |
| 4 | 10 |
| 5 | 16 |
| 6 | 18 |
| 7 | 23 |
| 8 | 24 or 25 |
| 9 | 32 |
| 10 | 34 |
| 11 | 39 |
| 12 | 40 or 41 |
| 13 | 47 |
| 14 | 48 or 49 |
| 15 | 54 |

## III. COVARIANT OBSERVABLES

### A. Projective unitary representations

The usual complication in any implementation of symmetry in a quantum system is that we cannot apriori restrict to unitary representations; instead, we have to deal with more general objects of projective unitary representations. In this subsection we recall some basic concepts and results related to projective unitary representations of finite groups. For more details, we refer to [7].

Let $G$ be a finite group. (In the rest of this paper, all groups are assumed to be finite even if this is not constantly repeated.) A *projective unitary representation* of $G$ is a mapping $g \mapsto U(g)$ from $G$ into the set of unitary operators on $\mathcal{H}$ such that $U(e) = \mathbb{1}$ and

$$U(gh) = \omega(g,h)U(g)U(h)\,, \tag{4}$$

with $\omega(g,h) \in \mathbb{T}$ ($\mathbb{T}$ denoting the group of unimodular complex numbers). The mapping $\omega : G\times G \to \mathbb{T}$, defined through (4), is called the *multiplier* of $U$ and it is required to satisfy

$$\begin{aligned}&\omega(g,e) = \omega(e,g) = 1 \quad \forall g \in G\\ &\omega(g,hk)\omega(h,k) = \omega(g,h)\omega(gh,k) \quad \forall g,h,k \in G\,.\end{aligned}$$

Clearly, a unitary representation of $G$ is a special type of a projective unitary representation; in that case $\omega(g,h) = 1$ for all $g,h \in G$.

From the quantum theoretic point of view, only transformation of *rays* of vectors is relevant. Therefore, if we multiply unitary operators $U(g)$ with numbers $f(g) \in \mathbb{T}$, we get a new projective representation $g \mapsto f(g)U(g)$ but the transformation of rays has not been changed. Two projective unitary representations $U$ and $U'$ are called *similar* if there exists a function $f : G \to \mathbb{T}$ such that $U'(g) = f(g)U(g)$ for all $g \in G$. A projective unitary representation $U$ is similar to a unitary representation if and only if its multiplier $\omega$ is *exact*, i.e., there exists a function $f : G \to \mathbb{T}$ such that

$$\omega(g,h) = f(g)f(h)\overline{f(gh)} \qquad \forall g,h \in G\,. \tag{5}$$

Indeed, this is equivelent to $U$ being similar to the unitary representation $U'$ given by $U'(g) = f(g)U(g)$

**Example 1.** (*Cyclic groups*) Every projective unitary representation $U$ of the cyclic group $\mathbb{Z}_d$ is similar to a unitary representation. Namely, a repeated application of (4) shows that, for each $k \in \mathbb{Z}$, there exists $\alpha(k) \in \mathbb{T}$ such that

$$U(1)^k = \alpha(k)U(k\,(\mathrm{mod}\,d))\,. \tag{6}$$

Let $\alpha(d) = \mathrm{e}^{i\theta}$, $\theta \in \mathbb{R}$, and, for each $k \in \mathbb{Z}$, define

$$U'(k) := \left(\mathrm{e}^{-\frac{i\theta}{d}}U(1)\right)^k = \mathrm{e}^{-\frac{ik\theta}{d}}\alpha(k)U(k\,(\mathrm{mod}\,d))\,. \tag{7}$$

Clearly, $U'$ is a unitary representation of $\mathbb{Z}$. Moreover, $U'$ factors to a unitary representation of $\mathbb{Z}_d$ as

$$U'(d) = \mathrm{e}^{-i\theta}\alpha(d)\mathbb{1} = \mathbb{1}\,.$$

Finally, $U$ and $U'$ are similar by (7).

In our later investigations the following criterion will be useful. (Recall that a subspace $\mathcal{K} \subset \mathcal{H}$ is called $U$-invariant if $U(g)v \in \mathcal{K}$ for all $g \in G$ and $v \in \mathcal{K}$.)

**Proposition 2.** *If a projective unitary representation $U$ has an invariant 1-dimensional subspace, then it is similar to a unitary representation.*

*Proof.* Let $U$ be a projective unitary representation with an invariant 1-dimensional subspace. Hence, there exists a nonzero vector $v \in \mathcal{H}$ such that $U(g)v \in \mathbb{C}v$ for all $g \in G$. We can thus define a map $f : G \to \mathbb{T}$ such that $U(g)v = f(g)v$. It follows that

$$\begin{aligned}f(gh)v &= U(gh)v = \omega(g,h)U(g)U(h)v\\ &= \omega(g,h)f(g)f(h)v\,.\end{aligned}$$

Therefore, $\omega(g,h) = f(gh)\overline{f(g)f(h)}$, hence $\omega$ is an exact multiplier. □

A useful trick when having a projective unitary representation $U$ is to pass from $U$ to a related unitary representation $\widetilde{U}$ that acts in the Hilbert space $\mathcal{L}(\mathcal{H})$ of operators. For each $g \in G$ and $L \in \mathcal{L}(\mathcal{H})$, we define

$$\widetilde{U}(g)L := U(g)LU(g)^*\,. \tag{8}$$

Notice that even if $U$ is a projective unitary representation, $\widetilde{U}$ is an ordinary unitary representation, since

$$\begin{aligned}\widetilde{U}(gh)L &= \omega(g,h)\overline{\omega(g,h)}U(g)U(h)LU(h)^*U(g)^* \\ &= \widetilde{U}(g)\widetilde{U}(h)L\,.\end{aligned}$$

Moreover, it is easy to see that $U(g)$ commutes with an operator $L \in \mathcal{L}(\mathcal{H})$ if and only if $\widetilde{U}(g)L = L$. Since every operator $U(g)$ commutes with the identity operator $\mathbb{1}$, we conclude that the 1-dimensional subspace $\mathbb{C}\mathbb{1}$ is invariant under $\widetilde{U}$. In particular, $\widetilde{U}$ is a reducible representation whenever $\dim \mathcal{H} \geq 2$.

### B. Structure of covariant observables

We will next recall some basic facts about covariant observables. More details and further references can be found e.g. in [8].

Let $H$ be a (proper) subgroup of the group $G$. In the following, we will choose $\Omega \equiv G/H$, i.e., our outcome space will be the quotient space consisting of left cosets $gH = \{gh : h \in H\}$, $g \in G$. We do not assume that $H$ is a normal subgroup, therefore $G/H$ need not be a group. However, there is a natural action of $G$ on $G/H$; for each $g' \in G$ and $gH \in \Omega$, we denote by $g' \cdot gH$ the left coset $g'gH$. This action is transitive, meaning that for any two points $g_1H, g_2H \in \Omega$, there exists $g \in G$ such that $g(g_1H) = g_2H$.

