Theory of decoherence-free fault-tolerant universal quantum computation

J. Kempe,[1,3,4] D. Bacon,[1,2] D. A. Lidar,[1,*] and K. B. Whaley[1]
[1]*Department of Chemistry, University of California, Berkeley, California 94720*
[2]*Department of Physics, University of California, Berkeley, California 94720*
[3]*Department of Mathematics, University of California, Berkeley, California 94720*
[4]*École Nationale Superieure des Télécommunications, Paris, France*
(Received 19 April 2000; revised manuscript received 5 September 2000; published 20 March 2001)

Universal quantum computation on decoherence-free subspaces and subsystems (DFSs) is examined with particular emphasis on using only physically relevant interactions. A necessary and sufficient condition for the existence of decoherence-free (noiseless) subsystems in the Markovian regime is derived here for the first time. A stabilizer formalism for DFSs is then developed which allows for the explicit understanding of these in their dual role as quantum error correcting codes. Conditions for the existence of Hamiltonians whose induced evolution always preserves a DFS are derived within this stabilizer formalism. Two possible collective decoherence mechanisms arising from permutation symmetries of the system-bath coupling are examined within this framework. It is shown that in both cases universal quantum computation which always preserves the DFS (natural fault-tolerant computation) can be performed using only two-body interactions. This is in marked contrast to standard error correcting codes, where all known constructions using one- or two-body interactions must leave the code space during the on-time of the fault-tolerant gates. A further consequence of our universality construction is that a single exchange Hamiltonian can be used to perform universal quantum computation on an encoded space whose asymptotic coding efficiency is unity. The exchange Hamiltonian, which is naturally present in many quantum systems, is thus asymptotically universal.

DOI: 10.1103/PhysRevA.63.042307 PACS number(s): 03.67.Lx, 03.65.Ta, 03.65.Fd, 89.70.+c

I. INTRODUCTION

The discovery that information encoded over quantum systems can exhibit strange and wonderful computational [1,2] and information theoretic [3,4] properties has led to an explosion of interest in understanding and exploiting the ''quantumness'' of nature. For the use of quantum information to progress beyond mere theoretical constructs into the realm of testable and useful implementations and experiments, it is essential to develop techniques for preserving quantum coherences. In particular, the coupling of a quantum system to its environment leads to a process known as decoherence, in which encoded quantum information is lost to the environment. In order to remedy this problem active quantum error correction codes (QECCs) [5–9] have been developed, by analogy with classical error correction. These codes encode quantum information over an entangled set of code words, the structure of which serves to preserve the quantum information, when used in conjunction with a frequently recurring error correcting procedure. It has been shown that when the rate of decoherence is below a certain threshold, fault tolerant quantum information manipulation is possible [10–15]. Since it is believed that there are no systems for which the decoherence mechanism entirely vanishes, QECCs will be essential if quantum information manipulation is to become practical.

An alternative approach has been proposed and developed recently, in which the central motivation is the desire to reduce the effect of a specific decoherence mechanism. This is the decoherence-free subspace (DFS) approach (also referred to as ''error avoiding,'' or ''noiseless'' quantum codes) [16–29]. In contrast to the active mode of QECC, DFS theory can be viewed as providing a passive approach, where a specific symmetry of the system-bath coupling is employed in order to seek out a quiet corner of the system's Hilbert space which does not experience decoherence. Information encoded here over a subspace of (usually entangled) system states is robust against a specific form of decoherence. We shall refer to this as the ''DFS supporting decoherence mechanism.'' When this is the dominant form of decoherence in the physical system, there are major gains to be had by operating in the DFS. Previous work has shown that collective decoherence of the type experienced in condensed phase systems at low temperatures can be successfully eliminated in this way [30,31]. Further research showed that DFSs are robust to perturbing error processes [24,27], and are thus ideally suited for concatenation in a QECC [25].

A third approach to decoherence explored recently employs dynamic decoupling [32–34] or related symmetrization procedures [35]. An interesting connection between all three of these methods to combat decoherence (active, passive, and symmetrization) was established in Ref. [36].

In this paper we address the problem of employing the decoherence-free subspace approach and generalizations of this to perform quantum computation. The motivating goal behind the DFS approach is to use symmetry first. Thus one first identifies a DFS for the major sources of decoherence, via the symmetry of the interaction with the environment. One then proceeds to use the DFS states as a basis for a QECC which can deal with additional perturbing error processes. In order for this scheme to be useful, DFSs must support the ability to perform universal quantum computa-

*Present address: Chemistry Department, University of Toronto, 80 St. George St., Toronto, Ontario, Canada M55 3H6.

tion on the encoded states. Towards this end, certain existential results [37] have been derived showing that in principle universal quantum computation can be performed on any DFS. Constructive results for a set of universal quantum gates on a particular class DFSs were subsequently constructed in [26] using known QECC constructions. However, these gates were constructed in such a way that during the operation of the gate, states within a DFS are taken outside of this subspace. Thus these gates would necessarily need to operate on a time scale faster than the DFS supporting decoherence mechanism, in order to be applied efficiently to a concatenated DFS-QECC scheme.[1] Similarly, a universal computation result on DFSs for atoms in cavities was recently presented by Beige *et al.* in [38,39]. It assumes that the interaction driving a system out of the DFS is much weaker than the coupling of non DF-states to the environment. It is then possible to make use of an environment-induced quantum Zeno effect. In order to make use of the robustness condition without resorting to gates which can be made faster than the main DFS supporting decoherence mechanism, one would prefer to explicitly construct a set of Hamiltonians which can be used to perform universal quantum computation, but which never allow states in the DFS to leak out of the DFS. Imperfections in these gates may be dealt with by the concatenation technique of Ref. [25] (see also Ref. [28]).

In addition, one would, from a practical standpoint, like to use Hamiltonians which involve at most two-body interactions (under the assumption that any three-body interactions will be weak and not useful for operations which must compete with the decoherence rate). In [40] such Hamiltonians were used for the important decoherence mechanism known as ''collective decoherence,'' on a system of four physical qubits. In collective decoherence the bath cannot distinguish between individual system qubits, and thus couples in a collective manner to the qubits. The corresponding two-body Hamiltonians used to implement universal quantum computation are those that preserve the collective symmetry. These consist of the exchange interaction between pairs of qubits. The first and main purpose of this paper is therefore to extend the constructive results obtained in [40] to other forms of collective decoherence and to larger DFSs. Two different forms of collective decoherence are considered here, and constructive results are obtained for these on DFSs of arbitrary numbers of qubits. These results have implications that extend far beyond the problem of dealing with collective decoherence. Since they imply that the exchange interaction by itself is sufficient to implement universal quantum computation on a subspace, it follows that using encoded (rather than physical) qubits can be advantageous when resources for physical operations are limited. After all, the standard results for universal quantum computation employ either arbitrary single-qubit operations in addition to a nontrivial two-qubit gate (e.g., a controlled-NOT), or at least two noncommuting two-qubit Hamiltonians [41–45]. The beginnings of these issues are explored in a separate publication [46].

Previous work established that DFSs correspond to the degenerate component of a QECC [25,47]. A second purpose of this work is to present new results on a recently discovered generalization of DFSs, which has been termed ''noiseless subsystems,'' and arises from a theory of QECC for general decoherence mechanisms [48,49]. In line with our previously established terminology [24] we will refer to these as ''decoherence-free subsystems,'' where we take the term ''decoherence'' to mean both dephasing (T_2) and dissipation (T_1). Essentially, the generalization corresponds to allowing for information to be encoded into states transforming according to arbitrary-dimensional irreducible representations (irreps) of the decoherence-operators' algebra, instead of just one-dimensional irreps as in the decoherence-free subspace case (we will present precise definitions later in this paper). These results all arise from a basic theorem on algebras that are closed under the Hermitian conjugation operation (''†-closed algebras''), and thereby unify the role of symmetry in both decoherence-free subspaces and quantum error correction. In this paper we extend the decoherence-free subsystem concept to situations governed by essentially non-†-closed evolution. Such situations arise from non-Hermitian terms in the system-bath interaction, which may occur, e.g., in generalized master equation and conditional Hamiltonian representations of open quantum dynamics [50]. In particular, we derive an if and only if (iff) condition for the existence of decoherence-free subsystems with dynamics governed by a semigroup master equation. This is important because it is well-known in decoherence-free subspace theory that such non-†-closed evolution can support different DFSs than in the †-closed case. A similar result is now shown here to hold for the decoherence-free subsystems.

Existential results for universal quantum computation on decoherence-free subsystems also exist [36]. The universal quantum computation results we obtain in this paper extend beyond decoherence-free subspaces: we show how to achieve constructive universal quantum computation on the decoherence-free subsystems supported under collective decoherence. This most significant achievement of our paper settles the question of universal quantum computation under collective decoherence using realistic Hamiltonians.

Another aim of this paper is to elucidate the close link between DFS and QECC. In [25,47] it was shown that DFSs are in fact maximally degenerate QECCs. This result was derived from the general condition for a code to be a QECC [8]. A very fruitful approach towards QECC has been the stabilizer formalism developed in [9] which led to the theory of universal fault-tolerant computation on QECCs [51]. In [26] we considered DFSs as Abelian stabilizer codes. Here we generalize the stabilizer-framework to *non-Abelian* stabilizers, and show that in general DFSs are stabilizer-codes that protect against errors in the stabilizer itself. This perspective allows one in return to view QECCs as DFSs against a certain kind of errors, and establishes a kind of duality of QECCs and DFSs.

The paper is structured as follows: In Sec. II we review decoherence-free subsystems and place them into the context of the Markovian master equation. For decoherence-free sub-

[1]Note that QECC fault-tolerant gates are also required to operate faster than the decoherence time of the main error process.

spaces this has been done in [24,27]. These earlier results are therefore generalized here to subsystems. In Sec. III we introduce a generalized stabilizer-formalism for DFS, and connect to the theory of stabilizers on QECC developed in [9]. This allows us to treat DFS and QECC within the same framework. It also sheds some light on the duality between DFS and QECC, in particular on the performance of a DFS viewed as a QECC and vice versa. In Sec. IV we deal with universal computation on DFS within both the stabilizer-framework and the representation-theoretic approach. We derive fault-tolerance properties of the universal operations. In particular, we show how to obtain operations that keep the states within a DFS during the entire switching-time of a gate. Further we define the allowed compositions of operations and review results on the length of gate sequences in terms of the desired accuracy of the target gates. In Sec. V we introduce the model of collective decoherence. Section VI explicitly deals with the Abelian case of weak collective decoherence in which system-bath interaction coupling involves only a single system operator. Stabilizer and error-correcting properties are developed for this case, and it is shown how universal computation can be achieved. The same is done for the non-Abelian and more general case of strong collective decoherence in Sec. VII. For both weak and strong collective decoherence we show how to fault-tolerantly encode into and read out of the respective DFSs. Finally, we analyze in Sec. VIII how to concatenate DFSs and QECCs to make them more robust against perturbing errors (as proposed in [25]) and show how the universality results can be applied to achieve fault-tolerant universal computation on these powerful concatenated codes. We conclude in Sec. IX. Derivations and proofs of a more technical nature are presented in the appendixes.

II. OVERVIEW OF DECOHERENCE-FREE SUBSPACES AND SUBSYSTEMS

A. Decoherence-free subspaces

Consider the dynamics of a system S (the quantum computer) coupled to a bath B via the Hamiltonian

$$\mathbf{H}=\mathbf{H}_S\otimes\mathbf{I}_B+\mathbf{I}_S\otimes\mathbf{H}_B+\mathbf{H}_I, \tag{1}$$

where $\mathbf{H}_S$ ($\mathbf{H}_B$) [the system (bath) Hamiltonian] acts on the system (bath) Hilbert space $\mathcal{H}_S$ ($\mathcal{H}_B$), $\mathbf{I}_S$ ($\mathbf{I}_B$) is the identity operator on the system (bath) Hilbert space, and $\mathbf{H}_I$, which acts on both the system and bath Hilbert spaces $\mathcal{H}_S\otimes\mathcal{H}_B$, is the interaction Hamiltonian containing all the nontrivial couplings between system and bath. In general $\mathbf{H}_I$ can be written as a sum of operators which act separately on the system ($\mathbf{S}_\alpha$'s) and on the bath ($\mathbf{B}_\alpha$'s):

$$\mathbf{H}_I=\sum_\alpha \mathbf{S}_\alpha\otimes\mathbf{B}_\alpha. \tag{2}$$

In the absence of an interaction Hamiltonian ($\mathbf{H}_I=0$), the evolution of the system and the bath are separately unitary: $\mathbf{U}(t)=\exp[-i\mathbf{H}t]=\exp[-i\mathbf{H}_St]\otimes\exp[-i\mathbf{H}_Bt]$ (we set $\hbar=1$ throughout). Information that has been encoded (mapped) into states of the system Hilbert space remains encoded in the system Hilbert space if $\mathbf{H}_I=0$. However, in the case when the interaction Hamiltonian contains nontrivial couplings between the system and the bath, information that has been encoded over the system Hilbert space does not remain encoded over solely the system Hilbert space but spreads out instead into the combined system and bath Hilbert space as the time evolution proceeds. Such leakage of quantum information from the system to the bath is the origin of the decoherence process in quantum mechanics.

Let $\tilde{\mathcal{H}}_S$ be a subspace of the system Hilbert space with a basis $|\tilde{\imath}\rangle$. The evolution of such a subspace will be unitary [19,25] if and only if (i)

$$\mathbf{S}_\alpha|\tilde{\imath}\rangle=c_\alpha|\tilde{\imath}\rangle,\quad c_\alpha\in\mathbb{C} \tag{3}$$

for all $|\tilde{\imath}\rangle\in\tilde{\mathcal{H}}_S$ and for all $\mathbf{S}_\alpha$, (ii) $\mathbf{H}_S$ does not mix states within the subspace with states that are outside of the subspace ($\langle j'|\mathbf{H}_S|\tilde{\imath}\rangle=0$ for all $|\tilde{\imath}\rangle$ in the subspace and all $|j'\rangle$ outside of the subspace: $\mathbf{H}_S=\tilde{\mathbf{H}}_S\oplus\mathbf{H}_S'$, where $\tilde{\mathbf{H}}_S$ acts only on the subspace and $\tilde{\mathbf{H}}_S'$ acts only outside of the subspace), and (iii) system and bath are initially decoupled $\rho(0)=\rho_S(0)\otimes\rho_B(0)$. We call a subspace of the system's Hilbert space which fulfills these requirements a decoherence-free subspace (DFS).

The above formulation of DFSs in terms of a larger closed system is exact. It is extremely useful for finding DFSs, providing often the most direct route via simple examination of the system components of the interaction Hamiltonian. In practical situations, however, the closed-system formulation of DFSs is often too strict. This is because the closed-system formulation incorporates the possibility that information which is put into the bath will back-react on the system and cause a recurrence. Such interactions will always occur in the closed-system formulation (due to the the Hamiltonian being Hermitian). However, in many practical situations the likelihood of such an event is extremely small. Thus, for example, an excited atom which is in a ''cold'' bath will radiate a photon and decohere but the bath will not in turn excite the atom back to its excited state, except via the (extremely long) recurrence time of the emission process. In these situations a more appropriate way to describe the evolution of the system is via a quantum dynamical semigroup master equation [52,53]. By assuming that (i) the evolution of system density matrix is a one-parameter semigroup, (ii) the system density matrix retains the properties of a density matrix including ''complete positivity,'' and (iii) the system and bath density matrices are initially decoupled, Lindblad [52] has shown that the most general evolution of the system density matrix $\rho_S(t)$ is governed by the master equation

$$\frac{d\rho_S(t)}{dt}=-i[\mathbf{H}_S,\rho_S(t)]+\mathsf{L}_D[\rho_S(t)],$$

$$\mathsf{L}_D[\rho_S(t)]=\frac{1}{2}\sum_{\alpha,\beta=1}^{M} a_{\alpha\beta}([\mathbf{F}_\alpha,\rho_S(t)\mathbf{F}_\beta^\dagger]+[\mathbf{F}_\alpha\rho_S(t),\mathbf{F}_\beta^\dagger]), \tag{4}$$

where $\mathbf{H}_S$ is the system Hamiltonian, the operators $\mathbf{F}_\alpha$ constitute a basis for the M-dimensional space of all bounded operators acting on $\mathcal{H}_S$, and $a_{\alpha\beta}$ are the elements of a positive semidefinite Hermitian matrix. As above, let $\tilde{\mathcal{H}}_S$ be a subspace of the system Hilbert space $\mathcal{H}_S$ with a basis $|\tilde{\imath}\rangle$. The evolution over such a subspace is then unitary [24] iff

$$\mathbf{F}_\alpha|\tilde{\imath}\rangle = c_\alpha|\tilde{\imath}\rangle, \quad c_\alpha \in \mathbb{C} \tag{5}$$

for all $|\tilde{\imath}\rangle$ and for all $\mathbf{F}_\alpha$. While this condition appears to be identical to Eq. (3), there is an important difference between the $\mathbf{S}_\alpha$'s and the $\mathbf{F}_\alpha$'s which makes these two decoherence-freeness conditions different. In the Hamiltonian formulation of DFSs, the Hamiltonian is Hermitian. Thus the expansion for the interaction Hamiltonian Eq. (2) can always be written such that the $\mathbf{S}_\alpha$ are also Hermitian. On the other hand, the $\mathbf{F}_\alpha$'s in the master equation, Eq. (4), need only be bounded operators acting on $\mathcal{H}_S$ and thus the $\mathbf{F}_\alpha$'s need not be Hermitian. Because of this difference, Eq. (5) allows for a broader range of subspaces than Eq. (3). For example, consider the situation where there are only two nonzero terms in a master equation for a two-level system, corresponding to $\mathbf{F}_1=\sigma_-$ and $\mathbf{F}_2=\sigma_z$ where $\sigma_-=|0\rangle\langle 1|$ and $\sigma_z=|0\rangle\langle 0| - |1\rangle\langle 1|$ (e.g., cooling with phase damping). In this case there is a DFS corresponding to the single state $|0\rangle$. In the Hamiltonian formulation, inclusion of $\mathbf{S}_1=\sigma_-$ in the interaction Hamiltonian expansion Eq. (2) would necessitate a second term in the Hamiltonian with $\mathbf{S}_2=\sigma_-^\dagger$, along with the $\mathbf{S}_z=\sigma_z$ as above. For this set of operators, however, Eq. (3) allows for no DFS.

B. Decoherence-free subsystems

If one desires to encode quantum information over a subspace and requires that this information remains decoherence-free, then Eqs. (3) and (5) provide necessary and sufficient conditions for the existence of such DFSs. The notion of a subspace which remains decoherence-free throughout the evolution of a system is not, however, the most general method for providing decoherence-free encoding of information in a quantum system. Recently, Knill, Laflamme, and Viola [48] have discovered a method for decoherence-free coding into subsystems instead of into subspaces.

