# Determining quantum coherence with minimal resources 

## OPEN ACCESS

RECEIVED
15 March 2018

## REVISED

22 May 2018
accepted for publication
12 June 2018

## PUBLISHED

25 June 2018

Claudio Carmeli ${ }^{1}$ (1) , Teiko Heinosaari ${ }^{2,6}$, Sabrina Maniscalco ${ }^{2,5}$, Jussi Schultz ${ }^{2}$ and Alessandro Toigo ${ }^{3,4}$ (1D)
$1^{1}$ DIME, Università di Genova, Via Magliotto 2, I-17100 Savona, Italy
2 QTF Centre of Excellence, Turku Centre for Quantum Physics, Department of Physics and Astronomy, University of Turku, FI-20014

3 Turku, Finland
${ }^{3}$ Dipartimento di Matematica, Politecnico di Milano, Piazza Leonardo da Vinci 32, I-20133 Milano, Italy
${ }^{4}$ I.N.F.N., Sezione di Milano, Via Celoria 16, I-20133 Milano, Italy
5 QTF Centre of Excellence, Department of Applied Physics, School of Science, Aalto University, FI-00076 Aalto, Finland
6 Author to whom any correspondence should be addressed.
E-mail: claudio.carmeli@gmail.com, teiko.heinosaari@utu.fi, smanis@utu.fi, jussi.schultz@gmail.com and alessandro.toigo@polimi.it
Keywords: coherence, quantum tomography, mutually unbiased bases, maximally correlated state

Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.



#### Abstract

We characterize minimal measurement setups for validating the quantum coherence of an unknown quantum state. We show that for a $d$-level system, the optimal strategy consists of measuring $d$ orthonormal bases such that each measured basis is mutually unbiased with respect to the reference basis, and together with the reference basis they form an informationally complete set of measurements. We prove that, in general, any strategy capable of validating quantum coherence allows one to evaluate also the exact value of coherence. We then give an explicit construction of the optimal measurements for arbitrary dimensions, and we derive a reconstruction formula for the off-diagonal terms. We also demonstrate that the same measurement setup is optimal for the modified task of verifying if the coherence is above or below a given threshold value. Finally, we show that the certification of entanglement of bipartite maximally correlated states is intimately connected with the certification of coherence.


## 1. Introduction

Quantum coherence, or the ability to form superpositions of quantum states, is one of the fundamental distinctions between the quantum and classical worlds. Quantum coherence is not merely a foundational curiosity, but it is the key element behind numerous quantum technological applications [1], including quantum algorithms [2] and quantum state merging [3]. This has lead to the identification of quantum coherence as a true physical resource $[1,4,5]$.

Due to the importance of quantum coherence, there have been various approaches and proposals for detecting or estimating the coherence of an unknown quantum state [6, 7]. In this paper, we address the problem of detecting coherence from a very fundamental point of view. We determine the minimal number, as well as characterize the optimal set, of measurements for the following tasks:
(a) Certification of the presence or absence of quantum coherence in an unknown quantum state.
(b) Determination of the exact value of quantum coherence in an unknown quantum state.

While these tasks are clearly defined and provide a foundational basis for more applicative studies, one may wish to have a more robust and physically motivated goal for comparison. Hence we also consider the following task:
(a) Verification that an unknown quantum state has more coherence than some chosen threshold value.

Mathematically speaking, quantum coherence is always defined with respect to some reference basis, that is, a fixed orthonormal basis $\left\{\varphi_{j}\right\}_{j=0}^{d-1}$ of a $d$-level quantum system. A state $\varrho$ represented by a density matrix is incoherent if it is diagonal in the reference basis, i.e., $\varrho=\sum_{j} p_{j}\left|\varphi_{j}\right\rangle\left\langle\varphi_{j}\right|$ for some probability distribution ( $p_{j}$ );
otherwise it is coherent. Quantum coherence can be quantified in various ways [8-10]. Task (b) does not depend on a particular choice of quantification; as a measure of coherence we can take any function which depends only on the off-diagonal elements of the state, and vanishes for all incoherent states and only for them. For task (c), we need to be more specific and fix a suitable measure. A natural choice is the $\ell_{1}$-norm of coherence, given as $C_{1}(\varrho)=\min _{\sigma \in \mathcal{I}}\|\varrho-\sigma\|_{\ell_{1}}=\sum_{j \neq k}\left|\varrho_{j, k}\right|$, where $\mathcal{I}$ is the set of all incoherent states and $\|\cdot\|_{\ell_{1}}$ is the $\ell_{1}$ matrix norm [11]. The $\ell_{1}$-norm of coherence is a reasonable quantification of coherence since the first formula gives a physically motivated definition while the second formula provides an easy way to calculate it. Further, it is monotonic under incoherent completely positive and trace preserving maps [12]. It has been recently shown that the distillable coherence of a state is bounded by the $\ell_{1}$-norm of coherence, and this provides a solid operational interpretation for its meaning [13].

We will first concentrate on quantum measurements related to orthonormal bases, so that the measurement of a basis $\left\{\psi_{k}\right\}_{k=0}^{d-1}$ on an initial state $\varrho$ gives an outcome $k$ with probability $\left\langle\psi_{k} \mid \varrho \psi_{k}\right\rangle$. A collection of finitely many different measurements is referred to as a measurement setup. This framework allows us to present a compact characterization of the optimal setups for tasks (a)-(c). We will later explain that considering more general measurements (described by positive operator valued measures (POVM)) does not alter the conclusions of our work.

To put our questions into a proper context, we recall that in order to perform full state tomography, a measurement setup consisting of $d+1$ bases is required; such a setup is called informationally complete [14, 15]. Informationally complete setups exist in all dimensions and are easy to construct as the only criterion is that the respective projections span the linear space of operators [16, 17]. The main goal of the present investigation is to determine how many measurements are needed in tasks (a)-(c), and to characterize the respective minimal measurement setups.

To further motivate the stated tasks, we recall that it is known that the certification of purity can be done with just five measurements [18], whereas the determination of the exact value of purity requires an informationally complete setup [19]. Another recent result regarding quantum correlations shows that any measurement setup which is not informationally complete will fail in certifying entanglement as well as nonclassicality of an unknown state [20]. It is therefore interesting to see how coherence compares with these other properties of quantum states.

Our main result shows that any measurement setup which can complete either task (a) or (c) is also capable of completing the more difficult task (b). In other words, the three tasks are equally demanding. We will prove that the minimal measurement setup for all tasks (a)-(c) consists of $d$ bases. The essential property that any measurement setup of this kind must satisfy is that each basis is mutually unbiased with respect to the reference basis. We recall that the mutual unbiasedness of two bases $\left\{\psi_{k}\right\}_{k=0}^{d-1}$ and $\left\{\phi_{\ell}\right\}_{\ell=0}^{d-1}$ means that the number $\left|\left\langle\psi_{k} \mid \phi_{\ell}\right\rangle\right|$ is independent of the indices $k$ and $\ell$, and it then follows that $\left|\left\langle\psi_{k} \mid \phi_{\ell}\right\rangle\right|=1 / \sqrt{d}$.