Let $U$ be a projective unitary representation of $G$. Then $G$ acts, on the one hand, on the outcome space $\Omega$, and on the other hand, on the space $\mathcal{L}(\mathcal{H})$ through the unitary representation $\widetilde{U}$. A covariant observable has the property of intertwining these two actions.

**Definition 2.** An observable $\mathsf{M}$ based on $\Omega$ is *$U$-covariant* if

$$\widetilde{U}(g)\mathsf{M}(x) = \mathsf{M}(g \cdot x) \tag{9}$$

for all $g \in G$, $x \in \Omega$.

It follows from (9) that

$$\widetilde{U}(g)\mathcal{S}_{\mathsf{M}} = \mathcal{S}_{\mathsf{M}} \tag{10}$$

for all $g \in G$, meaning that $\mathcal{S}_{\mathsf{M}}$ is a $\widetilde{U}$-invariant subspace. This implies that also $\mathcal{S}_{\mathsf{M}}^{\perp}$ is a $\widetilde{U}$-invariant subspace. The unitary representation $\widetilde{U}$ therefore splits into the direct sum

$$\widetilde{U} = \widetilde{U}^{\mathcal{S}_{\mathsf{M}}} \oplus \widetilde{U}^{\mathcal{S}_{\mathsf{M}}^{\perp}}\,, \tag{11}$$

where $\widetilde{U}^{\mathcal{S}_{\mathsf{M}}}$ and $\widetilde{U}^{\mathcal{S}_{\mathsf{M}}^{\perp}}$ are the restrictions of $\widetilde{U}$ to $\mathcal{S}_{\mathsf{M}}$ and $\mathcal{S}_{\mathsf{M}}^{\perp}$, respectively.

We also see that a $U$-covariant observable $\mathsf{M}$ must be of the form

$$\mathsf{M}(gH) = \widetilde{U}(g)M \tag{12}$$

for some positive operator $M \in \mathcal{L}(\mathcal{H})$. Namely, we denote $M \equiv \mathsf{M}(eH)$ for the identity element $e \in G$ and then (12) follows from (9). Notice that if $g', g \in G$ are such that $g' \in gH$, then $\mathsf{M}(g'H) = \mathsf{M}(gH)$, implying that

$$U(g)MU(g)^* = U(g')MU(g')^*\,. \tag{13}$$

This means that $[M, U(h)] = 0$ for all $h \in H$.

If we start from a positive operator $M \in \mathcal{L}(\mathcal{H})$ satisfying $[M, U(h)] = 0$ for all $h \in H$ and define $\mathsf{M}$ by formula (12), then the positivity and the covariance condition (9) holds but we need to check that $\sum_x \mathsf{M}(x) = \mathbb{1}$ in order to get an observable. This normalization is not automatically satisfied, and the suitable operators $M$ depend on the projective representation $U$.

**Example 2.** (*Irreducible projective representation*) Suppose that a projective unitary representation $U$ of $G$ is irreducible. Fix a nonzero positive operator $M \in \mathcal{L}(\mathcal{H})$ and define $\mathsf{M}$ on $G$ as $\mathsf{M}(g) = U(g)MU(g)^*$. In this example $H = \{e\}$, hence the commutativity condition $[M, U(h)] = 0$ for all $h \in H$ puts no constrains on $M$. For every $g' \in G$, we have

$$\begin{aligned}U(g')\left(\sum_g \mathsf{M}(g)\right) &= \sum_g U(g')U(g)MU(g)^* \\ &= \sum_g \overline{\omega(g',g)}U(g'g)MU(g)^*U(g')^*U(g') \\ &= \left(\sum_g \mathsf{M}(g)\right)U(g')\,.\end{aligned}$$

Therefore, $\sum_g \mathsf{M}(g) = c\mathbb{1}$ for some $c \in \mathbb{R}$, and we see that

$$c = \operatorname{tr}\left[\sum_g \mathsf{M}(g)\right]/\operatorname{tr}[\mathbb{1}] = \#G \cdot \operatorname{tr}[M]/d\,.$$

Redefining $M \to \frac{1}{c}M$ we thus obtain a covariant observable.

### C. Existence of covariant observables

Let $U$ be a projective unitary representation of $G$. We now pose our earlier question in a modified form:

> If a linear subspace $\mathcal{S} \subseteq \mathcal{L}(\mathcal{H})$ is given, is it possible to find a *$U$-covariant* observable $\mathsf{M}$ such that $\mathcal{S} = \mathcal{S}_{\mathsf{M}}$?

Obviously, $\mathcal{S}$ must satisfy the basic criterion (3) and the $\widetilde{U}$-invariance requirement (10), i.e.,

$$\mathbb{1} \in \mathcal{S}\,, \qquad \mathcal{S} = \mathcal{S}^*\,, \qquad \widetilde{U}(g)\mathcal{S} = \mathcal{S} \quad \forall g \in G\,. \tag{14}$$

But it will turn out that these conditions are not sufficient.

As we have seen earlier, for every $U$-covariant observable $\mathsf{M}$, there is a positive operator $M \in \mathcal{L}(\mathcal{H})$ such that (12) holds. It follows that

$$\mathcal{S}_{\mathsf{M}} = \text{span}\left\{\widetilde{U}(g)M : g \in G\right\}. \tag{15}$$

Therefore, the answer to the existence question can be affirmative only if there exists a positive operator $M \in \mathcal{S}$ such that

$$\mathcal{S} = \text{span}\left\{\widetilde{U}(g)M : g \in G\right\}. \tag{16}$$

In mathematical terms, this condition means that $M$ is a *cyclic vector* for the subrepresentation $\widetilde{U}^{\mathcal{S}}$, the restriction of $\widetilde{U}$ on the invariant subspace $\mathcal{S}$. Before we present a result that gives an important necessary condition to the existence question, let us recall the concepts of Schmidt rank and cyclic representation.

Let $\mathcal{H}_1, \mathcal{H}_2$ two Hilbert spaces. A vector $v \in \mathcal{H}_1 \otimes \mathcal{H}_2$ can be written in the so-called *Schmidt form*

$$v = \sum_j \sqrt{\lambda_j} v_j^{(1)} \otimes v_j^{(2)}, \tag{17}$$

where $\{v_j^{(1)}\} \subset \mathcal{H}_1$ and $\{v_j^{(2)}\} \subset \mathcal{H}_2$ are orthogonal sets. The number of nonzero coefficients $\lambda_j$ is called the *Schmidt rank* of $v$ and we denote it by $\operatorname{rank} v$. Let us notice that the Schmidt rank of $v$ is the same as the rank of $v$ regarded as a linear operator from $\mathcal{H}_1^*$ to $\mathcal{H}_2$.