Decoherence-free subsystems [48,36,54] are most easily presented in the Hamiltonian formulation of decoherence. Let $\mathcal{A}$ denote the associative algebra formed by the system Hamiltonian $\mathbf{H}_S$ and the system components of the interaction Hamiltonian, the $\mathbf{S}_\alpha$'s. To simplify our discussion we will assume that the system Hamiltonian vanishes. (It is easy to incorporate the system Hamiltonian into the $\mathbf{S}_\alpha$'s when one desires that the system evolution preserves the decoherence-free subsystem.) We also assume that the identity operator is included as $\mathbf{S}_0=\mathbf{I}_S$ and $\mathbf{B}_0=\mathbf{I}_B$. This will have no observable consequence but allows for the use of an important representation theorem. $\mathcal{A}$ consists of linear combinations of products of the $\mathbf{S}_\alpha$'s. Because the Hamiltonian is Hermitian the $\mathbf{S}_\alpha$'s must be closed under Hermitian conjugation: $\mathcal{A}$ is a †-closed operator algebra. A basic theorem of such operator algebras which include the identity operator states that, in general, $\mathcal{A}$ will be a reducible subalgebra of the full algebra of operators on $\mathcal{H}_S$ [55]. This means that the algebra is isomorphic to a direct sum of $d_J\times d_J$ complex matrix algebras, each with multiplicity n_J:

$$\mathcal{A} \cong \bigoplus_{J\in\mathcal{J}} \mathbf{I}_{n_J} \otimes \mathcal{M}(d_J,\mathbb{C}). \tag{6}$$

Here $\mathcal{J}$ is a finite set labeling the irreducible components of $\mathcal{A}$, and $\mathcal{M}(d_J,\mathbb{C})$ denotes a $d_J\times d_J$ complex matrix algebra. It is also useful at this point to introduce the commutant $\mathcal{A}'$ of $\mathcal{A}$. This is the set of operators which commutes with the algebra $\mathcal{A}$, $\mathcal{A}'=\{\mathbf{X}:[\mathbf{X},\mathbf{A}]=0,\forall\mathbf{A}\in\mathcal{A}\}$. They also form a †-closed algebra, which is reducible to

$$\mathcal{A}' = \bigoplus_{J\in\mathcal{J}} \mathcal{M}(n_J,\mathbb{C}) \otimes \mathbf{I}_{d_J} \tag{7}$$

over the same basis as $\mathcal{A}$ in Eq. (6).

The structure implied by Eq. (6) is illustrated schematically as follows, for some system operator $\mathbf{S}_\alpha$:

$$\mathbf{S}_\alpha = \begin{bmatrix} \boxed{J=1} & & & \\ & \boxed{J=2} & & \\ & & \ddots & \\ & & & \boxed{J=|\mathcal{J}|} \end{bmatrix} \tag{8}$$

In this block diagonal matrix representation, a typical block with given J may have a further block diagonal structure,

for a given J:

$$\begin{bmatrix} \boxed{M_\alpha} & & & \lambda=0 \\ & \boxed{M_\alpha} & & \lambda=1 \\ & & \boxed{M_\alpha} & \lambda=\mathrm{n_J} \end{bmatrix} \quad \begin{matrix} \mu \\ 0 \\ \vdots \\ d_J-1 \\ \mu' : 0 \ \cdots \ d_J-1 \end{matrix} \tag{9}$$

Here λ labels the different degenerate sub-blocks, $1\leqslant\lambda\leqslant n_J$ and μ labels the states inside each sub-block $1\leqslant\mu$

$\leqslant d_J$. Associated with this decomposition of the algebra $\mathcal{A}$ is the decomposition over the system Hilbert space:

$$\mathcal{H}_S = \sum_{J \in \mathcal{J}} \mathbb{C}^{n_J} \otimes \mathbb{C}^{d_J}. \tag{10}$$

Decoherence-free subsystems are defined as the situation in which information is encoded in a single subsystem space $\mathbb{C}^{n_J}$ of Eq. (10) (thus the dimension of the decoherence-free subsystem is n_J). The decomposition in Eq. (6) reveals that information encoded in such a subsystem will always be affected as identity on the subsystem space $\mathbb{C}^{n_J}$, and thus this information will not decohere. It should be noted that the tensor product nature which gives rise to the name subsystem in Eq. (6) is a tensor product over a direct sum, and therefore will not in general correspond to the natural tensor product of qubits. Further, it should be noted that the subsystem nature of the decoherence implies that the information should be encoded in a separable way. Over the tensor structure of Eq. (10) the density matrix should split into two valid density matrices: $\rho_S(0) = \rho \otimes \gamma$, where ρ is the decoherence-free subsystem and γ is the corresponding component of the density matrix which does decohere. Finally it should be pointed out that not all of the subsystems in the different irreducible representations can be simultaneously used: (phase) decoherence will occur between the different irreducible components of the Hilbert space labeled by $J \in \mathcal{J}$. For this reason, from now on we restrict our attention to the subspace defined by a given J.

Decoherence-free subspaces are now easily connected to decoherence-free subsystems. Decoherence-free subspaces correspond to decoherence-free subsystems possessing one-dimensional irreducible matrix algebras: $\mathcal{M}(1,\mathbb{C})$. The multiplicity of these one-dimensional irreducible algebras is the dimension of the decoherence-free subspaces. In fact it is easy to see how the decoherence-free subsystems arise out of a noncommuting generalization of the decoherence-free subspace conditions. Let $\{|\lambda_\mu\rangle\}$, $1 \leqslant \lambda \leqslant n_J$ and $1 \leqslant \mu \leqslant d_J$ denote a subspace of $\mathcal{H}_S$ with given J. Then the condition for the existence of an irreducible decomposition as in Eq. (6) is

$$\mathbf{S}_\alpha |\lambda_\mu\rangle = \sum_{\mu'=1}^{d_J} M_{\mu\mu',\alpha} |\lambda_{\mu'}\rangle, \tag{11}$$

for all $\mathbf{S}_\alpha$, λ, and μ. Notice that $M_{\mu\mu',\alpha}$ is not dependent on λ, in the same way that c_α in Eq. (3) is not the same for all $|\tilde{l}\rangle$ (there $\mu = 1$ and fixed). Thus for a fixed λ, the subspace spanned by $|\lambda_\mu\rangle$ is acted upon in some nontrivial way. However, because $M_{\mu\mu',\alpha}$ is not dependent on λ, each subspace defined by a fixed μ and running over λ is acted upon in an identical manner by the decoherence process.

At this point it should be noted that the generalization of the Lindblad master equation Eq. (4) with a decoherence-free subspace to the corresponding master equation for a decoherence-free system is not trivial. This is because, as above, the $\mathbf{F}_\alpha$ operators in Eq. (4) are (for all practical purposes) not required to be closed under conjugation. The representation theorem Eq. (6) is hence not directly applicable. We will show, however, that the master equation analog of Eq. (11)

$$\mathbf{F}_\alpha |\lambda_\mu\rangle = \sum_{\mu'=1}^{d_J} M_{\mu\mu',\alpha} |\lambda_{\mu'}\rangle \tag{12}$$

provides a necessary and sufficient condition for the preservation of decoherence-free subsystems.

As above, we consider a subspace of the system Hilbert space spanned by $|\lambda_\mu\rangle$, with $1 \leqslant \lambda \leqslant n_J$ and $1 \leqslant \mu \leqslant d_J$. Our notation will be significantly simpler if we explicitly write out the formal tensor product over this subspace: $|\lambda_\mu\rangle = |\lambda\rangle \otimes |\mu\rangle$. In the subsystem notation, we claim that the decoherence-free subsystem condition is

$$\mathbf{F}_\alpha |\lambda\rangle \otimes |\mu\rangle = |\lambda\rangle \otimes \mathbf{M}_\alpha |\mu\rangle. \tag{13}$$

A proper decomposition of the system Hilbert space requires, as noted above, that the system density matrix is a tensor product of two valid (Hermitian, positive) density matrices:

$$\rho_S(0) = \sum_{\lambda\lambda',\mu\mu'} \rho_{\lambda\lambda'}(0)\gamma_{\mu\mu'}(0) |\lambda_\mu\rangle\langle\lambda'_{\mu'}| = \rho(0) \otimes \gamma(0), \tag{14}$$

where $\rho(0)$ contains the information which will remain decoherence-free, and $\gamma(0)$ is an arbitrary but valid density matrix.

In general the operators $\mathbf{F}_\alpha$ will not be decomposable as a single tensor product corresponding to $\rho(0) \otimes \gamma(0)$. Rather, they will be a sum over such tensor products, corresponding to an expansion over an operator basis: $\mathbf{F}_\alpha = \Sigma_p \mathbf{N}_\alpha^p \otimes \mathbf{M}_\alpha^p$. The decohering generator of evolution (4) thus becomes

$$\begin{aligned} \mathsf{L}_D[\rho_S(0)] = \frac{1}{2} \sum_{\alpha\beta} a_{\alpha\beta} \sum_{pq} (&2\mathbf{N}_\alpha^p \rho(0) \mathbf{N}_\beta^{q\dagger} \otimes \mathbf{M}_\alpha^p \gamma(0) \mathbf{M}_\beta^{q\dagger} \\ &- \mathbf{N}_\beta^{q\dagger} \mathbf{N}_\alpha^p \rho(0) \otimes \mathbf{M}_\beta^{q\dagger} \mathbf{M}_\alpha^p \gamma(0) \\ &- \rho(0) \mathbf{N}_\beta^{q\dagger} \mathbf{N}_\alpha^p \otimes \gamma(0) \mathbf{M}_\beta^{q\dagger} \mathbf{M}_\alpha^p). \end{aligned} \tag{15}$$

Tracing over the γ component, and using the cyclic nature of the trace allows one to factor out a common $m_{\alpha\beta}^{pq} \equiv \mathrm{Tr}_\gamma(\mathbf{M}_\alpha^p \gamma(0) \mathbf{M}_\beta^{q\dagger})$, yielding:

$$\begin{aligned} \mathrm{Tr}_\gamma\{\mathsf{L}_D[\rho_S(0)\}] = \frac{1}{2} \sum_{\alpha\beta,pq} a_{\alpha\beta} m_{\alpha\beta}^{pq} (&2\mathbf{N}_\alpha^p \boldsymbol{\rho}(0) \mathbf{N}_\beta^{q\dagger} \\ &- \mathbf{N}_\beta^{q\dagger} \mathbf{N}_\alpha^p \boldsymbol{\rho}(0) - \boldsymbol{\rho}(0) \mathbf{N}_\beta^{q\dagger} \mathbf{N}_\alpha^p). \end{aligned}$$

The evolution of the ρ component of the density matrix thus satisfies the standard master equation (4), for which it is known that the evolution is decoherence-free [24] if and only if

$$\mathbf{N}_\alpha^q |\lambda\rangle = c_{\alpha,q} |\lambda\rangle \quad \forall \alpha. \tag{16}$$

This implies that the necessary and sufficient condition for a decoherence-free subsystem is

$$\mathbf{F}_\alpha = \sum_q c_{\alpha,q}\mathbf{I}\otimes\mathbf{M}_\alpha^q = \mathbf{I}\otimes\sum_q c_{\alpha,q}\mathbf{M}_\alpha^q = \mathbf{I}\otimes\mathbf{M}_\alpha, \quad (17)$$

which is the claimed generalization of the Hamiltonian condition of decoherence-free subsystems, Eq. (12).

We will use the acronym DFS to denote both decoherence-free subsystems and their restriction, decoherence-free subspaces, whenever no confusion can arise. When we refer to DF subspaces we will be specifically referring to the one-dimensional version of the DF subsystems.

III. THE STABILIZER FORMALISM AND ERROR-CORRECTION

In the theory of quantum error correcting codes (QECCs) it proved fruitful to study properties of a code by considering its stabilizer $\mathcal{S}$. This is the group formed by those system operators which leave the code words unchanged, i.e., they ''stabilize'' the code. Properties of stabilizer codes and the theory of quantum computation on these stabilizer codes have been developed in [51]. In the framework of QECCs, the stabilizer allows on the one hand to identify the errors the code can detect and correct. On the other hand it also permits one to find a set of universal, fault-tolerant gates by analyzing the centralizer of $\mathcal{S}$, defined as the set of operations that commute with all elements in $\mathcal{S}$ (equal to the normalizer, the set of operations that preserve $\mathcal{S}$ under conjugation, in the case of the Pauli group). In the context of QECCs, the stabilizer $\mathcal{S}$ is restricted to elements in the Pauli group, i.e., the group of tensor products of **I,X,Y,Z**, and is a finite Abelian group.

The extension of stabilizer theory yields much insight into DFSs. We do this here by defining a non-Abelian, and in certain cases infinite stabilizer group. The observation that DFSs are highly degenerate QECCs [25] will appear naturally from this formalism. Such a generalized stabilizer has already been defined in previous work dealing with decoherence-free subspaces [40], and its normalizer shown there to lead to identification of local gates for universal computation. A key consequence of this approach was the observation that the resulting gates do not take the system out of the DFS during the entire switching time of the gate.

We now review and extend the results in [40] to analyze the error detection and correction properties of DFSs and QECCs. We shall incorporate DFSs and QECCs into a unified framework, similarly to the representation-theoretic approach of [48,36]. The question of performing quantum computation on a specific DFS will be addressed in the next section.

A. The stabilizer-general theory

An operator $\mathbf{S}$ is said to stabilize a code $\mathcal{C}$ if

$$|\Psi\rangle\in\mathcal{C} \quad \text{iff} \quad \mathbf{S}|\Psi\rangle = |\Psi\rangle \quad \forall \mathbf{S}\in\mathcal{S}. \quad (18)$$

The set of operators $\{\mathbf{S}\}$ form a group $\mathcal{S}$, known as the stabilizer of the code [51]. Clearly, $\mathcal{S}$ is closed under multiplication. In the theory of QECC the stabilizers that have been studied are subgroups of the Pauli-group (tensor products of **I,X,Y,Z**). Since any two elements of the Pauli group either commute or anticommute, the stabilizer, in this case is always Abelian [26]. The code is thus the common eigenspace of the stabilizer elements with eigenvalue 1.

In general an error-process can be described by the Kraus operator-sum formalism [56,8]: $\rho\rightarrow\Sigma_\mu\mathbf{A}_\mu\rho\mathbf{A}_\mu^\dagger$. The Kraus-operators $\mathbf{A}_\mu$ can be expanded in a basis $\{\mathbf{E}_\alpha\}$ of ''errors.'' The standard fault-tolerant QECC model assumes that errors affect single qubits independently. QECC can also deal with higher-order correlations by using a code which is suitably constructed for the particular error model assumed. Therefore the theory of QECCs has focused on searching for codes that make quantum information robust against 1,2, . . . , or more erroneous qubits, as this is the most reasonable model when one assumes spatially separated qubits with their own local environments. Detection and correction procedures must then be implemented at a rate higher than the intrinsic error rate. In the QECC error-model, the independent errors are spanned by single-qubit elements $(\mathbf{I},\mathbf{X},\mathbf{Y},\mathbf{Z})$. An analysis of the error-correction properties can then be restricted to correction of combinations of these basic errors (which are also members of the Pauli group) acting on a certain number of qubits simultaneously.

The distance d of a QECC is the number of single-qubit errors that have to occur in order to transform one code word in $\mathcal{C}$ to another code word in $\mathcal{C}$. An error E is detectable if it takes a code word to a subspace of the Hilbert space that is orthogonal to the space spanned by $\mathcal{C}$ (this can be observed by a nonperturbing orthogonal von Neuman measurement). A distance d code can detect up to $d-1$ errors. In order to be able to correct an error on a certain code word the error (up to a degenerate action of different errors) also needs to be identified, so that it can be undone. Hence errors on different code words have to take the code words to different orthogonal subspaces. The above translates to the QECC-condition [8]:

A QECC $\mathcal{C}$ can correct errors $\mathcal{E}=\{\mathbf{E}_\alpha\}$ if and only if

$$\langle\Psi_j|\mathbf{E}_\beta^\dagger\mathbf{E}_\alpha|\Psi_i\rangle = c_{\alpha\beta}\delta_{ij} \quad \forall\mathbf{E}_\alpha,\mathbf{E}_\beta\in\mathcal{E}. \quad (19)$$

The stabilizer of a QECC offers a systematic analysis of the errors which the code can detect and correct [9]. Two types of errors can be dealt with by stabilizer codes: (i) errors $\mathbf{E}_\alpha^\dagger\mathbf{E}_\beta\neq\mathbf{I}$ that anticommute with an $\mathbf{S}\in\mathcal{S}$, and (ii) errors that are part of the stabilizer $(\mathbf{E}_\alpha\in\mathcal{S})$. It is straightforward to see that both (i) and (ii) imply the QECC condition Eq. (19). For case (i), if $\mathbf{E}_i^\dagger\mathbf{E}_j\mathbf{S} = -\mathbf{S}\mathbf{E}_i^\dagger\mathbf{E}_j$, then $\langle\Psi_j|\mathbf{E}_\beta^\dagger\mathbf{E}_\alpha|\Psi_i\rangle = \langle\Psi_j|\mathbf{E}_\beta^\dagger\mathbf{E}_\alpha\mathbf{S}|\Psi_i\rangle = -\langle\Psi_j|\mathbf{S}\mathbf{E}_\beta^\dagger\mathbf{E}_\alpha|\Psi_i\rangle = -\langle\Psi_j|\mathbf{E}_\beta^\dagger\mathbf{E}_\alpha|\Psi_i\rangle$. Hence $\langle\Psi_j|\mathbf{E}_\beta^\dagger\mathbf{E}_\alpha|\Psi_i\rangle = 0$ and $c_{\alpha\beta}=\delta_{\alpha\beta}$. Errors of type (ii), $\mathbf{E}_\alpha\in\mathcal{S}$, leave the code words unchanged and therefore trivially lead to Eq. (19). The first class, (i), are errors that require active correction. The second class, (ii), are ''degenerate'' errors that do not affect the code at all. QECCs can be regarded as (passive) DFSs for the errors in their stabilizer [26]. Conversely, being passive, highly degenerate codes [25,57], DFSs can be viewed as a class of stabilizer codes that provide passive protection type (ii) errors [i.e., where the $\mathbf{A}_\mu$ are linear combinations of elements generated (under

multiplication) by the stabilizer], and can detect and be used to correct the (usually small) set of errors that anticommute with the DFS stabilizer. The stabilizer thus provides a unified tool to identify the errors that a given code can deal with, as a DFS and as a QECC. An analysis of the properties of DFSs with a stabilizer in the Pauli group has been carried out in [26].

B. DFS-stabilizer

Most of the DFSs stemming from physical error-models will not have a stabilizer in the Pauli group, i.e., they are nonadditive codes. The stabilizer may even be infinite. In particular, the codes obtained from a noise model where errors arise from a symmetric coupling of the system to the bath and that form the focus of this paper, are of this type.