It is known that if the dimension $d$ is a prime power, then one can construct a complete set of mutually unbiased bases (MUB), i.e., $d+1$ bases that are all pairwisely mutually unbiased [21,22]. In prime power dimension one could therefore pick a complete set of MUB, transform all of them with a suitable unitary operator so that one of the bases becomes the reference basis, and then drop out the reference basis. However, as the existence of a complete set of MUB in other dimensions still remains an open question [23], this does not give a general solution. The criterion for a minimal measurement setup does not require all pairs of bases to be mutually unbiased with respect to each other, hence a positive answer to the MUB existence question is not a prerequisite to our result. In fact, we provide an explicit construction of the minimal measurement setup in arbitrary dimensions, and an explicit formula for the reconstruction of the off-diagonal elements of the density matrix in terms of such measurements.

Finally, based on the parametrization of the set of maximally correlated states given in [24], we show that there is an intimate connection between the entanglement of bipartite maximally correlated states and coherence.

## 2. Perturbation operators and the equivalence of tasks (a) and (b)

### 2.1. Warm up: coherence in a qubit system

As a warm up, we consider tasks (a) and (b) for a qubit system. For a qubit state $\varrho$ we have $C_{1}(\varrho)=2\left|\varrho_{0,1}\right|$, where $\varrho_{0,1}$ is the off-diagonal matrix element in the chosen reference basis. Assuming that this basis is the eigenbasis of $\sigma_{z}$, we see that from the numbers $\operatorname{tr}\left[\varrho \sigma_{x}\right]$ and $\operatorname{tr}\left[\varrho \sigma_{y}\right]$ we can calculate the off-diagonal elements and hence the value of $C_{1}(\varrho)$. Therefore, task (b) can be accomplished by measuring just two bases, namely, the eigenbases of $\sigma_{x}$ and $\sigma_{y}$. More generally, the eigenbases of $\sigma_{\mathbf{a}}=\mathbf{a} \cdot \boldsymbol{\sigma}$ and $\sigma_{\mathbf{b}}=\mathbf{b} \cdot \boldsymbol{\sigma}$ suffice for task (b) whenever $\mathbf{a}$ and $\mathbf{b}$ are nonparallel unit vectors in the $x y$-plane.


Figure 1. In the Bloch ball any choice of two nonparallel vectors in the plane $\pi$ orthogonal to $z$ determines two measurements that are mutually unbiased with respect to $\sigma_{z}$ and allows to certify coherence. Any other choice of a plane $\pi^{\prime}$ non orthogonal to $z$ cannot certify coherence.

A single basis is not enough even for task (a), since the measurement of, say, $\sigma_{x}$ gives the same outcome probabilities for the coherent state $\frac{1}{2}\left(\mathbb{1}+\sigma_{y}\right)$ and the incoherent state $\frac{1}{2} \mathbb{1}$. It is easy to extend this argument and see that for any basis, there is a coherent state and an incoherent state that give the same measurement outcome distribution.

Let us now look at the possible choices for the two measurements. To this end, let $\mathbf{a}$ and $\mathbf{b}$ be two nonparallel unit vectors in the Bloch ball, and assume that at least one of them is not orthogonal to the unit vector $\mathbf{k}(z$ direction). We can set $\mathbf{c}=\mathbf{a} \times \mathbf{b} /\|\mathbf{a} \times \mathbf{b}\|$ to obtain another unit vector which is not parallel to $\mathbf{k}$. The state $\varrho_{\mathbf{c}}=\frac{1}{2}\left(\mathbb{1}+\sigma_{\mathbf{c}}\right)$, with $\sigma_{\mathbf{c}}=\mathbf{c} \cdot \boldsymbol{\sigma}$, is then coherent, but since $\mathbf{c}$ is orthogonal to $\mathbf{a}$ and $\mathbf{b}$ we have $\operatorname{tr}\left[\varrho_{\mathbf{c}} \sigma_{\mathbf{a}}\right]=\operatorname{tr}\left[\frac{1}{2} 1 \sigma_{\mathbf{a}}\right]$ and $\operatorname{tr}\left[\varrho_{\mathbf{c}} \sigma_{\mathbf{b}}\right]=\operatorname{tr}\left[\frac{1}{2} \|_{\mathbf{b}}\right]$, which means that the eigenbases of $\sigma_{\mathbf{a}}$ and $\sigma_{\mathbf{b}}$ cannot distinguish the states $\varrho_{\mathbf{c}}$ and $\frac{1}{2} \mathbb{1}$. As we have seen, this kind of ambivalence does not occur if both $\mathbf{a}$ and $\mathbf{b}$ are orthogonal to $\mathbf{k}$; see figure 1 . We conclude that the respective orthonormal bases must be mutually unbiased with respect to the reference basis.

### 2.2. Coherence in a $d$-level system

In order to deal with task (a) in the case of a $d$-level system, we resort to a geometric framework, similar to that used in [19, 20]. The key concept is that of a perturbation operator, by which we mean any traceless selfadjoint operator. The nonzero perturbation operators $\Delta$ are precisely those operators that can be written, up to a scaling factor, as differences of distinct quantum states $\delta \Delta=\varrho^{\prime}-\varrho$ (see, for example, [25]).

The relevance of perturbation operators in the present context stems from the fact that, if we consider a measurement setup consisting of $m$ bases $\left\{\psi_{k}^{(1)}\right\}_{k=0}^{d-1}, \cdots,\left\{\psi_{k}^{(m)}\right\}_{k=0}^{d-1}$, then the condition

$$
\begin{equation*}
\left\langle\psi_{k}^{(\ell)} \mid \Delta \psi_{k}^{(\ell)}\right\rangle=\operatorname{tr}\left[\left|\psi_{k}^{(\ell)}\right\rangle\left\langle\psi_{k}^{(\ell)}\right| \Delta\right]=0 \quad \text { for all } k=0, \ldots, d-1 \text { and } \ell=1, \ldots, m, \tag{1}
\end{equation*}
$$

implies the equality of the probability distributions:

$$
\begin{equation*}
\operatorname{tr}\left[\varrho\left|\psi_{k}^{(\ell)}\right\rangle\left\langle\psi_{k}^{(\ell)}\right|\right]=\operatorname{tr}\left[\varrho^{\prime}\left|\psi_{k}^{(\ell)}\right\rangle\left\langle\psi_{k}^{(\ell)}\right|\right] \tag{2}
\end{equation*}
$$

and hence the impossibility to distinguish between $\varrho$ and $\varrho^{\prime}$ from the measurement statistics. Therefore, perturbation operators provide a convenient way to analyse which pairs of states a given measurement can distinguish. In other words, as the name 'perturbation operator' suggests, we see that we are in fact studying if the state $\varrho$ can be distinguished from its perturbed version $\varrho+\delta \Delta$.

We say that a perturbation operator $\Delta$ is detected by a measurement setup if for any state $\varrho$, the two states $\varrho$ and $\varrho+\delta \Delta$ give different measurement data whenever the scaling parameter $\delta$ is such that the latter operator is a valid state; otherwise $\Delta$ is undetected. It depends on the geometry of the property that we are considering which perturbation operators must be detected and which are allowed to be undetected; see figure 2.

