JOURNAL OF MATHEMATICAL PHYSICS **56**, 122104 (2015)

Hamiltonian purification

Davide Orsucci,[1] Daniel Burgarth,[2] Paolo Facchi,[3,4] Hiromichi Nakazato,[5] Saverio Pascazio,[3,4] Kazuya Yuasa,[5] and Vittorio Giovannetti[6]
[1]*Scuola Normale Superiore, I-56126 Pisa, Italy*
[2]*Department of Mathematics, Aberystwyth University, Aberystwyth SY23 3BZ, United Kingdom*
[3]*Dipartimento di Fisica and MECENAS, Università di Bari, I-70126 Bari, Italy*
[4]*INFN, Sezione di Bari, I-70126 Bari, Italy*
[5]*Department of Physics, Waseda University, Tokyo 169-8555, Japan*
[6]*NEST, Scuola Normale Superiore and Istituto Nanoscienze-CNR, I-56126 Pisa, Italy*

(Received 26 May 2015; accepted 10 November 2015; published online 4 December 2015)

The problem of Hamiltonian purification introduced by Burgarth *et al.* [Nat. Commun. **5**, 5173 (2014)] is formalized and discussed. Specifically, given a set of non-commuting Hamiltonians $\{h_1, \dots, h_m\}$ operating on a d-dimensional quantum system $\mathscr{H}_d$, the problem consists in identifying a set of commuting Hamiltonians $\{H_1, \dots, H_m\}$ operating on a larger d_E-dimensional system $\mathscr{H}_{d_E}$ which embeds $\mathscr{H}_d$ as a proper subspace, such that $h_j = PH_jP$ with P being the projection which allows one to recover $\mathscr{H}_d$ from $\mathscr{H}_{d_E}$. The notions of spanning-set purification and generator purification of an algebra are also introduced and optimal solutions for $\mathfrak{u}(d)$ are provided. © *2015 AIP Publishing LLC.* [http://dx.doi.org/10.1063/1.4936311]

I. INTRODUCTION

The possibility of achieving control over a quantum system is the fundamental prerequisite for developing a new form of technology based on quantum effects.[1–3] In particular, this is an essential requirement for quantum computation, quantum communication, and more generally for all other data processing procedures that involve quantum systems as information carriers.[4]

In many experimental settings, quantum control is implemented via an electromagnetic field interacting with the system of interest, as happens for *cold atoms* in optical lattices,[5] for *trapped ions*,[6] for *electrons* in quantum dots,[7] and actually in all experiments in low energy physics. In this context, the electromagnetic field can be often treated as a classical field (in the limit of many quanta), allowing a semiclassical description of control over the quantum system.[8–10] Furthermore in many cases of physical interest, the whole process can be effectively formalized by assuming that via proper manipulation of the field parameters the experimenter produces a series of pulses implementing some specially engineered control Hamiltonians from a discrete set $\{H_1, \dots, H_m\}$. Such pulses are assumed to be applied in any order, for any duration, by switching them on and off very sharply, the resulting transformation being a unitary evolution of the form $e^{-iH_{j_N}t_N} \cdots e^{-iH_{j_1}t_1}$ with $j_1, \dots, j_N \in \{1, \dots, m\}$ and $t_1, \dots, t_N$ being the selected temporal durations (here and hereafter $\hbar$ is set to unity for simplicity).[24] By the *Lie-algebraic rank condition*,[8] the unitary operators that can be realized via such a procedure are those in the connected Lie group associated to the real Lie algebra $\mathfrak{Lie}(H_1, \dots, H_m)$ generated by the Hamiltonians $\{H_1, \dots, H_m\}$, where $\mathfrak{Lie}(H_1, \dots, H_m)$ is formed by the real linear combinations of H_j and their iterated commutators $i[H_{j_1}, H_{j_2}]$, $i[H_{j_1}, i[H_{j_2}, H_{j_3}]]$, etc., i.e., operators in the form $e^{-i\Xi}$ with $\Xi \in \mathfrak{Lie}(H_1, \dots, H_m)$. In this framework, one then says that full (unitary) controllability is achieved if the dimension of $\mathfrak{Lie}(H_1, \dots, H_m)$ is large enough to permit the implementation of all possible unitary transformations on the system, i.e., if $\mathfrak{Lie}(H_1, \dots, H_m)$ coincides with the complete algebra $\mathfrak{u}(d)$ formed by self-adjoint $d \times d$ complex matrices,[25] d being the dimension of the controlled system.

The above scheme is the paradigmatic example of what is typically identified as *open-loop* or *non-adaptive* control, where all the operations are completely determined prior to the control experiment.[8,9] In other words, the system is driven in the absence of an external feedback loop, i.e., without using any information gathered (via measurement) *during* the evolution. It turns out that in quantum mechanics, an alternative mechanism of non-adaptive control is available: it is enforced via quantum Zeno dynamics.[11,12] In this scenario, while measurements are present, the associated outcomes are not used to guide the forthcoming operations: only their effects on the system evolution are exploited (a fact which has no analog in the classical domain). The underlying physical principle is the following. When a quantum system undergoes a sharp (von Neumann) measurement, it is projected into one of the associated eigenspaces of the observable, say, the space $\mathscr{H}_P$ characterized by an orthogonal projection P. It is then let to undergo a unitary evolution $e^{-iH\Delta t}$ for a short time Δt and is measured again via the same von Neumann measurement. The probability to find it in a different measurement eigenspace $\mathscr{H}_{P'}$ orthogonal to the original one $\mathscr{H}_P$ is proportional to $(\Delta t)^2$. Instead, with high probability, the system remains in $\mathscr{H}_P$, while experiencing an effective unitary rotation of the form $e^{-ih\Delta t}$ induced by the projected Hamiltonian $h := PHP$.[11–13] Accordingly, in the limit of infinitely frequent measurements performed within a fixed time interval t, the system remains in the subspace $\mathscr{H}_P$, evolving through an effective *Zeno dynamics* described by the operator

$$\lim_{N\to\infty} (Pe^{-iHt/N}P)^N = Pe^{-iPHPt} = Pe^{-iht}. \tag{1}$$

In Ref. 14, it was shown that, by adopting the quantum Zeno dynamics, the control that the experimenter can enforce on a quantum system can be greatly enhanced. For example, consider the case where the set of engineered Hamiltonians contains only two commuting elements H_1 and H_2. The associated Lie algebra they generate is just two-dimensional and hence is not sufficient to induce full controllability, even for the smallest quantum system, a qubit—indeed $\dim[\mathfrak{u}(d = 2)] = 4$. Under these conditions, it turns out that for a proper choice of the projection P it may happen that the projected counterparts $h_1 = PH_1P$ and $h_2 = PH_2P$ of the control Hamiltonians do not commute. Accordingly, the Lie algebra generated by $\{h_1, h_2\}$ can be much larger than the one associated with $\{H_1, H_2\}$, and consequently the control exerted much finer. In particular, the enhancement can be exponential in the system size. For instance, in Ref. 14, an explicit example is given where two commuting Hamiltonians H_1 and H_2 act on a chain of n qubits, and once a proper Zeno projection P is applied on the first qubit of the chain, the resulting Zeno Hamiltonians h_1 and h_2 generate the full algebra of traceless Hermitian operators acting on the remaining $n - 1$ qubits (which is a Lie algebra of dimension 4^{n-1}), thus allowing one to perform any unitary operations on them. Moreover, it can be shown that this is indeed a quite general phenomenon. In fact, a simple argument[14] shows that if a system is controllable for a specific choice of the parameters, then it is controllable for almost all choices of the parameters (with respect, e.g., to the Lebesgue measure). In the present case, it means that, for almost all choices of a rank-2^{n-1} projection P and of two commuting Hamiltonians $\{H_1, H_2\}$, the system is fully controllable in the projected subspace $\mathscr{H}_P$ with the Hamiltonians $h_1 = PH_1P$ and $h_2 = PH_2P$.

The aforementioned results of Ref. 14 show that as few as two commuting Hamiltonians, when projected on a smaller subspace of dimension d through the Zeno mechanism, may generate the whole Lie algebra $\mathfrak{u}(d)$. The scope of the present article is to investigate the opposite question: given a set of Hamiltonians $\{h_1, \ldots, h_m\}$, which are non-commuting in general, is it possible to extend them to a set of commuting Hamiltonians $\{H_1, \ldots, H_m\}$ from which h_j can be obtained via a proper projection of the latter (i.e., $h_j = PH_jP$)? We call this operation *Hamiltonian purification*, taking inspiration from similar problems which have been investigated in quantum information. For instance, we recall that by the *state purification*,[4] a quantum mixed state ρ on a system $S \cong \mathscr{H}_d$ is extended to a pure state $|\psi_\rho\rangle$ on a system $S + A \cong \mathscr{H}_d \otimes \mathscr{H}_d$, from which ρ can be recovered through a partial trace over the ancilla system $A \cong \mathscr{H}_d$. Another similar result can be obtained for the *channel purification (Stinespring dilation theorem)* or for the *purification of positive operator-valued measure (POVM) (Naimark extension theorem)*, according to which all the completely positive trace-preserving linear maps and all the generalized measurement procedures, respectively, can be described as unitary transformations on an extended system followed by partial trace.[4,15]

In what follows, we start by presenting a formal characterization of the Hamiltonian purification problem and of the associated notions of *spanning-set purification* and *generator purification* of an algebra (see Sec. II). Then, we prove some theorems regarding the minimal dimension $d_E^{(\min)}$ of the extended Hilbert space needed to purify any given set of operators $\{h_1, \ldots, h_m\}$. Specifically, in Sec. III, we analyze the case in which one is interested in purifying two linearly independent Hamiltonians. In this context, we provide the exact result $d_E^{(\min)} = 2d - 1$ when the input Hilbert space has dimension d. In Sec. IV, instead we present a generic construction which allows one to put a bound on $d_E^{(\min)}$ when the set of the operators $\{h_1, \ldots, h_m\}$ contains an arbitrary number m of linearly independent elements. In Sec. V, we discuss the case in which the total number of linearly independent elements of $\{h_1, \ldots, h_m\}$ is maximum, i.e., equal to d^2 with d being the dimension of the input Hilbert space. Under this condition, we compute the exact value of $d_E^{(\min)}$, showing that it is equal to d^2. As we shall see, this corresponds to providing a spanning-set purification of the whole algebra $\mathfrak{u}(d)$ in terms of the largest commutative subalgebra of $\mathfrak{u}(d^2)$. Finally in Sec. VI, we prove that it is always possible to obtain a generator purification of the algebra $\mathfrak{u}(d)$ with an extended space of dimension $d_E = d + 1$, i.e., in terms of the largest commutative subalgebra of $\mathfrak{u}(d + 1)$. Conclusions and perspectives are given in Sec. VII, and the proof of a theorem is presented in the Appendix.

II. DEFINITIONS AND BASIC PROPERTIES

In this section, we start by presenting a rigorous formalization of the problem and discuss some basic properties.

Definition 1 (Hamiltonian purification). Let $\mathcal{S} := \{h_1, \ldots, h_m\}$ be a collection of m self-adjoint operators (Hamiltonians) acting on a Hilbert space $\mathscr{H}_d$ of dimension d. Given then a collection $\mathcal{S}_{ext} := \{H_1, \ldots, H_m\}$ of self-adjoint operators acting on an extended Hilbert space $\mathscr{H}_{d_E}$ which includes $\mathscr{H}_d$ as a proper subspace (i.e., $d_E = \dim \mathscr{H}_{d_E} \geq d$), we say that $\mathcal{S}_{ext}$ provides a purification *for $\mathcal{S}$ if all elements of $\mathcal{S}_{ext}$* commute *with each other, i.e.,*

$$[H_j, H_{j'}] = 0, \quad \textit{for all } j, j', \tag{2}$$

and are related to those of $\mathcal{S}$ as

$$h_j = P H_j P, \quad \textit{for all } j, \tag{3}$$

where P is the orthogonal projection onto $\mathscr{H}_d$.[26]

Notice that each element of $\mathcal{S}_{\text{ext}}$ in general depends upon *all* the operators of the set $\mathcal{S}$ which one wishes to purify and not just upon the one it extends.