As discussed in the previous section, a DFS is completely specified by the condition:

$$\mathbf{S}_\alpha|\mu\rangle\otimes|\lambda\rangle=|\mu\rangle\otimes\mathbf{M}_\alpha|\lambda\rangle, \tag{20}$$

arising from the splitting of the algebra generated by the $\mathbf{S}_\alpha$'s: $\mathcal{A}=\oplus_{J\in\mathcal{J}}\mathbf{I}_{n_J}\otimes\mathcal{M}(d_J,\mathbb{C})$. This splitting of the algebra has allowed both DFSs and QECCs to be put into a similar framework [48,36]. We will now show that the DFS condition on the algebra $\mathcal{A}$ generated by the $\mathbf{S}_\alpha$ can be converted into a stabilizer condition on the complex Lie algebra generated by the $\mathbf{S}_\alpha$'s. We define the continuous DFS-stabilizer $\mathbf{D}(\vec{v})$ as

$$\mathbf{D}(v_1,v_2,\ldots,v_N)=\exp\left[\sum_\alpha v_\alpha(\mathbf{S}_\alpha-\mathbf{I}\otimes\mathbf{M}_\alpha)\right],\quad v_\alpha\in\mathbb{C}. \tag{21}$$

Clearly, if the DFS condition Eq. (20) is fulfilled for a set of states $|\mu\rangle\otimes|\lambda\rangle$, then

$$\mathbf{D}(\vec{v})|\mu\rangle\otimes|\lambda\rangle=|\mu\rangle\otimes|\lambda\rangle\quad\forall v_\alpha\in\vec{v}. \tag{22}$$

Thus the DFS condition implies that the $\mathbf{D}(\vec{v})$ stabilize the DFS. Further if Eq. (22) holds then in particular it must hold for a $\vec{v}$ which has only one nonvanishing component v_β. Thus Eq. (22) implies that $\mathbf{D}(0,\ldots,0,v_\beta,0,\ldots,0)|\mu\rangle\otimes|\lambda\rangle=|\mu\rangle\otimes|\lambda\rangle$. Recalling that $\exp[\cdot]$ is a one-to-one mapping from a neighborhood of the zero matrix to a neighborhood of the identity matrix, it follows that there must exist a small enough v_α such that Eq. (22) implies the DFS condition Eq. (20). Thus we see that we can convert the DFS condition into a condition on the stabilizer of the complex Lie algebra generated by the $\mathbf{S}_\alpha-\mathbf{I}\otimes\mathbf{M}_\alpha$'s:

$$|\Psi\rangle\in\text{DFS}\quad\text{iff}\quad\mathbf{D}(\vec{v})|\Psi\rangle=|\Psi\rangle\quad\forall\vec{v}\in\mathbb{C}^N. \tag{23}$$

In some cases we will be able to pick a finite subgroup from elements of $\mathbf{D}(\vec{v})$ which constitutes a stabilizer. We will mention these instances in the following sections. However, apart from the conceptual framework, our main motivation to introduce the stabilizer for a DFS is to be able to analyze the errors which a DFS (i) detects/corrects (as a QECC), and (ii) those which it avoids (passive error correction). The continuous stabilizer provided in Eq. (21) will be sufficient to study these errors.

As mentioned in the previous subsection, errors $\mathbf{E}_\alpha$ (i) that anticommute with an element in the stabilizer will take code words to subspaces that are orthogonal to the code. These errors will be detectable (and correctable if $\mathbf{E}_\beta^\dagger\mathbf{E}_\alpha$ anticommutes with a stabilizer element) [9]. In order to identify the QECC properties of a DFS, it will be convenient to look for elements of the Pauli group among the $\mathbf{D}(\vec{v})$.

A code $\mathcal{C}$ with stabilizer $\mathbf{D}(\vec{v})$ will avoid errors of type (ii) in its stabilizer in the sense that, if all of the Kraus operators of a given decoherence process can be expanded over stabilizer elements $\mathbf{A}_i(t)=\int_{\mathbb{C}^N}e_i(\vec{v},t)\mathbf{D}(\vec{v})d\vec{v}$, then

$$\rho(t)=\sum_i\mathbf{A}_i(t)\rho(0)\mathbf{A}_i^\dagger(t)=\sum_i\left|\int_{\mathbb{C}^N}e_i(\vec{v},t)d\vec{v}\right|^2\rho(0). \tag{24}$$

The normalization condition $\Sigma_i\mathbf{A}_i(t)^\dagger\mathbf{A}_i(t)=\mathbf{I}$ then implies that $\Sigma_i|\int_{\mathbb{C}^N}e_i(\vec{v},t)d\vec{v}|^2=1$. Consequently, as expected, the DFS does not evolve. Hence we see that the stabilizer provides an efficient method for identifying the errors which a code avoids. In later sections we analyze the concrete form of the stabilizer Eq. (21) for the error models studied in this paper.

IV. THE COMMUTANT AND UNIVERSAL QUANTUM COMPUTATION ON A DFS

A DFS is a promising way to store quantum information in a robust fashion [27]. From the perspective of quantum computation, however, it is even more important to be able to controllably transform states in a DFS, if it is to be truly useful for quantum information processing. More specifically, to perform quantum algorithms on a DFS one has to be able to perform universal quantum computation using decoherence-free states. The notion of universal computation is the following: with a restricted set of operations or interactions at hand, one wishes to implement any unitary transformation on the given Hilbert space, to an arbitrary degree of accuracy. From a physical implementation perspective it seems clear that the operations used (gates) should be limited to at most two-body interactions. In particular we wish to identify a finite set of such gates that is universal on a DFS.

Since we do not wish to implement active QECC, we impose a very stringent requirement on the operations we allow for computation using DFSs: we do not allow gates that ever take the decoherence free states outside the DFS, where the states would decohere under the noise-process considered.[2] As a first step towards this goal we thus need to be able to identify the physical operations which perform transformations entirely within the DFS.

[2]We shall lift this requirement in Sec. VIII.

A. Operations that preserve the DFS

There are essentially two equivalent approaches to identify the ''encoded'' operations that preserve a DFS. One is via the normalizer of the stabilizer of a code [40]; the second is via the commutant of the †-closed algebra generated by the error operators [48]. Both will be briefly reviewed here.

1. Computation on a stabilizer DFS

The stabilizer formalism is very useful for identifying allowed gates that take code words to code words [51]. An operation $\mathbf{U}$ keeps code words $|\Psi\rangle$ inside the code space, if and only if the transformed state $\mathbf{U}|\Psi\rangle$ is an element of the code $\mathcal{C}$. Thus using the stabilizer condition (18) for codes with stabilizer $\mathcal{S}$ and $\mathcal{C}=\{|\Psi\rangle:\mathbf{S}|\Psi\rangle=|\Psi\rangle\ \forall\mathbf{S}\in\mathcal{S}\}$, we have

$$\mathbf{U}|\Psi\rangle\in\mathcal{C} \quad \text{iff} \quad \mathbf{SU}|\Psi\rangle=\mathbf{U}|\Psi\rangle \quad \forall\mathbf{S}\in\mathcal{S}. \tag{25}$$

This implies $\mathbf{U}^{-1}\mathbf{SU}|\Psi\rangle=|\Psi\rangle$ and so $\mathbf{U}^{-1}\mathbf{SU}\in\mathcal{S}$: Allowed operations $\mathbf{U}$ transform stabilizer elements $\mathbf{S}$ by conjugation into stabilizer elements; $\mathbf{U}$ is in the normalizer of $\mathcal{S}$ (if $\mathcal{S}$ is a group). If we restrict the allowed operations to gates in the Pauli group (as is done in [51]), then the allowed gates $\mathbf{U}$ will fix the stabilizer pointwise (element by element). In the case of DFS with a continuous stabilizer $\mathbf{D}(\vec{v})$, the above translates to the following condition [40]

$$\mathbf{UD}(\vec{v})\mathbf{U}^{\dagger}=\mathbf{D}(\vec{v}'(\vec{v})), \tag{26}$$

together with the requirement that $\mathbf{D}(\vec{v}'(\vec{v}))$ must cover $\mathcal{S}$. To satisfy the covering condition, it is sufficient to have $\vec{v}'(\vec{v})$ be a one-to-one mapping.

Equation (26), derived by generalizing concepts from the theory of stabilizers in the Pauli group, is a condition that allows one to identify gates $\mathbf{U}$ that transform code words to code words. In a physical implementation these gates will be realized by turning on Hamiltonians $\mathbf{H}$ between physical qubits for a certain time t: $\mathbf{U}(t)=e^{-it\mathbf{H}}$. So far we only required that the action of the gate preserve the subspace at the conclusion of the gate operation, but not that the subspace be preserved throughout the entire duration of the gate operation. The stabilizer approach allows us to further identify the more restrictive set of Hamiltonians that keep the states within the DFS throughout the entire switching time of the gate. As a result, in the limit of ideal gates, the entire system is free from noise at all times. This is different from QECC, since there errors continuously take the code words outside of the code space [58], and hence error correction needs to be applied frequently even in the limit of perfect gate operations. Imperfections in gate operations can be dealt with in the DFS approach by concatenation with a QECC [25], as shown explicitly for the exchange interaction in [28].

By rewriting condition (26) as $\mathbf{U}(t)\mathbf{D}(\vec{v})=\mathbf{D}(\vec{v}'(\vec{v},t))\mathbf{U}(t)$, taking the derivative with respect to t and evaluating at $t=0$ we obtain $\mathbf{HD}(\vec{v})=\mathbf{D}(\vec{v}'(\vec{v},0))\mathbf{H}+i(\partial\mathbf{D}/\partial\vec{v}')(d\vec{v}'/dt)|_{t=0}$, so that:

Theorem 1: A sufficient condition for the generating Hamiltonian to keep a state at all times entirely within the DFS is $\mathbf{HD}(\vec{v})=\mathbf{D}(\vec{v}'(\vec{v}))\mathbf{H}$ where $\vec{v}'(\vec{v})$ is one-to-one and time independent.

For most applications we will only need gates that commute with all stabilizer elements. The condition for the generating Hamiltonian then simplifies to $\mathbf{HD}(\vec{v})=\mathbf{D}(\vec{v})\mathbf{H}$.

2. Computation on irreducible subspaces

We can derive conditions to identify allowed gates on a DFS by using the representation theoretic approach developed in [48], [36], and Sec. II. Recall that the decomposition of the algebra $\mathcal{A}\cong\oplus_{J\in\mathcal{J}}\mathbf{I}_{n_J}\otimes\mathcal{M}(d_J,\mathbb{C})$ generated by the errors $\{\mathbf{S}_\alpha\}$ induces a splitting of the Hilbert space $\mathcal{H}_S=\sum_{J\in\mathcal{J}}\mathbb{C}^{n_J}\otimes\mathbb{C}^{d_J}$ into subspaces possessing a tensor product structure suitable to isolate decoherence-free subsystems. The set of operators in the commutant of $\mathcal{A}$, $\mathcal{A}'=\{\mathbf{X}:[\mathbf{X},\mathbf{A}]=0,\forall\mathbf{A}\in\mathcal{A}\}=\mathcal{A}'=\oplus_{J\in\mathcal{J}}\mathcal{M}(n_J,\mathbb{C})\otimes\mathbf{I}_{d_J}$, obviously generate transformations that affect the code space only. In particular, they take states in a DFS to other states in that same DFS. $\mathcal{A}'$ is generated by operators which commute with the $\mathbf{S}_\alpha$. Again, our goal is to find gates that act within a DFS during the entire switching time, and to this end we need to identify Hermitian operators $\mathbf{H}$ in $\mathcal{A}'$ to generate an evolution $\mathbf{U}(t)=\exp[-it\mathbf{H}]$ on the DFS.

Theorem 2: A sufficient condition for a Hamiltonian $\mathbf{H}$ to generate dynamics $\mathbf{U}(t)=\exp[-it\mathbf{H}]$ which preserves a DFS is that $\mathbf{H}$ be in the commutant of the algebra $\mathcal{A}$.

However, because we can only use one particular DFS (corresponding to a specific $K\in\mathcal{J}$) to store quantum information (the coherences between superpositions of different DFSs are not protected), the operators which commute with the $\mathbf{S}_\alpha$'s are not the only operators which perform nontrivial operations on a specific DFS. The operations in $\mathcal{A}'$ preserve all DFSs in parallel. However, if we restrict our system to only one such DFS, we do not need any constraints on the evolution of the other subspaces. It is then possible to construct a necessary and sufficient condition for a Hamiltonian by modifying the commutant to:

$$\mathcal{T}\cong(\mathcal{M}(n_K,\mathbb{C})\otimes\mathbf{I}_{d_K})\oplus\mathcal{M}(d-d_Kn_K,\mathbb{C}), \tag{27}$$

where $d_K=\dim(\mathcal{H}_S)$ and just leaves the specific DFS (K) invariant.

Theorem 3: A necessary and sufficient condition for a Hamiltonian $\mathbf{H}$ to generate dynamics which preserves a DFS corresponding to the irreducible representation $K\in\mathcal{J}$, is $\mathbf{H}\in\mathcal{T}$.

We will use both the stabilizer and the commutant approaches to find a set of universal gates for decoherence processes of physical relevance. In the cases discussed in this paper, any one of the two approaches is clearly sufficient and we do not need all theorems in full generality. However, we provide here a general framework and the tools required to analyze DFS and QECC stemming from any error model.

Finally we should point out again that from a practical perspective, it is crucial to look for the Hermitian operations which perform nontrivial operations on the DFS and which

correspond to only one- or two-body physical interactions. Without this requirement, it is clear that one can always [37] construct a set of Hamiltonians (satisfying the conditions of Theorem 2) which span the allowed operations on a DFS. A primary goal of this paper is therefore to construct such one- and two-body Hamiltonians for specific decoherence mechanisms, in order to achieve true universal computation on the corresponding DFSs.

B. Universality and composition of allowed operations

Using the tools developed in the previous section, we can now find local one-and-two qubit gates that represent encoded operations on DFSs. However, in general, a discrete set of gates applied in alternation is not sufficient to generate a universal set of gates. Nor is it sufficient to obtain every encoded unitary operation exactly. Furthermore, for analysis of the complexity of computations performed with a given universal set of gates, it is essential to keep under control the number of operations needed to achieve a certain gate within a desired accuracy. In the theory of universality (e.g., [12]) the composition laws of operations have been analyzed extensively. We will review the essential results relevant for our purposes here.

Let us assume that we have a set of (up to two-body) Hamiltonians $\mathsf{H}=\{\mathbf{H}_i : i=1,\ldots,M\}$ that take DFS states to DFS states. We will construct gates using the following composition laws:

(1) Arbitrary phases: Any interaction can be switched on for an arbitrary time. Thus any gate of the form $\mathbf{U}(t)=\exp(-it\mathbf{H}_i)$ can be implemented.

(2) Trotter formula: Gates performing sums of Hamiltonians are implemented by using the short-time approximation to the Trotter formula $\exp[i(t_1\mathbf{H}_i+t_2\mathbf{H}_j)]=\lim_{n\to\infty}[\exp(i(t_1/n)\mathbf{H}_i)\exp(i(t_2/n)\mathbf{H}_j)]^n$:

$$e^{i(t_1\mathbf{H}_i+t_2\mathbf{H}_j)/n}=e^{it_1\mathbf{H}_i/n}e^{it_2\mathbf{H}_j/n}+O\left(\frac{1}{n^2}\right). \tag{28}$$

This is achieved by quickly turning on and off the two interactions $\mathbf{H}_i,\mathbf{H}_j$ with appropriate ratios of duration times. An alternative, direct, way of implementing this gate is to switch on the two interactions simultaneously for the appropriate time intervals.

(3) Commutator: It is possible to implement the commutator of operations that are already achievable. This is a consequence of the Lie product formula

$$\exp[\mathbf{H}_i,\mathbf{H}_j]=\lim_{n\to\infty}[\exp(i\mathbf{H}_i/\sqrt{n})\exp(i\mathbf{H}_j/\sqrt{n})\times\exp(-i\mathbf{H}_i/\sqrt{n})\exp(-i\mathbf{H}_j/\sqrt{n})]^n,$$

which has the short-time approximation

$$e^{t[\mathbf{H}_i,\mathbf{H}_j]/n}=e^{it\mathbf{H}_i/\sqrt{n}}e^{it\mathbf{H}_j/\sqrt{n}}e^{-it\mathbf{H}_i/\sqrt{n}}e^{-it\mathbf{H}_j/\sqrt{n}}+O\left(\frac{1}{n\sqrt{n}}\right). \tag{29}$$

Again, the gate $e^{it(-i[\mathbf{H}_i,\mathbf{H}_j])}$ can be implemented to high precision by alternately switching on and off the appropriate two interactions with a specific duration ratio.[3]

(4) Conjugation by unitary evolution: Another useful action in constructing universal sets of gates comes from the observation that if a specific gate $\mathbf{U}$ and its inverse $\mathbf{U}^\dagger$ can be implemented, then any Hamiltonian $\mathbf{H}$ which can be implemented can be modified by performing $\mathbf{U}$ before and $\mathbf{U}^\dagger$ after the gate $\exp(-it\mathbf{H})$. This gives rise to the transformed Hamiltonian

$$\mathbf{U}\exp(-it\mathbf{H})\mathbf{U}^\dagger=\exp(-it\mathbf{U}\mathbf{H}\mathbf{U}^\dagger)=\exp(-it\mathbf{H}_{\rm eff}). \tag{30}$$

Note that the laws (1)–(3) correspond to closing the set of allowed Hamiltonians as a Lie algebra (scalar multiplication, addition, and Lie commutators can be obtained out of the given Hamiltonians).

If (a subset of) the composition laws (1)–(4) acting on the set H give rise to a set of gates that is dense in the group $\mathrm{SU}(d_K)$ (via successive application of these gates), where d_K is the dimension of the DFS, then we shall refer to H as a universal set of generators. Equivalently, this means that H generates the Lie algebra $\mathrm{su}(d_K)$ (traceless matrices) via scalar multiplication, addition, Lie commutators, and conjugation by unitaries. The generators of this algebra can be obtained from H by these operations.

For all practical applications and implementations of algorithms, we will only be interested in approximating a certain gate sequence with a given accuracy. Note that the composition laws (2) and (3) use only repeated applications of (1) in order to approximate a certain gate. We can replace the requirement to perform an arbitrary phase, (1), by noting that $e^{i\mathbf{H}_i}$ is generically dense in the Abelian group $\{\exp(it\mathbf{H}_i)\}$. Repeated application of that gate can then approximate an arbitrary phase to any desired accuracy. Thus we can in principle restrict our available gates to $\{\exp(i\mathbf{H}_i)\}$. Repeated application of these gates can then be used to approximate any operation in $\mathrm{SU}(d_K)$ to arbitrary accuracy.

In order to prove that a set H generates a universal set of Hamiltonians, we use the fact that a large group of universal sets have already been identified [43,44,59]. It suffices to show that H generates one of these sets, in order to prove that H is a universal set of generators. We will use the fact that the set of one qubit operations SU(2) is generated by any two arbitrary rotations with irrational phase, around two nonparallel axes. Alternatively, if we are given these two rotations with any phase, then an Euler-angle construction can be used to yield any gate in SU(2) by application of a small number of rotations (three if the axes are orthogonal). In addition we will use (and prove) a lemma (enlarging lemma, Appendix C) that allows extension to $\mathrm{su}(n+1)$ of a given

[3]Note that in order to implement $e^{-it\mathbf{A}}$ we would use $e^{i\vartheta\mathbf{A}}=I$ and implement $e^{i(\vartheta-t)\mathbf{A}}$ instead. This depends on $\mathbf{A}$ having rationally related eigenvalues, which will always be the case for the Hamiltonians of interest to us.

su(n) acting on an n-dimensional subspace of a Hilbert space of dimension $n+1$, with the help of an additional su(2).