For certifying coherence (task (a)), a suitable measurement setup must be able to detect differences between coherent and incoherent states. Quite naturally, this means that all perturbation operators with at least some nonzero off-diagonal elements must be detected. To see this, note that for any perturbation $\Delta$, there exists a sufficiently small $\delta>0$ such that $\eta=\frac{1}{d} \mathbb{1}+\delta \Delta$ is a valid state. Clearly $\eta$ is coherent if and only if $\Delta$ has nonzero


Figure 2. The subset of states sharing a property $\mathcal{P}$ (e.g. coherence) is represented with the green colour. Any measurement distinguishing property $\mathcal{P}$ needs to detect the perturbation operator $\Delta_{2}$, as the direction of $\Delta_{2}$ crosses the boundary of $\mathcal{P}$. This does not happen for the perturbation operator $\Delta_{1}$, which therefore needs not to be detected.
off-diagonal elements, and since $\frac{1}{d} \mathbb{1}$ is incoherent, such $\Delta$ 's must be detected. Since diagonal perturbation operators can never be written as differences of coherent and incoherent states, their detection is irrelevant to us. This allows us to summarize the above discussion in the following statement.

Proposition 1. A measurement setup consisting of m bases completes task (a) if and only if all the undetected perturbation operators are diagonal in the reference basis.

This result gives a lower bound for the minimal number $m$. First of all, we observe that the undetected perturbations form a subspace of traceless selfadjoint operators. The dimension of this subspace cannot exceed $d-1$, since this is the dimension of the subspace of all diagonal perturbation operators. The defining equation (1) for undetected perturbation operators means that the undetected perturbations $\Delta$ are the orthogonal complement of the projections $\left|\psi_{k}^{(\ell)}\right\rangle\left\langle\psi_{k}^{(\ell)}\right|$ in the Hilbert-Schmidt inner product. Since the dimension of the real vector space of all selfadjoint operators is $d^{2}$, the required measurement setup must span a subspace of at least dimension $d^{2}-d+1$. Since $m$ bases give at most $d+(m-1)(d-1)$ linearly independent operators, this means that task (a) cannot be solved with less than $d$ orthonormal bases.

The next theorem is the main result of this section.
Theorem 1. Any measurement setup that completes task (a) also completes task (b).
Proof. Assume that we have a measurement setup $\left\{\psi_{k}^{(1)}\right\}_{k=0}^{d-1}, \cdots,\left\{\psi_{k}^{(m)}\right\}_{k=0}^{d-1}$ that completes task (a). By proposition 1 , any undetected perturbation operator $\Delta$ must be diagonal, and hence in the linear span of the operators $D_{j}=\left|\varphi_{j}\right\rangle\left\langle\varphi_{j}\right|-\left|\varphi_{j-1}\right\rangle\left\langle\varphi_{j-1}\right|$, where $1 \leqslant j \leqslant d-1$. For all indices $0 \leqslant j<k \leqslant d-1$, we further denote $A_{j, k}^{+}=\frac{1}{2}\left(\left|\varphi_{j}\right\rangle\left\langle\varphi_{k}\right|+\left|\varphi_{k}\right\rangle\left\langle\varphi_{j}\right|\right)$ and $A_{j, k}^{-}=\frac{i}{2}\left(\left|\varphi_{j}\right\rangle\left\langle\varphi_{k}\right|-\left|\varphi_{k}\right\rangle\left\langle\varphi_{j}\right|\right)$. Since the selfadjoint operators $A_{j, k}^{+}$ and $A_{j, k}^{-}$are orthogonal to all $D_{i}$ 's, they are also orthogonal to all the undetected perturbations $\Delta$. Hence $A_{j, k}^{+}$ and $A_{j, k}^{-}$must be in the linear span of the projections $\left|\psi_{k}^{(\ell)}\right\rangle\left\langle\psi_{k}^{(\ell)}\right|$, and the expectations $\operatorname{tr}\left[\varrho A_{j, k}^{+}\right], \operatorname{tr}\left[\varrho A_{j, k}^{-}\right]$can be evaluated from the probabilities $\left\langle\psi_{k}^{(\ell)} \mid \varrho \psi_{k}^{(\ell)}\right\rangle$. We observe that for any $j<k$, we have

$$
\begin{equation*}
\varrho_{j, k}=\operatorname{tr}\left[\varrho A_{j, k}^{+}\right]+i \operatorname{tr}\left[\varrho A_{j, k}^{-}\right] . \tag{3}
\end{equation*}
$$

Therefore, we can calculate the off-diagonal elements of $\varrho$ from the measurement data and hence calculate $C_{1}(\varrho)$ or any other measure of coherence.

## 3. Minimal measurement setups

### 3.1. Minimality implies mutual unbiasedness

We have concluded in section 2.2 that task (a) cannot be completed with less than $d$ orthonormal bases.
Although we have not yet shown that a suitable set of $d$ bases exists, we will next see what implications this would have. To this end, suppose that there is a set of $d$ bases $\left\{\psi_{k}^{(1)}\right\}_{k=0}^{d-1}, \cdots,\left\{\psi_{k}^{(d)}\right\}_{k=0}^{d-1}$ which completes task (a). By direct counting, the dimension of the corresponding subspace of undetected perturbation operators needs to be
at least $d-1$, hence we see that (1) must hold whenever $\Delta$ is a diagonal perturbation operator. In other words, there is no room to detect any perturbations that are not relevant for the task at hand.

Since the operators $\left|\varphi_{i}\right\rangle\left\langle\varphi_{i}\right|-\left|\varphi_{j}\right\rangle\left\langle\varphi_{j}\right|$ with $i \neq j$ span the subspace of diagonal perturbation operators, we find that (1) is equivalent to

$$
\begin{equation*}
\left|\left\langle\psi_{k}^{(\ell)} \mid \varphi_{i}\right\rangle\right|=\left|\left\langle\psi_{k}^{(\ell)} \mid \varphi_{j}\right\rangle\right| . \tag{4}
\end{equation*}
$$

But this is nothing else than the mutual unbiasedness condition for the reference basis and each measurement basis. Therefore, if a collection of $d$ bases completes task (a), then each basis must be mutually unbiased with respect to the reference basis.

There is an additional property that we can infer from the assumed minimal set of $d$ bases. The reference basis detects all diagonal perturbations. Hence, if we measure the reference basis together with the assumed set of $d$ bases, we can detect all perturbations. We summarize this discussion in the following theorem.

Theorem 2. A minimal measurement setup consisting of d bases completes task (a) (equivalently (b)) if and only if
(i) each basis is mutually unbiased with respect to the reference basis; and
(ii) together with the reference basis they form an informationally complete set.

We still need to show that $d$ orthonormal bases with these two required properties can be constructed in all dimensions.

### 3.2. Construction of a minimal setup

From theorem 2, it follows that, in the prime power dimensions, the construction of a minimal measurement setup is straightforward: we pick a complete set of $d+1 \mathrm{MUB}$, apply a unitary transformation which transforms one of the bases into the reference basis, and then drop out the reference basis. Since any complete set of MUB is informationally complete [21], it is an immediate consequence of theorem 2 that the remaining set of $d$ MUB completes tasks (a) and (b). For other dimensions we need to seek a different construction. However, one can expect this to be possible since the condition (i) in theorem 2 is a seemingly weaker condition than having a complete set of MUB.

