Stabilizing quantum information

Paolo Zanardi
Institute for Scientific Interchange (ISI) Foundation, Viale Settimio Severo 65, I-10133 Torino, Italy
and Istituto Nazionale per la Fisica della Materia

(Received 12 October 1999; published 5 December 2000)

The dynamical-algebraic structure underlying all the schemes for quantum information stabilization is argued to be fully contained in the reducibility of the operator algebra describing the interaction with the environment of the coding quantum system. This property amounts to the existence of a nontrivial group of symmetries for the global dynamics. We provide a unified framework that allows us to build systematically additional classes of error correcting codes and noiseless subsystems. It is shown that by using symmetrization strategies one can artificially produce noiseless subsystems supporting universal quantum computation.

DOI: 10.1103/PhysRevA.63.0123XX PACS number(s): 03.67.Lx, 03.65.Fd

Defending the quantum coherence of a processing device against environmental interactions is a vital goal for any foreseeable practical application of quantum information and quantum computation theory [1]. So far essentially three kinds of strategy have been devised in order to satisfy such a crucial requirement: (a) error correcting codes (ECC's) [2], which, in analogy with classical information theory, actively stabilize quantum information by using redundant encoding and measurements; (b) error avoiding (EA) codes [3], which pursue a passive stabilization by exploiting symmetry properties of the environment-induced noise for suitable redundant encoding; (c) noise suppression schemes [4], in which, with no redundant encoding, the decoherence-inducing interactions are averaged away by properly tailored external ''pulses'' frequently iterated. In this paper we shall show how all these schemes derive conceptually from a common dynamical-algebraic framework. The key notion to shed light on this underlying structure is that of the *noiseless subsystem* (NS) introduced by Knill *et al.* in Ref. [5]. In this paper we shall discuss how one can analyze in a unified fashion in terms of purely algebraic data all the possible strategies for quantum information stabilization. As a by-product a family of generalized ECC's will be introduced. We shall provide abstract characterization of quantum evolutions that support NS's, and show how to obtain them by symmetrization procedures [6]. Application to a realistic model of decoherence is given as well.

Let S be an open quantum system, with (finite-dimensional) state space $\mathcal{H}$, and self-Hamiltonian H_S, coupled to its environment through the Hamiltonian $H_I = \sum_\alpha S_\alpha \otimes B_\alpha$, where the S_α's (B_α's) are system (environment) operators. The unital associative algebra $\mathcal{A}$, closed under Hermitian conjugation $S \mapsto S^\dagger$, generated by the S_α's [7] and H_S will be referred to as the *interaction* algebra. (We shall sometime identify H_S with one of the S_α's and discard the closed case $H_I=0$.) The algebraic approach used in this paper is not restricted to a Hamiltonian description of the dynamics. Alternatively, the dynamics of S can be described by (i)a Markovian master equation, i.e., $\dot{\rho} = -i[H_S,\rho] + (1/2)\sum_\mu \lambda_\mu \{[L_\mu \rho, L_\mu^\dagger] + [L_\mu, \rho L_\mu^\dagger]\}$, for the density matrix ρ; or (ii)a finite time trace-preserving CP map $\rho \mapsto \mathcal{E}_t(\rho) := \sum_i e_i \rho e_i^\dagger (\sum_i e_i^\dagger e_i = \mathbb{1})$. In the first case the relevant interaction algebra is the one generated by H_S and the Lindblad operators L_μ. In the latter case $\mathcal{A}$ is generated by the ''error'' operators e_i.

In general $\mathcal{A}$ is a *reducible* †-closed subalgebra of the algebra End($\mathcal{H}$) of all the linear operators over $\mathcal{H}$. This implies that $\mathcal{A}$ can be written as a direct sum of $d_J \times d_J$ (complex) matrix algebras each one of which appears with a multiplicity n_J [8],

$$\mathcal{A} \cong \oplus_{J \in \mathcal{J}} \mathbb{1}_{n_J} \otimes M(d_J, \mathbb{C}), \tag{1}$$

where $\mathcal{J}$ is a suitable finite set labeling the irreducible components of $\mathcal{A}$. The associated state-space decomposition reads

$$\mathcal{H} \cong \oplus_{J \in \mathcal{J}} \mathbb{C}^{n_J} \otimes \mathbb{C}^{d_J}. \tag{2}$$

These decompositions encode all information about the possible quantum stabilization strategies.

