Universal control of quantum subspaces and subsystems

Paolo Zanardi[1,2] and Seth Lloyd[1]
[1]*Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*
[2]*Institute for Scientific Interchange (ISI) Foundation and Istituto Nazionale per la Fisica della Materia (INFM),*
Viale Settimio Severo 65, I-10133 Torino, Italy

(Received 2 May 2003; published 20 February 2004)

We describe a broad dynamical-algebraic framework for analyzing the quantum control properties of a set of naturally available interactions. General conditions under which universal control is achieved over a set of subspaces/subsystems are found in terms of the representation theory of the group $\mathcal{U}_A$ of allowed quantum evolutions. In some cases universal control can be achieved in all the state-space sectors carrying an irreducible action of $\mathcal{U}_A$. All known physical examples of universal control on subspaces/systems are related to the framework developed here. Implications for quantum-information processing are discussed.

DOI: 10.1103/PhysRevA.69.022313 PACS number(s): 03.67.Lx, 03.65.Fd

I. INTRODUCTION

The ability to manipulate information in an arbitrary fashion is a key requirement for both classical and quantum-information processing (QIP) [1]. Once information is suitably encoded one must be able to perform, at least approximately, any transformation over the state space of the physical medium supporting the encoding. When this goal is realized one says that universal control is achieved.

In the prototype case of QIP the physical system supporting the encoding is provided by a set of two-level systems, i.e., qubits, in which both external and mutual interactions are supposed to be controllable to a very high degree of accuracy. In this case the state space of the systems is given by the tensor product $\mathcal{H}\cong(\mathbb{C}^2)^{\otimes N}$ (N-qubit space). It is an important, and by-now standard result in QIP that almost any pair of two-qubit gates are universal [2,3]. Moreover the realizability of all single-qubit, i.e., SU(2) gates along with an (arbitrary) entangling two-qubit gates suffices to achieve universality [4].

On the other hand in many experimental situations there are operational constraints that force one to consider a smaller set of transformations as the actually available ones. For example all naturally available interactions could be commuting with some observable, e.g., total spin, whose value cannot then be changed. This lack of resources typically results in the impossibility of achieving universality in the full state space $\mathcal{H}$. It is then a very natural and practically important question whether there exists a subspace $\mathcal{C}$ of $\mathcal{H}$ over which the restricted set of naturally available interactions allows universality. When such an “encoding” is found one obtains the so-called *encoded universality* [5–9].

In this paper we shall analyze the problem of encoded universality from a general control-theoretic perspective. Broad conditions under which universal control over set of subspaces/subsystems can be achieved will be stated within a powerful algebraic framework. Our main results are presented in the form of three propositions, whose ingredients will be the representation theory of dynamical groups and algebras associated with the allowed interactions. A crucial role will be played by the symmetry properties of the realizable transformations. Several applications to physical systems relevant for quantum information processing will be pointed out.

II. PRELIMINARIES

Let $\mathcal{I}_A=\{H(\lambda)\}_{\lambda\in\mathcal{M}}\subset\mathrm{End}(\mathcal{H})$ denotes the set of “ naturally” available interactions acting over the quantum state space $\mathcal{H}$. $\mathcal{M}$ is the set of control parameters. We assume that one is able to enact all the quantum evolutions governed by the time-dependent Hamiltonians $H(\lambda(t))$ where λ belongs to the set $\mathcal{P}_A$ of $\mathcal{M}$-valued functions (paths) of time corresponding to the physically realizable control processes. We stress that we are not assuming that these latter can be arbitrary ones. We are also implicitly assuming that no other (uncontrollable) interactions, e.g., coupling with an environment, but the ones in $\mathcal{I}_A$ are present. In other words we are working in a *noiseless* scenario.

The *pair* $(\mathcal{I}_A,\mathcal{P}_A)$ describes the physical resources available in the given experimental situation; associated with it one has a set of allowed quantum evolutions $U(\lambda)=T\exp[-i\int_{\mathbb{R}}H(\lambda(t))dt](\lambda\in\mathcal{P}_A)$, where T denotes the chronological ordering operator.