First, let us recall a simple way to write a MUB with respect to a given one [26]. We denote $\omega=\mathrm{e}^{2 \pi \mathrm{i} / d}$. For each $j=0, \ldots, d-1$, we fix a complex number $\beta_{j}$ with $\left|\beta_{j}\right|=1$. Then, for each $k=0, \ldots, d-1$, we define a unit vector

$$
\begin{equation*}
\psi_{k}=\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \beta_{j} \omega^{j k} \varphi_{j} . \tag{5}
\end{equation*}
$$

It is straightforward to check that $\left\{\psi_{k}\right\}_{k=0}^{d-1}$ is an orthonormal basis and that it is unbiased with respect to the reference basis $\left\{\varphi_{j}\right\}_{j=0}^{d-1}$. Since the choice of the phases $\beta_{j}$ is arbitrary, we can construct arbitrarily many orthonormal bases that are mutually unbiased with respect to the reference basis. However, this is not enough as we also need to satisfy the condition (ii) in theorem 2 . We thus need to choose the phases $\beta_{j}$ in a specific way

For the construction of the bases having the required property, we need some additional notation. We denote by $\mathbb{Z}_{d}$ the ring of integers $\{0,1, \ldots, d-1\}$, where the addition and multiplication is understood modulo $d$. For clarity, we denote by $\dot{+}$ the addition modulo $d$. Unless $d$ is prime, $\mathbb{Z}_{d}$ has zero divisors, i.e., nonzero elements that give 0 when multiplied with some other nonzero element (e.g. in $\mathbb{Z}_{6}$ we have $2 \cdot 3=0$ modulo 6). This is the underlying fact why there are relatively easy constructions of complete set of MUB in prime dimensions but similar constructions do not work if the dimension is a composite number. For this reason, we define a map $s$ : $\mathbb{Z}_{d} \rightarrow \mathbb{Z}$ that maps $x \in \mathbb{Z}_{d}$ into $x \in \mathbb{Z}$. The purpose of the map $s$ is that we can use the modular arithmetic of $\mathbb{Z}_{d}$ when needed, but then perform calculations in $\mathbb{Z}$ when that is more convenient as $\mathbb{Z}$ has no zero divisors. Using this map we can now choose orthonormal bases in the following way:

Theorem 3. Let $\alpha$ be an irrational number. For each $\ell=1, \ldots, d$, define an orthonormal basis $\psi_{k}^{(\ell)}$ by

$$
\begin{equation*}
\psi_{k}^{(\ell)}=\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \mathrm{e}^{\alpha \pi \mathrm{i}(\ell-1) s(j)^{2}} \omega^{j k} \varphi_{j} \quad k=0, \ldots, d-1 . \tag{6}
\end{equation*}
$$

The set $\left\{\psi_{k}^{(1)}\right\}_{k=0}^{d-1}, \cdots,\left\{\psi_{k}^{(d)}\right\}_{k=0}^{d-1}$ is a minimal measurement setup consisting of d bases which accomplishes task (a).
Proof. By proposition 1, we need to verify that any undetected perturbation operator for this measurement setup is diagonal. To do this, we write a perturbation operator as $\Delta=\sum_{i, j} \nu_{i, j}\left|\varphi_{i}\right\rangle\left\langle\varphi_{j}\right|$. Taking the discrete Fourier transform of (1) with respect to index $k$, we obtain

$$
\begin{equation*}
\sum_{k=0}^{d-1} \omega^{-x k}\left\langle\psi_{k}^{(\ell)} \mid \Delta \psi_{k}^{(\ell)}\right\rangle=\sum_{j=0}^{d-1} \mathrm{e}^{\alpha \pi \mathrm{i}(\ell-1)\left[s(j+x)^{2}-s(j)^{2}\right]} \nu_{j, j \dot{j}+x} \equiv 0, \tag{7}
\end{equation*}
$$

which is required to hold for all $x \in \mathbb{Z}_{d}$ and $\ell=1, \ldots, d$. Since we need to confirm that $\nu_{j, j+x}=0$ for any $x \neq 0$, we fix $x \neq 0$ and consider (7) for $\ell=1, \ldots, d$ as a system of linear equations. It is then found that the corresponding matrix is invertible (a detailed mathematical calculation is given in the appendix), which means that $\nu_{j, j+x} \equiv 0$ is the only solution. Therefore, the measurement setup consisting of the $d$ orthonormal bases written in (6) completes tasks (a) and (b).

### 3.3. Reconstruction formula for off-diagonal elements

Having at disposal the explicit form of a minimal measurement setup for the determination of quantum coherence, one can write a reconstruction formula for the off-diagonal elements using only the measurement outcome probabilities of these bases. To do this, we denote

$$
\begin{equation*}
p^{(\ell)}(k)=\left\langle\psi_{k}^{(\ell)} \mid \varrho \psi_{k}^{(\ell)}\right\rangle \quad k=0, \ldots, d-1, \tag{8}
\end{equation*}
$$

where $\psi_{k}^{(\ell)}$ are given in (6). Then, the reconstruction formula reads as follows.
Theorem 4. With the notations above

$$
\begin{equation*}
\varrho_{h, h+z}=\left\langle\varphi_{h} \mid \varrho \varphi_{h+z}\right\rangle=\sum_{j, k=0}^{d-1} \frac{x_{h}(-1)^{d-j} \omega^{-k z}}{\prod_{i \neq h}\left(x_{h}-x_{i}\right)} \sigma_{d-j, d-1}^{h} p^{(j+1)}(k) . \tag{9}
\end{equation*}
$$

where $x_{h}=\mathrm{e}^{\alpha \pi \mathrm{i}\left[s(h+z)^{2}-s(h)^{2}\right]}$, and $\sigma_{r, d-1}^{h}$ is the sum of all products of r of the numbers $x_{1}, \ldots, x_{h-1}, x_{h+1}, \ldots, x_{d-1}$ without permutations or repetitions $\left(\sigma_{0, d-1}^{h} \equiv 1\right.$ ).

Proof. According to (7),

$$
\begin{equation*}
\sum_{k=0}^{d-1} \omega^{-k z} p^{(\ell)}(k)=\sum_{h=0}^{d-1} V_{\ell-1, h} \varrho_{h, h+z}, \tag{10}
\end{equation*}
$$

where $\left(V_{j, h}\right)_{j, h=0, \ldots, d-1}$ is the Vandermonde matrix

$$
\begin{equation*}
V_{j, h}=x_{h}^{j} \quad \text { with } \quad x_{h}=\mathrm{e}^{\alpha \pi \mathrm{i}\left[s(h \dot{+})^{2}-s(h)^{2}\right]} . \tag{11}
\end{equation*}
$$

Its inverse is [27]

$$
\begin{equation*}
\left(V^{-1}\right)_{h, j}=\frac{x_{h}(-1)^{d-j}}{\prod_{i \neq h}\left(x_{h}-x_{i}\right)} \sigma_{d-j, d-1}^{h} . \tag{12}
\end{equation*}
$$

Therefore,

$$
\begin{equation*}
\varrho_{h, h+z}=\sum_{j, k=0}^{d-1}\left(V^{-1}\right)_{h, j} \omega^{-k z} p^{(j+1)}(k)=\sum_{j, k=0}^{d-1} \frac{x_{h}(-1)^{d-j} \omega^{-k z}}{\prod_{i \neq h}\left(x_{h}-x_{i}\right)} \sigma_{d-j, d-1}^{h} p^{(j+1)}(k) . \tag{13}
\end{equation*}
$$

## 4. Completion of task (c)

In order to make task (c) more precise, we need to use a specific measure of coherence. We will use the $\ell_{1}$-norm of coherence, defined as

$$
\begin{equation*}
C_{1}(\varrho)=\sum_{j \neq k}\left|\varrho_{j, k}\right| . \tag{14}
\end{equation*}
$$

This measure clearly vanishes exactly for incoherent states, and the maximal value of $C_{1}$ is $d-1$ [12]. As we did earlier in the case of tasks (a) and (b), we aim to determine the minimal requirement for a measurement setup to be capable of deciding, for any state $\varrho$, whether $C_{1}(\varrho)$ is greater than a fixed threshold value $r(d-1)$ with $0<r<1$, or not. In the following we show that this task requires exactly the same measurement settings as the previously considered tasks.