In Ref. [5] the authors observed that in view of relation (1) each factor $\mathbb{C}^{n_J}$ in Eq. (2) corresponds to a sort of effective subsystem of S coupled to the environment in a state independent way. Such subsystems are then referred to as noiseless. In particular, one gets a noiseless code, i.e., a decoherence-free subspace $\mathcal{C} \subset \mathcal{H}$ when in Eq. (2) there appear one-dimensional irreducible representations (irreps) J_0 with multiplicity greater than one times $\mathcal{C} \cong \mathbb{C}^{n_{J_0}} \otimes \mathbb{C}$ [3]. The physical idea is very simple: one wants to identify a subspace of states that corresponds to a multipartite system in which one of the subsystems is coupled with the environment in such a way that quantum information cannot be extracted from it.

We define the commutant $\mathcal{A}'$ in End($\mathcal{H}$) of $\mathcal{A}$ by $\mathcal{A}' := \{X \mid [X, \mathcal{A}] = 0\}$. From Eq. (1) it is clear that the existence of a NS is equivalent to $\mathcal{A}' \cong \oplus_{J \in \mathcal{J}} M(n_J, \mathbb{C}) \otimes \mathbb{1}_{d_J} \neq \mathbb{C}\mathbb{1} := \{\lambda \mathbb{1} \mid \lambda \in \mathbb{C}\}$. For a NS to be relevant for quantum encoding it must be at least two-dimensional, i.e., $\max_J \{n_J\} \geqslant 2$. This amounts to having a *noncommutative* $\mathcal{A}'$. An interaction algebra satisfying the above condition will be called NS supporting. Of course when $\dim \mathcal{A}' = \sum_J n_J^2 = 1$ one is in the irreducible case $[|\mathcal{J}| = n_J = 1]$ in which no NS's exist.

In order to understand in what sense the NS's can be regarded as subsystems let us consider the projectors Q_J

$:=\mathbb{1}_{n_J}\otimes\mathbb{1}_{d_J}\in\mathcal{A}\cap\mathcal{A}'$; they correspond to conserved observables that constrain the accessible state space to be one of the summands in Eq. (2), i.e., $Q_J\mathcal{H}$. The identification of a bipartite structure stems from the fact that on the ''superselection sector'' $Q_J\mathcal{H}$ the full operator algebra is isomorphic to $\mathcal{A}\mathcal{A}'\cong\mathcal{A}\otimes\mathcal{A}'$ [9]. The duality $\mathcal{A}\mapsto\mathcal{A}'$, which will be used repeatedly later, is in this sense the algebraic ground for the notion of a subsystem.

An important special case is when $\{S_\alpha\}$ is a commuting set of Hermitian operators. Then $\mathcal{A}$ is an Abelian algebra and Eq. (2) (with $d_J=1$) is the decomposition of the state space according to the joint eigenspaces of the S_α's. The pointer basis [10] discussed in relation to so-called environment-induced superselection is nothing but an orthonormal basis associated with the resolution (2). The NS's provide the natural noncommutative generalization of the pointer basis. One might conjecture that, for any initial preparation ρ, a relation like $\lim_{t\to\infty}\mathcal{E}_t(\rho)\in\mathcal{A}'\mathcal{A}\cong\oplus_J M(n_J,\mathbb{C})\otimes M(d_J,\mathbb{C})$ holds at least approximately ($\{\mathcal{E}_t\}$ denotes the dynamical semigroup): The quantum coherence between the different J blocks is destroyed.

The decomposition (1) leads to a straightforward generalization of the notion of a stabilizer ECC [11] and allows us to build a general setting in which *nonadditive* quantum codes [12] can arise. Let $|J\lambda\mu\rangle$ ($J\in\mathcal{J},\lambda=1,\ldots,n_J;\mu=1,\ldots,d_J$) be an orthonormal basis associated with the decomposition (1). Let $\mathcal{H}^J_\mu:=\text{span}\{|J\lambda\mu\rangle\mid\lambda=1,\ldots,n_J\}$, and let $\mathcal{H}^J_\lambda$ be defined analogously. Now we consider a CP map description of the dynamics [see point (ii) in the Introduction], the interaction algebra $\mathcal{A}$ being generated by error operators. The next proposition shows that to any NS corresponds a family of ECC's (for a related proposition, see theorem 6 in Ref. [5]).