In order to use this approach to universality, it is crucial to have bounds on the length of the gate sequences approximating a certain gate in terms of the desired accuracy. This is all the more important if one universal set is to be replaced by any other with only polynomial overhead in the number of gates applied, for otherwise the complexity classes would not be robust under the exchange of one set for another. The whole notion of universality would then by questionable. The following key theorem proved independently by Solovay and Kitaev (see [12]) establishes the equivalence of universal sets, and provides bounds on the length of gate sequences for a desired accuracy of approximation. In order to quantify the accuracy of an approximation, we need to define a distance on matrices. Since our matrices act in a space of given (finite) dimension d_K, any metric is as good as any other. For example, we can use the trace-norm $d(\mathbf{U},\mathbf{V})=\sqrt{1-(1/d_K)\mathrm{Re}[\mathrm{Tr}(\mathbf{U}^\dagger\mathbf{V})]}$. A matrix $\mathbf{V}$ is then said to approximate a transformation $\mathbf{U}$ to accuracy ϵ if $d(\mathbf{U},\mathbf{V})\leqslant\epsilon$.

Theorem (Solovay-Kitaev): Given a set of gates that is dense in SU(2^k) and closed under Hermitian conjugation, any gate $\mathbf{U}$ in SU(2^k) can be approximated to an accuracy ϵ with a sequence of poly$[\log(1/\epsilon)]$ gates from the set.

DFS-Corollary to the Solovay-Kitaev Theorem: Assume that the DFS encodes a d_K-dimensional system into n physical qubits. Given that one can exactly implement the gate set $\{e^{i\tilde{t}_i\mathbf{H}_i}:\mathbf{H}_i\in\mathsf{H}\}$, [$\tilde{t}_i$ are (fixed) irrational multiples of π, and H is a universal generating set] it is possible to approximate any gate in SU(d_K) (any encoded operation) using $m=\mathrm{poly}[\log(1/\epsilon)]$ gates.

Furthermore, if we can only implement the given gates approximately, say to an accuracy δ, we will still be able to approximate the target gate: It is known that a sequence of m δ-imprecise unitary matrices is (in some norm) at most distance $m\delta$ from the desired gate. If a sequence of exactly implemented gates $\mathbf{U}_1,\ldots,\mathbf{U}_m$ approximates a target gate $\mathbf{U}$ up to ϵ, and instead of $\mathbf{U}_1,\ldots,\mathbf{U}_m$, we use gates that are at most some distance δ apart, then the total sequence will be at most $\epsilon+m\delta=\epsilon+\mathrm{poly}[\log(1/\epsilon)]\delta$ apart from $\mathbf{U}$. If we make sure that $\delta<\epsilon\mathrm{poly}[\log(1/\epsilon)]$ then the δ-faulty sequence will still approximate $\mathbf{U}$ to a precision 2ϵ.

If we further assume that the physical interaction that we switch on and off is given by the device and is unlikely to change its form, then the imprecision of the gate comes entirely through the coupling strength and the interaction time, i.e., a faulty gate is of the form $\mathbf{U}_f=e^{i(\phi+\Delta\phi)\mathbf{H}}$, where $\mathbf{U}=e^{i\phi\mathbf{H}}$ is the unperturbed gate. The distance

$$\begin{aligned} d(\mathbf{U},\mathbf{U}_f)&=\sqrt{1-\frac{1}{d_K}\mathrm{Re}[\mathrm{Tr}(e^{i\Delta\phi\mathbf{H}})]}\\ &=\sqrt{1-\frac{1}{d_K}\mathrm{Re}[\mathrm{Tr}(\cos\Delta\phi 1+i\sin\Delta\phi\mathbf{H})]}\\ &=\sqrt{1-\cos\Delta\phi}=\sqrt{2}\sin(\Delta\phi/2)\approx\frac{\Delta\phi}{\sqrt{2}}\equiv\delta \end{aligned} \quad (31)$$

is proportional to the error $\Delta\phi$ of the product of coupling strength and interaction time. This translates to (nearly) linear behavior in the desired final accuracy ϵ.

V. COLLECTIVE DECOHERENCE

We now focus on a particularly interesting and useful model of a DFS. This is the case of collective decoherence on n qubits. We distinguish between two forms of collective decoherence. The first, and simpler, type of collective decoherence is weak collective decoherence (WCD). We define the collective operators as

$$\mathbf{S}_\alpha\equiv\sum_{j=1}^{n}\sigma_\alpha^j, \quad (32)$$

where σ_α^j denotes a tensor product of the α^{th} Pauli matrix, $\alpha=x,y,z$,

$$\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad \sigma_y=\begin{pmatrix}0&-i\\i&0\end{pmatrix},\quad \sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix} \quad (33)$$

(in the basis spanned by σ_z eigenstates $|0\rangle$ and $|1\rangle$) operating on the jth qubit, and the identity on all of the other qubits, i.e., $\sigma_\alpha^j=I\otimes I\otimes\cdots\otimes\sigma_\alpha\otimes\cdots\otimes I$. WCD is the situation in which only one collective operator $\mathbf{S}_\alpha$ is involved in the coupling to the bath, i.e., $\mathbf{H}_I=\mathbf{S}_\alpha\otimes\mathbf{B}$.

The second, more general type of collective decoherence is strong collective decoherence (SCD). We define SCD as the general situation in which the interaction Hamiltonian is given by $\mathbf{H}_I=\Sigma_{\alpha=1}^3\mathbf{S}_\alpha\otimes\mathbf{B}_\alpha$. The $\mathbf{S}_\alpha$ provide a representation of the Lie algebra su(2):

$$[\mathbf{S}_\alpha,\mathbf{S}_\beta]=-2i\epsilon_{\alpha\beta\gamma}\mathbf{S}_\gamma. \quad (34)$$

The $\mathbf{B}_\alpha$'s are not required to be linearly independent.

Both of these collective decoherence mechanisms are expected to arise from the physical condition that the bath cannot distinguish the system qubits [16,17,21,24]. If there are n qubits interacting with a bath, the most general interaction Hamiltonian linear in the σ_α^i is given by

$$\mathbf{H}_I=\sum_{i=1}^{n}\sum_{\alpha=x,y,z}\sigma_\alpha^i\otimes\mathbf{B}_{i,\alpha}, \quad (35)$$

where the $\mathbf{B}_{i,\alpha}$ are bath operators. If the bath cannot distinguish between the system qubits, then $\mathbf{B}_{i,\alpha}$ should not depend on i and the Hamiltonian becomes $\mathbf{H}_I=\Sigma_{\alpha=x,y,z}\mathbf{S}_\alpha\otimes\mathbf{B}_\alpha$, i.e., strong collective decoherence.

As a concrete example of such collective decoherence, consider the situation in which the bath is the electromagnetic field, and the wavelength of the transition between the states of the qubits is larger than the spacing between the qubits. The electromagnetic field will interact with each of these qubits in an identical manner, because the field strength over a single wavelength will not vary substantially. This gives rise to the well-known phenomena of Dicke super- and sub-radiance [60]. Whenever the bath is a field whose energy

is dependent on its wavelength and this wavelength is much greater than the spacing between the qubits, one should expect collective decoherence to be the dominant decoherence mechanism. It is natural to expect this to be the case for condensed-phase high-purity materials at low temperatures. However, to the best of our knowledge at present a rigorous study quantifying the relevant parameter ranges for this interesting condition to hold in specific materials is still lacking (see Refs. [30,31] for an application to quantum dots, though).

VI. THE ABELIAN CASE: WEAK COLLECTIVE DECOHERENCE

For a decoherence mechanism with only one operator $\mathbf{S}_\alpha$ coupling to the bath, the implementation and discussion of universal computation with local interactions is simpler than in the general case, because we can work in the basis that diagonalizes $\mathbf{S}_\alpha$ ($\mathbf{S}_\alpha$ is necessarily Hermitian in the Hamiltonian model we consider here). The algebra generated by $\mathbf{S}_\alpha$ is Abelian and reduces to one-dimensional (irreducible) subalgebras corresponding to the eigenvalues of $\mathbf{S}_\alpha$. More specifically, $\mathcal{A}_1 = \oplus_{\lambda_K} \mathbf{I}_{n_K} \otimes \mathcal{M}(\lambda_K)$, where λ_K is the Kth eigenvalue with degeneracy n_K, and $\mathcal{M}(\lambda_K)$ is the algebra generated by λ_K. $\mathcal{M}(\lambda_K)$ acts by multiplying the corresponding vector by λ_K. In this situation the DF subsystems are only of the DF subspace type. This simpler case of weak collective decoherence allows us to present a treatment with examples that will make the general case of strong collective decoherence (SCD) more intuitive.

In the following we will, without loss of generality, focus on the case $\mathbf{S}_\alpha \equiv \mathbf{S}_z = \Sigma_{k=1}^n \sigma_z^k$.[4] This operator is already diagonal in the computational basis (the eigenstates are bitstrings of qubits in either $|0\rangle$ or $|1\rangle$). Since σ_z^k acting on the kth qubit contributes 1 if the qubit is $|0\rangle$, and -1 if the qubit is $|1\rangle$, the eigenvalue of a bitstring is (number of 0's $-$ number of 1's), and the eigenvalues of $\mathbf{S}_z$ are $\{n, n-2, \ldots, -n+2, -n\}$.

The degeneracy n_K of the eigenspace corresponding to an eigenvalue

$$\lambda_K = n - 2K \tag{36}$$

is

$$n_K = \binom{n}{K} \tag{37}$$

(the number of different bitstrings with $n-K$ 0's and K 1's). The Abelian algebra generated by $\mathbf{S}_z$ thus splits into one-dimensional subalgebras with degeneracy n_K. The largest decoherence-free subspaces in this situation correspond to the space spanned by bitstring vectors where the number of 0's and the number of 1's are either the same (n even), or differ by one (n odd).

[4]The cases $\alpha = x$ (y) follow by applying a bitwise Hadamard (Hadamard+phase) transform to the code.

A. The stabilizer and error correction properties

Following the formalism developed in Sec. III we find, using Eq. (21) with $v = i\theta$ (θ can be complex), the stabilizer for the weak case corresponding to a DFS with eigenvalue λ_K to be

$$\begin{aligned} \mathbf{Z}_K^{\otimes n}(\theta) &= \exp[i\theta(\mathbf{S}_z - \lambda_K \mathbf{I})] \\ &= \bigotimes_{k=1}^{n} e^{-i\lambda_K\theta}(\mathbf{I}\cos\theta + \sigma_z^k i \sin\theta) \\ &= e^{-i\lambda_K\theta}\mathbf{P}(\theta)^{\otimes n}, \end{aligned} \tag{38}$$

where

$$\mathbf{P}(\theta) = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}. \tag{39}$$

For strictly real θ some of the errors which are protected against are simply collective rotations about the σ_z axis (and an irrelevant global phase). For strictly imaginary θ we find that the errors which are protected against are contracting collective errors of the form $\mathrm{diag}(e^{\theta}, e^{-\theta})$, i.e., they result in loss of norm of the wave function. Any physical process with Kraus operators that are linear combinations of these errors will therefore not affect the DFS.

This is the right framework in which to present another form of the stabilizer. We note that in the case of weak collective decoherence, we can find a stabilizer group with a finite number of elements. Define

$$Z_{1/n} = \exp\left(\frac{2\pi i}{n}\sigma_z\right) = \begin{pmatrix} \exp\left(\frac{2\pi i}{n}\right) & 0 \\ 0 & \exp\left(-\frac{2\pi i}{n}\right) \end{pmatrix}. \tag{40}$$

Then the n-element group $\mathcal{Z}_n$ generated by $\exp(-i2\pi\lambda_K/n) Z_{1/n}^{\otimes n}$ is a stabilizer for the DFS corresponding to the eigenvalue λ_K. To see that

$$\exp\left(-\frac{2\pi i \lambda_K}{n}\right) Z_{1/n}^{\otimes n}|\Psi\rangle = |\Psi\rangle \quad \text{iff} \quad |\Psi\rangle \in \mathrm{DFS}(\lambda_K), \tag{41}$$

note that a $Z_{1/n}$ acting on a $|0\rangle$ contributes $\exp(2\pi i/n)$ to the total phase, whereas $Z_{1/n}$ acting on a $|1\rangle$ contributes $\exp(-2\pi i/n)$. So $Z_{1/n}^{\otimes n}$ gives a total phase of $\exp(2\pi i(\text{number of 0's} - \text{number of 1's})/n) = \exp(2\pi i \lambda_K/n)$ when acting on a bitstring. This stabilizer and Eq. (41) provide a simple criterion to check whether a state is in a DFS or not.

Let us now briefly comment on the error-correction and detection properties of the code in the WCD case. The stabilizer elements are all diagonal, and equal to a tensor product of identical 1-qubit operators. The element $\mathbf{Z}^{\otimes n}$ is in the stabilizer and anticommutes with odd-number $\mathbf{X}$ and $\mathbf{Y}$ errors. So odd-number qubit bit-flips are detectable errors. However, the code is not able to detect any form of error

involving **Z**'s and even-number **X**'s and **Y**'s, since any such error commutes with all elements in the stabilizer.

B. Nontrivial operations

Observe that the algebra $\mathcal{A}$ in the WCD case is generated entirely by $\mathbf{S}_z$. Hence by Theorem 2, the DFS-preserving operations are those that are in the commutant of $\mathbf{S}_z$. For single-body Hamiltonians it is easy to see that the only nontrivial such set is formed by interactions proportional to σ_z^i operators. As for two-qubit Hamiltonians, it is simpler to use Theorem 1 and the expression (38) for the stabilizer. We are then looking for 4×4 Hermitian matrices that commute with $\mathbf{P}(\theta)^{\otimes 2}$; these are of the form

$$\mathbf{T}_{ij}(z_1,z_2,z_3,z_4,h)=\begin{pmatrix} z_1 & 0 & 0 & 0 \\ 0 & z_2 & h & 0 \\ 0 & h^* & z_3 & 0 \\ 0 & 0 & 0 & z_4 \end{pmatrix}, \qquad (42)$$

where $\mathbf{T}_{ij}$ acts on qubits i and j only. Here z_i is real, h is complex, and the row space is spanned by the ith and jth qubit basis $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$. We note that systems with an internal Hamiltonian of the Heisenberg type,

$$\mathbf{H}_{\mathrm{Heis}}=\sum_{j=1}^{n}\epsilon_j\sigma_z^j+\frac{1}{2}\sum_{i,j=1}^{n}K_{ij}\vec{\sigma}_i\cdot\vec{\sigma}_j, \qquad (43)$$

have exactly the correct form for any pair of spins i,j. Indeed, it is not hard to see that $[\mathbf{H}_{\mathrm{Heis}},\mathbf{S}_z]=0$ [28]. The Heisenberg Hamiltonian is ubiquitous, and appears, e.g., in NMR. This means that the natural evolution of NMR systems under WCD (which is not necesarily the correct decoherence model for NMR systems), preserves the DFS, and implements a nontrivial computation.

The specific case

$$\mathbf{E}_{ij}\equiv\mathbf{T}_{ij}(1,0,0,1,1)=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad (44)$$

which flips the two states $|01\rangle$ and $|10\rangle$ of qubits i and j and leaves the other two states invariant, is especially important: it is the exchange interaction. The other interactions we employ are

$$\mathbf{T}_{ij}^{P}\equiv\mathbf{T}_{ij}(1,0,0,0,0)=\mathrm{diag}(1,0,0,0),$$

$$\mathbf{T}_{ij}^{Q}\equiv\mathbf{T}_{ij}(0,0,0,1,0)=\mathrm{diag}(0,0,0,1), \qquad (45)$$

which introduce a phase on the state $|00\rangle$ (P) and $|11\rangle$ (Q) of qubits i and j; and

$$\overline{\mathbf{Z}}_{12}\equiv\mathbf{T}_{12}(0,0,1,0,0)=\mathrm{diag}(0,0,1,0). \qquad (46)$$

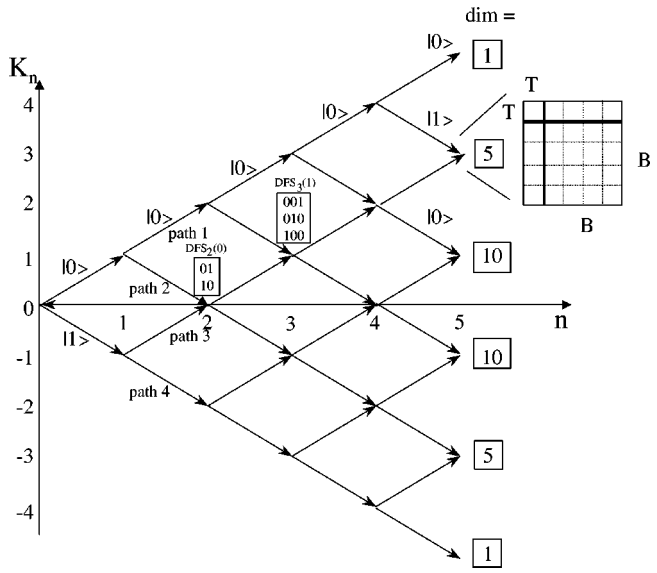


FIG. 1. Graphical representation of DFS states for weak collective decoherence (WCD). The horizontal axis marks the number of qubits. The vertical axis shows (number of 0's − number of 1's) in each state (K_n). Each state in the standard basis thus corresponds to a path from the origin which follows the indicated arrows. The dimension of a DFS corresponds to the multiple pathways through which one can arrive at the same J_n. The DFSs are labeled by their values of n and K_n, as $\mathrm{DFS}_n(K_n)$. The insert shows the matrix structure of operators acting on $\mathrm{DFS}_5(3)$, in terms of Top (T) and Bottom (B) states (see text for definition of these). Note that there is only one T-state entering $\mathrm{DFS}_5(3)$, whence the action of exchange is represented by a 1×1 block.

In the following we show that these special interactions are sufficient to obtain a universal generating set operating entirely within a weak-collective DFS.

C. Universal quantum computation inside the weak-Collective DFS

Let $\mathrm{DFS}_n(K)$ denote the decoherence-free subsystem on n physical qubits with eigenvalue K. We show here that

$$\mathsf{H}=\{\mathbf{E}_{i,i+1},\mathbf{T}_{i,i+1}^{P},\mathbf{T}_{i,i+1}^{Q}:i=1,\ldots,n-1,\overline{\mathbf{Z}}_{12}\} \qquad (47)$$

is a universal generating set for any of the DFSs occurring in a system of n physical qubits. It is convenient to work directly with the Hamiltonians, and to show that H gives rise to the Lie algebra $\mathrm{su}(d_K)$ on each $\mathrm{DFS}_n(K)$ [via scalar multiplication, addition, and Lie commutator; see the allowed compositions of operations (1)–(3) in Sec. IV B]. Exponentiation then gives the group $\mathrm{SU}(d_K)$ on the DFS. We will proceed by induction on n, the number of physical qubits, building the DFS states of n qubits out of DFS states for $n-1$ qubits. A graphical representation of this construction is useful (and will also generalize to the strong case presented in Sec. VII): see Fig. 1.