Theorem 5. A measurement setup consisting of m bases completes task (c) (with respect to $C_{1}$ ) if and only if it completes task (a) (or (b)).

Proof. By proposition 1 it is enough to show that a measurement setup completes task (c) if and only if it detects all the perturbation operators that are not diagonal in the reference basis. Indeed, if $C_{1}(\varrho) \leqslant r(d-1)$ and
$C_{1}\left(\varrho^{\prime}\right)>r(d-1)$, it is clear that the difference $\Delta=\varrho^{\prime}-\varrho$ is a non-diagonal perturbation operator; hence, detecting all non-diagonal perturbations is a sufficient condition for completing task (c). To prove the reverse implication, it is enough to show that for any non-diagonal perturbation operator $\Delta$, there exist states $\varrho$ and $\varrho^{\prime}=\varrho+\delta \Delta$ with $C_{1}(\varrho) \leqslant r(d-1)$ and $C_{1}\left(\varrho^{\prime}\right)>r(d-1)$.

To prove this statement, we fix a family of maximally coherent states $|\psi\rangle_{\phi}=\frac{1}{\sqrt{d}} \sum_{k=1}^{d} \mathrm{e}^{\mathrm{i} \phi_{k}}|k\rangle$, parametrized by an array of phases $\phi=\left(\phi_{1}, \ldots, \phi_{d}\right) \in[0,2 \pi)^{d}$. The convex mixture

$$
\begin{equation*}
\varrho_{\phi}^{r}=(1-r) \frac{\mathbb{1}}{d}+r|\psi\rangle_{\phi}\left\langle\left.\psi\right|_{\phi}, \quad 0<r<1,\right. \tag{15}
\end{equation*}
$$

is then a full-rank state with $C_{1}\left(\varrho_{\phi}^{r}\right)=r(d-1)$. It follows that the operator $\varrho_{\phi}^{r}+(\delta r / d) \Delta$ is still a valid state for all $|\delta|<(1-r) /(r\|\Delta\|)$, independently of the array of phases $\phi$.

Let $f_{\phi}(\delta)=C_{1}\left(\varrho_{\phi}^{r}+(\delta r / d) \Delta\right)$, where $\Delta$ is any non-diagonal perturbation operator. In the following we show that the function $f_{\phi_{0}}(\delta)$ has a nonzero derivative at the point $\delta=0$ for some set of parameters $\phi_{0}$. Possibly replacing $\delta$ with $-\delta$, this then yields $f_{\phi_{0}}(\delta)>f_{\phi_{0}}(0)$ for some $\delta \neq 0$, which is what we want to show.

Let $\Delta=A+\mathrm{i} B$ be the decomposition of $\Delta$ into its real symmetric and antisymmetric parts. A straightforward computation gives

$$
\begin{equation*}
f_{\phi}(\delta)=C_{1}\left(\varrho_{\phi}^{r}+\delta \frac{r}{d} \Delta\right)=\frac{r}{d} \sum_{p \neq q}\left[\left(\cos \left(\phi_{p}-\phi_{q}\right)+\delta A_{p, q}\right)^{2}+\left(\sin \left(\phi_{p}-\phi_{q}\right)+\delta B_{p, q}\right)^{2}\right]^{\frac{1}{2}} . \tag{16}
\end{equation*}
$$

Therefore,

$$
\begin{equation*}
g(\phi)=\left.f_{\phi}^{\prime}(\delta)\right|_{\delta=0}=\frac{2 r}{d} \sum_{p>q}\left[A_{p, q} \cos \left(\phi_{p}-\phi_{q}\right)+B_{p, q} \sin \left(\phi_{p}-\phi_{q}\right)\right] . \tag{17}
\end{equation*}
$$

We can now use the freedom in the choice of $\phi$ to obtain the result. Indeed, if $r>s$ we have

$$
\begin{align*}
& \iint_{[0,2 \pi)^{2}} g(\phi) \cos \left(\phi_{r}-\phi_{s}\right) \mathrm{d} \phi_{r} \mathrm{~d} \phi_{s}=\frac{(2 \pi)^{2} r}{d} A_{p, q},  \tag{18}\\
& \iiint_{[0,2 \pi)^{2}} g(\phi) \sin \left(\phi_{r}-\phi_{s}\right) \mathrm{d} \phi_{r} \mathrm{~d} \phi_{s}=\frac{(2 \pi)^{2} r}{d} B_{p, q} .
\end{align*}
$$

Hence, if $g(\phi)=0$ for every $\phi \in[0,2 \pi)^{d}$, then $A_{p, q}=B_{p, q}=0$ for every $p \neq q$, and $\Delta$ is diagonal, against our assumption.

## 5. General measurement setups

One may wonder if the proven equivalence of the tasks (a)-(c) is due to the fact that we consider only measurement setups that are related to orthonormal bases. A more general concept of a quantum measurement is that of a POVM. Using the perturbation operator method analogously as we have done earlier, one can show that the tasks (a)-(c) are equivalent also when we consider POVM measurements. Further, the minimal number of elements of a single POVM that can solve these tasks is found to be $d^{2}-d+1$. Since any measurement setup of $d$ bases yields a single POVM with $d^{2}-d+1$ elements which detects exactly the same perturbation operators, the optimal measurement setup constructed earlier then provides an optimal POVM measurement. In the following we explain the details of these statements.

Instead of a measurement setup consisting of $m$ orthonormal bases $\left\{\psi_{k}^{(1)}\right\}_{k=0}^{d-1}, \ldots,\left\{\psi_{k}^{(m)}\right\}_{k=0}^{d-1}$, a single POVM $\left\{E_{k}\right\}_{k=0}^{r-1}$ or even a collection of $m$ POVMs $\left\{E_{k}^{(1)}\right\}_{k=0}^{r_{1}-1}, \ldots,\left\{E_{k}^{(m)}\right\}_{k=0}^{r_{m}-1}$ may be used for tasks (a)-(c). Here, $r_{\ell}$ is the number of outcomes of the $\ell$ th POVM. Then, the perturbation operators $\Delta$ that are undetected by the POVMs at hand are those that satisfy the following analogue of (1):

$$
\operatorname{tr}\left[\Delta E_{k}^{(\ell)}\right]=0 \quad \text { for all } k=0, \ldots, r_{\ell}-1 \text { and } \ell=1, \ldots, m .
$$

By replacing each occurrence of the basis projections $\left|\psi_{k}^{(\ell)}\right\rangle\left\langle\psi_{k}^{(\ell)}\right|$ with the positive operators $E_{k}^{(\ell)}$, the same considerations leading to proposition 1 and theorems 1 and 5 yield the next conclusions.