Proposition 1. The $\mathcal{H}^J_\mu$'s are ECC's for any subset of errors in $\mathcal{A}$.

Proof. If $e_i,e_j\in\mathcal{A}$ then $e_i^\dagger e_j\in\mathcal{A}$. From Eq. (1) and the general results on ECC's [2] the following computation now suffices: $\langle J\lambda'\mu|e_i^\dagger e_j|J\lambda\mu\rangle=\langle J\lambda'\mu|\mathbb{1}\otimes X_{ij}|J\lambda\mu\rangle=\delta_{\lambda,\lambda'}c^{ij}_{J,\mu}$.

This kind of ECC will be referred to as $\mathcal{A}$ *codes*. The above result extends to any error set E such that $\forall e_i,e_j\in E\Rightarrow e_i^\dagger e_j\in\mathcal{B}$, where $\mathcal{B}$ is an operator algebra for which Eq. (1) holds. The proof above should make clear that the $\mathcal{H}^J_\lambda$ are $\mathcal{A}'$ codes. One recovers the usual picture by considering an N-partite qubit system, and an Abelian subgroup $\mathcal{G}$ of the Pauli group $\mathcal{P}:=\{\mathbb{1},\sigma_x,\sigma_y,\sigma_z\}^{\otimes N}$. Let us consider the state-space decomposition (2) associated with $\mathcal{G}$. If $\mathcal{G}$ has $k<N$ generators then $|\mathcal{G}|=2^k$, whereas from commutativity it follows that $d_J=1$ and $|\mathcal{J}|=|\mathcal{G}|$. Moreover, one finds $n_J=2^{N-k}$: each of the 2^k joint eigenspaces of $\mathcal{G}$ (stabilizer code) encodes $N-k$ logical qubits. Therefore one has $\mathcal{H}=\oplus_{J=1}^{2^k}\mathbb{C}^{2^{N-k}}\otimes\mathbb{C}\cong\mathbb{C}^{2^{N-k}}\otimes\mathbb{C}^{2^k}$. Now it is known [13] that correctable errors (belonging to the Pauli group) correspond to elements e_i,e_j such that $e_i^\dagger e_j$ either belongs to $\mathcal{G}$ or *anticommutes* with (at least) one element $\mathcal{G}$. In particular, the latter operators induce a nontrivial mixing of different eigenspaces, i.e., a nontrivial action on the $\mathbb{C}^{2^k}$ factor. In both cases they belong to the algebra $\mathcal{B}=\mathbb{1}_{2^{N-k}}\otimes M(2^k,\mathbb{C})$. The $\mathbb{C}^{2^k}$ factor corresponds in the usual stabilizer construction to the encoding of the error syndrome, i.e., it will be a bit string containing the eigenvalues of the stabilizer. The errors correspond to operations on this factor.

An example of this construction is given by considering any noiseless code. In this case since $\mathcal{A}|_\mathcal{C}\cong\mathbb{1}_{n_0}\otimes M(1,\mathbb{C})$ one finds $c^{ij}_{0,1}=c_ic_j$, since this matrix is not full rank. A noiseless code is a degenerate ECC [14].

It is well known that group-theoretical notions play a key role in the analysis of all the schemes so far devised for quantum noise control. This is true for the study of general NS-supporting dynamics as well. Indeed the condition $\mathcal{A}'\neq\mathbb{C}\mathbb{1}$ implies the existence of a nontrivial group of symmetries $\mathcal{G}\subset U\mathcal{A}'$. Conversely, given a group $\mathcal{G}$ of unitary operators over $\mathcal{H}$ its commutant is a reducible subalgebra of End($\mathcal{H}$) closed under Hermitian conjugation. Loosely speaking, the more symmetric a dynamics, the more likely it is NS supporting.