A problem which is mathematically equivalent to the one given in the above definition, specialized to a set of just two non-commuting Hermitian matrices, was first considered in the mathematical literature in Ref. 16 and then in Refs. 17–19. Moreover, the closely related problem of finding the "commuting extensions" of sets of real symmetric matrices (rather than of Hermitian matrices) was investigated in Ref. 20. Many results for those special cases are related to our work. In order to keep the exposition as straightforward and self-contained as possible, we will reproduce here the theorems that are most relevant for the discussion, in a form that is directly applicable to the Hamiltonian purification problem.

We begin stating some useful properties of the purification set that will allow one to simplify the analysis of the problem.

Lemma 1. Let $\mathcal{S} = \{h_1, \ldots, h_m\}$ be a collection of self-adjoint operators acting on the Hilbert space $\mathscr{H}_d$ and suppose that a purifying set $\mathcal{S}_{ext} = \{H_1, \ldots, H_m\}$ can be constructed on $\mathscr{H}_{d_E}$. Then, we have the following:

1. *Given $\mathcal{S}' = \{h'_1, \ldots, h'_{m'}\}$ a collection of self-adjoint operators obtained by taking linear combinations of the elements of $\mathcal{S}$, i.e.,*

$$h'_i = \sum_{j=1}^{m} \alpha_{i,j} h_j, \tag{4}$$

with $\alpha_{i,j}$ being elements of a real rectangular $m' \times m$ matrix, then a purifying set for $\mathcal{S}'$ on $\mathcal{H}_{d_E}$ is provided by $\mathcal{S}'_{ext} = \{H'_1, \ldots, H'_{m'}\}$ with elements

$$H'_i = \sum_{j=1}^{m} \alpha_{i,j} H_j. \tag{5}$$

2. *Any subset of linearly independent elements of $\mathcal{S}$ corresponds to a subset of linearly independent elements in $\mathcal{S}_{ext}$ (the opposite statement being not true in general, i.e., linear independence among the elements of $\mathcal{S}_{ext}$ does not imply linear independence among the elements of $\mathcal{S}$).*
3. *For $\lambda_1, \ldots, \lambda_m \in \mathbb{R}$, calling I_d the identity on $\mathcal{H}_d$ and I_{d_E} the identity on $\mathcal{H}_{d_E}$, a purifying set for*

$$\{h_1 + \lambda_1 I_d, \ldots, h_m + \lambda_m I_d\} \tag{6}$$

is given by

$$\{H_1 + \lambda_1 I_{d_E}, \ldots, H_m + \lambda_m I_{d_E}\}. \tag{7}$$

4. *For any unitary $U \in \mathcal{U}(d)$, setting $\widetilde{U} = U \oplus I_{d_E - d} \in \mathcal{U}(d_E)$, a purifying set for*

$$\{U h_1 U^\dagger, \ldots, U h_m U^\dagger\} \tag{8}$$

is given by

$$\{\widetilde{U} H_1 \widetilde{U}^\dagger, \ldots, \widetilde{U} H_m \widetilde{U}^\dagger\}. \tag{9}$$

Proof. These facts are all trivially verified. □

Property 1 of Lemma 1 implies that a purifying set $\mathcal{S}_{\text{ext}} = \{H_1, \ldots, H_m\}$ can be extended by linearity to a purification of any linear combinations of the elements of $\mathcal{S} = \{h_1, \ldots, h_m\}$. Accordingly, we can say that the purification of $\mathcal{S}$ by $\mathcal{S}_{\text{ext}}$ naturally induces a purification of the algebra spanned by the former by the algebra of the latter (more on this in Sec. II A). It is also clear that the fundamental parameter of the Hamiltonian purification problem is not the number of elements of $\mathcal{S}$ but instead the maximum number of linearly independent elements which can be found in $\mathcal{S}$. Therefore, without loss of generality, in the following we will assume m to coincide with such a number, i.e., that all the elements of $\mathcal{S}$ are linearly independent. Then, by Property 2 of Lemma 1 also the elements of $\mathcal{S}_{\text{ext}}$ share the same property. By the same token, also the normalization of the operators h_j can be fixed *a priori*. Property 3 can be used instead to assume that all the elements of $\mathcal{S}$ be traceless (an option which we shall invoke from time to time to simplify the analysis). Finally, Property 4 can be exploited to arbitrarily fix a basis on $\mathcal{H}_d$, e.g., the one which diagonalizes the first element of $\mathcal{S}$.

Lemma 2. The operators $\{H_1, \ldots, H_m\}$ are pairwise commuting if and only if such a set spans an Abelian (i.e., commutative) subalgebra of $\mathfrak{u}(d_E)$, so that H_j can be simultaneously diagonalized with a single unitary operator U,

$$H_1 = U D_1 U^\dagger, \ldots, H_m = U D_m U^\dagger, \tag{10}$$

with $D_1, \ldots, D_m$ being real diagonal matrices.

Proof. A formal proof of this fact can be found, e.g., in chapter 4 of Ref. 21. Here, we simply remember that in the formalism of quantum mechanics, this property is equivalent to the statement that each Hermitian operator in $\{H_1, \ldots, H_m\}$ can be written as

$$H_i = \sum_{\alpha} \lambda_\alpha^{(i)} |\psi_\alpha\rangle\langle\psi_\alpha| \tag{11}$$

where $|\psi_\alpha\rangle$ for $\alpha \in \{1, \ldots, d\}$ is a common set of orthonormal eigenvectors for all operators H_i and $\lambda_\alpha^{(i)}$ are the relative real eigenvalues. □

As we shall see in Secs. III and IV, the mere possibility of finding a purification for a generic set $\mathcal{S}$ can be easily proved. A less trivial issue is to determine the *minimal* dimension $d_E^{(\text{min})}(\mathcal{S})$ of the Hilbert space $\mathcal{H}_{d_E}$ which guarantees the existence of a purifying set for a given collection $\mathcal{S}$. We will also study the minimal dimension that allows one to obtain a purification for *any* collection $\mathcal{S}$ of m operators acting on $\mathscr{H}_d$, and we will denote this value with $d_E^{(\min)}(d,m)$. By construction, it is clear that such a quantity cannot be smaller than d and than m, i.e.,

$$d_E^{(\min)}(d,m) \geq \max\{d,m\}. \tag{12}$$

This is a simple relation which, on one side, follows from the observation that $\mathscr{H}_{d_E}$ being an extension of $\mathscr{H}_d$ must have dimension d_E at least as large as d. On the other hand, the inequality $d_E^{(\min)} \geq m$ can be verified by exploiting the fact that the diagonal $d_E \times d_E$ matrices D_j entering Eq. (10) must be linearly independent in order to fulfill Property 2 of Lemma 1. Actually for all non-trivial cases, the inequality is strict, resulting in

$$d_E^{(\min)}(d,m) \geq \max\{d+1,m+1\}. \tag{13}$$

In fact, when the initial Hamiltonians $\{h_1,\ldots,h_m\}$ do not already commute, we need to expand the dimension of the space at least by one, obtaining $d_E^{(\min)}(d,m) \geq d+1$. Moreover, the inequality $d_E \geq m+1$ always holds, unless the identity I_d lies in the span of $\{h_1,\ldots,h_m\}$. Suppose in fact that we could purify a set of m linearly independent Hamiltonians in dimension m, then the linear span of the m (linearly independent) diagonal matrices D_j in Lemma 2 includes also the identity matrix I_{d_E}. Because for any unitary U we have $UI_{d_E}U^\dagger = I_{d_E}$, the projection of I_{d_E} on $\mathscr{H}_d$ gives the identity on that subspace, and in conclusion we have that $I_d \in \mathrm{span}(h_1,\ldots,h_m)$. Since this is not true in the general case, we obtain $d_E^{(\min)}(d,m) \geq m+1$.

A. Algebra purification

As anticipated above in Sec. II, the linearity property of the Hamiltonian purification scheme allows us to introduce the notion of purification of an algebra. Specifically, there are at least two different possibilities:

Definition 2 (Purification(s) of an algebra). Let $\mathfrak{a}$ *be a Lie algebra of self-adjoint operators on* $\mathscr{H}_d$*. Given a commutative Lie algebra* $\mathfrak{A}$ *of self-adjoint operators on* $\mathscr{H}_{d_E}$ *we say that it provides the following:*

1. *a spanning-set purification (or simply an algebra purification) of* $\mathfrak{a}$ *when we can provide a Hamiltonian purification of a spanning set (e.g., a basis) of the latter in* $\mathfrak{A}$*;*
2. *a generator purification of* $\mathfrak{a}$ *when we can provide a Hamiltonian purification of a generating set of the latter in* $\mathfrak{A}$*.*

The spanning-set purification typically requires the purification of more Hamiltonians than the generator purification. For instance in Sec. V, we shall see that the (optimal) spanning-set purification of $\mathfrak{u}(d)$ requires $\mathfrak{A}$ to be the largest commutative subalgebra of $\mathfrak{u}(d^2)$, while in Sec. VI, we shall see that the generator purification requires $\mathfrak{A}$ to be the largest commutative subalgebra of $\mathfrak{u}(d+1)$. At the level of quantum control via the Zeno effect, the advantage posed by the spanning-set purification is associated with the fact that, in contrast to the scheme based on generator purification, no complicated concatenation of Zeno pulses would be necessary to realize a desired control over a system on $\mathscr{H}_d$: any unitary operator e^{-iht} on the latter can in fact be simply obtained as in Eq. (1) by choosing H to be the linear combination of commuting Hamiltonians which purifies h on $\mathscr{H}_{d^2}$. On the contrary, in the case of generator purification, first we have to decompose e^{-iht} into a sequence of pulses of the form $e^{-ih_{j_N}t_N}\cdots e^{-ih_{j_1}t_1}$ with h_j being taken from the generator sets of operators for which we do have a purification. Then, each of the pulses $e^{-ih_{j_k}t_k}$ entering the previous decomposition is realized as in Eq. (1) with a proper choice of the purifying Hamiltonians. See Fig. 1 for a pictorial representation.

III. PURIFICATION OF $m = 2$ OPERATORS

In this section, we discuss the case of the purification of two linearly independent Hamiltonians (i.e., $m=2$), providing bounds and exact solutions. We first present a few simple illustrative

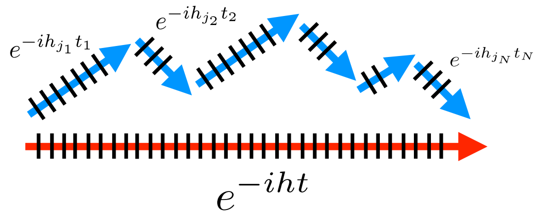

FIG. 1. Pictorial representation of the control achieved via spanning-set purification (red line) and generator purification (blue lines) of an algebra. In the former case, an arbitrary unitary transformation e^{-iht} on $\mathcal{H}_d$ is obtained via single Zeno sequence (1) with H being the purification of h. For generator purification, instead one has to use a collection of Zeno sequences, one for each of the generator pulses $e^{-ih_{j_k}t_k}$ which are needed to implement e^{-iht}. The black tick lines represent the iterated projections on the system.

examples. We show in Proposition 1 how to purify two operators into an extended Hilbert space $\mathcal{H}_{d_E}$ of dimension $d_E = 2d$, and then in Proposition 2 that it is possible to purify a set of two operators acting on a qubit ($d = 2$) into a qutrit system ($d_E = 3$). Then we will move on to prove more general and complex results. Actually, in this special case ($m = 2$) we can leverage the known results for the *normal completion* of a complex matrix[27] to useful criteria for the purification of two Hermitian matrices.