We have seen that in the WCD case the DFS states are simply bitstrings of n qubits in either $|0\rangle$ or $|1\rangle$. The different n-qubit DFSs are labeled by their eigenvalue

$$\lambda_K = (\text{number of } 0\text{'s} - \text{number of } 1\text{'s}) \equiv K_n . \quad (48)$$

To obtain a DFS state of n qubits out of a DFS state of $n-1$ qubits corresponding to K_{n-1} we can either add the nth qubit as $|0\rangle$ ($K_n = K_{n-1}+1$) or as $|1\rangle$ ($K_n = K_{n-1}-1$). Each DFS state can be built sequentially from the first qubit onward by adding successively $|0\rangle$ or $|1\rangle$, and is uniquely defined by a sequence $K_1, \ldots, K_n$ of eigenvalues. In the graphical representation of Fig. 1 the horizontal axis marks n, the number of qubits up to which the state is already built, and the vertical axis shows K_n, the difference (number of 0's − number of 1's) up to the nth qubit. Adding a $|0\rangle$ at the $n+1$th step will correspond to a line pointing upwards, adding a $|1\rangle$ to a line pointing down. Each DFS state of n qubits having eigenvalue $\lambda_K = K_n$, is thus in one-to-one correspondence with a path on the lattice from the origin to (n, K_n).

Consider the first nontrivial case, $n=2$, which gives rise to one DFS qubit: $\mathrm{DFS}_2(0)$. This corresponds to the two states $|0_L\rangle = |01\rangle$ [path 2 in Fig. 1] and $|1_L\rangle = |10\rangle$ (path 3) with $K_2 = 0$. The remaining Hilbert space is spanned by the one-dimensional $\mathrm{DFS}_2(2)$ $|00\rangle$ (path 1) corresponding to $K_2 = 2$, and $\mathrm{DFS}_2(-2)$ $|11\rangle$ (path 4) corresponding to $K_2 = -2$. The exchange $\mathbf{E}_{12}$ flips $|0_L\rangle$ and $|1_L\rangle$ (paths 2 and 3), and leaves the other two paths unchanged. The interaction $\mathbf{A}_{12} = \mathrm{diag}(0,0,1,0)$ induces a phase on $|1_L\rangle = |10\rangle$ (path 3). Their commutator forms an encoded σ_y acting entirely within the $\mathrm{DFS}_2(0)$ subspace. Its commutator with $\mathbf{E}_{12}$ in turn forms an encoded σ_z with the same property. Together they form the (encoded) Lie algebra su(2) acting entirely within this DFS. The Lie algebra is completed by forming the commutator between these $\overline{\mathbf{Y}}$ and $\overline{\mathbf{Z}}$ operations. To summarize:

$$\overline{\mathbf{Y}}_{12} = i[\overline{\mathbf{A}}, \mathbf{E}_{12}] = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & -i & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad (49)$$

$$\overline{\mathbf{Z}}_{12} \equiv i[\mathbf{E}_{12}, \overline{\mathbf{Y}}_{12}],$$

$$\overline{\mathbf{X}}_{12} \equiv i[\overline{\mathbf{Y}}_{12}, \overline{\mathbf{Z}}_{12}]. \quad (50)$$

We call the property of acting entirely within the specified DFS independence, meaning that the corresponding Hamiltonian has zero entries in the rows and columns corresponding to the other DFSs [$\mathrm{DFS}_2(2) = |00\rangle$ and $\mathrm{DFS}_2(-2) = |11\rangle$ in this case]. When the Hamiltonian is exponentiated, the corresponding gate will act as identity on all DFSs except $\mathrm{DFS}_2(0)$.

To summarize these considerations, the Lie algebra formed by $\mathsf{H}_0^2 = \{\overline{\mathbf{X}}, \overline{\mathbf{Z}}\}$ is su(2), and generates SU(2) on $\mathrm{DFS}_2(0)$ by exponentiation. In addition, this is an independent SU(2), namely, these operations act as identity on the other DFSs: when written as matrices over the basis of DFS states, their generators in H_0^2 have zeroes in the rows and columns corresponding to all other DFSs.

In the following we show how this construction generalizes to $n>2$ qubits, by proving the following theorem:

Theorem 4: For any $n \geqslant 2$ qubits undergoing weak collective decoherence, there exist sets of Hamiltonians $\mathsf{H}_{K_n}^n$ [obtained from H of Eq. (47) via scalar multiplication, addition, and Lie commutator] acting as su(d_{K_n}) on the DFS corresponding to the eigenvalue K_n. Furthermore each set acts independently on this DFS only (i.e., with zeroes in the matrix representation corresponding to their action on the other DFSs).

Before proving this theorem, we first explain in detail the steps taken in order to go from the $n=2$ to the $n=3$ case, so as to make the general induction procedure more transparent.

The structure of the DFSs for $n=2$ and 3 qubits is

$$\mathrm{DFS}_2(2) = \{|00\rangle\}, \quad \mathrm{DFS}_2(0) = \begin{cases} |01\rangle \\ |10\rangle \end{cases},$$

$$\mathrm{DFS}_2(-2) = \{|11\rangle\},$$

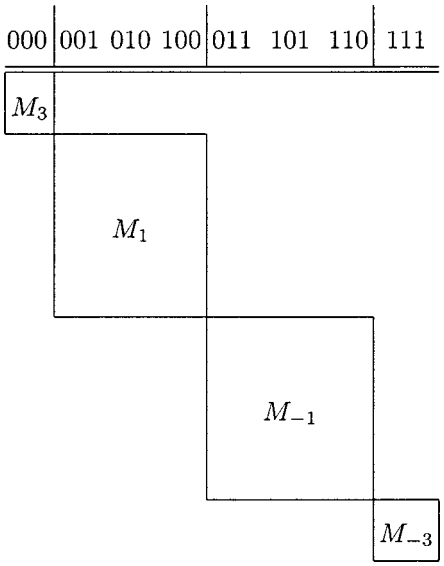
$$\mathrm{DFS}_3(3) = \{|000\rangle\}, \quad \mathrm{DFS}_3(1) = \begin{cases} |001\rangle \\ |010\rangle, \\ |100\rangle \end{cases}$$

$$\mathrm{DFS}_3(-1) = \begin{cases} |011\rangle \\ |101\rangle, \\ |110\rangle \end{cases} \quad \mathrm{DFS}_3(-3) = \{|111\rangle\}. \quad (51)$$

$\mathrm{DFS}_3(3)$ is obtained by appending a $|0\rangle$ to $\mathrm{DFS}_2(2)$. Similarly $\mathrm{DFS}_3(-3)$ is obtained by appending a $|1\rangle$ to $\mathrm{DFS}_2(-2)$. Graphically, this corresponds to moving along the only allowed pathway from $\mathrm{DFS}_2(2)$ [$\mathrm{DFS}_2(-2)$] to $\mathrm{DFS}_3(3)$ [$\mathrm{DFS}_3(-3)$], as shown in Fig. 1. The lowest and highest λ_K for n qubits will always be made up of the single pathway connecting the lowest and highest λ_K for $n-1$ qubits. The structure of $\mathrm{DFS}_3(\pm 1)$ is only slightly more complicated. $\mathrm{DFS}_3(1)$ is made up of one state, $|001\rangle$, which comes from appending a $|1\rangle$ (moving down) to $\mathrm{DFS}_2(2)$. We call $|001\rangle$ a ''Top-state'' in $\mathrm{DFS}_3(1)$. The two other states, $|010\rangle$ and $|100\rangle$, come from appending $|0\rangle$ (moving up) to $\mathrm{DFS}_2(0)$. Similarly, we call $|010\rangle$ and $|100\rangle$ ''Bottom-states'' in $\mathrm{DFS}_3(1)$. $\mathrm{DFS}_3(-1)$ is constructed in an analogous manner (Fig. 1).

We showed above that it is possible to perform independent su(2) operations on $\mathrm{DFS}_2(0)$. $\mathrm{DFS}_2(\pm 2)$ are also both acted upon independently, but because they are one-dimensional subspaces, independence implies that su(2) operations annihilate them. Since the states $\{|010\rangle, |100\rangle\} \in \mathrm{DFS}_3(1)$ and the states $\{|011\rangle, |101\rangle\} \in \mathrm{DFS}_3(-1)$ both have $\{|01\rangle, |10\rangle\} \in \mathrm{DFS}_2(0)$ as their first two qubits, one immediate consequence of the independent action on $\mathrm{DFS}_2(0)$ is that one can simultaneously perform su(2) operations on the corresponding daughter subspaces created by expanding $\mathrm{DFS}_2(0)$ into $\mathrm{DFS}_3(\pm 1)$. The first step in the general inductive proof is to eliminate this simultaneous action and to act independently on each of these subspaces (the ''independence step''). To see how this is achieved, it is convenient to

represent the operators acting on the eight-dimensional Hilbert space of 3 qubits in the basis of the 4 DFSs:



The simultaneous action on $\mathrm{DFS}_3(\pm 1)$ can now be visualized in terms of both $M_{\pm 1}$ being nonzero. Let us show how to obtain an action where, say, just M_1 is nonzero. This can be achieved by applying the commutator of two operators with the property that their intersection has nonvanishing action just on M_1. This is true for the $\mathbf{T}_{23}^P$ and $\overline{\mathbf{X}}_{12}$ Hamiltonians: $\mathbf{T}_{23}^P$ annihilates every state except those that are $|00\rangle$ over qubits 2 and 3, namely $|100\rangle \in \mathrm{DFS}_3(1)$ and $|000\rangle \in \mathrm{DFS}_3(3)$. This implies that the only nonzero blocks in its matrix are

$$M_3(\mathbf{T}_{23}^P)=1, \quad M_1(\mathbf{T}_{23}^P)=\begin{pmatrix} 0 & 0 & \\ 0 & 0 & \\ & & 1 \end{pmatrix}. \tag{52}$$

On the other hand, $\overline{\mathbf{X}}_{12}$ is nonzero only on those states that are $|01\rangle$ or $|10\rangle$ on qubits 1 and 2. Therefore it will be nonzero on all 3-qubit states that have $|01\rangle$ or $|10\rangle$ as ''parents.'' This means that in its matrix representation $M_{\pm 3}=0$ and

$$M_1(\overline{\mathbf{X}}_{12})=\begin{pmatrix} 0 & & \\ & 0 & 1 \\ & 1 & 0 \end{pmatrix}, \quad M_{-1}(\overline{\mathbf{X}}_{12})=\begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 0 \end{pmatrix}. \tag{53}$$

Clearly, taking the product of $\mathbf{T}_{23}^P$ and $\overline{\mathbf{X}}_{12}$ leaves nonzero just the lower 2×2 block of M_1, and this is the crucial point: it shows that an independent action on $\mathrm{DFS}_3(1)$ can be obtained by forming their commutator. Specifically, since the lower 2×2 block of $M_1(\mathbf{T}_{23}^P)$ is just $\frac{1}{2}(\mathbf{I}-\sigma_z)$:

$$i[\mathbf{T}_{23}^P, \overline{\mathbf{X}}_{12}]=\overline{\mathbf{Y}}_{\{|100\rangle,|010\rangle\}}, \tag{54}$$

i.e., this commutator acts as an encoded σ_y inside the $\{|100\rangle,|010\rangle\}$ subspace of $\mathrm{DFS}_3(1)$. Similarly, $\overline{\mathbf{Z}}_{\{|100\rangle,|010\rangle\}}=(i/2)[\overline{\mathbf{Y}}_{\{|100\rangle,|010\rangle\}}, \overline{\mathbf{X}}_{12}]$. Together $\{\overline{\mathbf{Y}}_{\{|100\rangle,|010\rangle\}}, \overline{\mathbf{Z}}_{\{|100\rangle,|010\rangle\}}$ generate su(2) acting independently on the $\{|100\rangle,|010\rangle\}$ subspace of $\mathrm{DFS}_3(1)$, which we achieved by subtracting out the action on $\mathrm{DFS}_3(-1)$.

In an analogous manner, an independent su(2) can be produced on the $\{|011\rangle,|101\rangle\}$ subspace of $\mathrm{DFS}_3(-1)$ by using the Hamiltonians acting on $\mathrm{DFS}_2(0)$ in conjunction with $\mathbf{T}_{23}^Q$ to subtract out the su(2) action on $\mathrm{DFS}_3(1)$.[5] Thus we can obtain independent action for each of the daughters of $\mathrm{DFS}_2(0)$, i.e., separate actions on the subspace spanned by $\{|010\rangle,|100\rangle\}$ and $\{|011\rangle,|101\rangle\}$.

Having established independent action on the two subspaces of $\mathrm{DFS}_3(1)$ and $\mathrm{DFS}_3(-1)$ arising from $\mathrm{DFS}_2(0)$, we need only show that we can obtain the full action on $\mathrm{DFS}_3(1)$ and $\mathrm{DFS}_3(-1)$. For $\mathrm{DFS}_3(1)$ we need to mix the subspace $\{|010\rangle,|100\rangle\}$ over which we can already perform independent su(2), with the $|001\rangle$ state. To do so, note that the effect of the exchange operation $\mathbf{E}_{23}$ is to flip $|001\rangle$ and $|010\rangle$, and leave $|100\rangle$ invariant. Thus the matrix representation of $\mathbf{E}_{23}$ is

$$M_1(\mathbf{E}_{23})=\begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix}. \tag{55}$$

Unfortunately, $\mathbf{E}_{23}$ has a simultaneous action on $\mathrm{DFS}_3(-1)$. This, however, is not a problem, since we have already constructed an independent su(2) on $\mathrm{DFS}_3(1)$ elements. Thus we can eliminate the simultaneous action by simply forming commutators with these su(2) elements. The Lie algebra generated by these commutators will act independently on all of $\mathrm{DFS}_3(1)$. In fact we claim this Lie algebra to be all of su(3) (see Appendix B for a general proof). In other words, the Lie algebra spanned by the su(2) elements $\{\sigma_x,\sigma_y,\sigma_z\}$ acting on the subspace $\{|100\rangle,|010\rangle\}$, together with the exchange operation $\mathbf{E}_{23}$, generate all of su(3) independently on DFS(1). A similar argument holds for $\mathrm{DFS}_3(-1)$. This construction illustrates the induction step: we have shown that it is possible to perform independent su(d_K) actions on all four of the $\mathrm{DFS}_3(K)$ ($K=\pm 3,\pm 1$), given that we can perform independent action on the three $\mathrm{DFS}_2(K)$ ($K=\pm 1,0$). In Fig. 2 we have further illustrated these considerations by depicting the action of exchange on two of the 4-qubit DFSs. Let us now proceed to the general proof.

Proof: By induction.

[5]Since $\mathbf{T}_{23}^Q$ annihilates every state except those that are $|11\rangle$ over qubits 2 and 3, namely $|011\rangle \in \mathrm{DFS}_3(-1)$ and $|111\rangle \in \mathrm{DFS}_3(-3)$, the only nonzero blocks in its matrix are

$$M_{-3}(\mathbf{T}_{23}^Q)=1, \quad M_{-1}(\mathbf{T}_{23}^Q)=\begin{pmatrix} 1 & & \\ & 0 & 0 \\ & 0 & 0 \end{pmatrix}.$$

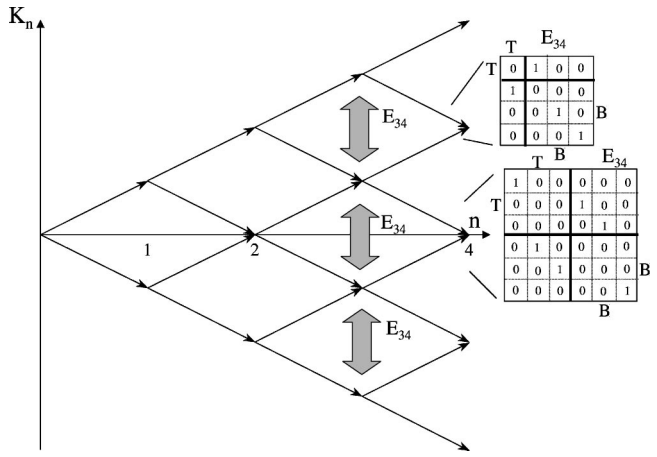


FIG. 2. Graphical representation of the action of exchange on DFS states for weak collective decoherence. Exchange acts to simultaneously flip different paths to a given $\mathrm{DFS}_n(K_n)$. Axes and labels are as defined in Fig. 1. E_{ij} denotes the exchange of the ith and jth qubits. The matrices displayed at right are the representations of $\mathbf{E}_{34}$ on $\mathrm{DFS}_4(0)$ (lower) and $\mathrm{DFS}_4(2)$ (upper).

The case $n=2$ already treated above will serve to initialize the induction. Assume now that the theorem is true for $n-1$ qubits and let us show that it is then true for n qubits as well.

First note that each $\mathrm{DFS}_n(K)$ is constructed either from the $\mathrm{DFS}_{n-1}(K-1)$ (to its lower left) by adding a $|0\rangle$ for the nth qubit, or from $\mathrm{DFS}_{n-1}(K+1)$ (to its upper left) by adding a $|1\rangle$: the states in $\mathrm{DFS}_n(K)$ correspond to all paths ending in (n,K) that either come from below (B) or from the top (T). See Fig. 3.

If we apply a certain gate $\mathbf{U}=\exp(i\mathbf{H}t)$ to $\mathrm{DFS}_{n-1}(K+1)$, then this operation will induce the same $\mathbf{U}$ on $\mathrm{DFS}_n(K)$, by acting on all paths (states) entering $\mathrm{DFS}_n(K)$ from above. At the same time $\mathbf{U}$ is induced on $\mathrm{DFS}_n(K+2)$ by acting on all paths entering this DFS from below.

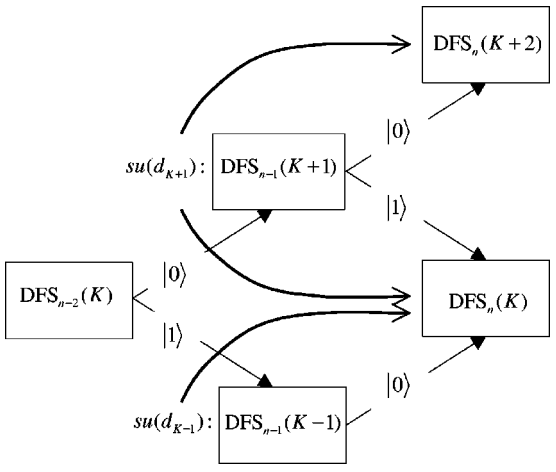


FIG. 3. Detailed structure of the pathways connecting adjacent DFSs in the weak collective decoherence case, with the action of the different su Lie algebras indicated by the superposed heavy arrows. $\mathrm{DFS}_n(K)$ denotes the DFS arising from n qubits and having eigenvalue K (see text).