Therefore one is naturally led to consider the action, via a representation ρ, of a finite order (or compact) group $\mathcal{G}$ on a quantum state space $\mathcal{H}$. The irrep decomposition for ρ has the form of Eq. (2) where now the $\mathcal{J}$ labels a set of $\mathcal{G}$ irreps ρ_J ($\dim\rho_J=d_J$). Extending ρ by linearity to the group algebra $\mathbb{C}\mathcal{G}:=\oplus_{g\in\mathcal{G}}\mathbb{C}|g\rangle$, one gets a decomposition like that in Eq. (1). It is now easy to provide a sufficient condition for an interaction algebra to be NS supporting.

Proposition 2. If $\mathcal{A}\subset\rho(\mathbb{C}\mathcal{G})$ then the dynamics supports (at least) $|\mathcal{J}|$ NS's with dimensions $\{n_J(\rho)\}_{J\in\mathcal{J}}$.

When $\mathcal{G}$ is a compact group Proposition 2 holds by replacing $\rho(\mathbb{C}\mathcal{G})$ with the associative algebra generated by $\tilde{\rho}(\mathcal{L})$, where $\mathcal{L}$ denotes the Lie algebra of $\mathcal{G}$ and $\tilde{\rho}$ its representation associated with ρ. An important instance of this case is given by collective decoherence, which will be discussed later in a more detailed manner. It should be stressed that the condition of belonging to a group algebra is always satisfied: it is sufficient to consider any group acting irreducibly over $\mathcal{H}$, e.g., the Pauli group in N-partite qubit systems. The nontrivial assumption is the reducibility of ρ. When this is not given one has, in order to achieve it, to resort to physical procedures for modifying the system dynamics.

Now we address the issue of the relation between NS-supporting dynamics and the quantum noise suppression schemes that have recently emerged as a third possible way to defeat decoherence in quantum computers [4]. In Refs. [15] and [6] ways to devise *physical* procedures were discussed, involving iterated external pulses or measurements, whereby a quantum dynamics generated by $\mathcal{A}$ can be modified to a dynamics generated by $\pi_\rho(\mathcal{A})$. Here the ''symmetrizing'' projector π_ρ is given by [6] $X\to\pi_\rho(X):=|\mathcal{G}|^{-1}\sum_{g\in\mathcal{G}}\rho_gX\rho_g^\dagger\in\rho(\mathbb{C}\mathcal{G})'$. If we are willing to retain the system self-dynamics (generated by H_S) and to get rid just of the unwanted interaction with the environment (the S_α's), then we have to look for a group $\mathcal{G}\subset U(\mathcal{H})$, such that (i) $H_S\in\mathbb{C}\mathcal{G}'$, and (ii) the interaction operators S_α transform according to nontrivial irreps under the (adjoint) action of $\mathcal{G}$. In this case, since $\pi_\mathcal{G}$ projects on the $\mathcal{G}$-invariant, i.e., trivial irrep, sector of End$(\mathcal{H})$, it can be shown that $\pi_{\mathcal{G}}(S_\alpha)=0$: the decoherence-inducing interactions have been averaged away, and the effective dynamics is unitary.

To make a connection between noise suppression schemes and NS's it is crucial to notice that Proposition 2 holds even on replacing the group algebra with its commutant and the n_J's with the d_J's. Indeed, since the $\mathcal{G}$ symmetrization belongs to $\rho(\mathbb{C}\mathcal{G})'$, one has the following proposition.

Proposition 3. The $\mathcal{G}$ symmetrization of $\mathcal{A}$ supports (at least) $|\mathcal{J}|$ NS's with dimensions $\{d_J(\rho)\}_{J\in\mathcal{J}}$.

The simplest instance of this result is given by S being an N-level system and $\mathcal{G}$ a finite group that acts irreducibly over $\mathcal{H}$, e.g., an error generating group [16]. Any $\mathcal{G}$-symmetrized interaction algebra is then proportional to the identity: the whole space is a NS. This situation corresponds to the decoupling scheme analyzed in [17].