Indeed, we will show that the following equality always holds:

$$d_E^{(\min)}(d, m = 2) = 2d - 1. \tag{14}$$

For a specific choice of $\{h_1, h_2\}$, the following more informative bounds hold:

$$d \;+\; \max(\, i_+(i[h_1, h_2])\,,\, i_-(i[h_1, h_2])\,) \le d_E^{(\min)}(\{h_1, h_2\}) \le 2d - 1, \tag{15}$$

where $i_+(A)$ and $i_-(A)$, respectively, denote the number of strictly positive and strictly negative eigenvalues of a Hermitian operator A. In fact when the traceless Hermitian operator $i[h_1, h_2]$ has $d - 1$ positive (or negative) eigenvalues, the upper and lower bounds of Eq. (15) coincide and we recover Eq. (14). See Theorem 1 (upper bound) and Theorem 2 (lower bound).

Proposition 1 (Purification of $m = 2$ operators with $d_E = 2d$). Let $\mathcal{S} = \{h_1, h_2\}$ be a collection of two self-adjoint operators acting on the Hilbert space $\mathcal{H}_d$. Then, a purifying set can be constructed on $\mathcal{H}_{d_E} = \mathcal{H}_d \otimes \mathcal{H}_2$, with $\mathcal{H}_2$ being two-dimensional (qubit space) (i.e., $d_E = 2d$). In particular, we can take

$$\begin{aligned} H_1 &= h_1 \otimes I_2 + h_2 \otimes X, \\ H_2 &= h_2 \otimes I_2 + h_1 \otimes X, \\ P &= I_d \otimes (I_2 + Z)/2, \end{aligned} \tag{16}$$

where X and Z are the Pauli operators on $\mathcal{H}_2$.[28]

Proof. The proof easily follows from the properties of Pauli operators. But to get a better intuition on what is going on, it is useful to adopt the following block-matrix representation for H_j and P, i.e.,

$$H_1 = \begin{pmatrix} h_1 & h_2 \\ h_2 & h_1 \end{pmatrix}, \quad H_2 = \begin{pmatrix} h_2 & h_1 \\ h_1 & h_2 \end{pmatrix}, \quad P = \begin{pmatrix} I_d & 0 \\ 0 & 0 \end{pmatrix}, \tag{17}$$

from which the commutativity is evident.[29] □

Proposition 2 (Optimal purification of $m = 2$ operators of a qubit). Let $\mathcal{S} = \{h_1, h_2\}$ be a collection composed of two self-adjoint operators acting on the Hilbert space $\mathcal{H}_2$ of a qubit. Then a purifying set can be constructed on the Hilbert space $\mathcal{H}_{d_E}$ of dimension $d_E = 3$ (qutrit space).

Proof. We prove the thesis by providing an explicit purification. To do so, we first notice that, up to irrelevant additive and renormalization factors, the operators h_1 and h_2 can be expressed as

$$h_1 = Z, \qquad h_2 = \alpha Z + \beta(X\cos\theta + Y\sin\theta), \tag{18}$$

with α, β, and θ being real parameters. Indicating then with $\{|0\rangle, |1\rangle\}$ the eigenvectors of Z, we define $\mathcal{H}_{d_E}$ as the space spanned by the vectors $\{|0\rangle, |1\rangle, |2\rangle\}$ with $|2\rangle$ being an extra state which is assumed to be orthogonal to both $|0\rangle$ and $|1\rangle$. We hence introduce the operators on $\mathcal{H}_{d_E}$ which in the basis $\{|0\rangle, |1\rangle, |2\rangle\}$ have the following matrix form:

$$\widetilde{H}_1 = \left(\begin{array}{cc|c} \multicolumn{2}{c|}{\multirow{2}{*}{Z}} & 0 \\ & & \sqrt{2} \\ \hline 0 & \sqrt{2} & 0 \end{array}\right), \qquad \widetilde{H}_2 = \left(\begin{array}{cc|c} \multicolumn{2}{c|}{\multirow{2}{*}{M}} & \sqrt{2}\,e^{-i\theta} \\ & & 0 \\ \hline \sqrt{2}\,e^{i\theta} & 0 & 0 \end{array}\right), \tag{19}$$

with $M := X\cos\theta + Y\sin\theta$. One can easily verify that they commute, $[\widetilde{H}_1, \widetilde{H}_2] = 0$, and when projected on the subspace $\{|0\rangle, |1\rangle\}$, they yield the matrices Z and M, respectively. Defining hence H_1 and H_2 as the operators,

$$H_1 = \widetilde{H}_1, \qquad H_2 = \alpha\widetilde{H}_1 + \beta\widetilde{H}_2, \tag{20}$$

one notices that this is indeed a purifying set of $\mathcal{S}$. □

For arbitrary values of d, an improvement with respect to Proposition 1 is obtained as follows:

Theorem 1 (Purification of $m = 2$ operators with $d_E = 2d - 1$). *Let $\mathcal{S} = \{h_1, h_2\}$ be a collection composed of two self-adjoint operators acting on the Hilbert space $\mathcal{H}_d$. Then, a purifying set can be constructed on $\mathcal{H}_{d_E} = \mathcal{H}_{2d-1}$, implying hence $d_E^{(\min)}(d, m = 2) \le 2d - 1$.*

Proof. A proof of this theorem can be found in Ref. 16, but here we provide a different construction.

According to Eq. (10), to obtain a purifying set, we have to find a unitary matrix $U \in \mathcal{U}(2d - 1)$ such that

$$\begin{aligned} h_1 &= PUD_1U^\dagger P, \\ h_2 &= PUD_2U^\dagger P, \end{aligned} \tag{21}$$

with $D_1, D_2 \in \mathcal{D}iag(2d - 1)$ being real diagonal matrices of dimension $2d - 1$. In $\mathcal{H}_{d_E} = \mathcal{H}_d \oplus \mathcal{H}_{d-1}$, we can write

$$P = \left(\begin{array}{c|c} I_d & 0 \\ \hline 0 & 0_{d-1} \end{array}\right), \qquad PU = \left(\begin{array}{c|c} L & R \\ \hline 0 & 0_{d-1} \end{array}\right), \tag{22}$$

where L is a $d \times d$ matrix, R is a $d \times (d - 1)$ matrix, and the rows of PU are orthogonal to each other, $LL^\dagger + RR^\dagger = I_d$, since $PUU^\dagger P = P$. We then write

$$D_1 = \left(\begin{array}{c|c} D_1^L & 0 \\ \hline 0 & D_1^R \end{array}\right), \quad D_2 = \left(\begin{array}{c|c} D_2^L & 0 \\ \hline 0 & D_2^R \end{array}\right), \tag{23}$$

where D_1^L, D_2^L are diagonal $d \times d$ matrices and D_1^R, D_2^R are diagonal $(d - 1) \times (d - 1)$ matrices. Then we notice that the equations in Eq. (21) are equivalent to

$$\begin{aligned} h_1 &= LD_1^LL^\dagger + RD_1^RR^\dagger, \\ h_2 &= LD_2^LL^\dagger + RD_2^RR^\dagger, \\ LL^\dagger + RR^\dagger &= I_d. \end{aligned} \tag{24}$$

To find the purification, we need to solve these equations.

First equation: we choose without loss of generality h_1 to be positive definite: this can be obtained by adding αI_d with $\alpha > -\min \sigma(h_1)$ [where $\sigma(X)$ denotes the spectrum of X]. Then, $\sqrt{h_1}$ is the Hermitian positive-definite matrix such that $(\sqrt{h_1})^2 = h_1$. We also choose

$$L = \frac{1}{\lambda}\sqrt{h_1}\,V, \tag{25}$$

where V is an arbitrary unitary matrix, $VV^\dagger = I_d$. Notice that for any unitary V, we have $\lambda^2 LL^\dagger = \sqrt{h_1}\,VV^\dagger\sqrt{h_1} = h_1$. Accordingly to solve the first of the equations in Eq. (24), we can simply take $D_1^L = \lambda^2 I_d$ and $D_1^R = 0$.

Third equation: recast the third equation in the form

$$RR^\dagger = I_d - LL^\dagger = I_d - \frac{1}{\lambda^2}h_1. \tag{26}$$

This equation can be solved for R if and only if the right-hand side is a positive semi-definite matrix with non-null kernel. This can be accomplished by choosing $\lambda^2 := \max\sigma(h_1)$, so that the smallest eigenvalue of $I_d - \lambda^{-2}h_1$ is equal to zero (this is easily seen in the basis in which h_1 is diagonal).[30] Explicitly, we can write

$$I_d - \frac{1}{\lambda^2}h_1 = W\left(\begin{array}{c|c} D' & 0 \\ \hline 0 & 0\end{array}\right)W^\dagger = \left(\begin{array}{c|c} W' & 0\end{array}\right)\left(\begin{array}{c|c} D' & 0 \\ \hline 0 & 0\end{array}\right)\left(\begin{array}{c} W'^\dagger \\ \hline 0\end{array}\right), \tag{27}$$

where W and D' are obtained with the spectral theorem and W' is a $d\times(d-1)$ matrix obtained from W deleting its last column. So, a solution to the third equation is given by $R = W'\sqrt{D'}$.

Second equation: we exploit the fact that V is so far an arbitrary unitary matrix. We take $D_2^R = 0$, and then we are left with

$$h_2 = \frac{1}{\lambda^2}\sqrt{h_1}\,VD_2^L V^\dagger\sqrt{h_1} \tag{28}$$

or equivalently

$$\lambda^2 h_1^{-1/2}h_2 h_1^{-1/2} = VD_2^L V^\dagger, \tag{29}$$

which can be solved for V and D_2^L using the spectral theorem.

In conclusion, the explicit purification of h_1 and h_2, with h_1 positive definite is found by extending

$$PU = \left(\begin{array}{c|c} \lambda^{-1}\sqrt{h_1}\,V & W'\sqrt{D'} \\ \hline 0 & 0_{d-1}\end{array}\right) \tag{30}$$

to a unitary matrix U and then expressing H_1 and H_2 as

$$H_1 = U\left(\begin{array}{c|c} \lambda^2 I_d & 0 \\ \hline 0 & 0_{d-1}\end{array}\right)U^\dagger, \quad H_2 = U\left(\begin{array}{c|c} D_2^L & 0 \\ \hline 0 & 0_{d-1}\end{array}\right)U^\dagger. \tag{31}$$

□

Now we introduce a simple lower bound on $d_E^{(\min)}$ on the purification of pairs of Hamiltonians, given by $d_E^{(\min)}(\{h_1,h_2\}) \geq d + \frac{1}{2}\mathrm{rank}(i[h_1,h_2])$. To purify h_1 and h_2, we extend them to H_1 and H_2 by adding $q := d_E - d$ new rows and columns

$$H_1 = \left(\begin{array}{c|c} h_1 & B_1 \\ \hline B_1^\dagger & C_1\end{array}\right), \qquad H_2 = \left(\begin{array}{c|c} h_2 & B_2 \\ \hline B_2^\dagger & C_2\end{array}\right) \tag{32}$$

and we impose $i[H_1,H_2] = 0$ (with a factor i added to deal with Hermitian, rather than anti-Hermitian, operators). Writing the commutator in block form, we obtain the following three equations:

$$\begin{aligned} i\,[h_1,h_2] &= -i(B_1B_2^\dagger - B_2B_1^\dagger)\,, \\ i(h_1B_2 - h_2B_1) &= -i(B_1C_2 - B_2C_1)\,, \\ i(B_1^\dagger B_2 - B_2^\dagger B_1) &= -i[C_1,C_2]\,. \end{aligned} \tag{33}$$

Consider the first of these equations. The ranks of B_1 and B_2 are at most equal to q (the number of their columns), so $-i(B_1B_2^\dagger - B_2B_1^\dagger)$ has rank at most equal to $2q$. Therefore, we have to impose $2q \geq \mathrm{rank}(i[h_1,h_2])$, which is equivalent to $d_E^{(\min)}(\{h_1,h_2\}) \geq d + \frac{1}{2}\,\mathrm{rank}(i[h_1,h_2])$.