Let $V$ be a representation of $G$ acting on the Hilbert space $\mathcal{H}$. A vector $v \in \mathcal{H}$ is *cyclic* for $V$ if the linear span of the set $\{V(g)v : g \in G\}$ is $\mathcal{H}$. If there exists a cyclic vector, then we say that $V$ is a *cyclic representation*.

The following result is a particular case of [9, Theorem 1.10], the only difference being that we provide an explicit way to construct cyclic vectors.

**Proposition 3.** *Let $\widehat{G}$ be the (finite) set of irreducible unitary representations of $G$, each $\pi \in \widehat{G}$ acting in the Hilbert space $\mathcal{K}_\pi$. Then we have the following facts.*

*(1) Let $\pi \in \widehat{G}$, and suppose $v \in \mathcal{K}_\pi \otimes \mathcal{V}_\pi$. Then the vector $v$ is cyclic for the representation $\pi \otimes \mathbb{1}_{\mathcal{V}_\pi}$ if and only if $\operatorname{rank} v = \dim \mathcal{V}_\pi$.*

*(2) Suppose $V$ is a unitary representation of $G$ in $\mathcal{H}$, and let*

$$\mathcal{H} = \oplus_{\pi\in\widehat{G}} \mathcal{K}_\pi \otimes \mathcal{V}_\pi \qquad V = \oplus_{\pi\in\widehat{G}} \pi \otimes \mathbb{1}_{\mathcal{V}_\pi}$$

*be the isotypic decomposition of $V$. Here, $\dim \mathcal{V}_\pi$ is the multiplicity of each irreducible unitary representation $\pi$ in $V$. For each $\pi \in \widehat{G}$, let $P_\pi : \mathcal{H} \to \mathcal{K}_\pi \otimes \mathcal{V}_\pi$ be the projection of $\mathcal{H}$ onto $\mathcal{K}_\pi \otimes \mathcal{V}_\pi$. Then, a vector $v \in \mathcal{H}$ is cyclic for $V$ if and only if $P_\pi v$ is cyclic for the representation $\pi \otimes \mathbb{1}_{\mathcal{V}_\pi}$ for all $\pi \in \widehat{G}$.*

*(3) With the notations of item (2), $V$ is a cyclic representation if and only if $\dim \mathcal{V}_\pi \leq \dim \mathcal{K}_\pi$ for all $\pi \in \widehat{G}$.*

*Proof.* (1) For a fixed a linear basis $\{k_1, k_2, \ldots, k_d\}$ of $\mathcal{K}_\pi$, with dual basis $\{k_1^*, k_2^*, \ldots, k_d^*\}$, there exist vectors $\{v_1, v_2, \ldots, v_d\}$ in $\mathcal{V}_\pi$ such that

$$v = \sum_i k_i \otimes v_i .$$

Clearly, the dimension of the linear space $\mathcal{V}_\pi^0 = \text{span}\,\{v_1, v_2, \ldots, v_d\}$ is the rank of $v$.

By irreducibility of the representation $\pi$, the algebra $\mathcal{A} = \text{span}\,\{\pi(g) : g \in G\}$ coincides with the whole $\mathcal{L}(\mathcal{K}_\pi)$. Indeed, its commutant $\mathcal{A}' = \mathbb{C}\mathbb{1}_{\mathcal{K}_\pi}$ by Schur lemma, hence $\mathcal{A} = \mathcal{A}'' = \mathcal{L}(\mathcal{K}_\pi)$. For all $k \in \mathcal{K}_\pi$, the operator $A = kk_i^*$ thus belongs to $\mathcal{A}$, and $(A \otimes \mathbb{1}_{\mathcal{V}_\pi})v = k \otimes v_i$. It follows that

$$\text{span}\,\{(\pi(g) \otimes \mathbb{1}_{\mathcal{V}_\pi})v : g \in G\} = (\mathcal{A} \otimes \mathbb{1}_{\mathcal{V}_\pi})v \supseteq \mathcal{K}_\pi \otimes \mathcal{V}_\pi^0 .$$

On the other hand, the reverse inclusion is trivial, hence the equality

$$\text{span}\,\{(\pi(g) \otimes \mathbb{1}_{\mathcal{V}_\pi})v : g \in G\} = \mathcal{K}_\pi \otimes \mathcal{V}_\pi$$

holds if and only if $\mathcal{V}_\pi^0 = \mathcal{V}_\pi$, i.e., $\operatorname{rank} v = \dim \mathcal{V}_\pi$.

(2) Each map $P_\pi : \mathcal{H} \to \mathcal{K}_\pi \otimes \mathcal{V}_\pi$ satisfies $P_\pi V(g) = (\pi(g) \otimes \mathbb{1}_{\mathcal{V}_\pi})P_\pi$ for all $g$. If $v \in \mathcal{H}$ is cyclic for $V$, then necessarily $P_\pi v$ is cyclic for $\pi \otimes \mathbb{1}_{\mathcal{V}_\pi}$, as the condition

$$\begin{aligned} 0 &= \langle\, (\pi(g) \otimes \mathbb{1}_{\mathcal{V}_\pi})P_\pi v \,|\, P_\pi w \,\rangle \\ &= \langle\, V(g)v \,|\, P_\pi w \,\rangle \qquad \forall g \in G \end{aligned}$$

implies $P_\pi w = 0$. Conversely, suppose that $P_\pi v$ is cyclic for $\pi \otimes \mathbb{1}_{\mathcal{V}_\pi}$ for all $\pi \in \widehat{G}$, and let $w \in \mathcal{H}$ be such that $\langle\, V(g)v \,|\, w \,\rangle = 0$ for all $g \in G$. By [10, Théorème 8],

$$P_\pi = \frac{\dim \mathcal{K}_\pi}{\#G} \sum_g \operatorname{tr}\left[\pi(g)\right] V(g) ,$$

which implies

$$\begin{aligned} \langle\, (\pi(g) \otimes \mathbb{1}_{\mathcal{V}_\pi})P_\pi v \,|\, P_\pi w \,\rangle &= \langle\, V(g)v \,|\, P_\pi w \,\rangle \\ &= \frac{\dim \mathcal{K}_\pi}{\#G} \sum_h \operatorname{tr}\left[\pi(h)\right] \langle\, V(g)v \,|\, V(h)w \,\rangle \\ &= \frac{\dim \mathcal{K}_\pi}{\#G} \sum_h \operatorname{tr}\left[\pi(h)\right] \langle\, V(h^{-1}g)v \,|\, w \,\rangle \\ &= 0 . \end{aligned}$$

By cyclicity of $P_\pi v$ in $\mathcal{K}_\pi \otimes \mathcal{V}_\pi$, then it follows $P_\pi w = 0$. Since this holds for all $\pi \in \widehat{G}$, we have $w = 0$. Hence, $v$ is cyclic for $V$.