The next proposition straightforwardly generalizes a result of Ref. [18]. The key mathematical observations are (i) the Lie algebra spanned by a *generic* couple of Hermitian operators H_1,H_2 is the full $u(\mathcal{H})$; (ii) the unitary group $U\mathcal{A}'$ of the commutant restricted to one of the summands in Eq. (2) provides the full unitary group over the associated NS. From (i) it follows that, if one is physically able to switch H_1 and H_2 on and off, any unitary transformation can be generated with arbitrary accuracy [19]. More specifically, in view of (ii), if one starts from Hamiltonians in $\mathcal{A}'$ any unitary transformation over the NS can be (approximately) obtained. Finally, if such Hamiltonians are not available to the experimenter from the outset, they can, in principle, be obtained from a generic, i.e., not invariant, pair of Hamiltonians by a symmetrization procedure [18]. The formal proposition follows.

Proposition 4. Given a generic pair of Hamiltonians $\{H_i\}_{i=1}^2$ on the state space of S, their $\mathcal{G}$ symmetrizations $\{\pi_\rho(H_i)\}_{i=1}^2$ allow for universal quantum computation over each of the NS's.

This result about universal quantum computation over a NS is just existential; nevertheless, it is remarkable in that it shows how only a specific class of gates is required for generating arbitary computations completely within the NS. For practical purposes it is also important that the desired operations can be efficiently enacted in terms of physical interactions, i.e., one- and two-body couplings. These requirements must be checked case by case in that they do not follow from Proposition 4. Constructive results for the case of collective decoherence were recently found in Ref. [20], in which it is shown how to achieve universal computations by resorting to exchange Hamiltonians only. More generally, it is likely that the schemes with fast switching on and off of Hamiltonians discussed in Ref. [17] for control of decoupled systems will turn out to be useful for achieving universal and efficient quantum computation over a NS.

We now discuss the case of collective decoherence when a multipartite quantum system, whose degrees of freedom are used for information encoding/processing, is coupled symmetrically with a common environment. This is the paradigmatic case for EA strategies [3] [as opposed to ECC in which noise acts independently on each subsystem]. We shall show that it provides a setting for NS's as well. Here the (minimal) symmetry group is the symmetric group $\mathcal{S}_N$ exchanging different subsystems. It follows that the (maximal) interaction algebra that one can consider is given by the space of totally symmetric operators. In the following we shall specialize to many-qubit systems. All the results straightforwardly extend to general d-level systems coupled to their environment by $sl(d)$ interactions.

Let us consider an N-qubit system $\mathcal{H}_N:=(\mathbb{C}^2)^{\otimes N}$. Over $\mathcal{H}_N$ acts the group SU(2) via the N-fold (tensor) power of the defining irrep, i.e., $U\mapsto U^{\otimes N}$. The associated representation of the Lie algebra $\mathrm{su}(2)=\mathrm{span}\{\sigma_\alpha\}_{\alpha=1}^3$ is given, with obvious notation, by $\rho_N:\sigma_\alpha\mapsto S_\alpha:=\Sigma_{i=1}^N\sigma_\alpha^{(i)}$. The associative algebra generated by $\rho_N(\mathrm{su}(2))$ will be denoted by $\mathcal{A}_N$. We recall that [21] (1) $\mathcal{A}_N$ coincides with the algebra of completely symmetric operators over $\mathcal{H}_N$; (2) the commutant $\mathcal{A}_N'$ is the group algebra $\nu(\mathbb{C}\mathcal{S}_N)$, where ν is the natural representation of the symmetric group $\mathcal{S}_N$ over $\mathcal{H}_N$: $\nu(\pi)\otimes_{j=1}^N|j\rangle=\otimes_{j=1}^N|\pi(j)\rangle(\pi\in\mathcal{S}_N)$. The following proposition derives from su(2) representation theory [21].

Proposition 5. $\mathcal{A}_N$ supports NS's with dimensions $n_J=[(2J+1)N!]/[(N/2+J+1)!(N/2-J)!]$ where J runs from 0 (1/2) for N even (odd).