In general, any traceless Hermitian operator can be written as $i[h_1,h_2]$;[31] in particular it can be a full rank matrix (rank equal to d). Hence, the previous result immediately holds the inequality $d_E^{(\min)}(d,m=2) \geq \frac{3}{2}d$.

In Theorem 1, we have proved that a purification of two d-dimensional Hamiltonians can always be attained in dimension $d_E \leq 2d-1$. Thus, the lower bound $d_E^{(\min)}(d,m=2) \geq \frac{3}{2}d$, together with the upper bound given in Theorem 1, is sufficient to completely determine $d_E^{(\min)}(d,m=2)$ for pairs of Hamiltonians acting on qubits ($d=2$) and on qutrits ($d=3$). Explicitly we get

$$d_E^{(\min)}(d=2,m=2) = 3, \quad \text{for a qubit,} \tag{34}$$

$$d_E^{(\min)}(d=3,m=2) = 5, \quad \text{for a qutrit.} \tag{35}$$

But actually, we can extend this result and obtain $d_E^{(\min)}(d,m=2) = 2d-1$ for any dimension d. To obtain this result, we use the key theorem proved in Ref. 17, which gives a tighter lower bound for $d_E^{(\min)}(\{h_1,h_2\})$. We reproduce an adapted version of the theorem here.

Theorem 2 (Lower bound on the purification of $m=2$ operators). *Given two Hamiltonians $\{h_1,h_2\}$ acting on $\mathcal{H}_d$, the minimum dimension of the extended space on which it is possible to find a purification is bounded by the inequality $d_E^{(\min)}(\{h_1,h_2\}) \geq d + \max(\, i_+(i[h_1,h_2])\,,\ i_-(i[h_1,h_2])\,)$.*

Proof. We impose Eq. (33). This can be rewritten as

$$i\,[h_1,h_2] = (B_1 + iB_2)(B_1+iB_2)^\dagger - B_1B_1^\dagger - B_2B_2^\dagger. \tag{36}$$

We denote with $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_d$ the eigenvalues of $B_{1+2} := (B_1+iB_2)(B_1+iB_2)^\dagger$ and with $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_d$ the eigenvalues of $B_{1+2} - B_1B_1^\dagger - B_2B_2^\dagger$. Notice that B_{1+2} is a positive semi-definite operator of rank at most $q := d_E - d$, so its last $d-q$ eigenvalues are equal to 0, i.e., $\mu_{q+1} = \cdots = \mu_d = 0$. We now appeal to the Courant-Fischer min-max theorem (a formal proof of which can be also found in chapter 4 of Ref. 21) to obtain for any $k \in \{1,\ldots,d\}$,

$$\lambda_k = \max_{\substack{V\subset\mathcal{H}_{d_E}\\ \dim(V)=k}} \min_{|x\rangle\in V} \langle x|B_{1+2} - B_1B_1^\dagger - B_2B_2^\dagger|x\rangle \leq \max_{\substack{V\subset\mathcal{H}_{d_E}\\ \dim(V)=k}} \min_{|x\rangle\in V} \langle x|B_{1+2}\,|x\rangle = \mu_k, \tag{37}$$

in which the maximum is taken over all vectors $|x\rangle$ in V which are normalized to one, and the minimum over all the k-dimensional subspaces V contained in $\mathcal{H}_{d_E}$. Hence inequality (37) tells us that for $k \geq q+1$, we have $\lambda_k \leq \mu_k = 0$, and so the right hand side of Eq. (33) has at most q strictly positive eigenvalues. This forces us to impose $q \geq i_+(i[h_1,h_2])$.

For the negative eigenvalues of $i[h_1,h_2]$, we notice that Eq. (33) can be rewritten as

$$-i\,[h_1,h_2] = (B_2+iB_1)(B_2+iB_1)^\dagger - B_1B_1^\dagger - B_2B_2^\dagger \tag{38}$$

and then the same argument as above also applies to the negative eigenvalues. □

Corollary 1. The minimum dimension $d_E^{(\min)}$ on which it is possible to purify any arbitrary set of two Hamiltonians $\{h_1,h_2\}$ acting on $\mathcal{H}_d$ is greater or equal to $2d-1$, i.e., $d_E^{(\min)}(d,m=2) \geq 2d-1$. Because of Theorem 1, the bound is tight.

Proof. It is sufficient to notice that, because $i[h_1,h_2]$ can be an arbitrary traceless Hermitian matrix[31] in d dimensions, it can have up to $d-1$ strictly positive (or strictly negative) eigenvalues. In such a case, the inequality given in Theorem 2 implies $d_E^{(\min)}(\{h_1,h_2\}) \geq 2d-1$, hence the thesis. □

IV. PURIFICATION OF ARBITRARY NUMBER OF OPERATORS

Here, we will provide two different explicit constructions which generalize Proposition 1 to the case in which $\mathcal{S}$ is composed of $m \geq 2$ linearly independent elements. The first method is presented in Theorem 3 and provides a simple method which allows one to purify an arbitrary set $\mathcal{S}$ in dimension $d_E = dm$. We notice that an analogous result, based on block circulant matrices, was derived in Ref. 20 (see Theorem 1 of that reference): however, that specific method is not directly applicable to our case as the resulting extensions are never Hermitian, except in the case $m = 2$, in which case it coincides with the construction given in Proposition 1. The second construction we analyze is presented in Theorem 4 (see below). It is slightly more involved than the one given in Theorem 3 but it yields a Hamiltonian purification which uses an extended space of dimension $d_E = m(d-1)+1$, hence allowing us to prove the following upper bound:

$$d_E^{(\min)}(d,m) \le m(d-1)+1. \tag{39}$$

Notice that for $m = 2$, it reduces to the result proven in Theorem 1 [$d_E^{(\min)}(d, m=2) \le 2d-1$]; this is tight because of Corollary 1, while for larger values of m, on the contrary, inequality (39) is not tight.

Theorem 3 (Purification of m operators with $d_E = md$). *Let $\mathcal{S} = \{h_1, \ldots, h_m\}$ be a collection of self-adjoint operators acting on the Hilbert space $\mathcal{H}_d$. Then, a purifying set can be constructed on $\mathcal{H}_{d_E} = \mathcal{H}_d \otimes \mathcal{H}_m$, implying hence $d_E^{(\min)}(d,m) \le md$.*

Proof. We work in a fixed orthonormal basis, in which $\{|e_1\rangle, \ldots, |e_d\rangle\}$ span $\mathcal{H}_d$, $\{|f_1\rangle, \ldots, |f_m\rangle\}$ span $\mathcal{H}_m$, and thus $\{|e_\ell\rangle \otimes |f_i\rangle\}_{\ell\in\{1,\ldots,d\}, i\in\{1,\ldots,m\}}$ span the extended space $\mathcal{H}_{d_E} = \mathcal{H}_d \otimes \mathcal{H}_m$. We then use the spectral theorem to write $h_i = U_i D_i U_i^\dagger$, $\forall i$, with D_i and U_i being operators which, in the orthonormal basis $\{|e_1\rangle, \ldots, |e_d\rangle\}$, are described by diagonal and unitary matrices, respectively. A purifying set can then be assigned by introducing the following operator in $\mathcal{H}_{d_E}$:

$$W := \frac{1}{\sqrt{m}} \sum_{i=1}^{m} U_i \otimes f_{1i}, \tag{40}$$

where $f_{ij} := |f_i\rangle\langle f_j|$, $f_i := f_{ii} = |f_i\rangle\langle f_i|$. One gets

$$WW^\dagger = \frac{1}{m} \sum_{i,j=1}^{m} U_i U_j^\dagger \otimes f_{1i} f_{j1} = I_d \otimes f_1 =: P. \tag{41}$$

Therefore, W is a partial isometry in $\mathcal{H}_{d_E}$ and P is the orthogonal projection onto its range $\mathcal{H}_d \otimes \mathbb{C}|f_1\rangle \cong \mathcal{H}_d$. Now consider its polar decomposition $W = PU$ for some (non-unique) unitary U on $\mathcal{H}_{d_E}$. [In terms of representative matrices in the canonical basis, the projection P selects the first d rows of an arbitrary $md \times md$ matrix. Therefore, since the first d rows of W are orthonormal, they can be extended to build up a unitary matrix $U \in \mathcal{U}(md)$, such that $W = PU$.] By explicit computation, one can then observe that the following identity holds:

$$h_i \otimes f_1 = PU(mD_i \otimes f_i)U^\dagger P. \tag{42}$$

Accordingly, the purifying set can be identified with the operators $H_i = U(mD_i \otimes f_i)U^\dagger$. □

We now give the second more involved construction that achieves a tighter lower bound.

Theorem 4 (Purification of m operators with $d_E = m(d-1)+1$). *Let $\mathcal{S} = \{h_1, \ldots, h_m\}$ be a collection of self-adjoint operators acting on the Hilbert space $\mathcal{H}_d$. Then, a purifying set can be constructed on a space $\mathcal{H}_{d_E}$ of dimension $d_E = m(d-1)+1$, implying hence $d_E^{(\min)}(d,m) \le m(d-1)+1$.*

Proof. According to Lemma 2 to construct a purifying set in dimension $d_E = m(d-1)+1$, we have to find a unitary matrix $U \in \mathcal{U}(m(d-1)+1)$ such that

$$h_i = PUD_iU^\dagger P, \qquad \forall i \in \{1, \ldots, m\}, \tag{43}$$

with $D_i \in \mathcal{D}iag(m(d-1)+1)$ being real diagonal matrices of dimension $m(d-1)+1$. In $\mathcal{H}_{d_E} = \mathcal{H}_d \oplus \left(\bigoplus_{i=2}^m \mathcal{H}_{d-1}\right)$, we can write in block form

$$PU = \left(\begin{array}{c|c|c|c} R_1 & R_2 & \cdots & R_m \\ \hline 0 & 0_{d-1} & \cdots & 0 \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & \cdots & 0_{d-1} \end{array}\right), \tag{44}$$

where R_1 is a $d \times d$ matrix, R_k are $d \times (d-1)$ matrices for $k \in \{2, 3, \ldots, m\}$ (i.e., for $k \neq 1$), and the first d rows of PU are mutually orthogonal and normalized to one, $\sum_{k=1}^m R_k R_k^\dagger = I_d$, since $PUU^\dagger P = P$. We then write $\forall i \in \{1, \ldots, m\}$,

$$D_i = \left(\begin{array}{c|c|c|c} D_1^{(i)} & 0 & \cdots & 0 \\ \hline 0 & D_2^{(i)} & \cdots & 0 \\ \hline \vdots & \vdots & \ddots & 0 \\ \hline 0 & 0 & \cdots & D_m^{(i)} \end{array}\right), \tag{45}$$

where $D_1^{(i)} \in \mathcal{D}iag(d)$, $\forall i$, and $D_k^{(i)} \in \mathcal{D}iag(d-1)$ $\forall i$ and $\forall k \neq 1$. Then, we notice that equations in Eq. (43) are equivalent to

$$h_i = \sum_{k=1}^m R_k D_k^{(i)} R_k^\dagger, \quad \forall i \in 1, \ldots, m, \tag{46}$$

$$I_d = \sum_{k=1}^m R_k R_k^\dagger, \tag{47}$$

in which the last equation encodes the requirement that the rows of PU must be orthonormal. To find the purification, we thus need to solve these equations.