We will assume that if U is an allowed evolution, then $U^\dagger$ is allowed as well; we also assume that the trivial, i.e., $U=\mathbb{1}$, evolution is an allowed one. It follows that set of unitary transformations one can generate by resorting to interactions in $\mathcal{I}_A$ and control processes in $\mathcal{P}_A$ has the structure of *subgroup* $\mathcal{U}_A$ of the full group $\mathcal{U}(\mathcal{H})$ of unitary transformations over $\mathcal{H}$. If $\mathcal{U}_A$ is dense in $\mathcal{U}(\mathcal{H})$ one says that *universality* is achieved: an arbitrary unitary transformation over $\mathcal{H}$ can be realized to an arbitrary accuracy by means of the available resources.

It is useful now to recall a well-known result in quantum control theory. When (i) one can drive the control parameters along arbitrary paths in $\mathcal{M}$ and (ii) $\mathcal{I}_A=\{\sum_i\lambda_iH_i\}$, one has

$$\mathcal{U}_A=e^{\mathcal{L}_A}, \tag{1}$$

where by $\mathcal{L}_A$ we denoted the Lie algebra generated by the set of operators $\mathcal{I}_A$, i.e., the linear span of all possible multiple commutators of elements of $\mathcal{I}_A$. This result generally *does not* hold when a restricted set of paths $\mathcal{P}_A$ is considered: in this case $\mathcal{U}_A \subset e^{\mathcal{L}_A}$.

For example, in holonomic quantum computation [10] $\mathcal{I}_A$ comprises a set of isodegenerate Hamiltonians and $\mathcal{P}_A$ is given by adiabatic *loops* around a $\lambda_0 \in \mathcal{M}$. From the adiabatic theorem it follows that, if one start from an initial state lying in a eigenspace of $H(\lambda_0)$, any evolutions obtained by driving the control parameter adiabatically along a loop in $\mathcal{M}$ will result in a final state in the same eigenspace. This means that the state space is dynamically decoupled in orthogonal sectors corresponding to the eigenprojectors of $H(\lambda_0)$. This decoupling is clearly an obstruction to universality.

Before moving to the main part of the paper let us notice that the control-theoretic perspective adopted in this paper is somewhat different from the one of some recent quantum control papers, e.g., [11]. There the control by laser pulses of a multilevel indecomposable systems have been analyzed. On the contrary our focus is mostly on *multipartite* quantum systems (the ones ultimately relevant to quantum information processing) and the on the control of many-body, e.g., Heisenberg, couplings.

III. ENCODED UNIVERSALITY

Suppose that there exist a set of invariant subspaces $\mathcal{C}_i \subset \mathcal{H} (i=1,\ldots,M)$ of $\mathcal{U}_A$, such that

$$\overline{\mathcal{U}_A|_{\mathcal{C}_i}} = \mathcal{U}(\mathcal{C}_i), \quad (i=1,\ldots,M). \tag{2}$$

(Here the bar denotes topological closure.) In this case, we say that $\mathcal{U}_A$ is $\mathcal{C}_i$ universal. The $\mathcal{C}_i$'s will be referred to as codes. When $\mathcal{U}_A$ is $\mathcal{H}$ universal we will simply say that it is universal. Note that in order to attain $\mathcal{C}_i$ universality the group $\mathcal{U}_A$ has to be an *infinite* one. Finite groups cannot be dense on the set of unitary transformations on $\mathcal{C}_i$.

Example 1. The most favorable case of holonomic quantum computation occurs when there is an irreducible connection [10]. In this case, one has $\mathcal{U}_A = \oplus_r \mathcal{U}(\mathcal{H}_r)$ where $\mathcal{H}_r$ is the rth eigenspace of $H(\lambda_0)$ with dimension n_r. Since for nontrivial $H(\lambda_0)$ one has $\Sigma_r n_r^2 < (\Sigma_r n_r)^2$, it follows that $\mathcal{U}_A$ is strictly contained in $\mathcal{U}(\mathcal{H})$. Here $\mathcal{U}_A$ allows only for $\mathcal{H}_r$ universality.