(3) If $v \in \mathcal{H}$ is a cyclic vector for $V$, then $P_\pi v$ must be cyclic for $\pi \otimes \mathbb{1}_{\mathcal{V}_\pi}$ for all $\pi \in \widehat{G}$ by item (2). By item (1), this implies $\operatorname{rank} P_\pi v = \dim \mathcal{V}_\pi$, which can happen only if $\dim \mathcal{V}_\pi \leq \dim \mathcal{K}_\pi$. □

Let $\mathcal{F}(G)$ be the vector space of all complex valued functions on $G$, with the inner product $\langle\, f_1 \,|\, f_2 \,\rangle =$

$\sum_g \overline{f_1(g)} f_2(g)$. We recall that the *regular representation* $R$ of $G$ acts on $\mathcal{F}(G)$ and is defined as

$$[R(g)\phi](g') = \phi(g^{-1}g')\,. \tag{18}$$

The regular representation is reducible and each irreducible unitary representation $\pi \in \widehat{G}$ occurs in $\mathcal{F}(G)$ with a multiplicity equal to its dimension. Therefore, from Proposition 3 we conclude the following consequence.

**Corollary 1.** *Let $V$ be a unitary representation of $G$. Then $V$ is a cyclic representation if and only if it is equivalent to a subrepresentation of the regular representation $R$ of $G$.*

**Example 3.** (*Representation consisting of* 1*-dimensional irreps.*) Suppose that $V$ is a direct sum of 1-dimensional representations of $G$. Then $V$ is cyclic if and only if every 1-dimensional representation $\chi \in \widehat{G}$ is contained in $V$ at most once. Indeed, the regular representation contains each 1-dimensional representation exactly once. The claim thus follows from Corollary 1.

## IV. EXISTENCE OF COVARIANT PIC OBSERVABLES

It has now become clear that the existence of a covariant observable that is pure-state informationally complete depends crucially on the group $G$ and its projective unitary representation $U$. In this section we derive some conditions that preclude the existence of a $U$-covariant PIC observable.

**Proposition 4.** *Let $U$ be a projective unitary representation of the group $G$ on $\mathcal{H}$. Suppose there exist two linearly independent vectors $v_1, v_2 \in \mathcal{H}$ and functions $f_1, f_2 : G \to \mathbb{T}$ such that $U(g)v_i = f_i(g)v_i$ for all $g \in G$ and $i \in \{1,2\}$. Then there exists no $U$-covariant PIC observable.*

*Proof.* We define two pure states $\varrho_i = |v_i\rangle\langle v_i| / \|v_i\|^2$, $i = 1,2$ and we will show that no $U$-covariant observable can separate these states. Notice that $\varrho_1 \neq \varrho_2$ by the linear independence of $\{v_1, v_2\}$.

Suppose $\mathsf{M}$ is a $U$-covariant observable based on a quotient space $\Omega = G/H$ and let $i \in \{1,2\}$. Then, for every $x = gH \in \Omega$,

$$\begin{aligned}\operatorname{tr}[\mathsf{M}(gH)\varrho_i] &= \operatorname{tr}[U(g)\mathsf{M}(eH)U(g)^*\varrho_i] \\ &= f_i(g)\overline{f_i(g)}\operatorname{tr}[M\varrho_i] = \operatorname{tr}[M\varrho_i]\,,\end{aligned}$$

hence the map $x \mapsto \operatorname{tr}[\mathsf{M}(x)\varrho_i]$ is constant. Since

$$\sum_x \operatorname{tr}[\mathsf{M}(x)\varrho_i] = \operatorname{tr}[\mathbb{1}\varrho_i] = 1\,, \tag{19}$$

we must have

$$\operatorname{tr}[\mathsf{M}(x)\varrho_i] = \frac{1}{\#\Omega} \qquad \forall x \in \Omega\,. \tag{20}$$

In particular, $\operatorname{tr}[\mathsf{M}(x)\varrho_1] = \operatorname{tr}[\mathsf{M}(x)\varrho_2]$ for all $x \in \Omega$. Therefore, $\mathsf{M}$ is not PIC. □

**Proposition 5.** *Let $G$ be an abelian group and $\dim \mathcal{H} \geq 2$. Then, in the following two cases there exists no $U$-covariant PIC observable:*

*(a) if $U$ is a unitary representation;*

*(b) if $G$ is cyclic and $U$ is a projective unitary representation.*

*Proof.* (a) If $U$ is a unitary representation, then the Hilbert space $\mathcal{H}$ decomposes into the orthogonal sum of 1-dimensional subrepresentations, each one carrying the action of a 1-dimensional unitary representation of $G$. Then the claim follows by Proposition 4.

(b) If $G$ is cyclic and $U$ is a projective unitary representation, then $U$ is similar to a unitary representation (see Example 1), and the claim follows from (a). □

## V. EXISTENCE OF COVARIANT AND MINIMAL PIC OBSERVABLES

In this section we combine the earlier concepts and methods and search for a minimal PIC observable that is covariant under some projective unitary representation of some finite group. As it turns out, the existence of such an observables depends on the Hilbert space dimension $d$. In particular, we will investigate the existence question for the dimensions $d = 3$ and $d = 7$. These two instances demonstrate that a desired observable may exist or not.

### A. Dimension 3

We first investigate the case when the dimension of $\mathcal{H}$ is 3. We want to find an observable $\mathsf{M}$ such that $\mathsf{M}$ is PIC and has minimal number of outcomes, and further that $\mathsf{M}$ is covariant with respect to some group $G$. We will restrict our search for observables based on $\Omega \equiv G$ since already in this situation we can find two possible symmetry groups.

The minimal number of outcomes for a PIC in dimension 3 is 8 [1]. There are five groups with 8 elements: three abelian groups $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and two non-abelian groups $D$ (dihedral group) and $Q$ (quaternionic units). We will show that the abelian groups are unsuitable while the non-abelian groups can be used to construct a desired observable.

Let $G$ be a group with 8 elements, $U$ a projective unitary representation of $G$ and $\mathsf{M}$ a $U$-covariant PIC observable on $G$. In the following we will proceed in steps to reveal the limitations in the choice of $G$ and $U$.