Solution to Eq. (46) for $i \neq 1$: We choose without loss of generality h_i to be singular matrices (i.e., $\mathrm{rank}(h_i) < d$), $\forall i \neq 1$: this can be obtained using Property 2 of Lemma 1, by adding $-\alpha_i I_d$ to h_i, with $\alpha_i \in \sigma(h_i)$ $\forall i \neq 1$ (where $\sigma(X)$ denotes the spectrum of X).[32]

We then choose $D_k^{(i)} = 0$ for all $k \neq i$. In this way Eq. (46) becomes

$$h_i = R_i D_i^{(i)} R_i^\dagger, \qquad \forall i \neq 1. \tag{48}$$

Notice that R_i are $d \times (d-1)$ matrices for $i \neq 1$, thus indeed these equations can be solved if and only if h_i are not full-rank matrices, for $i \neq 1$. Explicitly, we can write

$$h_i = U_i \left(\begin{array}{c|c} \widetilde{D}_i & 0 \\ 0 & 0 \end{array}\right) U_i^\dagger = \left(U_i' \mid 0\right) \left(\begin{array}{c|c} \widetilde{D}_i & 0 \\ 0 & 0 \end{array}\right) \begin{pmatrix} U_i'^\dagger \\ 0 \end{pmatrix}, \tag{49}$$

where U_i and $\widetilde{D}_i$ are obtained with the spectral theorem and U_i' is a $d \times (d-1)$ matrix obtained from U_i deleting its last column.[33] So a set of solutions of Eqs. (46) is given by setting $R_i = U_i'$ and $D_i^{(i)} = \widetilde{D}_i$. However, other correct solutions are given by the re-scaling $R_i = U_i'/\sqrt{k_i}$ and $D_i^{(i)} = k_i \widetilde{D}_i$, for any choice of $k_i \in \mathbb{R}^+$.

Solution to Eq. (46) for $i = 1$ and to Eq. (47): We now have to solve the equations

$$h_1 = R_1 D_1^{(1)} R_1^\dagger, \tag{50}$$

$$I_d - \sum_{i=2}^m R_i R_i^\dagger = R_1 R_1^\dagger, \tag{51}$$

where we are still free to choose R_1, $D_1^{(1)}$ and the normalization of R_i for all $i \neq 1$. Notice that the right hand side of Eq. (51) is always a positive (semi-) definite matrix, so in order for the equation to be solvable, also the left hand side must be positive definite. This can be always accomplished by re-scaling all the $R_i \to R_i/\sqrt{k_i}$, with the constants k_i large enough, so that $M := I_d - \sum_{k=2}^m R_i R_i^\dagger$ is a positive definite operator. Then we call $\sqrt{M}$ the Hermitian positive-definite matrix such that $(\sqrt{M})^2 = M$, and thus we choose

$$R_1 = \sqrt{M}\, V, \tag{52}$$

where V is a unitary matrix, $VV^\dagger = I_d$. In this way, $R_1 R_1^\dagger = M$ is always satisfied.

The only equation to be satisfied now is Eq. (50). We exploit the fact that V is so far an arbitrary unitary matrix and $D_1^{(1)}$ is unspecified, and we rewrite the equation as

$$V D_1^{(1)} V^\dagger = M^{-1/2} h_1 M^{-1/2}, \tag{53}$$

which can be solved for V and $D_1^{(1)}$ using the spectral theorem. □

We briefly comment on the results obtained in this section. We have provided in Theorem 4 the upper bound

$$d_E^{(\min)}(d,m) \le m(d-1)+1. \tag{54}$$

If we need to purify a specific set $\mathcal{S} = \{h_1, \ldots, h_m\}$ of Hamiltonians, it is straightforward to see that the construction given in Theorem 4 actually allows one to purify $\mathcal{S}$ in dimension $d_E = md + 1 - \sum_{k=2}^m g_k^{(\max)}$, where $g_k^{(\max)}$ is the highest multiplicity of the eigenvalues of h_k (see Refs. 32 and 33). Thus

$$d_E^{(\min)}(\mathcal{S}) \le md + 1 - \sum_{k=2}^{m} g_k^{(\max)}. \tag{55}$$

Moreover, the lower bound established in Corollary 1 trivially applies also here,

$$d_E^{(\min)}(d,m) \ge 2d-1. \tag{56}$$

Finally, for a specific set $\mathcal{S} = \{h_1, \ldots, h_m\}$ of Hamiltonians, the result obtained in Theorem 2 simply extends as

$$d_E^{(\min)}(\mathcal{S}) \ge d + \max_{j,\ell} \max_{\varepsilon \in \{+,-\}} \left(i_\varepsilon(i[h_j, h_\ell]) \right). \tag{57}$$

V. OPTIMAL PURIFICATION OF THE WHOLE ALGEBRA ($m = d^2$)

In this section, we focus on the case where the set $\mathcal{S}$ one wishes to purify is large enough to span the whole algebra $\mathfrak{u}(d)$ of $\mathscr{H}_d$, i.e., according to Definition 2, we study the spanning-set purification problem of $\mathfrak{u}(d)$. This corresponds to having $m = d^2$ linearly independent elements in $\mathcal{S}$ (the maximum allowed by the dimension of the Hilbert space of the problem). It turns out that for this special case, $d_E^{(\min)}$ can be computed exactly showing that it saturates the bound of Eq. (12), i.e.,

$$d_E^{(\min)}(d, m = d^2) = d^2. \tag{58}$$

On one hand, this incidentally confirms that the bound of Theorem 4 is not tight. On the other hand, it shows that a spanning-set purification for $\mathfrak{u}(d)$ requires the largest commutative subalgebra of $\mathfrak{u}(d^2)$ as minimal purifying algebra.

We start by proving this result for the case of n qubits (i.e., $d = 2^n$), as this special case admits a simple analysis (see Proposition 3 and Corollary 2). The case of arbitrary d is instead discussed in Theorem 5 by presenting a construction which allows one to purify an arbitrary set of $m = d^2$ linearly independent Hamiltonians in an extended Hilbert space of dimension d^2. Finally in Theorem 6, we prove that the explicit solution proposed in Theorem 5 is far from being unique.

Proposition 3 (Optimal purification of $\mathfrak{u}(2)$*). A spanning-set purification for the algebra of* $\mathfrak{u}(2)$ *can be constructed on an extended Hilbert space of dimension* $d_E = 4$*, i.e.,* $\mathscr{H}_{d_E} = \mathscr{H}_4$*. This is the optimal solution.*

Proof. By Property 3 of Lemma 1, we can restrict the problem to the case of the traceless operators of $\mathscr{H}_2$, i.e., we can focus on $\mathfrak{su}(2)$ subalgebra. A set of linearly independent elements for such a space is provided by the Pauli matrices $\{X, Y, Z\}$. A purifying set $\{\Sigma_x, \Sigma_y, \Sigma_z\}$ of $\{X, Y, Z\}$ on $\mathscr{H}_4$ can then be exhibited explicitly, considering the following 4×4 matrices:

$$\Sigma_x = \left(\begin{array}{cc|cc} 0 & 1 & 1+i & 0 \\ 1 & 0 & 1+i & 0 \\ \hline 1-i & 1-i & 1 & 0 \\ 0 & 0 & 0 & -1 \end{array}\right),$$

$$\Sigma_y = \left(\begin{array}{cc|cc} 0 & -i & i & \frac{2+4i}{3} \\ i & 0 & 1 & \frac{1-i}{3} \\ \hline -i & 1 & 0 & -1 \\ \frac{2-4i}{3} & \frac{1+i}{3} & -1 & 0 \end{array}\right),$$

$$\Sigma_z = \left(\begin{array}{cc|cc} 1 & 0 & -\frac{4+4i}{9} & \frac{7+8i}{9} \\ 0 & -1 & \frac{5+5i}{9} & -\frac{16-i}{9} \\ \hline -\frac{4-4i}{9} & \frac{5-5i}{9} & 0 & -i \\ \frac{7-8i}{9} & -\frac{16+i}{9} & i & 0 \end{array}\right), \tag{59}$$

and taking $P = I_2 \otimes (I_2 + Z)/2$. It can be seen by direct calculation that they indeed commute. The optimality of the solution follows from inequality (13), which applies since $I_d \notin \mathrm{span}(X, Y, Z)$. □

Corollary 2 (Optimal purification of $\mathfrak{u}(2^n)$*). Consider* $\mathfrak{u}(2^n)$*, the Lie algebra of self-adjoint operators acting on n qubits (i.e.,* $\mathcal{H}_d = \mathcal{H}_2^{\otimes n}$*). Then, a spanning-set purification for this algebra can be constructed with operators acting on* $\mathcal{H}_{d_E} = \mathcal{H}_4^{\otimes n}$*. This is the optimal solution.*

Proof. This result follows by observing that any element of $\mathfrak{u}(2^n)$ can be expressed as a linear combination of tensor products of n (generalized) Pauli operators S_ℓ, with the definitions $S_0 = I_2$, $S_1 = X$, $S_2 = Y$, $S_3 = Z$,

$$h_j = \sum_{\substack{\ell_1,\dots,\ell_n \\ \in\{0,1,2,3\}}} \beta^{(j)}_{\ell_1,\dots,\ell_n} S_{\ell_1} \otimes \cdots \otimes S_{\ell_n} \quad (j = 1, \dots, 2^{2n}). \tag{60}$$

Consider then the set formed by the operators

$$H_j = \sum_{\substack{\ell_1,\dots,\ell_n \\ \in\{0,x,y,z\}}} \beta^{(j)}_{\ell_1,\dots,\ell_n} \Sigma_{\ell_1} \otimes \cdots \otimes \Sigma_{\ell_n}, \tag{61}$$

with Σ_ℓ defined in Eq. (59). The operators H_j act on the Hilbert space $\mathcal{H}_{d_E} = \mathcal{H}_4^{\otimes n} = \mathcal{H}_2^{\otimes 2n}$ and commute with each other (this is because they are tensor products of commuting elements). Finally, by projecting them with $P = [I_2 \otimes (I_2 + Z)/2]^{\otimes n}$, they yield h_j. The solution is optimal due to Eq. (12). □

The above can be used to bound the minimal value of d_E for the case of an arbitrary finite-dimensional system $\mathcal{H}_d$ by simply embedding it into a collection of qubit systems. Specifically consider $\mathcal{S} = \{h_1, \dots, h_m\}$, a collection of m (not necessarily commuting) self-adjoint operators acting on the Hilbert space $\mathcal{H}_d$ of finite dimension d. Then, setting $n_0 = \lceil \log_2 d \rceil$, a purifying set for $\mathcal{S}$ can be constructed on $\mathcal{H}_{d_E} = \mathcal{H}_4^{\otimes n_0}$. This implies that d_E can be chosen to be equal to $4^{n_0} = (2^{n_0})^2 \simeq d^2$. As a matter of fact, this result can be strengthened by showing that indeed $d_E = d^2$ independently of the dimension d.

Theorem 5 (Optimal purification of $\mathfrak{u}(d)$). *A spanning-set purification for* $\mathfrak{u}(d)$ *can be constructed on* $\mathcal{H}_{d_E} = \mathcal{H}_{d^2}$*. This is the optimal solution.*

Proof. The optimality of the construction follows from inequality (12). From Lemma 2, we can prove that such a solution exists by showing that there are a unitary $U \in \mathcal{U}(d^2)$ and a rank-d

projection P defined on $\mathscr{H}_{d^2}$ such that the linear map $f_{PU} : \mathcal{D}iag(d^2) \to \mathfrak{u}(d)$,

$$f_{PU}(D) \oplus 0_{d^2-d} = PUDU^\dagger P, \tag{62}$$

is surjective. An explicit construction of a surjective linear map $f_{PU} : \mathcal{D}iag(d^2) \to \mathfrak{u}(d)$ is given in the Appendix. □

The construction presented in the Appendix thus provides a matrix U that allows one to perform the purification of all the Hermitian matrices in $\mathfrak{u}(d)$. But actually we notice that almost any unitary matrix will do the job equally well, as we show now. So, there is almost free choice in determining a matrix U that accomplishes the task, which can even be chosen at random in the space of unitaries.