Example 2. Let $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$ be a two-qubit space and $\mathcal{I}_A = \{\sigma^x\otimes\sigma^x + \sigma^y\otimes\sigma^y, \sigma^x\otimes\sigma^y - \sigma^y\otimes\sigma^x, \sigma^z\otimes\mathbb{1} - \mathbb{1}\otimes\sigma^z\}$ (here the σ^α's denote the Pauli matrices). Under the assumptions for the validity of Eq. (1) it is easy to see that this set is $\mathcal{H}_1$-universal, where $\mathcal{H}_1$ is the linear span of $|01\rangle$ and $|10\rangle$ [8]. This is easily seen by noticing that $(\mathcal{L}_A) \cong \mathrm{su}(2)$; consequently $\mathcal{H}$ splits according the su(2) irreducible representation in a doublet $(\mathcal{H}_1)$ and two singlets $(\mathcal{H}_0 = \mathrm{span}\{|00\rangle, |11\rangle\})$. The decomposition of the entire two-qubit space is obtained by considering $\mathcal{I}'_A = \{\sigma^x\otimes\sigma^x - \sigma^y\otimes\sigma^y, \sigma^x\otimes\sigma^y + \sigma^y\otimes\sigma^x, \sigma^z\otimes\mathbb{1} + \mathbb{1}\otimes\sigma^z\}$. In this case, the role of $\mathcal{H}_0$ and $\mathcal{H}_1$ are interchanged.

It is important to realize that in the general case the codes do *not* have to be $\mathcal{I}_A$ invariant subspaces; in other words, one can temporarily leave the coding subspace during the time evolution and return to it just at the end. An instance of this situation is provided by the obvious fact that if $(\mathcal{I}_A, \mathcal{P}_A)$ is $\mathcal{C}$ universal then, for any subspace $\mathcal{C}' \subset \mathcal{C}$, there exists a subset $\mathcal{P}'_A \subset \mathcal{P}_A$ such that $(\mathcal{I}_A, \mathcal{P}'_A)$ is $\mathcal{C}'$ universal. The elements of $\mathcal{U}_A$ will generally temporarily draw states out of $\mathcal{C}'$; the states in $(\mathcal{C}')^\perp$ play the the role of *auxiliary* intermediate states that do not have to appear at the beginning and at the end of the control process. The QIP literature provides a multitude of illustrations of this state of affairs, i.e., the use of *ancillæ* . Another possibility consists in generating from the interactions in $\mathcal{I}_A$ (which do not leave $\mathcal{C}$ invariant) a set $\mathcal{I}_A^{eff}$ of effective interactions (which do leave $\mathcal{C}$ invariant).

Now the main question is: *given the available set $\mathcal{U}_A$ of operations, can some encoded universality be achieved?*

To see whether a suitable encoding exists, i.e., a subspace $\mathcal{C}$ for which $\mathcal{U}_A$ is $\mathcal{C}$ universal, it is useful to resort to the tools of group representation theory [13] Let us consider the decomposition of $\mathcal{H}$ into the $\mathcal{U}_A$ irreducible representation

$$\mathcal{H} \cong \oplus_J \mathbb{C}^{n_J} \otimes \mathcal{H}_J \tag{3}$$

The $\mathbb{C}^{n_J}$ factors in the Eq. (3) above simply take into account that the Jth irreducible representation $\mathcal{H}_J$, with dimension d_J, appears with multiplicity n_J. The appearance of these factors amounts to the existence of *symmetries* for the set of allowed transformations $\mathcal{U}_A$. We observe in passing that symmetries for $\mathcal{U}_A$ are not necessarily symmetries for $\mathcal{I}_A$, whereas the converse holds true.