Theorem 6. For a collection of m POVMs $\left\{E_{k}^{(1)}\right\}_{k=0}^{r_{1}-1}, \ldots,\left\{E_{k}^{(m)}\right\}_{\substack{r_{m}-1 \\ k=0}}^{\substack{\text {, the }}}$ following facts hold:

## 1. tasks (a)-(c) are equivalent;

2. the collection completes the three equivalent tasks (a)-(c) if and only if all the undetected perturbation operators are diagonal in the reference basis.

As in the $m$ bases case, theorem 6 gives a lower bound for the number of outcomes of $m$ POVMs completing tasks (a)-(c): the POVM operators $\left\{E_{k}^{(\ell)}: k=1, \ldots, r_{\ell}, \ell=1, \ldots, m\right\}$ must span a subspace of at least dimension $d^{2}-d+1$ inside the real vector space of all selfadjoint operators; since the $m$ POVMs give at most

$$
\begin{equation*}
r_{1}+\sum_{\ell=2}^{m}\left(r_{\ell}-1\right)=\sum_{\ell=1}^{m} r_{\ell}-m+1 \tag{19}
\end{equation*}
$$

linearly independent operators, this sum must be greater than or equal to $d^{2}-d+1$.
Now, one may be interested in using a single POVM $\left\{E_{k}\right\}_{k=0}^{r-1}$ in order to complete one of the equivalent tasks (a)-(c). In this case, the amount of needed quantum resources is the number $r$ of the required measurement outcomes. By the discussion above, it must be $r \geqslant d^{2}-d+1$; the next result shows that such a lower bound is actually attained.

Theorem 7. For a single POVM, the minimal number of outcomes needed to complete one of the three equivalent tasks $(a)-(c)$ is $r=d^{2}-d+1$

Proof. The POVM $\left\{E_{0}, E_{\ell, k}: \ell=1, \ldots, d, k=1, \ldots, d-1\right\}$, with

$$
\begin{align*}
E_{0} & =\frac{1}{d-1} \mathbb{1}-\frac{1}{d^{2}-d} \sum_{\ell=1}^{d}\left|\psi_{0}^{(\ell)}\right\rangle\left\langle\psi_{0}^{(\ell)}\right|,  \tag{20}\\
E_{\ell, k} & =\frac{1}{d^{2}-d}\left(\mathbb{1}-\left|\psi_{k}^{(\ell)}\right\rangle\left\langle\psi_{k}^{(\ell)}\right|\right) \quad \ell=1, \ldots, d, k=1, \ldots, d-1
\end{align*}
$$

is a $\left(d^{2}-d+1\right)$-outcome POVM detecting the same perturbation operators as those detected by the $d$ orthogonal bases $\left\{\psi_{k}^{(1)}\right\}_{k=0}^{d-1}, \ldots,\left\{\psi_{k}^{(d)}\right\}_{k=0}^{d-1}$. Indeed,

$$
\begin{align*}
\left|\psi_{0}^{(\ell)}\right\rangle\left\langle\psi_{0}^{(\ell)}\right| & =\left(d^{2}-d\right) \sum_{k=1}^{d-1} E_{\ell, k}-(d-2) \mathbb{1}  \tag{21}\\
\left|\psi_{k}^{(\ell)}\right\rangle\left\langle\psi_{k}^{(\ell)}\right| & =\mathbb{1}-\left(d^{2}-d\right) E_{\ell, k} .
\end{align*}
$$

Then, by choosing $d$ bases which complete the tasks, e.g., those given by formula (6), we obtain a POVM with the same property.

## 6. Certification of entanglement of maximally correlated states

We show that the certification of entanglement of bipartite maximally correlated states is intimately connected with the certification of coherence. This result is based on [24]. Here, we give a brief account of that paper in a form that is more suited to our framework and discuss some direct consequences of the previous sections.

We let $\mathbb{C}^{d}$ be the Hilbert space of our quantum system, and in it we choose the computational basis $\left\{\varphi_{j}=|j\rangle\right\}_{j=0}^{d-1}$ as the reference basis. We recall that a bipartite state on $\mathbb{C}^{d} \otimes \mathbb{C}^{d}$ is called maximally correlated if it is of the form

$$
\begin{equation*}
\tilde{\varrho}=\sum_{i, j=0}^{d-1} \varrho_{i, j}|i\rangle\langle j| \otimes|i\rangle\langle j| . \tag{22}
\end{equation*}
$$

We define a unitary map $U: \mathbb{C}^{d} \otimes \mathbb{C}^{d} \rightarrow \mathbb{C}^{d} \otimes \mathbb{C}^{d}$ as

$$
\begin{equation*}
U=\sum_{i, j=0}^{d-1}|i\rangle\langle i| \otimes|i+j\rangle\langle j|, \tag{23}
\end{equation*}
$$

whereas usual $\dot{+}$ is the addition modulo $d$. We then denote the corresponding unitary channel as $\Lambda$, i.e., $\Lambda(\tilde{\varrho})=U^{*} \tilde{\varrho} U$. Note that $\Lambda=\left(\Lambda^{S A}\right)^{-1}$, where $\Lambda^{S A}$ is the incoherent operation defined in [24, equation (10)] for the particular case when the dimension of the ancilla equals that of the system.

If $\tilde{\varrho}$ is as in (22), it is easily checked that

$$
\begin{equation*}
\Lambda(\tilde{\varrho})=\varrho \otimes|0\rangle\langle 0| \quad \text { where } \quad \varrho=\sum_{i, j} \varrho_{i, j}|i\rangle\langle j| . \tag{24}
\end{equation*}
$$

Hence, the channel $\Lambda$ establishes a bijective correspondence between maximally correlated bipartite states on $\mathbb{C}^{d} \otimes \mathbb{C}^{d}$ and all states on $\mathbb{C}^{d}$. Even more is true; indeed as it is shown in [24], we have the following fact.

Proposition 2. The maximally correlated state $\varrho$ of (22) is entangled if and only if the state $\varrho$ of (24) is coherent.
Proof. The result follows from the following three facts:

1. a state $\sigma$ on $\mathbb{C}^{d} \otimes \mathbb{C}^{d}$ is entangled if and only if

$$
E_{r}(\sigma)>0
$$

where $E_{r}$ is the relative entropy of entanglement (see [28, equation (7)]);
2. a state $\varrho$ on $\mathbb{C}^{d}$ is coherent if and only if

$$
C_{r}(\varrho)>0
$$

where $C_{r}$ is the relative entropy of coherence (see [12, equation (8)]);
3. with the notations above, we have

$$
C_{r}(\varrho)=E_{r}\left(\sum_{i, j} \varrho_{i, j}|i\rangle\langle j| \otimes|i\rangle\langle j|\right)
$$

(see [24, equations (8), (10)]).

Hence, if we have any maximally correlated state $\tilde{\varrho}$ and we want to determine whether it is entangled or not, we can first apply the channel $\Lambda$, then trace away the second system which is always in the fixed state $|0\rangle\langle 0|$, and finally perform a measurement on the first system. The initial maximally correlated state $\tilde{\varrho}$ being entangled is now equivalent to the final state $\varrho=\operatorname{tr}_{2}[\Lambda(\tilde{\varrho})]$ being coherent. Certifying entanglement of $\tilde{\varrho}$ is thus equivalent to task (a) for the final state $\varrho$; in particular, such a task requires a POVM with least $d^{2}-d+1$ outcomes in the bipartite system.