**• Projective representation $U$ must be reducible**

For a minimal PIC observable $\mathsf{M}$ we have $\dim \mathcal{S}_{\mathsf{M}} = 8$, hence the orthogonal space $\mathcal{S}_{\mathsf{M}}^{\perp}$ is generated by a single selfadjoint operator $T$ which satisfies $\mathrm{tr}\,[T] = 0$ and by Proposition 1 must have rank 3, i.e., is invertible. Thus, from (10) it follows that

$$U(g)TU(g)^* = c_g T \qquad \forall g \in G \tag{21}$$

for some numbers $c_g \in \mathbb{R}$. This implies that

$$\det(T) = \det(U(g)TU(g^*)) = \det(c_g T) = c_g^3 \det(T)\,.$$

Since $\det(T) \neq 0$, we conclude that $c_g = 1$ for every $g \in G$. Therefore,

$$U(g)T = TU(g) \qquad \forall g \in G\,. \tag{22}$$

But since $\mathrm{tr}\,[T] = 0$, we see that $T$ cannot be a scalar multiple of the identity operator. Therefore, the projective representation $U$ is reducible.

**• Projective representation $U$ is similar to an ordinary unitary representation**

We can infer more about $U$ by using the spectral decomposition for $T$. By changing $T$ to $-T$ if necessary (this does not change $\mathcal{S}_{\mathsf{M}}^{\perp}$), we can write $T$ as

$$T = \lambda_1 P_1 - \lambda_2 P_2 - \lambda_3 P_3\,, \tag{23}$$

where $\lambda_j > 0$, $\lambda_1 = \lambda_2 + \lambda_3$ and $P_1, P_3, P_3$ are orthogonal 1-dimensional projections. Depending on the eigenvalues of $T$, we have two alternative situations:

(a) If $\lambda_2 \neq \lambda_3$, then $U$ commutes with each of the three projections $P_1$, $P_2$ and $P_3$.

(b) If $\lambda_2 = \lambda_3$, then $U$ commutes with $P_1$ and $P_2 + P_3$ (but not necessarily with $P_2$ and $P_3$ separately).

In both cases $U$ leaves invariant the 1-dimensional subspace $P_1\mathcal{H}$. By Proposition 2 we conclude that $U$ is similar to an ordinary unitary representation.

**• Symmetry group must be non-abelian**

We have seen that $U$ must be an ordinary unitary representation of $G$. It follows from Proposition 5 that the symmetry group $G$ must be non-abelian, hence either the dihedral group $D$ or the group of unit quaternions $Q$.

The two situations that were separated according to the eigenvalues of $T$ lead to different conclusions:

(a) If $\lambda_2 \neq \lambda_3$, then $U$ leaves invariant all the 1-dimensional spaces $P_1\mathcal{H}$, $P_2\mathcal{H}$ and $P_3\mathcal{H}$. By Proposition 4, there exists no $U$-covariant PIC observable.

TABLE II: The 1-dimensional irreducible representations of the quaternionic group $Q$ and the dihedral group $D$.

| irrep | value in the case of $Q$ | value in the case of $D$ |
|---|---|---|
| $\chi_0(g)$ | 1 $\quad \forall g$ | 1 $\quad \forall g$ |
| $\chi_1(g)$ | 1 if $g \in \{\pm\mathbb{1}\,,\, \pm i\sigma_1\}$<br>-1 otherwise | 1 if $g \in \{\pm\mathbb{1}\,,\, \pm i\sigma_1\}$<br>-1 otherwise |
| $\chi_2(g)$ | 1 if $g \in \{\pm\mathbb{1}\,,\, \pm i\sigma_2\}$<br>-1 otherwise | 1 if $g \in \{\pm\mathbb{1}\,,\, \pm\sigma_2\}$<br>-1 otherwise |
| $\chi_3(g)$ | 1 if $g \in \{\pm\mathbb{1}\,,\, \pm i\sigma_3\}$<br>-1 otherwise | 1 if $g \in \{\pm\mathbb{1}\,,\, \pm\sigma_3\}$<br>-1 otherwise |

(b) If $\lambda_2 = \lambda_3$, then $U$ leaves invariant the 1-dimensional space $P_1\mathcal{H}$ and the 2-dimensional space $(P_2 + P_3)\mathcal{H}$. If the space $(P_2 + P_3)\mathcal{H}$ is irreducible, then Proposition 4 does not exclude the existence of $U$-covariant PIC observables. To determine whether $U$-covariant PIC observables exist or not, one further needs to establish if the representation $\widetilde{U}$ is cyclic.

**• Quaternionic and dihedral symmetry groups**

The quaternionic group $Q$ consists of 8 elements $\pm 1, \pm i, \pm j, \pm k$ satisfying the relations

$$\begin{gathered}(-1)^2 = 1 \qquad (\pm 1)g = g(\pm 1) = \pm g \quad \forall g \in Q \\ i^2 = j^2 = k^2 = -1 \qquad ij = -ji = k\,.\end{gathered} \tag{24}$$

For our purposes, it is convenient to use a matrix realization of $Q$. We denote by $M_2(\mathbb{C})$ the Hilbert space of complex $2 \times 2$ matrices, equipped with the Hilbert-Schmidt inner product. The identity matrix $\mathbb{1}$ together with the Pauli matrices $\sigma_1$, $\sigma_2$, $\sigma_3$ form an orthogonal basis of $M_2(\mathbb{C})$. The quaternionic group $Q$ can be described as the collection of matrices $\{\pm\mathbb{1}\,,\, \pm\sigma_1\,,\, \pm\sigma_2\,,\, \pm\sigma_3\}$, endowed with the usual matrix product rule, according to the correspondence

$$\pm 1 \leftrightarrow \pm\mathbb{1}\,, \quad \pm i \leftrightarrow \pm i\sigma_1\,, \quad \pm j \leftrightarrow \mp i\sigma_2\,, \quad \pm k \leftrightarrow \pm i\sigma_3\,.$$

The dual $\widehat{Q}$ consists of four 1-dimensional unitary representations and a single 2-dimensional unitary representation. The 2-dimensional unitary representation is the identity map $\pi(g) = g$, and the 1-dimensional representations are given in Table II.

The unitary representation

$$\widetilde{\pi}(g)L := \pi(g)L\pi(g)^* \qquad \forall L \in M_2(\mathbb{C})$$

decomposes into the direct sum

$$M_2(\mathbb{C}) = \mathbb{C}\mathbb{1} \oplus \mathbb{C}\sigma_1 \oplus \mathbb{C}\sigma_2 \oplus \mathbb{C}\sigma_3\,, \qquad \widetilde{\pi} = \chi_0 \oplus \chi_1 \oplus \chi_2 \oplus \chi_3\,.$$

The contragradient representation $\bar{\pi}$ in the dual space $\mathbb{C}^{2\,*}$ of row vectors is defined as

$$\bar{\pi}(g)v^t := v^t\pi(g^{-1}) \qquad \forall v \in \mathbb{C}^2\,. \tag{25}$$

The representation $\bar{\pi}$ is equivalent to $\pi$, and an intertwining operator $V : \mathbb{C}^{2\,*} \to \mathbb{C}^2$ is given by

$$Vv^t = \sigma_2 v \qquad \forall v \in \mathbb{C}^2\,. \tag{26}$$

In the following it is convenient to use block form for matrices, for instance

$$\begin{pmatrix} 0 & \bar{v}^t \\ v & 0 \end{pmatrix} \equiv \begin{pmatrix} 0 & \overline{v}_1 & \overline{v}_2 \\ v_1 & 0 & 0 \\ v_2 & 0 & 0 \end{pmatrix}$$

where $v_1, v_2$ are the components of the vector $v \in \mathbb{C}^2$.