Let us now then suppose that $\mathcal{I}_A$ admits a nontrivial group of symmetries $\mathcal{G}$, i.e., $g \in \mathcal{G} \Rightarrow [g, \mathcal{I}_A] = 0$. A paradigmatic instance is given when one is dealing with a quantum system consisting of N copies of an elementary one, e.g., one qubit, and cannot discriminate the different subsystems. Permutations of these latter are therefore symmetries of the allowed interactions ($\mathcal{G}$ is given by the symmetric group $\mathcal{S}_N$). This kind of situation is often encountered in decoherence free subspaces (DFS) [14] and noiseless subsystem theory [15,16,6]. where $\mathcal{I}_A$ is the set of system operators coupled with the environment. The associative algebra generated by $\mathcal{I}_A$ is the basic algebraic object underlying all the quantum noise avoidance, correction, and suppression schemes developed to date [16,12]. In the following given a group $\mathcal{G}$ we will denote by $\mathbb{C}\mathcal{G}$ its group algebra [17], moreover given the algebra $\mathcal{A}$ we will denote by $\mathcal{A}' := \{X / [\mathcal{A}, X] = 0\}$ its commutant.

In Eq. (3) now the $\mathbb{C}^{n_J}$ factors represent the $\mathcal{G}$-irreducible representations and d_J their multiplicities. In this case universality is obviously prevented because $\mathcal{U}_A \subset (\mathbb{C}\mathcal{G})' \cong \oplus_J \mathbb{1}_{n_J} \otimes U(d_J)$: different J sectors are never coupled by the allowed operations in $\mathcal{U}_A$. In order to better illustrate these notions let us go back to example 2; here one can choose as symmetry group $\mathcal{G} = \{\mathbb{1}, \sigma^{z\otimes 2}\} \cong \mathbf{Z}_2$. Its commutant is then given by $(\mathbb{C}\mathcal{G})' = \mathrm{span}\{\mathbb{1}, \sigma^z\otimes\mathbb{1}, \mathbb{1}\otimes\sigma^z, \sigma^{z\otimes 2}, \sigma^\alpha\otimes\sigma^\beta (\alpha,\beta = x,y)\}$. This algebra contains both the su(2)'s mentioned above and it allows one to operate *simultaneously* over $\mathcal{H}_0$ and $\mathcal{H}_1$.

The group $\mathcal{U}_A$ acts irreducibly over the subspaces $\mathcal{C}_J = |\phi\rangle \otimes \mathcal{H}_J$, where $|\phi\rangle$ is an arbitrary vector in the multiplicity factor $\mathbb{C}^{n_J}$ in Eq. (3). It is elementary, yet important to keep in mind that irreducibility on itself does not imply that all the unitaries over $\mathcal{C}$ are realized as group elements (see Proposition below). The most general of such transformations, as written above, is given by a suitable *linear combination* of elements from $\mathcal{U}_A$. Technically this is expressed by saying that the group of unitaries over $\mathcal{C}$ is given by the restriction to $\mathcal{C}$ of the unitary part $U\mathbb{C}\mathcal{U}_A|_{\mathcal{C}}$ of the *group algebra* of $\mathcal{U}_A$. One can easily prove the following.

Proposition 1. Let $\mathcal{U}_A$ be a Lie group. If dim $\mathcal{U}_A|_{\mathcal{C}_J}=d_J^2$ then $\mathcal{U}_A$ is $\mathcal{C}_J$ universal where $\mathcal{C}_J$ is any d_J dimensional subspace of the form $|\phi\rangle\otimes\mathcal{H}_J, (|\phi\rangle\in\mathbb{C}^{n_J})$.

Proof. From Eq. (3) it is clear that any of the $\mathcal{C}_J$ is an irreducible representation space of $\mathcal{U}_A$ and it is therefore $\mathcal{U}_A$ invariant. Moreover under the current assumptions the Lie group $\mathcal{U}_A$ has dimension d_J^2, this means that it coincides with the whole set of unitary transformations over $\mathcal{C}_J$.