If in Proposition 5 $\mathcal{A}_N$ is replaced by its commutant, the above result holds with $n_J=2J+1$. Moreover, from Proposition 1 it is clear that collective decoherence allows for $\mathcal{A}_N$ codes as well. For example, let us consider $N=3$ qubits. One has $(\mathbb{C}^2)^{\otimes 3}\cong\mathbb{C}\otimes\mathbb{C}^4+\mathbb{C}^2\otimes\mathbb{C}^2$. The last term can be written as $\mathrm{span}\{|\psi_\beta^\alpha\rangle\}_{\alpha\beta=1}^2$ where $|\psi_1^1\rangle=2^{-1/2}(|010\rangle-|100\rangle)$, $|\psi_2^1\rangle=2^{-1/2}(|011\rangle-|101\rangle)$ and $|\psi_1^2\rangle=2/\sqrt{6}[1/2(|010\rangle+|100\rangle)-|001\rangle]$, $|\psi_2^2\rangle=2/\sqrt{6}[|110\rangle-1/2(|011\rangle+|101\rangle)]$. One can check, for example, that $|\psi_\beta^1\rangle$ and $|\psi_\beta^2\rangle$ ($|\psi_1^\alpha\rangle$ and $|\psi_2^\alpha\rangle$) span a two-dimensional $\mathcal{A}_3$ code ($\mathcal{A}_3'$ code). Taking the trace with respect to the index α (β) one gets the $\mathcal{A}_3'$ ($\mathcal{A}_3$) NS's. Moreover, the first term corresponds to a trivial four-dimensional $\mathcal{A}_3'$ code. Notice that any permutation error can be written as the product of transpositions that in turn, in this representation, corresponds to the so-called exchange errors [22].

A weaker kind of collective decoherence is obtained when the symmetry group breaks down: $\mathcal{S}_N\rightarrow\Pi_{c=1}^R\mathcal{S}_{n_c}(\Sigma_{c=1}^R n_c=N)$. The maximal NS-supporting interaction algebra is then isomorphic to the tensor product $\otimes_{c=1}^R\mathcal{A}_{n_c}$, for which the obvious extension of Proposition 5 holds: NS's exist, given by all possible tensor products of the cluster NS's. Physically this situation corresponds to R uncorrelated clusters of subsystems such that within each cluster the condition of collective decoherence is fulfilled [23]. As limiting cases one obtain collective decoherence and independent ones in which no NS's exist

We finally comment on possible infinite-dimensional extensions of the ideas and results presented in this paper. They would be relevant for quantum computation with continuous variables [24]. The crucial observation in this respect is that, adding a suitable closure assumption on the interaction algebra, a generalized form of the basic decompositions (2) and

(1) holds [[8], p. 9]. It is then likely that at least some of the constructions of this paper can be properly reformulated in the continuous case. This important issue will be addressed elsewhere; here we limit ourselves to a very simple example that represents the continuous analog of the collective decoherence case previously discussed. Let us consider N copies of a continuous quantum system described by conjugate variables $x_j, p_l([x_j, p_l]=i\,\delta_{lj})$ coupled with a common environment only through the collective coordinates $X := \sum_{j=1}^N x_j, P := \sum_{j=1}^N p_j$. This assumption implies that the interaction Hamiltonian can be written as $H_I = \sum_\alpha f_\alpha(X,P)\otimes B_\alpha$, where the f_α are operator-valued functions generating the relevant interaction algebra $\mathcal{A}_\infty$ and the B_α's are environment operators. We define creation and annihilation operators by $a_k^\pm := 1/\sqrt{2N}\sum_{j=1}^N \exp[i(2\pi/N)kj](x_j \pm i\,p_j)(k=0,\ldots,N-1)$. Then one has $\mathrm{End}(\mathcal{H})\cong \otimes_k \mathcal{A}_k$, where $\mathcal{A}_k$ denotes the algebra generated by $\{a_k^\pm\}$. One can check that $\mathcal{A}_\infty \subset \mathbb{1}_{k>0}\otimes \mathcal{A}_0$. It follows that the factor of $\mathcal{H}$ corresponding to nonzero modes realizes an infinite-dimensional NS.