We now consider the Hilbert space $\mathcal{H} = \mathbb{C}^3$ and introduce the following unitary representation $U$ in $\mathcal{H}$:

$$U(g) = \begin{pmatrix} 1 & 0 \\ 0 & \pi(g) \end{pmatrix}. \tag{27}$$

If $\lambda > 0$ and $T$ is defined as

$$T = \begin{pmatrix} 2\lambda & 0 \\ 0 & -\lambda\mathbb{1}_{\mathbb{C}^2} \end{pmatrix}, \tag{28}$$

then clearly $\mathrm{tr}\,[T] = 0$ and $U(g)TU(g)^* = T$ for all $g$. These choices satisfy the necessary requirements found earlier; $U$ is reducible and $T$ has a degenerate eiegenvalue.

With these preliminary observations, we are ready for the following result.

**Proposition 6.** *Let $M \in \mathcal{L}(\mathcal{H})$ be the operator*

$$M = \frac{1}{8}\mathbb{1} + \alpha_1 \begin{pmatrix} 0 & 0 \\ 0 & \sigma_1 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 & 0 \\ 0 & \sigma_2 \end{pmatrix} + \alpha_3 \begin{pmatrix} 0 & 0 \\ 0 & \sigma_3 \end{pmatrix} + \begin{pmatrix} 0 & \bar{v}^t \\ v & 0 \end{pmatrix} \tag{29}$$

*with*

$$\alpha_1\,,\, \alpha_2\,,\, \alpha_3 \in \mathbb{R}\,, \qquad v \in \mathbb{C}^2$$

*such that*

$$\alpha_1 \neq 0\,, \quad \alpha_2 \neq 0\,, \quad \alpha_3 \neq 0 \tag{30}$$

$$v \neq 0 \tag{31}$$

*and*

$$M \geq 0\,. \tag{32}$$

*Then the map*

$$\mathsf{M}(g) = U(g)MU(g)^*\,, \qquad g \in Q \tag{33}$$

*is a $U$-covariant observable. Moreover, $\mathcal{S}_{\mathsf{M}} = T^\perp$, hence $\mathsf{M}$ is a PIC with minimal number of outcomes.*

*Proof.* We first show that $\mathcal{S}_{\mathsf{M}} = T^\perp$, i.e., the operator $M$ is a cyclic vector for the restriction of the representation $\widetilde{U}$ to the invariant subspace $T^\perp$ of $\mathcal{L}(\mathcal{H})$. Under the action of $\widetilde{U}$, the space $T^\perp$ decomposes into the direct sum of irreducible invariant subspaces

$$T^\perp = \mathbb{C}\mathbb{1} \oplus \mathbb{C}\begin{pmatrix} 0 & 0 \\ 0 & \sigma_1 \end{pmatrix} \oplus \mathbb{C}\begin{pmatrix} 0 & 0 \\ 0 & \sigma_2 \end{pmatrix} \oplus \mathbb{C}\begin{pmatrix} 0 & 0 \\ 0 & \sigma_3 \end{pmatrix} \oplus \begin{pmatrix} 0 & \mathbb{C}^{*2} \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ \mathbb{C}^2 & 0 \end{pmatrix},$$

and according to such splitting the representation $\widetilde{U}$ restricted to $T^\perp$ decomposes as

$$\widetilde{U} = \chi_0 \oplus \chi_1 \oplus \chi_2 \oplus \chi_3 \oplus \bar{\pi} \oplus \pi\,.$$

As $\pi$ and $\bar{\pi}$ are equivalent, the representations $\bar{\pi} \oplus \pi$ and $\pi \otimes \mathbb{1}_{\mathbb{C}^2}$ are equivalent. A linear map

$$W : \begin{pmatrix} 0 & \mathbb{C}^{*2} \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ \mathbb{C}^2 & 0 \end{pmatrix} \to \mathbb{C}^2 \otimes \mathbb{C}^2$$

explicitely yelding this equivalence is given by

$$W \begin{pmatrix} 0 & u^t \\ v & 0 \end{pmatrix} = v \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} + Vu^t \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

where $V$ is the map defined in (26). The condition (31) is the same of $V\bar{v}^t \notin \mathbb{C}v$ (indeed, $\sigma_2\bar{v} \notin \mathbb{C}v$ if and only if $v \neq 0$), which in turn is equivalent to $\mathrm{rank}\, W \begin{pmatrix} 0 & \bar{v}^t \\ v & 0 \end{pmatrix} = 2$. By item (1) of Proposition 3, this implies that the vector $\begin{pmatrix} 0 & \bar{v}^t \\ v & 0 \end{pmatrix}$ is cyclic for the subrepresentation $\bar{\pi} \oplus \pi \simeq \pi \otimes \mathbb{1}_{\mathbb{C}^2}$ of $\widetilde{U}$. Moreover, each 1-dimensional subrepresentation $\chi_i$ of $\widetilde{U}$ is clearly cyclic. Condition (30) and the cyclicity of $\begin{pmatrix} 0 & \bar{v}^t \\ v & 0 \end{pmatrix}$ then imply that $M$ is cyclic in $T^\perp$ by item (2) of Proposition 3, as claimed.

We still need to show that $\mathsf{M}$ is an observable. First, since $\mathsf{M}$ is of the form (33) and $M \geq 0$, it follows that every $\mathsf{M}(g)$ is positive. Second, we need to prove that $\Sigma_g \mathsf{M}(g) = \mathbb{1}$. We denote

$$A := \sum_g \mathsf{M}(g)\,. \tag{34}$$

Then, $U(g)A = AU(g)$ for all $g$. It follows that

$$A = \begin{pmatrix} \beta_1 & 0 \\ 0 & \beta_2\mathbb{1}_{\mathbb{C}^2} \end{pmatrix} \qquad \beta_1, \beta_2 \in \mathbb{C}\,. \tag{35}$$