This proposition provides in principle a protocol for determining whether a set of Hamiltonians $\mathcal{I}_A$ allows for encoded universality. (i) Determine the group $\mathcal{U}_A$ of allowed unitaries, (ii) Decompose the total state-space $\mathcal{H}$ according the $\mathcal{U}_A$ irreducible sectors, (iii) compute for all J's, the numbers $d_J^2-\dim\mathcal{U}_A|_{\mathcal{C}_J}\geqslant 0$; those equal zero give rise to a n_J parameter families of codes over which $\mathcal{I}_A$ is universal. Of course all the steps above are in general not trivial and represent a challenge on their own. The situation gets somewhat simplified when the conditions for the validity of Eq. (1) hold. In this case everything can be formulated in terms of the Lie algebra $\mathcal{L}_A$. In several instances of interest one has that $\mathcal{L}_A$ is the image of a known Lie algebra $\mathcal{L}$, e.g., su(L) through a *faithful*, i.e., zero kernel, irreducible representation ρ_A. In this case $\dim\mathcal{L}_A|_{\mathcal{H}_J}=\dim\mathcal{L}$, so it is sufficient to check the d_J^2's against a single number, e.g., dim $u(2)=4$.

Example 3. Let us consider L bosonic modes, $[b_i,b_j^\dagger]=\delta_{ij}, (i,j=1,\ldots,L)$. The set of controllable interactions is given by $\mathcal{I}_A=\{b_j^\dagger b_i/i,j=1,\ldots,L\}$. It is a standard matter to see that the bilinears $b_j^\dagger b_i$ span an algebra $\mathcal{L}_A$ isomorphic to $u(L)$. The Fock space $\mathcal{H}_F=h_\infty^{\otimes L}$ (h_∞ is the state-space of a single quantum oscillator) splits in su(L)-invariant subspaces $\mathcal{H}_N$ with dimensions $d_{N,L}=\binom{N+L-1}{L-1}$ corresponding to the eigenvalues N of the total number operator $\Sigma_{j=1}b_j^\dagger b_j$. Typically $d_{N,L}^2>L^2=\dim u(L)$ and therefore $\mathcal{L}_A$ is *not* $\mathcal{H}_N$-universal. When $N=1$, with L arbitrary, one obtains the fundamental irreducible representation for which $d_{1,L}=L$.

IV. GROUP ALGEBRA UNIVERSALITY

We illustrate now another general route to encoded universality; particular instances of this scheme have already found explicit important applications in spin-based QIP [7,5,6] and fault-tolerant computation over DFS's [6]. In the following we will adopt the standard mathematical usage of the term *generic*: always but for zero-measure set.

Proposition 2. Suppose that the allowed interactions have the form $H=\Sigma_{\lambda_i}H_i$ with completely controllable λ_i's and happen to belong to the group algebra of a non-Abelian group $\mathcal{K}$, i.e., $\mathcal{I}_A\subset\mathbb{C}\mathcal{K}$. Then the group $\mathcal{U}_A$ is *generically* $\mathcal{C}$ universal for all $\mathcal{C}=|\phi\rangle\otimes\mathcal{H}_J$, where $\mathcal{H}_J$ is a $\mathcal{K}$-irreducible representation space and $|\phi\rangle\in\mathbb{C}^{n_J}$ [n_J is the multiplicity of the Jth irreducible representation, see decompostion (3)].