So, $\mathbf{U}$ affects two DFSs simultaneously. In other words, the set of valid Hamiltonians H_{K+1}^{n-1} [acting on $n-1$ qubits and generating $\mathrm{su}(d_{K+1})$] on $\mathrm{DFS}_{n-1}(K+1)$, that we are given by the induction hypothesis, induces a simultaneous action of $\mathrm{su}(d_{K+1})$ on $\mathrm{DFS}_n(K)$ (on the paths coming from above only) and $\mathrm{DFS}_n(K+2)$ (on the paths coming from below only). Additionally, it does not affect any other n-qubit DFS, since we assumed that the action on $\mathrm{DFS}_{n-1}(K+1)$ was independent, and the only n-qubit DFSs built from $\mathrm{DFS}_{n-1}(K+1)$ are $\mathrm{DFS}_n(K)$ and $\mathrm{DFS}_n(K+2)$. These considerations are depicted schematically in Fig. 3.

We now show how to annihilate, for a given nontrivial (i.e., dimension >1) $\mathrm{DFS}_n(K)$, the unwanted simultaneous action on other DFSs (the ''independence step''). Then we proceed to obtain the full $\mathrm{su}(d_K)$, by using the $\mathrm{su}(d_{K\pm1})$ on $\mathrm{DFS}_{n-1}(K\pm1)$ that are given by the induction hypothesis (the ''mixing step'').

1. Independence

Let us call all the t_K paths converging on $\mathrm{DFS}_n(K)$ from above ''Top-states,'' or T-states for short, and the b_K paths converging from below ''Bottom- (or B) states'' (recall that there is a one-to-one correspondence between paths and states). The total number of paths converging on a given DFS is exactly its dimension, so $d_K=t_K+b_K$. By using the induction hypothesis on $\mathrm{DFS}_{n-1}(K+1)$ we can obtain $\mathrm{su}(t_K)$ (generated by H_{K+1}^{n-1}) on the T-states of $\mathrm{DFS}_n(K)$, which will simultaneously affect the B-states in the higher lying $\mathrm{DFS}_n(K+2)$ as $\mathrm{su}(b_{K+2})$ (note that $t_K=b_{K+2}$). The set H_{K+1}^{n-1} is nonempty only if $n-3\geqslant K+1\geqslant-(n-3)$ [because the ''highest'' and ''lowest'' DFS are always one-dimensional and $\mathrm{su}(1)=0$]. If this holds then $\mathrm{DFS}_n(K+2)$ ''above'' $\mathrm{DFS}_n(K)$ is nontrivial (dimension >1), and there are paths in $\mathrm{DFS}_n(K)$ ending in $|11\rangle$ (''down, down''). This is exactly the situation in which we can use $\mathbf{T}_{n-1,n}^{Q}$ to wipe out the unwanted action on $\mathrm{DFS}_n(K+2)$: recall that $\mathbf{T}_{n-1,n}^{Q}$ annihilates all states except those ending in $|11\rangle$, and therefore affects nontrivially only these special T-states in each DFS. Since the operations in H_{K+1}^{n-1} affect only B-states on $\mathrm{DFS}_n(K+2)$, $\mathbf{T}_{n-1,n}^{Q}$ commutes with H_{K+1}^{n-1} on $\mathrm{DFS}_n(K+2)$. Therefore the commutator of $\mathbf{T}_{n-1,n}^{Q}$ with elements in H_{K+1}^{n-1} annihilates all states not in $\mathrm{DFS}_n(K)$.[6] To show that commuting $\mathbf{T}_{n-1,n}^{Q}$ with H_{K+1}^{n-1} generates $\mathrm{su}(t_K)$ on the T-states of $\mathrm{DFS}_n(K)$ we need the following lemma, which shows how to form $\mathrm{su}(d)$ from an overlapping $\mathrm{su}(d-1)$ and $\mathrm{su}(2)$:

Enlarging Lemma: Let $\mathcal{H}$ be a Hilbert space of dimension d and let $|i\rangle\in\mathcal{H}$. Assume we are given a set of Hamiltonians H_1 that generates $\mathrm{su}(d-1)$ on the subspace of $\mathcal{H}$ that does not contain $|i\rangle$ and another set H_2 that generates $\mathrm{su}(2)$ on the subspace of $\mathcal{H}$ spanned by $\{|i\rangle,|j\rangle\}$, where $|j\rangle$ is another

[6]The argument thus far closely parallels the discussion above showing how to generate an independent su(2) on the $\{|011\rangle,|101\rangle\}$ subspace of $\mathrm{DFS}_3(-1)$, starting from the su(2) on $\mathrm{DFS}_2(0)$ and $\mathbf{T}_{23}^{Q}$.

state in $\mathcal{H}$. Then $[\mathsf{H}_1,\mathsf{H}_2]$ (all commutators) generates su(d) on $\mathcal{H}$ under closure as a Lie algebra (i.e., via scalar multiplication, addition, and Lie commutator).

Proof: See Appendix C.

Now consider two states $|i\rangle,|j\rangle \in \mathrm{DFS}_n(K)$ such that $|i\rangle$ ends in $|11\rangle$ and $|j\rangle$ is a T-state, but does not end in $|11\rangle$. Then we can generate su(2) on the subspace spanned by $\{|i\rangle,|j\rangle\}$ as follows: (i) We use the exchange interaction $\overline{\mathbf{X}}_{ij}=|i'\rangle\langle j'|+|j'\rangle\langle i'|$ [a prime indicates the bitstring with the last bit (a 1 in this case) dropped] in su$(t_K)\in \mathsf{H}_{K+1}^{n-1}$ to generate a simultaneous action on $\mathrm{DFS}_n(K)$ and $\mathrm{DFS}_n(K+2)$. This interaction is represented by a 2×2 σ_x matrix in the subspace spanned by $\{|i\rangle,|j\rangle\}$. (ii) $\mathbf{T}_{n-1,n}^{Q}$ is represented by the 2×2 matrix diag$(1,0)=\frac{1}{2}(\mathbf{I}+\sigma_z)$ in the same subspace, and commutes with $\overline{\mathbf{X}}_{ij}$ on $\mathrm{DFS}_n(K+2)$ [since $\overline{\mathbf{X}}_{ij}$ affects only B-states in $\mathrm{DFS}_n(K+2)$, and $\mathbf{T}_{n-1,n}^{Q}$ is nonzero only on states ending in $|11\rangle$]. Thus we can use it to create an independent action on $\mathrm{DFS}_n(K)$ alone: $\overline{\mathbf{Y}}_{ij}=i[\mathbf{T}_{n-1,n}^{Q},\overline{\mathbf{X}}_{ij}]$, $\overline{\mathbf{Z}}_{ij}=i/2[\overline{\mathbf{Y}}_{ij},\overline{\mathbf{X}}_{ij}]$.

Together $\{\overline{\mathbf{Y}}_{ij},\overline{\mathbf{Z}}_{ij}\}$ generate su(2) independently on $\{|i\rangle,|j\rangle\}\in \mathrm{DFS}_n(K)$. Since these operators vanish everywhere except on $\mathrm{DFS}_n(K)$, their commutators with elements in H_{K+1}^{n-1} [acting as su(t_K)] will annihilate all other DFSs. Therefore using the enlarging lemma, in this way all operations in su(t_K) acting on $\mathrm{DFS}_n(K)$ only can be generated.

So far we have shown how to obtain an independent su(t_K) on the T-states of $\mathrm{DFS}_n(K)$ using H_{K+1}^{n-1} (for $K\leqslant n-4$). To obtain an independent su(b_K) on the *B-states* of $\mathrm{DFS}_n(K)$ we use Hamiltonians in H_{K-1}^{n-1} [acting on $\mathrm{DFS}_{n-1}(K-1)$ – the DFS from below]. This will generate a simultaneous su(b_K) in $\mathrm{DFS}_n(K)$ and su(t_{K-2}) in $\mathrm{DFS}_n(K-2)$. To eliminate the unwanted action on $\mathrm{DFS}_n(K-2)$ we apply the previous arguments almost identically, except that now we use $\mathbf{T}_{n-1,n}^{P}$ to wipe out the action on all states except those ending in $|00\rangle$. We thus get an independent su(b_K) on $\mathrm{DFS}_n(K)$. Together, the ''above'' and ''below'' constructions, respectively, provide independent su(t_K) and su(b_K) on $\mathrm{DFS}_n(K)$. Finally, note that we did not really need both $\mathbf{T}_{ij}^{P}$ and $\mathbf{T}_{ij}^{Q}$, since once we established independent action on the T-states, we could have just subtracted out this action when considering the B-states. Also, the specific choice of $\mathbf{T}_{ij}^{P,Q}$ was rather arbitrary (though convenient): in fact almost any other diagonal interaction would do just as well.

2. Mixing

In order to induce operations between the two sets of paths (from ''above'' and from ''below'') that make up $\mathrm{DFS}_n(K)$ consider the effect of $\mathbf{E}_{n-1,n}$. This gate does not affect any paths that ''ascend'' two steps to (n,K) (corresponding to bitstrings ending in $|00\rangle$) and paths that ''descend'' two steps (ending in $|11\rangle$), but it flips the paths that pass from $(n-2,K)$ via $(n-1,K+1)$ with the paths from $(n-2,K)$ via $(n-1,K-1)$ (see Fig. 3). It does this for all DFSs simultaneously.

In order to get a full su(d_K) on $\mathrm{DFS}_n(K)$ we need to ''mix'' $su(t_K)$ (on the T-states) and su(b_K) (on the B-states) which we already have. We show how to obtain an independent su(2) between a T-state and a B-state. By the enlarging lemma this generates su(d_K).

Since $n\geqslant 3$ $\mathrm{DFS}_n(K)$ contains states terminating in $|00\rangle$ and/or $|11\rangle$. Let us assume, without loss of generality, that states terminating in $|00\rangle$ are present, and let $|i\rangle$ be such a state (B-state). Let $|j\rangle$ be a B-state not terminating in $|00\rangle$, and let $|k\rangle=\mathbf{E}_{n-1,n}|j\rangle$ ($|k\rangle$ is a T-state). Let $\overline{\mathbf{Z}}_{ij}=|i\rangle\langle i|-|j\rangle\langle j|\in \mathrm{su}(b_K)$, and recall that we have independent su(b_K). Then as is easily checked, $i[\mathbf{E}_{n-1,n},\overline{\mathbf{Z}}_{ij}]\equiv\overline{\mathbf{Y}}_{jk}$ yields σ_y between $|j\rangle$ and $|k\rangle$ only.[7] In addition, $\overline{\mathbf{Z}}_{jk}\equiv(i/2)\times[\mathbf{E}_{n-1,n},\overline{\mathbf{Y}}_{jk}]$ gives σ_z between $|j\rangle$ and $|k\rangle$, thus completing a generating set for su(2) on the B-state $|j\rangle$ and the T-state $|k\rangle$, that affects these two states only and annihilates all other states. This completes the proof.

To summarize, we have shown constructively that it is possible to generate the entire Lie algebra su(d_K) on a given weak collective-decoherence $\mathrm{DFS}_n(K)$ of dimension d_K, from the elementary composition of the operations of scalar multiplication, addition, and Lie commutators (conjugation by unitaries was not necessary in the WCD case). Moreover, this su(d_K) can be generated independently on each DFS, implying that universal quantum computation can be performed inside each $\mathrm{DFS}_n(K)$. Naturally, one would like to do this on the largest DFS. Since given the number of qubits n the dimensions of the DFSs are $d_K=\binom{n}{K}$, the largest DFS is the decoherence-free subspace $K=0$. In principle it is possible, by virtue of the independence result, to universally quantum compute in parallel on all DFSs.

D. State preparation and measurement on the weak collective decoherence DFS

To make use of a DFS for encoding information in a quantum computer, in addition to the universal quantum computation described above, it must also be possible to initially prepare encoded states and to decode the quantum information on the DFS at the end of a computation. Encoding requires that the density matrix of the prepared states should have a large overlap with the DFS. Note that it is not necessary to prepare states that have support exclusively within the DFS, i.e., that have no component outside of the DFS. This follows from the fact that in our construction, while a computation is performed, there is no mixing of states inside and outside of the DFS. If an initially prepared state is ''contaminated'' (has some support outside the DFS we want to compute on), then the result of the computation will have the same amount of contamination, i.e., the initial error does not spread.

For example, suppose we can prepare the state $\rho=(1-p)|\psi\rangle\langle\psi|+p|\psi_\perp\rangle\langle\psi_\perp|$ where $|\psi\rangle$ is a state of a particular DFS and $|\psi_\perp\rangle$ is a state outside of this DFS. Then the computation will proceed independently on the DFS and the states outside of the DFS. Readout will then obtain the result of the computation with probability $1-p$. Repeated applica-

[7]Since $\mathbf{E}_{n-1,n}=|i\rangle\langle i|+|k\rangle\langle j|+|j\rangle\langle k|+O$, where O is some action on an orthogonal subspace.

tion of the quantum computation will give the desired result to arbitrary confidence level.

There are many choices for the initial states of a computation and the decision as to which states to prepare should be guided by the available gates and measurements and the accuracy that is achievable. For efficient computation one should try to maximize the overlap of the prepared state with the desired initial DFS state.

For the WCD case preparation of initial pure states is very simple. Suppose we are concerned with the $\mathbf{S}_z$ error WCD-DFS. Pure state preparation into such a DFS then corresponds to the ability to prepare a state which has support over states with a specific number of $|0\rangle$ and $|1\rangle$ (eigenstates of the σ_z operator). This is particularly simple if measurements in the σ_z basis ($|0\rangle,|1\rangle$) as well as σ_x gates (to ''flip'' the bits) are available.

The second crucial ingredient for computation on a DFS (in addition to preparation) is the decoding or readout of quantum information resulting from a computation. Once again, there are many options for how this can be performed. For example, in the WCD case one can make a measurement which distinguishes all of the DFSs and all of the states within this DFS by simply making a measurement in the σ_z basis on every qubit. Further, all measurements with a given number of distinct eigenvalues can be performed by first rotating the observable into one corresponding to a measurement in the computational basis (which, in turn, corresponds to a unitary operation on the DFS) and then performing the given measurement in the σ_z basis, and finally rotating back. There are other situations where one would like to, say, make a measurement of an observable over the DFS which has only two different eigenvalues. This type of measurement can be most easily performed by a conjoined measurement [40]. In this scheme, one attaches another DFS to the original DFS, forming a single larger DFS. Then, assuming universal quantum computation over this larger DFS one can always perform operations which allow a measurement of the first DFS by entangling it with the second DFS, and reading out (destructively as described for the WCD above) the second DFS. For example, suppose the first DFS encodes two bits of quantum information, $|k,l\rangle_L$, $k,l=\{0,1\}$, and the second DFS encodes a single bit of quantum information $\{|0\rangle_L,|1\rangle_L\}$. Then one can make a measurement of the observable $\sigma_z\otimes\mathbf{I}$ on the first DFS by performing an encoded controlled-NOT operation between the first and the second DFS, and reading out the second DFS in the encoded σ_z basis. For the WCD case the ability to make this destructive measurement on the ancilla (not on the code) simply corresponds to the ability to measure single σ_z operations.

Finally, we note that for a WCD-DFS there is a destructive measurement which distinguishes between different DFSs (corresponding to a measurement of the number of $|1\rangle$'s). One can fault-tolerantly prepare a WCD-DFS state by repeatedly performing such a measurement to guarantee that the state is in the proper DFS. The conjoined measurement procedures described above for any DFS are naturally fault-tolerant in the sense that they can be repeated and are nondestructive [40,51]. Thus fault-tolerant preparation and decoding is available for the WCD-DFS.

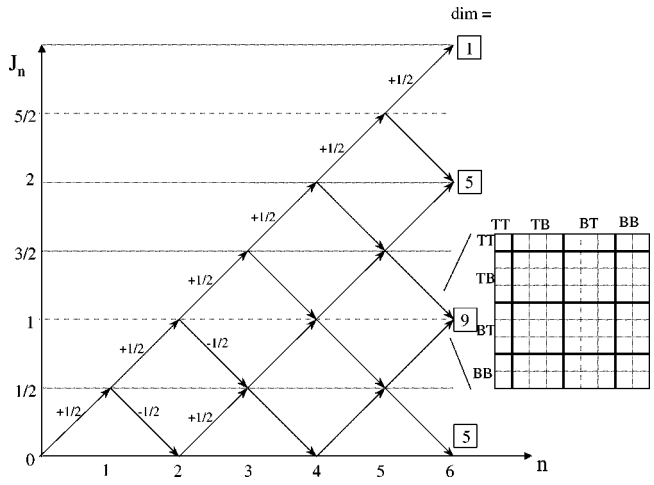


FIG. 4. Graphical representation of DFS states for strong collective decoherence (SCD). The horizontal axis is the number of qubits, *n*, just as in Fig. 1 for WCD. The vertical axis is now the total angular momentum **J** obtained by summing angular momenta of *n* spin 1/2 particles representing the *n* qubit, rather than just the *z* component of this. The DFSs are denoted by $\mathrm{DFS}_n(J)$ as before. Each state in the DFS is represented by a pathway from the origin along the arrows as indicated. The insert shows the matrix structure of operators acting on $\mathrm{DFS}_6(1)$, given in terms of TT-, TB-, BT-, and BB-states.

VII. STRONG COLLECTIVE DECOHERENCE

Strong collective decoherence on *n* qubits is characterized by the three system operators $\mathbf{S}_x$, $\mathbf{S}_y$, and $\mathbf{S}_z$. These operators form a representation of the semisimple Lie algebra su(2). The algebra $\mathcal{A}$ generated by these operators can be decomposed as[8]

$$\mathcal{A}\cong\bigoplus_{J=0(1/2)}^{n/2}\mathbf{I}_{n_J}\otimes\mathrm{gl}(2J+1,\mathbb{C}), \tag{56}$$

where J labels the total angular momentum of the corresponding Hilbert space decomposition (and hence the 0 or 1/2 depending on whether *n* is even or odd, respectively) and $\mathrm{gl}(2J+1,\mathbb{C})$ is the general linear algebra acting on a space of size $2J+1$. The resulting decomposition of the system Hilbert space

$$\mathcal{H}_S\cong\bigoplus_{J=0(1/2)}^{n/2}\mathbb{C}_{n_J}\otimes\mathbb{C}_{2J+1} \tag{57}$$

is exactly the reduction of the Hilbert states into different Dicke states [60,61]. The multiplicity for each J is given by [61]:

$$n_J=\frac{(2J+1)n!}{(n/2+J+1)!(n/2-J)!}. \tag{58}$$

[8]Note that as a complex algebra $\{\mathbf{S}_x,\mathbf{S}_y,\mathbf{S}_z\}$ span all of gl(2), not just su(2).

This multiplicity is just the degeneracy associated with the angular momentum J. Equation (56) shows that given J, a state $|J,\lambda,\mu\rangle$ is acted upon as identity on its λ component. Thus a DFS is defined by fixing J and μ. As we will show later, the degeneracy index λ corresponds to the paths leading to a given point (n,J) on the diagram of Fig. 4. In the strong collective decoherence case, we shall denote the n-qubit DFS labeled by a particular angular momentum J, by $\mathrm{DFS}_n(J)$.

The DFSs corresponding to the different J values for a given n can be computed using standard methods for the addition of angular momentum. We use the convention that $|1\rangle$ represents a $|j=1/2,m_j=1/2\rangle$ particle and $|0\rangle$ represents a $|j=1/2,m_j=-1/2\rangle$ particle in this decomposition although, of course, one should be careful to treat this labeling as strictly symbolic and not related to the physical angular momentum of the particles.