Theorem 6. *Almost all unitary matrices $U \in \mathcal{U}(d^2)$ [with respect to (every absolutely continuous measure with respect to) the Haar measure] are such that the map f_{PU} defined in the proof of Theorem 5 is surjective. This implies that almost all unitary matrices $U \in \mathcal{U}(d^2)$ provide a purification for all sets of Hermitian operators.*

Proof. The linear application f_{PU} defined in Eq. (62) maps $\mathcal{D}iag(d^2)$ into $\mathfrak{u}(d)$, which are both d^2-dimensional real vector spaces, and so it is surjective if and only if its determinant is different from zero. Calling $x_{\ell,k}$ the entries of the matrix U, we see that f_{PU} depends quadratically on the complex variables $x_{\ell,k}$, and its determinant det f_{PU} is a polynomial in these variables.

Preliminarily, if we take U to be an arbitrary complex matrix, i.e., not necessarily unitary, the theorem can be straightforwardly proved. In fact, the set of U's which make f_{PU} non-surjective are the zeros of the polynomial $p(u_1, u_2, \ldots) := \det f_{PU}$, where $u_1, u_2, \ldots$ are real parameters which encode the matrix U. Such a polynomial is clearly non-vanishing, as we have found in Theorem 5 an instance of U for which f_{PU} is surjective. The zero set of a non-null analytic function is a closed set (as it is a preimage of a closed set), nowhere dense (otherwise the analytic function would be zero on all its connected domain of convergence), and has zero Lebesgue measure (for a proof, see chapter I of Ref. 23).

The same argument applies also when we restrict U to be unitary. In fact, any unitary matrix can be obtained as an exponential of a Hermitian matrix. So the same results as above apply to the analytic function $g(h_1, \ldots, h_K) = \det f(e^{iH})$ where $h_1, \ldots, h_K$ are real parameters which encode the Hermitian matrix H [formally, the proof proceeds by considering a set of local charts that cover the manifold $\mathcal{U}(d^2)$]. Moreover, it can be shown that the Haar measure on $\mathcal{U}(d^2)$ is obtained from the Lebesgue measure on $\mathfrak{u}(d^2)$ via multiplication by a Jacobian of an analytic function, which is always regular, and the property of having zero measure is preserved under this operation. □

VI. GENERATOR PURIFICATION OF $\mathfrak{u}(d)$ INTO $\mathscr{H}_{d+1}$

The propositions in Sec. III concern the purification of two Hamiltonians ($m = 2$). In particular, it was proved in Proposition 2 that two non-commuting Hamiltonians acting on the Hilbert space $\mathscr{H}_2$ of a qubit can be purified into two commuting Hamiltonians in an extended Hilbert space $\mathscr{H}_3$, namely, by extending the Hilbert space *by only one dimension*. It is in general not the case for a larger system: adding one dimension is typically not enough to purify a couple of Hamiltonians for a system of dimension $d \geq 3$, as proved in Theorem 2. See also Eq. (15).

On the other hand, Proposition 2 on the optimal purification for $m = 2$ and $d = 2$ helps us to prove that one can always find a purification of a generating set of $\mathfrak{u}(d)$ which only involves a $d_E = d + 1$ dimensional space. Expressed in the language introduced in Definition 2, this implies that the largest commutative subalgebra of $\mathfrak{u}(d+1)$ provides a generator purification of $\mathfrak{u}(d)$. More precisely, we have the following:

Theorem 7. *A pair of randomly chosen commuting Hamiltonians H_1 and H_2 on $\mathscr{H}_{d+1}$ almost surely provides a pair of Hamiltonians h_1 and h_2 which generate the full Lie algebra on $\mathscr{H}_d$, i.e., $\mathfrak{Lie}(h_1, h_2) = \mathfrak{u}(d)$. In other words, almost all pairs of commuting Hamiltonians in $\mathscr{H}_{d+1}$ are capable of quantum computation in $\mathscr{H}_d$.*

Proof. To prove this statement, we have to find only an example of such a set $\{H_1, H_2, P\}$ on $\mathscr{H}_{d+1}$ that yields $\{h_1, h_2\}$ generating the full Lie algebra on $\mathscr{H}_d$ (see Ref. 14). There is a particularly simple pair of generators $\{h_1, h_2\}$ of $\mathfrak{u}(d)$, namely,

$$h_1 = \begin{pmatrix} 1 & & & & \\ & 0 & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & 0 \end{pmatrix}, \quad h_2 = \begin{pmatrix} 0 & 1 & & & \\ 1 & 0 & 1 & & \\ & 1 & 0 & \ddots & \\ & & \ddots & \ddots & 1 \\ & & & 1 & 0 \end{pmatrix}. \tag{63}$$

A proof that these generate $\mathfrak{u}(d)$ is given in Ref. 22. We can purify them in $\mathscr{H}_{d+1}$, by exploiting the formulas presented in Proposition 2 for the purification of a couple of Hamiltonians of a qubit. Indeed, two 2×2 matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{64}$$

are essentially Pauli matrices Z and X and can be purified to

$$\left(\begin{array}{c|cc} 1/2 & -1/\sqrt{2} & 0 \\ \hline -1/\sqrt{2} & 1 & 0 \\ 0 & 0 & 0 \end{array}\right), \qquad \left(\begin{array}{c|cc} 0 & 0 & \sqrt{2} \\ \hline 0 & 0 & 1 \\ \sqrt{2} & 1 & 0 \end{array}\right), \tag{65}$$

where we have used Properties 1 and 3 of Lemma 1 (multiplication by a constant and shift by the identity matrix) to convert the first matrix into $-(1/2)Z$ and applied the purification formulas in Eq. (19), extending the matrices to the top-left by one dimension, instead of to the right-bottom. This suggests the purification of the above h_1 and h_2 to

$$H_1 = \left(\begin{array}{c|ccccc} 1/2 & -1/\sqrt{2} & 0 & & & \\ \hline -1/\sqrt{2} & 1 & 0 & & & \\ 0 & 0 & 0 & & & \\ & & & \ddots & & \\ & & & & \ddots & \\ & & & & & 0 \end{array}\right), \tag{66}$$

$$H_2 = \left(\begin{array}{c|ccccc} 0 & 0 & \sqrt{2} & & & \\ \hline 0 & 0 & 1 & & & \\ \sqrt{2} & 1 & 0 & 1 & & \\ & & 1 & 0 & \ddots & \\ & & & \ddots & \ddots & 1 \\ & & & & 1 & 0 \end{array}\right). \tag{67}$$

These matrices actually commute $[H_1, H_2] = 0$ and reproduce h_1 and h_2 once projected by the projection

$$P = \left(\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & I_d & \\ 0 & & & \end{array}\right). \tag{68}$$

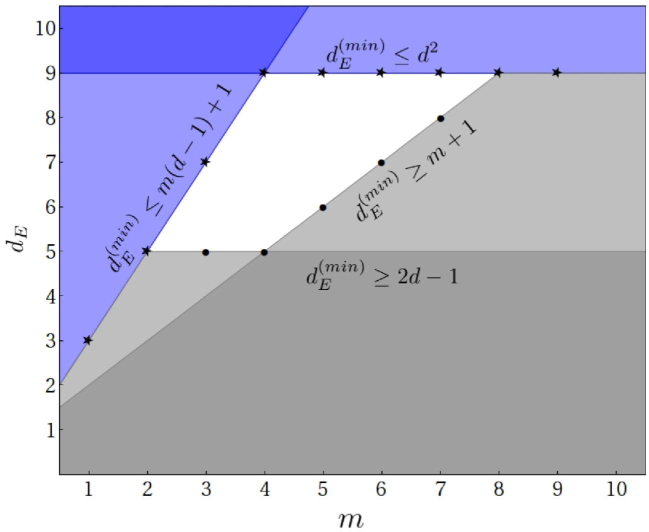

FIG. 2. Plots of the admissible regions for $d_E^{(\min)}(d,m)$ for the qutrit case ($d = 3$) as functions of m. The black points give the known lower bounds on $d_E^{(\min)}(3,m)$. The black stars give the dimensions for which an explicit construction is known, providing the upper bounds. The blue and gray shaded regions highlight the regions excluded by the upper and lower bounds, respectively.

The existence of an example makes us sure that all the sets $\{H_1, H_2, P\}$ on $\mathscr{H}_{d+1}$ except for discrete sets of measure zero do the same job, yielding $\{h_1, h_2\}$ and generating the full $\mathfrak{u}(d)$.[14] □

In Ref. 14, it is shown that almost all pairs of commuting Hamiltonians $\{H_1, H_2\}$ of n qubits are turned into $\{h_1, h_2\}$ capable of quantum computation on $n-1$ qubits, by projecting only a single qubit (i.e., $d_E = 2^n$ and $d = 2^{n-1} = d_E/2$). The above Theorem 7 shows that the reduction by only one dimension can already make a big difference.

VII. CONCLUSIONS

In this work, we have introduced the notion of Hamiltonian purification and the associated notion of algebra purification. As discussed in the Introduction, these mathematical properties arise in the context of quantum control induced via a quantum Zeno effect.[14] We focus specifically on the problem of identifying the minimal dimension $d_E^{(\min)}(d,m)$ which is needed in order to purify a generic set of m linearly independent Hamiltonians, providing bounds and exact analytical results in many cases of interest. In particular, the value of $d_E^{(\min)}(d, m = 2)$ and $d_E^{(\min)}(d, m = d^2)$ has been exactly computed. The former case is the one where one wishes to purify two Hamiltonians, the latter where one wants to induce a spanning-set purification of the whole algebra of operators acting on the input Hilbert space. For intermediate values of m, apart from some special cases discussed in Sec. III, the quantity $d_E^{(\min)}(d,m)$ is still unknown, e.g., see Fig. 2, which refers to the case $d = 3$. Finally for generator purification of $\mathfrak{u}(d)$, we showed that a $(d+1)$-dimensional Hilbert space can be sufficient. This allows us to strengthen the argument in Ref. 14: a rank-d projection suffices to turn commuting Hamiltonians on the $(d+1)$-dimensional Hilbert space into a universal set in the d-dimensional Hilbert space.

ACKNOWLEDGMENTS

This work was partially supported by the Italian National Group of Mathematical Physics (GNFM-INdAM), by PRIN No. 2010LLKJBX on "Collective quantum phenomena: from strongly correlated systems to quantum simulators," and by Grants-in-Aid for Scientific Research (C) (Nos. 22540292 and 26400406) from JSPS, Japan.