Proof. Under the current assumptions one has $\mathcal{U}_A=\exp\mathcal{L}_A$, but for *generic* $\mathcal{I}_A\subset\mathbb{C}\mathcal{K}$ one has [2] the Lie algebra generated by the allowed interactions is the *whole* algebra of anti-Hermitian elements of the group-algebra $\mathbb{C}\mathcal{K}$, i.e., $u(\mathbb{C}\mathcal{K})$. Thus $\mathcal{U}_A|_{\mathcal{C}}=\exp u(\mathbb{C}\mathcal{K})|_{\mathcal{C}}=U\mathbb{C}\mathcal{K}|_{\mathcal{C}}$. But it is a basic fact of group representation theory that the unitary part of the group-algebra restricted to an irreducible representation-space amounts the *whole* unitary group over that space. Formally $U\mathbb{C}\mathcal{K}|_{\mathcal{C}}=\mathcal{U}(\mathcal{C})$; this relation along with the preceding one completes the proof.

Example 4. Let $\mathcal{H}\cong\mathbb{C}^2$, the $\mathcal{K}=\mathrm{SU}(2)$ fundamental representation space (one irreducible representation with multiplicity one). A generic Hamiltonian in $\mathbb{C}\mathrm{SU}(2)$ has the form $H=\Sigma_{\alpha=x,yz}\lambda_\alpha\sigma^\alpha$. This latter set is universal over $\mathcal{H}$.

At this point it is worthwhile to emphasize that, even if both Propositions 1 and 2 have been formulated in terms of subspaces $\mathcal{C}$'s, simply by tracing out the $|\phi\rangle$ vectors one gets conditions under which universal control is achieved over the factors $\mathcal{H}_J$ in Eq. (3). The $\mathcal{H}_J$ factors correspond to "virtual" subsystems in which one can decompose the systems according to the given available operational resources [18]. This kind of quantum subsystem generalizes the noiseless subsystems [15] that form the basis of general error correction or avoidance strategies [16,12]. It is also interesting to note that Proposition 2 provides us with an example of a group, i.e., $U\mathbb{C}\mathcal{K}$ for which Propositon 1 *always* holds true (note that $\forall J$, $\dim U\mathbb{C}\mathcal{K}=|\mathcal{K}|>d_J^2$).

An instance of Proposition 2 is the well-known case of N spin 1/2 systems coupled by exchange interactions [7]. In this case the naturally allowed Hamiltonians are actually members of the symmetric group $\mathcal{S}_N$ (and so are *a fortiori* elements of its group algebra). As a result, universality can be generically achieved in any irreducible subspace of the permutation group. For example, for $N=3$ one has one totally symmetric irreducible representation (corresponding to the maximal spin $J=3/2$) and a two-dimensional $\mathcal{S}_3$ irreducible representation (corresponding to two $J=1/2$ SU(2) irreducible representations). So one has a two-parameter family of encoded qubits over which the exchange Hamiltonians are universal.

Example 5. Let us consider as $\mathcal{K}$ the simplest non-Abelian group: the dihedral group D_3 [13], i.e., the group of spatial rigid symmetries of a triangle (notice that $D_3\cong\mathcal{S}_3$). D_3 has order six and is generated by a $2\pi/3$ rotation R and a reflection P satisfying the relations $R^3=P^2=RPRP=\mathbb{1}$. A three-dimensional representation is provided by $\hat{R}(z_1,z_2,z_3)=(z_3,z_1,z_2)$, $\hat{P}(z_1,z_2,z_3)=(z_2,z_1,z_3)$ $(z_i\in\mathbb{C})$. This is a reducible representation: $\mathbb{C}^3$ splits in a two-dimensional reducible representation $\mathcal{C}\cong\mathrm{span}\{\Sigma_{j=1}^3 e^{2i\pi/3kj}|j\rangle,(k=1,2)\}$ and a one-dimensional reducible representation $|s\rangle=1/\sqrt{3}\Sigma_{j=1}^3|j\rangle$. The two-dimensional reducible representation can encode for a qubit. Now it is easy to check that $P|_{\mathcal{C}}=\sigma^x$, moreover $(R-R^{-1})|_{\mathcal{C}}$ is proportional to σ^z. The controllability of generic Hermitian element of $\mathbb{C}D_3$, e.g.,

$H(\lambda_1,\lambda_2)=\lambda_1 P+\lambda_2 R+\overline{\lambda}_2 R^{-1}$ then suffices for universal control over $\mathcal{C}$.