The smallest n which supports a DFS and encodes at least a qubit of information is $n=3$ [48]. For $n=3$ there are two possible values of the total angular momentum: $J=3/2$ or $J=1/2$. The four $J=3/2$ states $|J,\lambda,\mu\rangle=|3/2,0,\mu\rangle$ ($\mu=m_J=\pm 3/2,\pm 1/2$) are singly degenerate; the $J=1/2$ states have degeneracy 2. They can be constructed by either adding a $J_{12}=1$ (triplet) or a $J_{12}=0$ (singlet) state to a $J_3=1/2$ state. These two possible methods of adding the angular momentum to obtain a $J=1/2$ state are exactly the degeneracy of the algebra, i.e., $\lambda=1,2$. The four $J=1/2$ states are:

$$|0_L\rangle=\begin{cases}\left|\frac{1}{2},0,0\right\rangle=|0,0\rangle\otimes\left|\frac{1}{2},-\frac{1}{2}\right\rangle=\frac{1}{\sqrt{2}}(|010\rangle-|100\rangle)\\ \left|\frac{1}{2},0,1\right\rangle=|0,0\rangle\otimes\left|\frac{1}{2},\frac{1}{2}\right\rangle=\frac{1}{\sqrt{2}}(|011\rangle-|101\rangle),\end{cases}$$

$$|1_L\rangle=\begin{cases}\left|\frac{1}{2},1,0\right\rangle=\frac{1}{\sqrt{3}}\left(-\sqrt{2}|1,-1\rangle\otimes\left|\frac{1}{2},\frac{1}{2}\right\rangle+|0,0\rangle\otimes\left|\frac{1}{2},-\frac{1}{2}\right\rangle\right)=\frac{1}{\sqrt{6}}(-2|001\rangle+|010\rangle+|100\rangle)\\ \left|\frac{1}{2},1,1\right\rangle=\frac{1}{\sqrt{3}}\left(\sqrt{2}|1,1\rangle\otimes\left|\frac{1}{2},-\frac{1}{2}\right\rangle-|1,0\rangle\otimes\left|\frac{1}{2},\frac{1}{2}\right\rangle\right)=\frac{1}{\sqrt{6}}(2|110\rangle-|101\rangle-|011\rangle),\end{cases}\tag{59}$$

where in the first column we indicated the grouping forming a logical qubit; in the second we used the $|J,\lambda,\mu\rangle$ notation; in the third we used tensor products of the form $|J_{12},m_{J_{12}}\rangle\otimes|J_3,m_{J_3}\rangle$; and in the fourth the states are expanded in terms of the single-particle $|j=1/2,m_j=\pm 1/2\rangle$ basis using Clebsch-Gordan coefficients. These states form a decoherence-free subsystem: the decomposition of Eqs. (56) and (57) ensures that the states $\{|\frac{1}{2},0,0\rangle,|\frac{1}{2},0,1\rangle\}$ are acted upon identically by any $\mathbf{S}_\alpha$, i.e., they can be mixed among themselves but not with states in $|1_L\rangle$. The same holds for the states $\{|\frac{1}{2},1,0\rangle,|\frac{1}{2},1,1\rangle\}$. Thus information of a qubit $\alpha|0_L\rangle+\beta|1\rangle$ should be encoded into these states as

$$\rho=\underbrace{\left[\left|\frac{1}{2}\right\rangle\left\langle\frac{1}{2}\right|\right]}_{J}\underbrace{[(\alpha^*|0_L\rangle+\beta^*|1_L\rangle)(\alpha\langle 0_L|+\beta\langle 1_L|)]}_{\lambda}\underbrace{[\gamma_{00}|0\rangle\langle 0|+\gamma_{01}|0\rangle\langle 1|\gamma_{01}+\gamma_{10}|1\rangle\langle 0|+\gamma_{11}|1\rangle\langle 1|]}_{\mu}\tag{60}$$

where γ_{ij} form the components of a valid density matrix (unity trace and positive). The important point to note is that one encodes quantum information into the degeneracy index λ. Using Eq. (56) it follows that each of the $\mathbf{S}_\alpha$'s act on ρ in such a manner that only the μ component is changed. Indeed, the $\mathbf{S}_\alpha$'s act like a corresponding σ_α in the μ basis because this basis is two-dimensional, and σ_α are the two-dimensional irreducible representations of su(2). If these are the only error processer then the encoded information is completely protected. These considerations are illustrated in detail for the exchange interaction in Sec. VII C.

The smallest decoherence-free subspace (as opposed to subsystem) supporting a full encoded qubit comes about for $n=4$. Subspaces for the SCD mechanism correspond to the

degeneracy of the zero total angular momentum eigenstates (there are also two decoherence-free subsystems with degeneracy 1 and 3). This subspace is spanned by the states:

$$
\begin{aligned}
|0_L\rangle &= |0,0,0\rangle = |0,0\rangle \otimes |0,0\rangle \\
&= \frac{1}{2}(|01\rangle - |10\rangle)(|01\rangle - |10\rangle) \\
|1_L\rangle &= |0,1,0\rangle \\
&= \frac{1}{\sqrt{3}}(|1,1\rangle \otimes |1,-1\rangle - |1,0\rangle \\
&\quad \otimes |1,0\rangle + |1,-1\rangle \otimes |1,1\rangle) \\
&= \frac{1}{\sqrt{12}}(2|0011\rangle + 2|1100\rangle - |0101\rangle \\
&\quad - |1010\rangle - |0110\rangle - |1001\rangle). \qquad (61)
\end{aligned}
$$

The notation is the same as in Eq. (59), except that in the third column we have used the notation $|J_{12},m_{J_{12}}\rangle \otimes |J_{34},m_{J_{34}}\rangle$ which makes it easy to see how the angular momentum is added. One encodes into λ, as in Eq. (60).

As seen from Eqs. (59) and (61), there is a variety of useful bases which one can choose for the SCD-DFSs. We now show how the generic basis $|J,\lambda,\mu\rangle$ can be given both a graphical and an angular momentum interpretation. Consider the addition of angular momentum as more particles are included, similar to the construction we used in the WCD case. To construct the n qubit SCD-DFS for a specific J, one takes $\mathrm{DFS}_{n-1}(J-1/2)$ and $\mathrm{DFS}_{n-1}(J+1/2)$, and uses the angular momentum addition rules to add another qubit ($j=1/2$). Table I presents the degeneracy of the Jth irreducible representation for n qubits. The entries are obtained just as in Pascal's triangle, except that half of the triangle (the bottom according to the scheme of Table I) is missing.

Table I demonstrates how the degeneracies of the $(n-1)$-qubit $J\pm 1/2$ irreducible representations (irreps), i.e., the dimensions of $\mathrm{DFS}_{n-1}(J\pm 1/2)$, add to determine the dimension of $\mathrm{DFS}_n(J)$. This method of addition of the angular momentum leads to a natural interpretation of the $|J,\lambda,\mu\rangle$ basis for the SCD-DFSs which we now present.

Define the partial collective operators

$$
\mathbf{S}_\alpha^k \equiv \mathbf{S}_\alpha^{(1,2,\ldots,k)} = \sum_{i=1}^{k} \sigma_\alpha^i . \qquad (62)
$$

This can be used to find a set of mutually commuting operators for the SCD-DFSs: the partial total angular momentum operators

$$
(\mathbf{S}^k)^2 = \sum_{\alpha=x,y,z} (\mathbf{S}_\alpha^k)^2 . \qquad (63)
$$

As shown in Appendix A:

$$
[(\mathbf{S}^k)^2, (\mathbf{S}^l)^2] = 0 \quad \forall k,l. \qquad (64)
$$

Thus the $\{(\mathbf{S}^k)^2\}$ can be used to label the SCD-DFSs by their eigenvalues J_k.

In order to make the connection between the addition of angular momentum and the Dicke states one should, however, use

$$
\mathbf{s}_\alpha^k \equiv \sum_{i=1}^{k} \frac{1}{2}\sigma_\alpha^i = \frac{1}{2}\mathbf{S}_\alpha^k . \qquad (65)
$$

With this definition $(\mathbf{s}^k)^2 = \Sigma_\alpha (\mathbf{s}_\alpha^k)^2$ is just the operator whose eigenvalue for the Jth irrep of the k qubit case is $J_k(J_k+1)$. We label the basis determined by the eigenvalues of $(\mathbf{s}^k)^2$ by

$$
|J_1,J_2,J_3,\ldots,J_{n-1},J;m_J\rangle, \qquad (66)
$$

where

$$
\begin{aligned}
(\mathbf{s}^k)^2 |J_1,J_2,J_3,\ldots,J_{n-1},J;m_J\rangle \\
= J_k(J_k+1)|J_1,J_2,J_3,\ldots,J_{n-1},J;m_J\rangle, \qquad (67)
\end{aligned}
$$

and where for consistency with the $|J,\lambda,\mu\rangle$ notation we use J for J_n. As in the WCD case, the degeneracy which leads to the SCD-DFS can be put into a one-to-one correspondence with a graphical representation of the addition of angular momentum, shown in Fig. 2. Here, however, each step does not simply correspond to adding a $|0\rangle$ or $|1\rangle$ state but instead corresponds to combining the previous spin J particle with a spin 1/2 particle to create a $J+1/2$ or $|J-1/2|$ particle (note the absolute value so that the total spin is positive). In the graphical representation of Fig. 4 the horizontal axis counts qubits, and the vertical axis corresponds to the total angular momentum J_i up to the ith qubit (note the similarity to Table I). Each SCD-DFS state then corresponds to a path constructed by successively moving up or down 1/2 unit of angular momentum, starting from a single qubit with $J_1=1/2$. For example, the two $\mathrm{DFS}_3(1/2)$ states are $\{|1/2,0,1/2;\pm 1/2\rangle, |1/2,1,1/2;\pm 1/2\rangle\}$ (corresponding, respectively, to the paths ''up, down, up'' and ''up, up, down'' and $m_{J_3=1/2}=\pm 1/2$), and the two $\mathrm{DFS}_4(0)$ states are $\{|1/2,0,1/2,0;0\rangle, |1/2,1,1/2,0;0\rangle\}$. Clearly, the set of paths $\mathbf{J}_n \equiv \{J_1,J_2,J_3,\ldots,J_{n-1},J_n\}$ with fixed J_n counts the degeneracy of $\mathrm{DFS}_n(J_n)$. Therefore we can identify the general degeneracy index λ (of $|J,\lambda,\mu\rangle$) with $\mathbf{J}_n$. Similarly, the dimensionality index μ can now be identified with m_{J_n}. Finally, as claimed above J is just the final J_n.

A. The stabilizer and error correction properties

Note from Eq. (62) that the system operators $\mathbf{S}_\alpha = \mathbf{S}_\alpha^n$. Therefore they can only affect the last component $|J_n;m_{J_n}\rangle$ of the DFS states. By the identification of the degeneracy index λ with the paths $\{J_1,\ldots,J_{n-1},J\}$, and from the general expression (56) for the action of the $\mathbf{S}_\alpha$, we know that $\mathbf{S}_\alpha$ acts only on the dimensionality component:

$$
\mathbf{S}_\alpha |J_1,\ldots,J_{n-1},J;m_J\rangle = |J_1,\ldots,J_{n-1},J\rangle \otimes (\mathbf{P}_\alpha |m_J\rangle), \qquad (68)
$$

where the $\mathbf{P}_\alpha$ are a $2J+1$ dimensional representation of su(2) acting directly on the $|m_J\rangle$ components of the DFS. The corresponding DFS stabilizer is

$$\mathbf{D}(\vec{v})=\mathbf{D}(v_x,v_y,v_z)=\exp\left[\sum_{\alpha=x,y,z} v_\alpha(\mathbf{S}_\alpha-\mathbf{I}\otimes\mathbf{P}_\alpha)\right]. \tag{69}$$

For the $J=0$ DFSs this reduces to all collective rotations +contractions [27]:

$$\begin{aligned}\mathbf{D}(\vec{v})&=\exp\left[\sum_{\alpha=x,y,z} v_\alpha\mathbf{S}_\alpha\right]\\&=\bigotimes_{i=1}^{n}\exp[\vec{v}\cdot\vec{\sigma}_i]\\&=\left[\mathbf{I}\cos\|\vec{v}\|+\frac{\vec{\sigma}\cdot\vec{v}}{\|\vec{v}\|}\sin\|\vec{v}\|\right]^{\otimes n},\end{aligned}$$

where $||v||\equiv(\Sigma_\alpha v_\alpha^2)^{1/2}$ may be complex. Thus $\mathrm{DFS}_n(0)$ protects against all processes described by Kraus operators that are linear combinations of collective rotations+contractions $\exp[\vec{v}\cdot\vec{\sigma}]$. The situation for $J\neq 0$ is more complicated to calculate analytically.

Let us now comment briefly on the error-correction and detection properties of $\mathrm{DFS}_n(0)$: The stabilizer elements are tensor products of identical 1-qubit operators, including the following elements of the Pauli group: $\mathbf{X}^{\otimes n}$, $\mathbf{Y}^{\otimes n}$, and $\mathbf{Z}^{\otimes n}$. Thus for any odd-multiple $2k-1<n$ of single qubit errors **X**, **Y**, and **Z** there is an element in the stabilizer that anticommutes with it: The code can detect any such error. The $J=0$ SCD-DFS is an error correcting code of distance 2.

B. Nontrivial Operations

Are there any single-qubit operators which preserve a SCD-DFS (and thus allow for nontrivial operations on the DFS)? There are no nontrivial single-qubit operators that commute with all $\mathbf{S}_\alpha$ operators, since

$$[\mathbf{S}_\alpha,\sigma_\beta^j]=\sum_i[\sigma_\alpha^i,\sigma_\beta^j]=i\sum_i\delta_{ij}\varepsilon_{\alpha\beta\gamma}\sigma_\gamma^i \tag{70}$$

which vanishes iff $\alpha=\beta$. Therefore there are no single-qubit operators which preserve all SCD-DFSs simultaneously.

As for two-qubit operators, the only such Hermitian operators which commute with the $\mathbf{S}_\alpha$ are those that are proportional to the exchange interaction [Eq. (44)]: $\mathbf{E}_{ij}|k\rangle_i|l\rangle_j=|l\rangle_i|k\rangle_j$, where i,j label the qubits acted upon [37]. In both the single- and two-qubit cases, there could be additional operators in the generalized commutant $\mathcal{T}$ (e.g., for $n=4$ qubits there is an operator which mixes the different J's and preserves $\mathrm{DFS}_4(0)$: $\mathbf{T}=|J=1,\lambda_1,\mu_1\rangle\langle J=2,\lambda_1,\mu_1|+\mathrm{H.c.}$). We will not be concerned with such operations as they are not needed in order to demonstrate universality, and since we will show that the exchange operator is sufficient for any SCD-DFS. Our task is thus to show that exchange interactions alone suffice to generate the entire SU(N) group on each N-dimensional DFS, in the SCD case.

C. Quantum computation on the $n=3$ and $n=4$ qubit SCD-DFS

We begin our discussion of universal quantum computation on SCD-DFSs by examining the simplest SCD-DFS which supports encoding of quantum information: the $n=3$ decoherence-free subsystem. We label these states as in Eq. (59) by $|J,\lambda,\mu\rangle$. Recall that the $J=3/2$ irrep is not degenerate and the $J=1/2$ irrep has degeneracy 2. The $J=3/2$ states can be written as $|\frac{3}{2},0,\mu\rangle$, with $\mu=m_J=\pm 3/2,\pm 1/2$. Since the action of exchange does not depend on μ (recall that it affects paths, i.e., the λ component only) it suffices to consider the action on the representative $\mu=3/2$ only: $|111\rangle$. Let us then explicitly calculate the action of exchanging the first two physical qubits on this state and the four $J=1/2$ states. Using Eq. (59):

$$\begin{aligned}\mathbf{E}_{12}\left|\frac{3}{2},0,\frac{3}{2}\right\rangle&=\mathbf{E}_{12}|111\rangle=\left|\frac{3}{2},0,\frac{3}{2}\right\rangle,\\\mathbf{E}_{12}\left|\frac{1}{2},0,0\right\rangle&=\mathbf{E}_{12}\frac{1}{\sqrt{2}}(|010\rangle-|100\rangle)\\&=\frac{1}{\sqrt{2}}(|100\rangle-|010\rangle)=-\left|\frac{1}{2},0,0\right\rangle,\\\mathbf{E}_{12}\left|\frac{1}{2},0,1\right\rangle&=\mathbf{E}_{12}\frac{1}{\sqrt{2}}(|011\rangle-|101\rangle)\\&=\frac{1}{\sqrt{2}}(|101\rangle-|011\rangle)=-\left|\frac{1}{2},0,1\right\rangle,\\\mathbf{E}_{12}\left|\frac{1}{2},1,0\right\rangle&=\mathbf{E}_{12}\frac{1}{\sqrt{6}}(-2|001\rangle+|010\rangle+|100\rangle)=\left|\frac{1}{2},1,0\right\rangle,\\\mathbf{E}_{12}\left|\frac{1}{2},1,1\right\rangle&=\mathbf{E}_{12}\frac{1}{\sqrt{6}}(2|110\rangle-|101\rangle-|011\rangle)=\left|\frac{1}{2},1,1\right\rangle.\end{aligned} \tag{71}$$

Focusing just on the $J=1/2$ states, the exchange action on $|\lambda\rangle\otimes|\mu\rangle$ can thus be written as

$$\mathbf{E}_{12}=-\sigma_z\otimes\mathbf{I}. \tag{72}$$

Since the action of the $\mathbf{S}_\alpha$ operators on the $J=1/2$ states is $\mathbf{I}_{n_{1/2}}\otimes\mathrm{gl}(2)$ according to Eq. (56), this explicit form for $\mathbf{E}_{12}$ confirms that is has the expected structure of operators in the commutant of the algebra spanned by the $\mathbf{S}_\alpha$. It can also be seen that quantum information should be encoded in the $|\lambda\rangle$ component, as discussed before Eq. (60).

Using similar algebra it is straightforward to verify that the effect of the three possible exchanges on the $n=3$ DFS states is given by:

$$\mathbf{E}_{12}=\begin{pmatrix}1&0&0\\0&-1&0\\0&0&1\end{pmatrix},\quad \mathbf{E}_{23}=\begin{pmatrix}1&0&0\\0&\frac{1}{2}&-\frac{\sqrt{3}}{2}\\0&-\frac{\sqrt{3}}{2}&-\frac{1}{2}\end{pmatrix},$$

$$\mathbf{E}_{13}=\begin{pmatrix}1&0&0\\0&\frac{1}{2}&\frac{\sqrt{3}}{2}\\0&\frac{\sqrt{3}}{2}&-\frac{1}{2}\end{pmatrix}, \tag{73}$$

where the rows and columns of these matrices are labeled by the basis elements $\{|J=3/2,\lambda=0\rangle,|J=1/2,\lambda=0\rangle,|J=1/2,\lambda=1\rangle\}$. As expected from general properties of the commutant, the exchange operators do not mix the different J irreps. Now,

$$\frac{1}{3}(\mathbf{E}_{12}+\mathbf{E}_{13}+\mathbf{E}_{23})=\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix},$$

$$\frac{1}{2}(-\mathbf{E}_{12}+\mathbf{E}_{13}+\mathbf{E}_{23})=\begin{pmatrix}0&0&0\\0&1&0\\0&0&-1\end{pmatrix},$$

$$\frac{1}{\sqrt{3}}(\mathbf{E}_{13}-\mathbf{E}_{23})=\begin{pmatrix}0&0&0\\0&0&1\\0&1&0\end{pmatrix}, \tag{74}$$

showing that the last two linear combinations of exchanges look like the Pauli σ_z and σ_x on $\mathrm{DFS}_3(1/2)$. Using a standard Euler angle construction it is thus possible to perform any SU(2) gate on this DFS. Moreover, it is possible to act independently on $\mathrm{DFS}_3(3/2)$ and $\mathrm{DFS}_3(1/2)$. In other words, we can perform U(1) on $\mathrm{DFS}_3(3/2)$ alone, and SU(2) on $\mathrm{DFS}_3(1/2)$ alone. Note, however, that at this point we cannot yet claim universal quantum computation on a register composed of clusters of $\mathrm{DFS}_3(J)$'s (J constant) because we have not shown how to couple such clusters.