Since $A \in T^\perp$, we have $\mathrm{tr}\,[AT] = 0$, which implies $\beta_1 = \beta_2$. On the other hand,

$$\mathrm{tr}\,[A] = \sum_g \mathrm{tr}\,[\mathsf{M}(g)] = 8 \cdot \mathrm{tr}\,[M] = 8 \cdot \mathrm{tr}\,[(1/8)\mathbb{1}] = 3\,,$$

therefore $\beta_1 = \beta_2 = 1$. This means that $A = \mathbb{1}$. □

**Remark 1.** The nonzero eigenvalues of the matrices

$$\alpha_1 \begin{pmatrix} 0 & 0 \\ 0 & \sigma_1 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 & 0 \\ 0 & \sigma_2 \end{pmatrix} + \alpha_3 \begin{pmatrix} 0 & 0 \\ 0 & \sigma_3 \end{pmatrix} \tag{36}$$

and

$$\begin{pmatrix} 0 & \bar{v}^t \\ v & 0 \end{pmatrix} \tag{37}$$

are $\pm\sqrt{\alpha_1^2 + \alpha_2^2 + \alpha_3^2}$ and $\pm\sqrt{|v_1|^2 + |v_2|^2}$, respectively. Therefore, the positivity condition (32) is satisfied if we choose $\alpha_1, \alpha_2, \alpha_3$ and $v$ such that

$$\sqrt{\alpha_1^2 + \alpha_2^2 + \alpha_3^2} + \sqrt{|v_1|^2 + |v_2|^2} \leq \frac{1}{8}\,.$$

However, this inequality is not a necessary condition for (32) to hold, but only a convenient sufficient condition.

**Example 4.** (*Rank-1 PIC observable*) Suppose $\gamma \in [0, 2\pi)$ and $\alpha_1, \alpha_2, \alpha_3$ are nonzero real numbers satisfying $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 1/64$. Then the operator

$$M = \begin{pmatrix} \frac{1}{8} & \frac{\mathrm{e}^{-i\gamma}\sqrt{1+8\alpha_3}}{8} & \frac{\mathrm{e}^{-i\gamma}(\alpha_1 - i\alpha_2)}{\sqrt{1+8\alpha_3}} \\ \frac{\mathrm{e}^{i\gamma}\sqrt{1+8\alpha_3}}{8} & \frac{1}{8} + \alpha_3 & \alpha_1 - i\alpha_2 \\ \frac{\mathrm{e}^{i\gamma}(\alpha_1 + i\alpha_2)}{\sqrt{1+8\alpha_3}} & \alpha_1 + i\alpha_2 & \frac{1}{8} - \alpha_3 \end{pmatrix}$$

is of the form (29) and satisfies conditions (30) and (31). Moreover, a direct calculation yelds $M^2 = (3/8)M$, which shows that $M \geq 0$ and $\operatorname{rank} M = 1$. It follows from Proposition 6 that the map $g \mapsto U(g)MU(g)^*$ is a $U$-covariant PIC observable.

Except some minor details, the previous construction can be done by using the dihedral group $D$ instead of the quaternionic group $Q$. We briefly explain the needed modifications. It is convenient to describe $D$ as a collection of $2 \times 2$ complex matrices,

$$D = \{\mathbb{1}\,,\, -\mathbb{1}\,,\, i\sigma_1\,,\, -i\sigma_1\,,\, \sigma_2\,,\, -\sigma_2\,,\, \sigma_3\,,\, -\sigma_3\}\,.$$

As in the case of $Q$, the dual $\widehat{D}$ consist of four 1-dimensional unitary representations and a single 2-dimensional unitary representation. The 2-dimensional unitary representation is the identity map $\pi(g) = g$ , and the 1-dimensional representations are given in Table II. The unitary representation

$$\widetilde{\pi}(g)L := \pi(g)L\pi(g)^* \qquad \forall L \in M_2(\mathbb{C})$$

decomposes into the direct sum

$$M_2(\mathbb{C}) = \mathbb{C}\mathbb{1} \oplus \mathbb{C}\sigma_1 \oplus \mathbb{C}\sigma_2 \oplus \mathbb{C}\sigma_3\,, \qquad \widetilde{\pi} = \chi_0 \oplus \chi_1 \oplus \chi_2 \oplus \chi_3\,.$$

The contragradient representation $\bar{\pi}$ in the dual space $\mathbb{C}^{2\,*}$ of row vectors is defined as

$$\bar{\pi}(g)v^t := v^t\pi(g^{-1}) \qquad \forall v \in \mathbb{C}^2\,, \tag{38}$$

TABLE III: The dimensions $d \leq 1000$ that are known to have the property that the number of outcomes of a minimal PIC is a prime number.

| dimension | min # of outcomes |
|---|---|
| 7 | 23 |
| 13 | 47 |
| 19 | 71 |
| 21 | 79 |
| 49 | 191 |
| 67 | 263 |
| 69 | 271 |
| 97 | 383 |
| 259 | 1031 |
| 261 | 1039 |
| 273 | 1087 |
| 289 | 1151 |
| 321 | 1279 |
| 517 | 2063 |
| 529 | 2111 |

and it is equivalent to $\pi$. An intertwining operator $V : \mathbb{C}^{2\,*} \to \mathbb{C}^2$ is given by

$$Vv^t = \sigma_3 v \qquad \forall v \in \mathbb{C}^2\,. \tag{39}$$

The unitary representation $U$ and the operator $T$ are defined similarly as in (27) and (28), respectively. Then, Proposition 6 holds if the condition (31) is replaced with

$$|v_1| \neq |v_2|\,. \tag{40}$$

### B. Dimension 7

If the dimension of the Hilbert space $\mathcal{H}$ is 7, then, according to Table I, the minimal number of outcomes for a PIC observable is 23, which is a prime number. The next result shows that, if $p$ is a prime number, there are no covariant PIC observables with $p$ outcomes. This rules out the existence of minimal covariant PIC observables in dimension 7.

There are other cases, in addition to $d = 7$, which do not admit minimal covariant PIC observables for the same reason. The dimensions whose minimal PIC observables are known to have a prime number of outcomes (and which consequently do not have minimal covariant PIC observables) are listed in Table III up to $d \leq 1000$. This list is calculated using the results from [1].

**Proposition 7.** *Let $G$ be a group, $H \subset G$ a proper subgroup and $U$ a projective unitary representation of $G$ in $\mathcal{H}$. Suppose $\#(G/H)$ is prime. If $\mathsf{M} : G/H \to \mathcal{L}(\mathcal{H})$ is a $U$-covariant observable, it is not PIC.*

The proof is a consequence of the following lemma. Let us first notice that any subgroup $G_0 \subseteq G$ acts on the quotient space $G/H$ in the natural way; $x\cdot(gH) = (xg)H$ for all $x \in G_0$ and $g \in G$. But this action need not be transitive.

**Lemma 1.** *Suppose $G$ is a group and $H \subseteq G$ a subgroup such that $\#(G/H)$ is prime. There exists a cyclic subgroup $G_0 \subset G$ such that the action of $G_0$ on $G/H$ is transitive.*

*Proof.* We recall that, if $p$ denotes a prime number, a *$p$-Sylow subgroup* $G_p \subseteq G$ is a subgroup whose order is $p^q$ for some integer $q \geq 1$, and $p^q$ is the highest power dividing the order of $G$. For any prime $p$ dividing the order of $G$, there exists a $p$-Sylow subgroup $G_p$ of $G$ (see e.g. [11, Theorem 6.1 of Chapter 1] or [12, Theorem 1.7]).