V. TENSOR PRODUCT STRUCTURE

Above, it was shown generically how universal quantum control can be obtained over subspaces/subsystems. To relate these results to quantum computation [1], we investigate the subcase of quantum control in which the control space possesses a tensor product structure. We then consider a state space $\mathcal{H}_N=\mathcal{H}^{\otimes N}$ associated to N copies of a basic one. We assume that $\mathcal{U}_A\subset\mathcal{U}(\mathcal{H}_N)\supset\mathcal{U}(\mathcal{H})^{\otimes N}$ is *locally* universal, in the sense that it contains a subgroup $\mathcal{U}_{A,loc}^{\otimes n}$, such that $\mathcal{U}_{A,loc}\subset\mathcal{U}(\mathcal{H})^{\otimes M}$ is $\mathcal{C}$ universal for some $\mathcal{C}\subset\mathcal{H}^{\otimes M}(n=N/M\in\mathbf{N})$. In other words we assume that there exists a *local* encoding, involving a cluster of M basic subsystems, for which universality is achieved; let $\mathcal{C}^{(i)}$ is the code corresponding to the ith cluster. Example 1 above provides an instance of this situation in which two physical qubits are used to encode a single logical one over which the allowed operations are universal. Now what one wants is to be universal over the global code $\mathcal{C}_N=\mathcal{C}^{\otimes n}$. By the results in universality contained in Ref. [4] the following formal result follows.

Proposition 3. Let $\mathcal{U}_A$ be locally universal such that for any pair $i,j=1,\ldots,n$ it exists $X\in\mathcal{U}_A$ such that (i) X acts as the identity in all the clusters but the ith and the jth; (ii) $\mathcal{C}^{(i)}\otimes\mathcal{C}^{(j)}$ is an X-invariant subspace and X is an entangling operator over it. Then $\mathcal{U}_A$ is $\mathcal{C}_N$ universal.

The DFS theory [14] provides once again a clear example of this result. Let $\mathcal{H}\cong\mathbb{C}^d$ and suppose that one is able just to turn on and off exchange Hamiltonians between the different factors in $\mathcal{H}^{\otimes M}$. In this case the available interactions lie in $\mathbb{C}\mathcal{S}_M$. The commutant of the latter is given by the M-fold tensor representation of $\mathrm{SU}(d)$. For $M=2\,d$ the state space contains a two-dimensional $\mathrm{SU}(d)$-*singlet* sector $\mathcal{C}$, i.e., states in $\mathcal{C}$ that are invariant under all the $\mathrm{SU}(d)$ transformations. This logical qubit—which requires a cluster of $2\,d$ physical qudits—supports a $\mathcal{S}_M$-irreducible representation [13]. Now we consider $n=N/M$ clusters coupled together by Hamiltonians in $\mathbb{C}\mathcal{S}_N$ (which supports a $\mathcal{S}_N$ irreducible representation). The crucial point is now that the $\mathrm{SU}(d)$-singlet sector of $\mathcal{H}^{\otimes N}$ strictly *includes* $\mathcal{C}^{\otimes n}$. Since exchange Hamiltonians allow generically for universality on the former (Proposition 2), one gets $\mathcal{C}^{\otimes n}$ universality as well. This, in the qubit case $d=2$, has been constructively shown in Ref. [5].

Even the tensorized form of Example 1 falls in our scheme. Here, the code is the (tensor power of) the trivial irreducible representation of group generated by $i e^{i\pi/2\,\sigma^z\otimes\sigma^z}$. The commutant of this group—besides all the transformations needed for one-qubit gates—contains elements of the form $\sigma_j^z\sigma_{j+1}^z$, which are used to enact an entangling two-qubit gate [8].