Combining proposition 2 with theorem 3, we easily obtain also the following result.
Theorem 8. The vectors $\left\{\tilde{\xi}_{j, k}\right\}_{j, k=0}^{d-1}$, with

$$
\begin{equation*}
\tilde{\xi}_{j, k}=\frac{1}{d} \sum_{x, y=0}^{d-1} \mathrm{e}^{\alpha \pi \mathrm{ij}(x)^{2}} \omega^{x(k-j)+y j}|x\rangle \otimes|y\rangle, \tag{25}
\end{equation*}
$$

constitute an orthonormal basis of $\mathbb{C}^{d} \otimes \mathbb{C}^{d}$, which accomplishes the task of certifying the presence or absence of entanglement in an unknown maximally correlated state.
Proof. Let $\left\{\psi_{k}^{(1)}\right\}_{k=0}^{d-1}, \cdots,\left\{\psi_{k}^{(d)}\right\}_{k=0}^{d-1}$ be the measurement setup given by (6). Note that $\left\{\psi_{k}^{(j+1)} \otimes \psi_{j}^{(1)}\right\}_{j, k=0}^{d-1}$ is an orthonormal basis of $\mathbb{C}^{d} \otimes \mathbb{C}^{d}$, and $\tilde{\xi}_{j, k}=U\left(\psi_{k}^{(j+1)} \otimes \psi_{j}^{(1)}\right)$, where $U$ is the unitary operator (23). Hence, the set $\left\{\tilde{\xi}_{j, k} d_{j, k=0}^{d-1}\right.$ is an orthonormal basis of $\mathbb{C}^{d} \otimes \mathbb{C}^{d}$. If the states $\tilde{\varrho}, \varrho$ are as in (22), (24), then

$$
\begin{aligned}
\frac{1}{d}\left\langle\psi_{k}^{(\ell)} \mid \varrho \psi_{k}^{(\ell)}\right\rangle & =\left\langle\psi_{k}^{(\ell)} \otimes \psi_{\ell-1}^{(1)} \mid(\varrho \otimes|0\rangle\langle 0|)\left(\psi_{k}^{(\ell)} \otimes \psi_{\ell-1}^{(1)}\right)\right\rangle \\
& =\left\langle\psi_{k}^{(\ell)} \otimes \psi_{\ell-1}^{(1)} \mid U^{*} \tilde{\varrho} U\left(\psi_{k}^{(\ell)} \otimes \psi_{\ell-1}^{(1)}\right)\right\rangle \\
& =\left\langle\tilde{\xi}_{\ell-1, k} \mid \tilde{\varrho} \tilde{\xi}_{\ell-1, k}\right\rangle .
\end{aligned}
$$

Since the measurement setup $\left\{\psi_{k}^{(1)}\right\}_{k=0}^{d-1}, \cdots,\left\{\psi_{k}^{(d)}\right\}_{k=0}^{d-1}$ accomplishes the task of certifying coherence of $\varrho$ by theorem 3, the basis $\left\{\tilde{\xi}_{j, k}\right\}_{j, k=0}^{d-1}$ certifies entanglement of $\tilde{\varrho}$ by proposition 2 .

This result should be compared with the fact that, for certifying the presence or absence of entanglement in an arbitrary bipartite state, at least $d^{2}+1$ orthonormal bases of $\mathbb{C}^{d} \otimes \mathbb{C}^{d}$ are needed [20].

## 7. Discussion

The development of quantum technologies will bring us applications capable of outperforming any of their classical counterparts. The superiority of these applications rests on the ability to take advantage of properties of physical systems which are genuinely quantum. For this reason, it is essential to be able to verify that a given source produces systems which have such a property. Here we have investigated optimal measurement strategies for verifying the presence of quantum coherence. We have shown that this simple verification task is actually as difficult as determining the exact value of quantum coherence. We have both characterized the optimal setups in terms of a mutual unbiasedness condition, as well as constructed explicit examples in arbitrary dimensions.

One of the core assumptions behind our results is that there is no prior information available regarding the initial state of the system at hand. In many practical situations this may not be the case, and by exploiting the
available prior information it may be possible to further optimize the setup. As a simple example, suppose that we know the system to be in a pure state. Then quantum coherence can be verified by simply measuring the reference basis, as the incoherent states are exactly the eigenstates of this observable. The geometric framework exploited in this work is flexible enough to be used also in questions with prior information.

It has been recently shown that there are connections between the theories of coherence and entanglement [24]. This allows us to find direct applications of our results in the context of entanglement detection. Indeed, the problem of detecting the entanglement of an unknown maximally correlated state can be translated into the coherence detection problem. In particular, we found that the minimal number of POVM elements needed for detecting the entanglement of a maximally correlated state is $d^{2}-d+1$, and that a measurement setup made up of only one orthonormal basis is enough for such a task; these should be compared with the respective numbers $d^{4}$ and $d^{2}+1$, which are needed for general bipartite states [20]. This drastic reduction serves as a motivation for further studies regarding the exploitation of this connection within our framework.

## Acknowledgments

The authors thank Tom Bullock for his comments on an earlier version of this paper. TH and SM acknowledge financial support from the Horizon 2020 EU collaborative projects QuProCS (Grant Agreement No. 641277), the Academy of Finland (Project no. 287750), and the Magnus Ehrnrooth Foundation. This work was performed as part of the Academy of Finland Centre of Excellence program (project 312058).

Appendix. Proof that $\nu_{j, j+x}=0$ for any $x \neq 0$.
In the main text we have obtained the equation

$$
\begin{equation*}
\sum_{j=0}^{d-1} \mathrm{e}^{\alpha \pi \mathrm{i}(\ell-1)\left[s(j+x)^{2}-s(j)^{2}\right]} \nu_{j, j+x}=0, \tag{26}
\end{equation*}
$$

required to hold for all $x \in \mathbb{Z}_{d}$ and $\ell=1, \ldots, d$. We need to confirm that $\nu_{j, j+x}=0$ for any $x \neq 0$, and for this purpose we fix $x \neq 0$ and consider (26) for $\ell=1, \ldots, d$ as a system of linear equations. We denote

$$
u_{x}(j)=\mathrm{e}^{\alpha \pi \mathrm{i}\left[s(j+x)^{2}-s(j)^{2}\right]},
$$

and observe that the matrix of the linear system (26) is a Vandermonde matrix generated by the numbers $\left(u_{x}(j)\right)_{j=0}^{d-1}$. Hence, its determinant equals to

$$
\begin{equation*}
\prod_{(i<i \leqslant d-1}\left(u_{x}(j)-u_{x}(i)\right) . \tag{27}
\end{equation*}
$$

The last effort is to verify that all the factors in this product are nonzero. Since $\alpha$ is irrational, we see that $u_{x}(j)=u_{x}(i)$ if and only if

$$
\begin{equation*}
s(j \dot{+} x)^{2}-s(j)^{2}=s(i \dot{+} x)^{2}-s(i)^{2} . \tag{28}
\end{equation*}
$$

We thus need to prove that the only solution to (28) is $i=j$ as the expression (27) contains only terms with $i \neq j$.