APPENDIX: PROOF OF THEOREM 5

Here, we prove Theorem 5 in Sec. V. We have to show that there are a unitary $U \in \mathcal{U}(d^2)$ and a rank-d projection P defined on $\mathscr{H}_{d^2}$ such that the linear map $f_{PU} : \mathcal{D}iag(d^2) \to \mathfrak{u}(d)$,

$$f_{PU}(D) \oplus 0_{d^2-d} = PUDU^\dagger P, \tag{A1}$$

is surjective. Without loss of generality, we are considering $\mathscr{H}_{d^2} = \mathscr{H}_d \oplus \mathscr{H}_{d^2-d}$, so that $P = I_d \oplus 0_{d^2-d}$, and (A1) reads

$$f_{PU}(D) = WDW^\dagger, \tag{A2}$$

where we can parametrize the matrix $W : \mathscr{H}_{d^2} \to \mathscr{H}_d$ as

$$\begin{aligned} W &= \left(\begin{array}{ccc|cccc} x_{1,1} & \cdots & x_{1,d} & x_{1,d+1} & \cdots & \cdots & x_{1,d^2} \\ \vdots & \ddots & \vdots & \vdots & \cdots & \cdots & \vdots \\ x_{d,1} & \cdots & x_{d,d} & x_{d,d+1} & \cdots & \cdots & x_{d,d^2} \end{array}\right) \\ &\equiv \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_d \end{pmatrix} \equiv \left(\begin{array}{ccc|ccc} X^1 & \cdots & X^d & X^{d+1} & \cdots & \cdots & X^{d^2} \end{array}\right). \end{aligned} \tag{A3}$$

Here, $x_{\ell,j}$ is the matrix element associated with the ℓth row and the jth column of the unitary U, and where for $\ell \in \{1,\ldots,d\}$, we define X_ℓ as the complex row vector of $\mathbb{C}^{d^2}$ whose jth component is $x_{\ell,j}$, while for $j \in \{1,\ldots,d^2\}$, we define X^j as the complex column vector of $\mathbb{C}^d$ whose ℓth component is $x_{\ell,j}$. The unitarity condition for U requires the row vectors $X_1,\ldots,X_d$ to be orthonormal, i.e.,

$$X_\ell \cdot X_{\ell'}^\dagger = \sum_{j=1}^{d^2} x_{\ell,j} x_{\ell',j}^* = \delta_{\ell,\ell'}. \tag{A4}$$

The surjectivity condition for f_{PU} instead can be analyzed in terms of the column vectors X^j. Consider in fact the basis for $\mathcal{D}iag(d^2)$ consisting of matrices $\hat{u}_{ii}$ with $i \in \{1,\ldots,d^2\}$ with only one non-zero entry, 1 in the ith position on the diagonal. The function f_{PU} is then surjective if the matrices $f_{PU}(\hat{u}_{11}),\ldots,f_{PU}(\hat{u}_{d^2d^2})$ are linearly independent, i.e., if they span the whole algebra $\mathfrak{u}(d)$. These are explicitly given by

$$\begin{aligned} f_{PU}(\hat{u}_{ii}) &= W\hat{u}_{ii}W^\dagger \\ &= \begin{pmatrix} |x_{1,i}|^2 & x_{1,i}x_{2,i}^* & \cdots & x_{1,i}x_{d,i}^* \\ x_{2,i}x_{1,i}^* & |x_{2,i}|^2 & \cdots & x_{2,i}x_{d,i}^* \\ \vdots & \vdots & \ddots & \vdots \\ x_{d,i}x_{1,i}^* & x_{d,i}x_{2,i}^* & \cdots & |x_{d,i}|^2 \end{pmatrix} \\ &= X^i \times X^{i\dagger}, \end{aligned} \tag{A5}$$

where the last identity stresses the fact that, by construction, $f_{PU}(\hat{u}_{ii})$ can be seen as the outer product "×" of the vector X^i with itself.[34]

In order to identify a solution for the problem we have hence to find an assignment for the coefficients $x_{\ell,j}$ which fulfill condition (A4) while ensuring that matrices (A5) span the whole $\mathfrak{u}(d)$. To show this, we proceed by steps. First, we identify values for $x_{\ell,i}$ in such a way that the associated $d \times d^2$ matrix $\widetilde{W}$ guarantees that $\{\widetilde{W}\hat{u}_{ii}\widetilde{W}^\dagger\}_{i\in\{1,\ldots,d^2\}}$ provides a basis for $\mathfrak{u}(d)$, hence that the associated mapping $f_{\widetilde{W}}$ is surjective. Then we modify $\widetilde{W}$ in such a way that condition (A4) is fulfilled by orthonormalizing its rows, while making sure that the surjectivity condition of the associated mapping is preserved.

Calling e_i the row vector of $\mathbb{C}^d$ with 1 in the ith position and introducing $e^{(+)}_{n,m} \coloneqq e_n + e_m$ and $e^{(-)}_{n,m} \coloneqq e_n - ie_m$, a basis for $\mathfrak{u}(d)$ is given by the following matrices:[35]

$$\begin{cases} e_n^\dagger \times e_n, & n \in \{1,\dots,d\}, \\ e^{(+)\dagger}_{n,m} \times e^{(+)}_{n,m}, & n < m \in \{1,\dots,d\}, \\ e^{(-)\dagger}_{n,m} \times e^{(-)}_{n,m}, & n < m \in \{1,\dots,d\}. \end{cases} \tag{A6}$$

From Eq. (A5), it follows that this set can be obtained as $f_{\widetilde{W}}(\hat{u}_{ii}) = \widetilde{W}\hat{u}_{ii}\widetilde{W}^\dagger$ if we take as matrix $\widetilde{W}$ the one with column vectors,

$$\begin{cases} X^1 = e_1^\dagger, \\ \quad\vdots \\ X^d = e_d^\dagger, \end{cases} \tag{A7}$$

$$\begin{cases} X^{d+1} = e^{(+)\dagger}_{1,2}, \\ \quad\vdots \\ X^{2d} = e^{(+)\dagger}_{1,d}, \\ X^{2d+1} = e^{(+)\dagger}_{2,3}, \\ \quad\vdots \\ X^{\frac{d(d+1)}{2}} = e^{(+)\dagger}_{d-1,d}, \end{cases} \quad \begin{cases} X^{\frac{d(d+1)}{2}+1} = e^{(-)\dagger}_{1,2}, \\ \quad\vdots \\ X^{\frac{d(d+3)}{2}} = e^{(-)\dagger}_{1,d}, \\ X^{\frac{d(d+3)}{2}+1} = e^{(-)\dagger}_{2,3}, \\ \quad\vdots \\ X^{d^2} = e^{(-)\dagger}_{d-1,d}. \end{cases} \tag{A8}$$

For instance, in the case $d = 4$, this choice gives

$$\widetilde{W} = \left(\begin{array}{cccc|cccccccccccc} 1&0&0&0&1&1&1&0&0&0&1&1&1&0&0&0 \\ 0&1&0&0&1&0&0&1&1&0&i&0&0&1&1&0 \\ 0&0&1&0&0&1&0&1&0&1&0&i&0&i&0&1 \\ 0&0&0&1&0&0&1&0&1&1&0&0&i&0&i&i \end{array}\right). \tag{A9}$$

Accordingly $f_{\widetilde{W}}(\hat{u}_{ii}) = \widetilde{W}\hat{u}_{ii}\widetilde{W}^\dagger$ span all $\mathfrak{u}(d)$ and so $f_{\widetilde{W}}$ is a surjective (hence invertible) linear function. Now, $\widetilde{W}$ does not have orthonormal rows, so it cannot be straightforwardly extended to a unitary operator on $\mathscr{H}_{d^2}$: we have to orthonormalize them. We observe that the scalar product between the rows $X_1,\dots,X_d$ of $\widetilde{W}$ gives

$$\begin{cases} X_n \cdot X_n^\dagger = 2d-1, & n \in \{1,\dots,d\}, \\ X_n \cdot X_m^\dagger = 1-i, & n < m \in \{1,\dots,d\}, \\ X_n \cdot X_m^\dagger = 1+i, & n > m \in \{1,\dots,d\}. \end{cases} \tag{A10}$$

We can orthogonalize them by changing only the entries of the leftmost $d \times d$ submatrix of $\widetilde{W}$. In the case $d = 4$, we start with

$$A_{(0)} = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{pmatrix}. \tag{A11}$$

Then, we make the first row orthogonal to all the others by adding $-1-i$ to all subdiagonal elements in the first column,

$$A_{(1)} = \begin{pmatrix} 1&0&0&0 \\ -1-i&1&0&0 \\ -1-i&0&1&0 \\ -1-i&0&0&1 \end{pmatrix}. \tag{A12}$$

Now, $X_2 \cdot X_3^\dagger = X_2 \cdot X_4^\dagger = 1 - i + (-1-i)(-1+i) = 3 - i$, so we can make X_2 orthogonal to all the other rows with

$$A_{(2)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1-i & 1 & 0 & 0 \\ -1-i & -3-i & 1 & 0 \\ -1-i & -3-i & 0 & 1 \end{pmatrix}. \tag{A13}$$

Finally, $X_3 \cdot X_4^\dagger = 1 - i + (-1-i)(-1+i) + (-3-i)(-3+i) = 13 - i$, and we can make all the vectors orthogonal with

$$A_{(3)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1-i & 1 & 0 & 0 \\ -1-i & -3-i & 1 & 0 \\ -1-i & -3-i & -13-i & 1 \end{pmatrix}. \tag{A14}$$

This can be extended to any dimension d replacing the leftmost $d \times d$ matrix of $\widetilde{W}$ with the triangular matrix

$$A_{(d-1)} = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ a_1 & 1 & 0 & 0 & \cdots & 0 \\ a_1 & a_2 & 1 & 0 & \cdots & 0 \\ a_1 & a_2 & a_3 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & a_4 & \cdots & 1 \end{pmatrix}, \tag{A15}$$

where $a_1 = -1 - i$ while for $n \in \{2, \ldots, d-1\}$ the remaining subdiagonal elements are obtained by solving the recursive equation

$$a_n = -1 - i - \sum_{k=1}^{n-1} |a_k|^2. \tag{A16}$$

For future reference, we notice that all a_n have negative real and imaginary parts,

$$\text{Re } a_n = -\left(1 + \sum_{k=1}^{n-1} |a_k|^2\right), \qquad \text{Im } a_n = -1. \tag{A17}$$

Next, the rows of the submatrix $A_{(d-1)}$ are normalized to 1 obtaining

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ a_1/N_1 & 1/N_1 & 0 & \cdots & 0 \\ a_1/N_2 & a_2/N_2 & 1/N_2 & \cdots & 0 \\ a_1/N_3 & a_2/N_3 & a_3/N_3 & \ddots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ a_1/N_{d-1} & a_2/N_{d-1} & a_3/N_{d-1} & \cdots & 1/N_{d-1} \end{pmatrix}, \tag{A18}$$

with $N_n = \sqrt{1 + \sum_{k=1}^{n} |a_k|^2} = \sqrt{|\text{Re } a_{n+1}|}$. We now replace this into the $\widetilde{W}$ and normalize the resulting rows to 1 by dividing them by the constants $\sqrt{2d-1}$. The resulting $d \times d^2$ matrix is our solution W. By construction, it has orthonormal rows as required by Eq. (A4), so it can be extended to a unitary matrix U, such that $W = PU$.