Denote $p = \#(G/H)$, and let $\#G = p^q m$, with $p$ not dividing $m$. Fix a $p$-Sylow subgroup $G_p \subseteq G$. Then, $G_p \nsubseteq H$, as otherwise

$$\#G = \#(G/H)\cdot\#(H/G_p)\cdot\#G_p = p^{q+1}\cdot\#(H/G_p)$$

and this contradicts the assumption that $\#G = p^q m$, with $p$ not dividing $m$. Thus, we can pick $g_0 \in G_p$ such that $g_0 \notin H$, and we denote by $G_0$ the cyclic subgroup generated by $g_0$. Since $G_0$ is a subgroup of $G_p$, we must have $\#G_0 = p^r$ for some $1 \leq r \leq q$. On the other hand, $G_0 \neq G_0 \cap H$ since $g_0 \notin H$. It follows that $\#(G_0/(G_0 \cap H)) = p^s$, with $s \geq 1$.

We define a map $\Lambda : G_0/(G_0 \cap H) \to G/H$ by

$$\Lambda(g(G_0 \cap H)) = gH \quad \forall g \in G_0\,.$$

This map is well defined and is an injection, since, for all $g, g' \in G_0$, $g^{-1}g' \in H$ if and only if $g^{-1}g' \in H \cap G_0$. Therefore, $\#(G_0/(G_0 \cap H)) \leq \#(G/H)$. Since $\#(G/H) = p$ and $\#(G_0/(G_0 \cap H)) = p^s$ with $s \geq 1$, we conclude that $\#(G_0/(G_0 \cap H)) = p$. It follows that $\Lambda$ is a bijection. It is easy to verify that for $g, g' \in G_0$, we have

$$g'\cdot\Lambda(g(G_0 \cap H)) = g'gG/H\,.$$

Since $G_0$ acts transitively on $G_0/(G_0 \cap H)$ and $\Lambda$ is a bijection, we see that this formula defines a transitive action of $G_0$ on $G/H$. □

*Proof of Proposition 7.* Let $\mathsf{M} : G/H \to \mathcal{L}(\mathcal{H})$ be a $U$-covariant observable. Choose a cyclic subgroup $G_0 \subset G$ as in Lemma 1 and let $U'$ be the restriction of $U$ to $G_0$. Then, $\mathsf{M}$ is a $U'$-covariant observable and not PIC by Proposition 5. □

We remark that in Lemma 1 the condition that $\#(G/H)$ is prime is essential. Indeed, if e.g. $G = Q$ and $H = \{\mathbb{1}, -\mathbb{1}\}$, then $\#(Q/H) = 4$, but there is no cyclic subgroup $G_0 \subseteq Q$ whose action on $Q/H$ is transitive. Indeed, by direct inspection, one can check that every cyclic subgroup $G_0 \subseteq Q$ has order 2 or 4 and contains $H$, so $\#(G_0/(G_0 \cap H)) = 1$ or $2 \neq 4$.

## VI. CONCLUSIONS

The minimal number of outcomes for a pure-state informationally complete (PIC) observable has been recently solved in [1]. One would hope that it is possible to find a minimal PIC observable with some simple mathematical structure, possibly in some symmetric form. An obvious try is to use covariance with respect to some finite group since this works so nicely in the case of minimal informationally complete observables. It would provide a simple and easy way to construct minimal observables with the desired property.

We have seen that the approach of using covariant observables fails in general; for some dimensions there are no minimal PIC observables that would be covariant under any finite group. We conclude that this kind of symmetry is lacking in the duality of observables and pure states, although it exists between observables and all states.

One can turn into a more general question: Is it possible to have a minimal PIC observable $\mathsf{M}$ with all operators having the same set of eigenvalues? For such $\mathsf{M}$ any pair of operators $\mathsf{M}(x)$ and $\mathsf{M}(x')$ are unitarily equivalent. Hence, $\mathsf{M}$ bears some symmetry although it need not be covariant under any projective unitary representation.

A particularly appealing observable of this type would consists of rank-1 operators. It has been shown in [13] that in every finite dimension $d$, there exists an observable consisting of $2d$ operators with rank-1 and identifying all pure states up to a measure zero. This, however, does not answer to the question of rank-1 PIC observables, which are required to identify all states and therefore must have at least $4d - 4 - \delta(d)$ outcomes [1].

### Acknowledgements

The authors wish to thank Jussi Schultz for his comments on an earlier version of this paper. T.H. acknowledges financial support from the Academy of Finland (grant no. 138135). A.T. acknowledges the financial support of the Italian Ministry of Education, University and Research (FIRB project RBFR10COAQ).

[1] M.M. Wolf T. Heinosaari, L. Mazzarella. Quantum tomography under prior information. *Comm. Math. Phys., in press.*, arXiv:1109.5478 [quant-ph], 2011.

[2] E. Prugovečki. Information-theoretical aspects of quantum measurements. *Int. J. Theor. Phys.*, 16:321–331, 1977.

[3] C.M. Caves, C.A. Fuchs, and R. Schack. Unknown quantum states: the quantum de Finetti representation. *J. Math. Phys.*, 43:4537–4559, 2002.

[4] G.M. D'Ariano, P. Perinotti, and M.F. Sacchi. Informationally complete measurements and group representation. *J. Opt. B: Quantum Semiclass. Opt.*, 6:S487–S491, 2004.

[5] T. Heinosaari, C. Carmeli, A. Toigo Informationally complete joint measurements on finite quantum systems. *Phys. Rev. A*, 85:012109, 2012.

[6] P. Busch. Informationally complete sets of physical quantities. *Internat. J. Theoret. Phys.*, 30(9):1217–1227, 1991.

[7] I. Martin Isaacs. *Character theory of finite groups*. AMS Chelsea Publishing, Providence, RI, 2006. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423].

[8] A.S. Holevo. *Statistical Structure of Quantum Theory*. Springer-Verlag, Berlin, 2001.

[9] Frederick Greenleaf and Martin Moskowitz. Cyclic vectors for representations of locally compact groups. *Mathematische Annalen*, 190:265–288, 1971.

[10] Jean-Pierre Serre. *Représentations linéaires des groupes finis*. Hermann, Paris, 1967.

[11] Serge Lang. *Algebra*. Addison-Wesley Publishing Co., Inc., Reading, Mass., 1965.

[12] I. Martin Isaacs. *Finite group theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.

[13] J. Finkelstein. Pure-state informationally complete and "really" complete measurements. *Phys. Rev. A*, 70:052107, 2004.