We recall that the function $s$ is defined as $s: \mathbb{Z}_{d} \rightarrow \mathbb{Z}, s(x)=x$. For two elements $x, y \in \mathbb{Z}_{d}$, we have

$$
s(x-y)= \begin{cases}s(x)-s(y) & \text { if } s(x) \geqslant s(y),  \tag{29}\\ s(x)-s(y)+d & \text { if } s(x)<s(y),\end{cases}
$$

where - denotes the subtraction modulo $d$.
The following result is the last step needed in the construction of the $d$ bases.
Proposition 3. Let $x, i, j \in \mathbb{Z}_{d}$ and $x \neq 0$. Then, the only solution to (28) is $i=j$.
Proof. One can prove the claim by considering the different possible cases separately, i.e., $s(j \dot{+} x) \geqslant s(j)$ and $s(j+x)<s(j)$. We go through the first case, the latter being similar.

Assume $s(j+x) \geqslant s(j)$. Then by (28) we also have $s(i+x) \geqslant s(i)$. Using (29) we can thus write $s(j \dot{+} x)-s(j)=s(x)$ and $s(i+x)-s(i)=s(x)$, and (28) becomes

$$
\begin{equation*}
s(x)(s(j \dot{+} x)+s(j))=s(x)(s(i \dot{+} x)+s(i)) . \tag{30}
\end{equation*}
$$

As $s(x) \neq 0$, we further get

$$
\begin{equation*}
s(j \dot{+} x)+s(j)=s(i+x)+s(i) . \tag{31}
\end{equation*}
$$

We then split the proof further into two cases.
(a) Assume $s(j) \geqslant s(i)$. From (31), it follows that $s(i+x) \geqslant s(j+x)$. Using (29) and (31), we obtain

$$
\begin{equation*}
s(j-i)=s(i-j) \tag{32}
\end{equation*}
$$

and further

$$
\begin{equation*}
2(j-i)=0 \text { modulo } d \tag{33}
\end{equation*}
$$

due to the injectivity of $s$. If $d$ is odd, then (33) immediately implies $i=j$. If $d$ is even, then either $i=j$ or $s(j-i)=d / 2$. Since $s(j) \geqslant s(i)$ and $s(i+x) \geqslant s(j+x)$, by (29) the latter option can be realized only if $s(j) \geqslant d / 2, s(i)<d / 2$ and $s(i+x) \geqslant d / 2, s(j \dot{+} x)<d / 2$. But this is not consistent with assumed condition $s(j \dot{+} x) \geqslant s(j)$. We thus conclude that $i=j$.
(b) Assume $s(j)<s(i)$. From (31) it follows that $s(i \dot{+} x)<s(j \dot{+} x)$. Using (29) and (31), we obtain (32) and (33) as in the previous case. Then, the rest of the proof is similar.

## ORCIDiDs

Claudio Carmeli © https:// orcid.org/0000-0003-1660-3677
Teiko Heinosaari © https:// orcid.org/0000-0003-2405-5439
Alessandro Toigo (1) https:// orcid.org/0000-0003-1715-2441

## References

[1] Plenio M B, Streltsov A and Adesso G 2017 Quantum coherence as a resource Rev. Mod. Phys. 89041003
[2] Hillery M 2016 Coherence as a resource in decision problems: the Deutsch-Jozsa algorithm and a variation Phys. Rev. A 93012111
[3] Streltsov A, Chitambar E, Rana S, Bera M N, Winter A and Lewenstein M 2016 Entanglement and coherence in quantum state merging Phys. Rev. Lett. 116240405
[4] Winter A and Yang D 2016 Operational resource theory of coherence Phys. Rev. Lett. 116120404
[5] Streltsov A, Rana S, Bera M N and Lewenstein M 2017 Towards resource theory of coherence in distributed scenarios Phys. Rev. X 7 011024
[6] Girolami D 2014 Observable measure of quantum coherence in finite dimensional systems Phys. Rev. Lett. 113170401
[7] Wang Y-T, Tang J-S, Wei Z-Y, Yu S, Ke Z-J, Xu X-Y, Li C-F and Guo G-C 2017 Directly measuring the degree of quantum coherence using interference fringes Phys. Rev. Lett. 118020403
[8] Chitambar E and Gour G 2016 Comparison of incoherent operations and measures of coherence Phys. Rev. A 94052336
[9] Napoli C, Bromley T R, Cianciaruso M, Piani M, Johnston N and Adesso G 2016 Robustness of coherence: an operational and observable measure of quantum coherence Phys. Rev. Lett. 116150502
[10] Rastegin A E 2016 Quantum-coherence quantifiers based on the Tsallis relative $\alpha$ entropies Phys. Rev. A 93032136
[11] Horn R A and Johnson C R 1991 Matrix Analysis (Cambridge: Cambridge University Press)
[12] Baumgratz T, Cramer M and Plenio M B 2014 Quantifying coherence Phys. Rev. Lett. 113140401
[13] Rana S, Parashar P, Winter A and Lewenstein M 2017 Logarithmic coherence: operational interpretation of $\ell_{1}$-norm coherence Phys. Rev. A 96052336
[14] Prugovečki E 1977 Information-theoretical aspects of quantum measurements Int. J. Theor. Phys. 16 321-31
[15] Busch P and Lahti P 1989 The determination of the past and the future of a physical system in quantum mechanics Found. Phys. 19 633-78
[16] Busch P 1991 Informationally complete sets of physical quantities Int. J. Theor. Phys. 30 1217-27
[17] Singer M and Stulpe W 1992 Phase-space representations of general statistical physical theories J. Math. Phys. 33 131-42
[18] Chen J, Dawkins H, Ji Z, Johnston N, Kribs D, Shultz F and Zeng B 2013 Uniqueness of quantum states compatible with given measurement results Phys. Rev. A 88012109
[19] Carmeli C, Heinosaari T, Schultz J and Toigo A 2017 Probing quantum state space: does one have to learn everything to learn something? Proc. R. Soc. A 47320160866
[20] Carmeli C, Heinosaari T, Karlsson A, Schultz J and Toigo A 2016 Verifying the quantumness of bipartite correlations Phys. Rev. Lett. 116230403
[21] Wootters W K and Fields B D 1989 Optimal state-determination by mutually unbiased measurements Ann. Phys. 191 363-81
[22] Carmeli C, Schultz J and Toigo A 2016 Covariant mutually unbiased bases Rev. Math. Phys. 281650009
[23] Durt T, Englert B-G, Bengtsson I and Zyczkowski K 2010 On mutually unbiased bases Int. J. Quantum Inf. 8535-640
[24] Streltsov A, Singh U, Dhar H S, Bera M N and Adesso G 2015 Measuring quantum coherence with entanglement Phys. Rev. Lett. 115 020403
[25] Carmeli C, Heinosaari T, Schultz J and Toigo A 2014 Tasks and premises in quantum state determination J. Phys. A: Math. Theor. 47 0753092
[26] Bandyopadhyay S, Boykin P O, Roychowdhury V and Vatan F 2002 A new proof for the existence of mutually unbiased bases Algorithmica 34 512-28
[27] Macon N and Spitzbart A 1958 Inverses of Vandermonde matrices Am. Math. Mon. 65 95-100
[28] Vedral V, Plenio M B, Rippin M A and Knight P L 1997 Quantifying entanglement Phys. Rev. Lett. 782275