Moreover, the associated function f_{PU} is still surjective. This can be proven by induction. To this end we find it useful to introduce the notion of k-submatrix: specifically a k-lower-right submatrix (k-LRS) is a $d \times d$ Hermitian matrix whose non-zero entries are only in lower-right submatrix associated with the last k rows and columns. We then call R the right part of the matrix W (the last

$d^2 - d$ columns), which is the same as the one we had for the $\widetilde{W}$ apart from the global rescaling by the factor $1/\sqrt{2d-1}$. The basic step is to show that, under outer products with themselves, X^d and the columns of R span all the 1-LRS. This is obvious, as such matrices are obtained as a multiple of $X^d \cdot X^{d\dagger}$. Then, we have to show that, if we have $X^d, X^{d-1}, \ldots, X^{d-k}$ and the columns of R, we can span all $(k+1)$-LRSs. By induction hypothesis, we suppose that we can already obtain all k-LRSs. To prove the thesis is then sufficient to show that we can generate the set of $(k+1)$-LRSs whose non-zero elements are given by

$$\left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \sharp & \\ 0 & & & \end{array}\right), \left(\begin{array}{c|ccc} 0 & 1 & \cdots & 0 \\ \hline 1 & & & \\ \vdots & & \sharp & \\ 0 & & & \end{array}\right), \ldots, \left(\begin{array}{c|ccc} 0 & 0 & \cdots & 1 \\ \hline 0 & & & \\ \vdots & & \sharp & \\ 1 & & & \end{array}\right), \left(\begin{array}{c|ccc} 0 & -i & \cdots & 0 \\ \hline i & & & \\ \vdots & & \sharp & \\ 0 & & & \end{array}\right), \ldots, \left(\begin{array}{c|ccc} 0 & 0 & \cdots & -i \\ \hline 0 & & & \\ \vdots & & \sharp & \\ i & & & \end{array}\right), \tag{A19}$$

where the symbol "♯" represents a generic $k \times k$ matrix. To achieve this we are allowed to use arbitrary linear combinations of the following set of $(k+1)$-LRSs, which are trivially generated via outer product by the vectors $X^d, X^{d-1}, \ldots, X^{d-k}$ and by the columns of R,

$$\left(\begin{array}{c|ccc} 1/N_{d-k-1} & a^*_{d-k}/N_{d-k} & \cdots & a^*_{d-k}/N_{d-1} \\ \hline a_{d-k}/N_{d-k} & & & \\ \vdots & & \sharp & \\ a_{d-k}/N_{d-1} & & & \end{array}\right), \tag{A20}$$

$$\left(\begin{array}{c|ccc} 1 & 1 & \cdots & 0 \\ \hline 1 & & & \\ \vdots & & \sharp & \\ 0 & & & \end{array}\right), \ldots, \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 1 \\ \hline 0 & & & \\ \vdots & & \sharp & \\ 1 & & & \end{array}\right), \tag{A21}$$

$$\left(\begin{array}{c|ccc} 1 & -i & \cdots & 0 \\ \hline i & & & \\ \vdots & & \sharp & \\ 0 & & & \end{array}\right), \ldots, \left(\begin{array}{c|ccc} 1 & 0 & \cdots & -i \\ \hline 0 & & & \\ \vdots & & \sharp & \\ i & & & \end{array}\right). \tag{A22}$$

The result can then be trivially proved by showing that among such linear combinations one can identify the $(k+1)$-LRSs whose non-zero elements are in the form

$$\left(\begin{array}{c|ccc} c & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \sharp & \\ 0 & & & \end{array}\right), \tag{A23}$$

with $c \neq 0$. This is done by starting from matrix (A20) and then subtracting the off-diagonal elements using matrices (A21) and (A22). As a result, we get matrix (A23) with

$$c = \frac{1}{N_{d-k-1}} - \sum_{j=1}^{k} \frac{1}{N_{d-j}} (\mathrm{Re}\, a_{d-k} + \mathrm{Im}\, a_{d-k}), \tag{A24}$$

which is indeed different from zero, as according to Eq. (A17) all the terms are positive. This concludes the induction step, and the theorem is proven. □

[1] J. P. Dowling and G. J. Milburn, Philos. Trans. R. Soc., A **361**, 1655 (2003).

[2] D. Deutsch, in *Proceedings of the Sixth International Conference on Quantum Communication, Measurement and Computing*, edited by J. H. Shapiro and O. Hirota (Rinton Press, Princeton, NJ, 2003).

[3] P. Zoller, Th. Beth, D. Binosi, R. Blatt, H. Briegel, D. Bruss, T. Calarco, J. I. Cirac, D. Deutsch, J. Eisert, A. Ekert, C. Fabre, N. Gisin, P. Grangiere, M. Grassl, S. Haroche, A. Imamoglu, A. Karlson, J. Kempe, L. Kouwenhoven, S. Kröll, G.

Leuchs, M. Lewenstein, D. Loss, N. Lütkenhaus, S. Massar, J. E. Mooij, M. B. Plenio, E. Polzik, S. Popescu, G. Rempe, A. Sergienko, D. Suter, J. Twamley, G. Wendin, R. Werner, A. Winter, J. Wrachtrup, and A. Zeilinger, Eur. Phys. J. D **36**, 203 (2005).

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

[5] I. Bloch, J. Dalibard, and S. Nascimbene, Nat. Phys. **8**, 267 (2012).

[6] R. Blatt and C. F. Roos, Nat. Phys. **8**, 277 (2012).

[7] L. P. Kouwenhoven, D. G. Austing, and S. Tarucha, Rep. Prog. Phys. **64**, 701 (2001).

[8] D. D'Alessandro, *Introduction to Quantum Control and Dynamics* (Chapman & Hall/CRC, Boca Raton, FL, 2008).

[9] D. Dong and I. R. Petersen, IET Control Theory Appl. **4**, 2651 (2010).

[10] G. Dirr and U. Helmke, GAMM-Mitt. **31**, 59 (2008).

[11] P. Facchi and S. Pascazio, Phys. Rev. Lett. **89**, 080401 (2002).

[12] P. Facchi and S. Pascazio, J. Phys. A: Math. Theor. **41**, 493001 (2008).

[13] P. Facchi, S. Tasaki, S. Pascazio, H. Nakazato, A. Tokuse, and D. A. Lidar, Phys. Rev. A **71**, 022302 (2005).

[14] D. K. Burgarth, P. Facchi, V. Giovannetti, H. Nakazato, S. Pascazio, and K. Yuasa, Nat. Commun. **5**, 5173 (2014).

[15] A. S. Holevo and V. Giovannetti, Rep. Prog. Phys. **75**, 046001 (2012).

[16] H. J. Woerdeman, Linear Multilinear Algebra **42**, 239 (1997).

[17] D. P. Kimsey and H. J. Woerdeman, Int. J. Inf. Syst. Sci. **4**, 50 (2008), http://www.math.ualberta.ca/ijiss/SS-Volume-4-2008/No-1-08/SS-08-01-06.pdf.

[18] D. S. Kaliuzhnyi-Verbovetskyi, I. M. Spitkovsky, and H. J. Woerdeman, Oper. Matrices **3**, 401 (2009).

[19] R. D. Wasson and H. J. Woerdeman, Linear Algebra Appl. **438**, 3530 (2013).

[20] I. Degani, J. Schiff, and D. J. Tannor, Numer. Math. **101**, 479 (2005).

[21] R. A. Horn and C. R. Johnson, *Matrix Analysis* (Cambridge University Press, Cambridge, 1990).

[22] D. Burgarth and K. Yuasa, Phys. Rev. Lett. **108**, 080502 (2012).

[23] G. R. Clifford and H. Rossi, *Analytic Functions of Several Complex Variables* (American Mathematical Society, 2009).

[24] Actually one should work in an *interaction picture*, in which the system undergoes a spontaneous unitary evolution given by a free Hamiltonian H_{free}, to which an interaction is added as prescribed by the experimenter.[10] To simplify the discussion, we will assume that this step has already been factored out, i.e., we imagine that $H_{\text{free}} = 0$.

[25] As a matter of fact, since global phases are irrelevant in quantum mechanics, it would be sufficient to focus on the algebra $\mathfrak{su}(d)$ formed by the traceless self-adjoint $d \times d$ complex matrices.

[26] More precisely, $P = I_d \oplus 0$ is a rank-d orthogonal projection acting on the Hilbert space $\mathscr{H}_{d_E} = \mathscr{H}_d \oplus \mathscr{H}_d^{\perp}$, and Eq. (3) should read $h_j \oplus 0 = P H_j P$. By abuse of notation, we will use the same symbol for h_j on $\mathscr{H}_d$ and for its extension $h_j \oplus 0$ on $\mathscr{H}_{d_E}$. More generally, we can consider a Hamiltonian purification in a space $\mathscr{H}_{d_E} = \widetilde{\mathscr{H}}_d \oplus \widetilde{\mathscr{H}}_d^{\perp}$, where $\widetilde{\mathscr{H}}_d$ is isomorphic to $\mathscr{H}_d$. Again, in the following, we will not be pedantic in distinguishing isomorphic spaces and will commit the sin of denoting them with the same symbols.

[27] A *normal completion* of a complex matrix $M \in \mathbb{C}^{d\times d}$ is a *normal matrix* $M_E \in \mathbb{C}^{d_E \times d_E}$ such that $M = P M_E P$, with P an orthogonal projector from $\mathbb{C}^{d_E}$ to $\mathbb{C}^d$. There is a one to one correspondence between complex matrices M and ordered pairs of Hermitian matrices (h_1, h_2), given by $M \equiv h_1 + i h_2$. It is straightforward to verify that M is normal if and only if h_1 and h_2 commute. Thus, there is a one to one correspondence among purifications of pairs of Hermitian matrices and normal completions of complex matrices. Therefore, all the results on normal completions given in Refs. 17–19 apply also to purifications of two Hamiltonians.

[28] Notice that this provides a Hamiltonian purification up to the identification $\mathscr{H}_d \cong \mathscr{H}_d \otimes \mathbb{C}|0\rangle$, with the subspace $\mathscr{H}_d \otimes \mathbb{C}|0\rangle \subset \mathscr{H}_{d_E}$, and the extension of h_j in $\mathscr{H}_{d_E}$ is $h_j \otimes |0\rangle\langle 0|$. See Ref. 26.

[29] It is worth observing that the set of operators defined by

$$H_1 = \frac{1}{2}(h_1 \otimes I_2 + h_2 \otimes X),$$
$$H_2 = \frac{1}{2}(h_2 \otimes I_2 + h_1 \otimes X)$$

are still commuting and allow one to recover h_1 and h_2 by simply tracing out the ancilla system $\mathscr{H}_2$. This is a sort of purification of $\mathcal{S}$ where the ancilla system is simply forgotten.

[30] We assume that $\max \sigma(h_1)$ is not degenerated, but it is not a restrictive assumption: if it is degenerated, one can purify the operators in a Hilbert space with a smaller dimension d_E.

[31] Consider a Hermitian traceless operator A. This is always unitarily equivalent to a Hermitian operator with zeros on the diagonal. Hence we assume, without loss of generality, that A has zero diagonal. Take h_1 diagonal with real and distinct diagonal entries $\lambda_1, \ldots, \lambda_d$. The equation $A = i[h_1, h_2]$ then is equivalent to $i(\lambda_i - \lambda_j) h_{ij}^{(2)} = a_{ij}$, which has a solution $h_{ij}^{(2)} = a_{ij}/[i(\lambda_i - \lambda_j)]$.

[32] Denote with λ_k^* the eigenvalue with highest multiplicity of h_k, and with $g_k^{(\max)}$ its multiplicity. Then, with the replacement $h_k \to h_k - I_d \lambda_k^*$, we can assume h_k to be of rank $d - g_k^{(\max)}$.

[33] In general, h_i is of rank $d - g_i^{(\max)}$, so U_i' can be taken as a $d \times (d - g_i^{(\max)})$ matrix and $\widetilde{D}_i \in \mathcal{D}iag(d - g_i^{(\max)})$.

[34] Identity (A5) clarifies that the $f_{PU}(\hat{u}_{ii})$ cannot be all mutually orthogonal with respect to the Hilbert-Schmidt scalar product. Indeed there can be at most d such matrices which are orthogonal. To see this simply observe that $\mathrm{Tr}[f_{PU}(\hat{u}_{ii}) f_{PU}^{\dagger}(\hat{u}_{jj})] = |X^{j\dagger} \cdot X^i|^2$ and remember that the X^i are d^2 column vectors of $\mathbb{C}^d$.

[35] To see this simply observe that for $n < m$, the matrices $e_n^{\dagger} \times e_n \pm e_m^{\dagger} \times e_m$, $e_{n,m}^{(+)\dagger} \times e_{n,m}^{(+)} - e_n^{\dagger} \times e_n - e_m^{\dagger} \times e_m$ and $e_{n,m}^{(-)\dagger} \times e_{n,m}^{(-)} - e_n^{\dagger} \times e_n - e_m^{\dagger} \times e_m$ form the set of generalized Pauli operators in the subspace spanned by the vectors e_n and e_m.