In this paper we faced the problem of stabilizing quantum information against decoherence in a dynamical-algebraic fashion. The analysis of the operator algebra $\mathcal{A}$ generated by interactions with the environment and the self-Hamiltonian of the information processing system provides the general conceptual framework. The notion of a noiseless subsystem [5] has been shown to be the key tool for unveiling the common structure at the root of all the (quantum) error correction, error avoiding, and error suppression schemes discovered so far: the reducibility of $\mathcal{A}$ provides sectors of the state space from which information cannot be extracted by unwanted interactions. Additional families of ECC's have been presented. We have described general symmetrizing strategies designed to synthesize quantum evolutions with the desired capability of supporting noiseless subsystems. The general ideas have been exemplified by the collective decoherence case. In our opinion, the overall emerging picture is conceptually quite satisfactory in that, on the one hand it allows us to clarify the strict mutual relations between apparently different techniques; on the other hand, in view of its generality, it is likely to open different ways to practical realization of noiseless quantum information processing.

I thank M. Rasetti for useful discussions and critical reading of the manuscript, and Elsag (a Finmeccanica company) for financial support.

[1] For a review, see A. Steane, Rep. Prog. Phys. **61**, 117 (1998).

[2] E. Knill, R. Laflamme, Phys. Rev. A **55**, 900 (1997), and references therein.

[3] L.M. Duan and G.C. Guo, Phys. Rev. Lett. **79**, 1953 (1997); Phys. Rev. A **57**, 737 (1998); P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997); Mod. Phys. Lett. B **25**, 1085 (1997); D.A. Lidar, I.L. Chuang, and K.B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).

[4] L. Viola and S. Lloyd, Phys. Rev. A **58**, 2733 (1998); L-M. Duan and G.-C. Guo, Phys. Lett. A **261**, 139 (1999); D. Vitali and P. Tombesi, Phys. Rev. A **59**, 4178 (1999).

[5] E. Knill, R. Laflamme, and L. Viola, Phys. Rev. Lett. **84**, 2525 (2000).

[6] P. Zanardi, Phys. Lett. A **258**, 77 (1999).

[7] Given $\mathcal{S}\subset \mathrm{End}(\mathcal{H})$, the associative unital †-closed algebra generated by $\mathcal{S}$ is the norm closure of the linear span of the monomials built with operators in $\mathcal{S}\cup\mathcal{S}^\dagger$ plus the identity $\mathbb{1}$.

[8] N.P. Landsman, e-print math-ph/9807030.

[9] Compare this with the ''real'' bipartite case $\mathcal{H}=\mathcal{H}_1\otimes\mathcal{H}_2$. One has $\mathrm{End}(\mathcal{H})=\mathcal{A}\mathcal{A}'\cong\mathcal{A}\otimes\mathcal{A}'$, where $\mathcal{A}:=\mathrm{End}(\mathcal{H}_1)\otimes\mathbb{1}_2, \mathcal{A}' = \mathbb{1}_1\otimes\mathrm{End}(\mathcal{H}_2)$. Here $\mathcal{A}$ is a *factor* [8].

[10] W.H. Zurek, Phys. Rev. D **24**, 1516 (1981); **26**, 1862 (1982).

[11] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).

[12] E.M. Rains *et al.*, Phys. Rev. Lett. **79**, 953 (1997).

[13] A.R. Calderbank *et al.*, Phys. Rev. Lett. **78**, 405 (1997).

[14] D.A. Lidar, D. Bacon, and K.B. Whaley, Phys. Rev. Lett. **82**, 4556 (1999).

[15] L. Viola, E. Knill, and S. Lloyd, Phys. Rev. Lett. **82**, 2417 (1999).

[16] E. Knill, e-print quant-ph/9608048.

[17] L. Viola, S. Lloyd, and E. Knill, Phys. Rev. Lett. **83**, 4888 (1999).

[18] P. Zanardi, Phys. Rev. A **60**, R729 (1999).

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

[20] D. Bacon *et al.*, Phys. Rev. Lett. **85**, 1758 (2000).

[21] J.F. Cornwell, *Group Theory in Physics* (Academic, New York, 1984), Vols. I-III.

[22] M.B. Ruskai, Phys. Rev. Lett. **85**, 194 (2000); D.A. Lidar *et al.*, Phys. Rev. A **61**, 052307 (2000).

[23] P. Zanardi, Phys. Rev. A **57**, 3276 (1998).

[24] S. Lloyd and S.L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999).