VI. CONCLUSIONS

In this paper we have formulated the problem of universal quantum control and quantum-information processing on subspaces/subsystems within a general algebraic-dynamical framework. All physical examples known so far fit in this framework. Constructions have been given providing general conditions under which encoded-universality can be established. This has been done by exploiting the algebraic formalism introduced to describe in a unified fashion all known error correction or avoidance schemes [15,16,12]. This unification is on the one hand pretty remarkable in view of the apparent sharp diversity of the initial physical problems; on the other hand, the existence of fundamental connection between diverse error compensation schemes is not totally surprising once one realizes the *duality* between the task of ‘‘not allowing many bad things to happen’’ in error correction and ‘‘making as many as good things happen as possible’’ in quantum control.

ACKNOWLEDGMENTS

P.Z. gratefully acknowledges financial support by Cambridge-MIT Institute Limited and by the European Union project TOPQIP (Contract No. IST-2001-39215).

[1] For reviews, see D.P. DiVincenzo and C. Bennett, Nature (London) **404**, 247 (2000); A. Steane, Rep. Prog. Phys. **61**, 117 (1998).

[2] S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995).

[3] D. Deutsch, A. Barenco, and A. Ekert, Proc. R. Soc. London, Ser. A **449**, 669 (1995); D.P. Di Vincenzo, Phys. Rev. A **50**, 1015 (1995).

[4] J.L. Brylinski and R. Brylinski, e-print quant-ph/0108062; M.J. Bremner *et al.*, Phys. Rev. Lett. **89**, 247902 (2003).

[5] D. Bacon, J. Kempe, D.A. Lidar, and K.B. Whaley, Phys. Rev. Lett. **85**, 1758 (2000); for a nice review see also D. Bacon, e-print quant-ph/0305025.

[6] Kempe, D. Bacon, D.A. Lidar, and K.B. Whaley, Phys. Rev. A **63**, 042307 (2001).

[7] D.P. Di Vincenzo *et al.*, Nature (London) **408**, 339 (2000).

[8] D. Lidar and L.-A Wu, Phys. Rev. Lett. **88**, 017905 (2002); L.-A. Wu and D.A. Lidar, *ibid.* **88**, 207902 (2002); M.S. Byrd and D. Lidar, *ibid.* **89**, 047901 (2002).

[9] L. Viola, Phys. Rev. A **66**, 012307 (2002).

[10] P. Zanardi and M. Rasetti, Phys. Lett. A **264**, 94 (1999); J. Pachos, P. Zanardi, and M. Rasetti, Phys. Rev. A **61**, 010305(R) (2000).

[11] S.G. Schirmer, J.V. Leahy, and A.I. Solomon, Phys. Rev. A **35**, 4125 (2002); S.G. Schirmer, H. Fu, and A.I. Solomon, *ibid.* **63**, 063410 (2001).

[12] P. Zanardi and S. Lloyd, Phys. Rev. Lett. **90**, 067902 (2003).

[13] J.F. Cornwell, *Group Theory in Physics* (Academic, New York, 1984), Vol. I–III.

[14] L.M. Duan and G.C. Guo, Phys. Rev. Lett. **79**, 1953 (1997); P. Zanardi and M. Rasetti, *ibid.* **79**, 3306 (1997); D.A. Lidar, I.L.

Chuang, and K.B. Whaley, *ibid.* **81**, 2594 (1998).

[15] E. Knill, R. Laflamme, and L. Viola, Phys. Rev. Lett. **84**, 2525 (2000); L. Viola, E. Knill, and S. Lloyd, *ibid.* **85**, 3520 (2000).

[16] P. Zanardi, Phys. Rev. A **63**, 12 301 (2001).

[17] The group algebra $\mathbb{C}\mathcal{K}$ of a group $\mathcal{K}$ is the vector space generated by complex linear combination of elements of $\mathcal{K}$. By extension of the group multiplication $\mathbb{C}\mathcal{K}$ gets the structure of associative algebra.

[18] P. Zanardi, Phys. Rev. Lett. **87**, 077901 (2001).