For $n=4$ the Hilbert space splits up into one $J=2$-irrep $[\mathrm{DFS}_4(2)]$, three $J=1$-irreps $[\mathrm{DFS}_4(1)]$, and two $J=0$-irreps $[\mathrm{DFS}_4(0)]$, see Table I. Direct calculation of the effect of exchange on these DFSs shows that we can independently perform su(1) (i.e., zero), su(3), and su(2). In particular, we find that [28,40]:

$$\mathbf{X}=\frac{1}{\sqrt{3}}(\mathbf{E}_{23}-\mathbf{E}_{13}),\quad \mathbf{Y}=\frac{i}{2\sqrt{3}}[\mathbf{E}_{23}-\mathbf{E}_{13},\mathbf{E}_{34}],$$

$$\mathbf{Z}=\frac{i}{2}[\mathbf{Y},\mathbf{X}]=-\mathbf{E}_{12} \tag{75}$$

act as the corresponding su(2) Pauli operators on $\mathrm{DFS}_4(0)$ only. Further, the following operators act independently on the $J=1$-irreps (rows and columns are labeled by $\lambda=0,1,2$. The action occurs simultaneously on all three μ components corresponding to a given λ):

$$\mathbf{Y}_{13}=\frac{3i}{2\sqrt{2}}[\mathbf{E}_{12},\mathbf{E}_{34}]=\begin{pmatrix}0&0&-i\\0&0&0\\i&0&0\end{pmatrix},$$

$$\mathbf{X}_{13}=\frac{i}{2}[\mathbf{E}_{12},\mathbf{Y}_{13}]=\begin{pmatrix}0&0&1\\0&0&0\\1&0&0\end{pmatrix},$$

$$\mathbf{Z}_{13}=\frac{i}{2}[\mathbf{Y}_{13},\mathbf{X}_{13}]=\begin{pmatrix}1&0&0\\0&0&0\\0&0&-1\end{pmatrix},$$

$$\mathbf{Y}_{23}=\frac{2i}{\sqrt{3}}[\mathbf{E}_{23},\mathbf{Z}_{13}]=\begin{pmatrix}0&0&0\\0&0&-i\\0&i&0\end{pmatrix}. \tag{76}$$

These operators clearly generate su(3), and hence we have an independent SU(3) action on $\mathrm{DFS}_4(1)$.

D. Universal quantum computation on the $n\geqslant 5$ qubit SCD-DFSs

We are now ready to prove our central result: that using only the two-body exchange Hamiltonians every unitary operation can be performed on a SCD-DFS. More specifically:

Theorem 5: For any $n\geqslant 2$ qubits undergoing strong collective decoherence, there exist sets of Hamiltonians H_J^n obtained from exchange interactions only via scalar multiplication, addition, Lie commutator, and unitary conjugation, acting as su(d_J) on the DFS corresponding to the eigenvalue J. Furthermore, each set acts independently on this DFS only (i.e., with zeroes in the matrix representation corresponding to their action on the other DFSs).

In preparation for the proof of this result let us note several useful facts:

(i) The exchange operators do not change the value of m_J because they are in the commutant of $\mathcal{A}=\{S_\alpha\}$ [recall Eq. (68)]. Therefore in order to evaluate the action of the ex-

TABLE I. Strong collective decoherence DFS dimensions, given by the degeneracy n_J, Eq. (58).

	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$	$n=6$
$J=3$						1
$J=\frac{5}{2}$					1	
$J=2$				1		5
$J=\frac{3}{2}$			1		4	
$J=1$		1		3		9
$J=\frac{1}{2}$	1		2		5	
$J=0$		1		2		5

change operators on the different $\mathrm{DFS}_n(J)$ (n given) it is convenient to fix m_J, and in particular to work in the basis given by the maximal m_J value ($m_J=J$). Expressions for these ''maximal'' states in terms of $|J_1,J_2,\ldots,J_{n-2};m_J\rangle$ and the single qubit states of the last two qubits are given in Appendix B.

(ii) Every $(\mathbf{s}^k)^2$ can be written as a sum of exchange operators and the identity operation [28]. This follows from Eq. (A1) and noting that the exchange operator can be expanded as

$$\mathbf{E}_{ij}=\frac{1}{2}(\mathbf{I}+\sigma_x^i\sigma_x^j+\sigma_y^i\sigma_y^j+\sigma_z^i\sigma_z^j), \tag{77}$$

so that

$$(\mathbf{s}^k)^2=k\left(1-\frac{k}{4}\right)\mathbf{I}+\frac{1}{2}\sum_{i\neq j=1}^{k}\mathbf{E}_{ij}. \tag{78}$$

Thus $(\mathbf{s}^k)^2$ is a Hamiltonian which is at our disposal.

We are now ready to present our proof by induction. Recall the DFS-dimensionality formula for n_J, Eq. (58). We assume that it is possible to perform $\mathrm{su}(n_J)$ on each of the different $\mathrm{DFS}_{n-1}(J)$ independently using only exchange operators and the identity Hamiltonian. Our construction above proves that this is true for 3 and 4 qubits. The assumption that the actions we can perform can be performed independently translates into the ability to construct Hamiltonians which annihilate all of the DFSs except a desired one on which they act as $\mathrm{su}(n_J)$.

As in the WCD case a specific $\mathrm{DFS}_n(J)$ of dimension n_J splits into states which are constructed by the subtraction of angular momentum from $\mathrm{DFS}_{n-1}(J+1/2)$ (T-states), or by the addition of angular momentum to $\mathrm{DFS}_{n-1}(J-1/2)$ (B-states) (see Fig. 5). Performing $\mathrm{su}(n_{J+1/2})$ on $\mathrm{DFS}_{n-1}(J+1/2)$ will simultaneously act on $\mathrm{DFS}_n(J)$ and $\mathrm{DFS}_n(J+1)$. In other words, $\mathrm{su}(n_{J+1/2})$ on $\mathrm{DFS}_{n-1}(J+1/2)$ acts on both the B-states of $\mathrm{DFS}_n(J+1)$ and on the T-states of $\mathrm{DFS}_n(J)$. We split the proof into three steps. In the first step we obtain an su(2) set of operators which acts only on $\mathrm{DFS}_n(J)$ and mixes particular B- and T-states. In the second step we expand the set of operators which mix B- and T-states to cover all possible su(2) algebras between any two B- and T-states. Finally, in the third step we apply a Mixing Lemma which shows that we can obtain the full $\mathrm{su}(n_J)$ (i.e., also mix B-states and mix T-states).

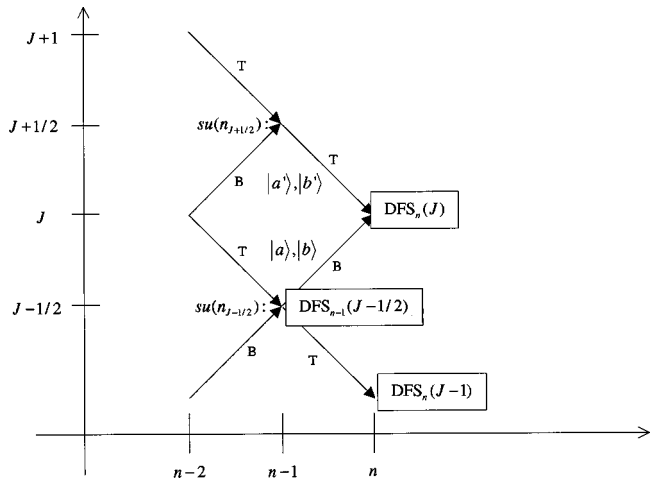


FIG. 5. Scheme to visualize the inductive proof of universal computation using only the exchange Hamiltonian, for the strong collective decoherence case. TB- and BT-states of $\mathrm{DFS}_n(J)$ are indicated. $\mathrm{su}(n_{J-1/2})$ acts on $\mathrm{DFS}_n(J-1)$ and on $\mathrm{DFS}_n(J)$ via $\mathrm{DFS}_{n-1}(J-1/2)$. See Sec. VII D for details.

1. T- and B-mixing

There are two simple instances where there is no need to show independent action in our proof: (i) The (upper) $J=n/2$ -irrep is always one-dimensional, so the action on it is always trivial (i.e., the Hamiltonian vanishes and hence the action is independent by definition); (ii) For odd n the ''lowest'' $\mathrm{DFS}_n(1/2)$ is acted upon independently by the $\mathrm{su}(n_0)$ from $\mathrm{DFS}_{n-1}(0)$ [i.e., $\mathrm{su}(n_0)$ cannot act ''downward'']. In order to facilitate our construction we extend the notion of T- and B-states one step further in the construction of the DFS. TB-states are those states which are constructed from T-states on $(n-1)$-qubits and from the B-states on n-qubit states (see Fig. 5). Similarly we can define the BT-, TT-, and BB-states:

$$|\mathrm{TT}\rangle\equiv|J_1,\ldots,J_{n-3},J_n+1,J_n+\frac{1}{2},J_n;m_J=J_n\rangle=\searrow\!\searrow \tag{79}$$

$$|\mathrm{BT}\rangle\equiv|J_1,\ldots,J_{n-3},J_n,J_n+\frac{1}{2},J_n;m_J=J_n\rangle=\nearrow\!\searrow$$

$$|\mathrm{TB}\rangle\equiv|J_1,\ldots,J_{n-3},J_n,J_n-\frac{1}{2},J_n;m_J=J_n\rangle=\searrow\!\nearrow$$

$$|\mathrm{BB}\rangle\equiv|J_1,\ldots,J_{n-3},J_n-1,J_n-\frac{1}{2},J_n;m_J=J_n\rangle=\nearrow\!\nearrow \tag{80}$$

Every $\mathrm{DFS}_n(J)$ can be broken down into a direct sum of TT-, BT-, TB-, and BB-states; e.g., as seen in Fig. 4, in $\mathrm{DFS}_6(1)$ there are 1 TT, 3 TB, 3 BT, and 2 BB states. Note that for $J=n/2-1$ there are no TT-states, for $J=0$ there are no BB- and BT-states, for $J=1/2$ there are no BB-states, and otherwise there are as many TB as there are BT-states,

At this point it is useful to explicitly give the action of exchange on the last two qubits of a SCD-DFS. Using Eq. (B8) we find (assuming the existence of the given states, i.e., n large enough and J not too large) the representation

$$\mathbf{E}_{n,n-1}=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -\cos(\theta_{J+1}) & \sin(\theta_{J+1}) & 0 \\ 0 & \sin(\theta_{J+1}) & \cos(\theta_{J+1}) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{matrix} \mathrm{TT} \\ \mathrm{BT} \\ \mathrm{TB'} \\ \mathrm{BB} \end{matrix} \tag{81}$$

where $\tan(\theta_J)=2\sqrt{J(J+1)}$. Thus exchange acts to transform the BT- and TB-states entering a given DFS into linear combinations of one another, while leaving invariant the BB- and TT-states.

Let us now consider the action of $\mathrm{su}(n_{J-1/2})$ from $\mathrm{DFS}_{n-1}(J-1/2)$ (see Fig. 5). It acts on $\mathrm{DFS}_n(J-1)$ and $\mathrm{DFS}_n(J)$ simultaneously. However, since the T-states of $\mathrm{DFS}_n(J-1)$ and the B-states of $\mathrm{DFS}_n(J)$ share the same set of quantum numbers $\{J_1,\ldots,J_{n-1}\}$, the action of the $\mathrm{su}(n_{J-1/2})$ operators is identical on these two sets of states.

We first deal with the case where the number of BT-states of $\mathrm{DFS}_n(J)$ is greater than 1. As can be inferred from Fig. 4, this condition corresponds to $J<n/2-1$ and $n>4$. We will separately deal with the $J=n/2-1$ case at the end of the proof. Let $|a\rangle$ and $|b\rangle$ be any two orthogonal BT-states of $\mathrm{DFS}_n(J)$ (i.e., states differing only by the paths on the first $n-2$ qubits). Corresponding to these are $\{|a'\rangle,|b'\rangle\}$: a pair of orthogonal BT-states of $\mathrm{DFS}_n(J)$. One of the elements in $\mathrm{su}(n_{J-1/2})$ is the traceless operator $\mathbf{C}=|a\rangle\langle a|-|b\rangle\langle b|$, which we have at our disposal by the induction hypothesis. Consider $i[\mathbf{E}_{n,n-1},\mathbf{C}]$: since $\mathbf{E}_{n,n-1}$ acts as identity on BB-states, even though $\mathbf{C}$ has an action on $\mathrm{DFS}_n(J-1)$ the commutator acting on the BB-states of $\mathrm{DFS}_n(J-1)$ vanishes. The action of $i[\mathbf{E}_{n,n-1},\mathbf{C}]$ on the BT- and TB-states can be calculated by observing, using Eq. (81), that the matrix representations of $\mathbf{C}$ and $\mathbf{E}_{n,n-1}$ are, in the ordered $\{|a'\rangle,|b'\rangle,|a\rangle,|b\rangle\}$ basis:

$$\mathbf{C}=\mathrm{diag}(0,0,1,-1)=\frac{1}{2}(\mathbf{I}\otimes\sigma_z-\sigma_z\otimes\sigma_z),$$

$$\mathbf{E}_{n,n-1}=\begin{pmatrix} -\cos(\theta_J) & 0 & \sin(\theta_J) & 0 \\ 0 & -\cos(\theta_J) & 0 & \sin(\theta_J) \\ \sin(\theta_J) & 0 & \cos(\theta_J) & 0 \\ 0 & \sin(\theta_J) & 0 & \cos(\theta_J) \end{pmatrix}$$
$$=-\cos(\theta_J)\sigma_z\otimes\mathbf{I}+\sin(\theta_J)\sigma_x\otimes\mathbf{I}. \tag{82}$$

This yields

$$i[\mathbf{E}_{n,n-1},\mathbf{C}]=-\sin(\theta_J)\sigma_y\otimes\sigma_z$$
$$=i\sin(\theta_J)(-|a\rangle\langle a'|+|a'\rangle\langle a|$$
$$+|b\rangle\langle b'|-|b'\rangle\langle b|). \tag{83}$$

Now let $|c\rangle$ be a TT-state of $\mathrm{DFS}_n(J)$. Such a state always exists unless $J=n/2-1$, which is covered at the end of the proof. Then there is an operator $\mathbf{D}=|a'\rangle\langle a'|-|c\rangle\langle c|$ in $\mathrm{su}(n_{J+1/2})$.[9] It follows that

$$\mathbf{X}_{aa'}\equiv\frac{1}{\sin(\theta_J)}i[i[\mathbf{E}_{n,n-1},\mathbf{C}],\mathbf{D}]=|a\rangle\langle a'|+|a'\rangle\langle a| \tag{84}$$

acts like an encoded σ_x on $|a\rangle$ and $|a'\rangle$ and annihilates all other states. Further, one can implement the commutator

$$\mathbf{Y}_{aa'}=i[\mathbf{X}_{aa'},\mathbf{D}]=i(|a\rangle\langle a'|-|a'\rangle\langle a|), \tag{85}$$

which acts like an encoded σ_y on $|a\rangle$ and $|a'\rangle$. Finally, one can construct $\mathbf{Z}_{aa'}=i[\mathbf{X}_{aa'},\mathbf{Y}_{aa'}]=|a\rangle\langle a|-|a'\rangle\langle a'|$. Thus we have shown that for $J<n/2-1$ we can validly (using only exchange Hamiltonians) perform su(2) operations between $|a\rangle$, a specific B-state, and $|a'\rangle$, its corresponding T-state, on $\mathrm{DFS}_n(J)$ only.

2. Extending the su(2)'s

We now show that by using the operation of conjugation by a unitary we can construct su(2) between any two B- and T-states. To see this recall Eq. (30), which allows one to take a Hamiltonian $\mathbf{H}$ and turn it via conjugation by a unitary gate into the new Hamiltonian $\mathbf{H}_{\mathrm{eff}}=\mathbf{UHU}^\dagger$. By the induction hypothesis we have at our disposal every SU gate which acts on the T-states of $\mathrm{DFS}_n(J)$ [and simultaneously acts on the B-states of $\mathrm{DFS}_n(J+1)$] and also every SU gate which acts on the B-states of $\mathrm{DFS}_n(J)$ [and simultaneously acts on the T-states of $\mathrm{DFS}_n(J-1)$]. Above we have shown how to construct $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{Z}$ operators between specific T- and B-states: $|a'\rangle$ and $|a\rangle$. Let $|i'\rangle$ and $|i\rangle$ be some other T- and B-states of $\mathrm{DFS}_n(J)$, respectively. Then we have at our disposal the gate $\mathbf{P}_{i'i}=|a'\rangle\langle i'|+|i'\rangle\langle a'|+|a\rangle\langle i|+|i\rangle\langle a|+\mathbf{O}$ where $\mathbf{O}$ is an operator which acts on a DFS other than $\mathrm{DFS}_n(J)$ (included to make $\mathbf{P}_{i'i}$ an SU operator). It is simple to verify that

$$\mathbf{X}_{i'i}=\mathbf{P}_{i'i}\mathbf{X}_{aa'}\mathbf{P}_{i'i}^\dagger=|i'\rangle\langle i|+|i\rangle\langle i'|, \tag{86}$$

which acts as an encoded σ_x between $|i'\rangle$ and $|i\rangle$. Note that because $\mathbf{X}_{aa'}$ only acts on $\mathrm{DFS}_n(J)$, $\mathbf{X}_{i'i}$ will also only act on the same DFS. Similarly one can construct $\mathbf{Y}_{i'i}=\mathbf{P}_{i'i}\mathbf{Y}_{aa'}\mathbf{P}_{i'i}^\dagger$ and $\mathbf{Z}_{i'i}=\mathbf{P}_{i'i}\mathbf{Z}_{aa'}\mathbf{P}_{i'i}^\dagger$ which act, respectively, as encoded σ_y and σ_z on $|i'\rangle$ and $|i\rangle$. Thus we have shown that one can implement every su(2) between any two T- and B-states in $\mathrm{DFS}_n(J)$. Each of these su(2) operations is performed independently on $\mathrm{DFS}_n(J)$.

[9] We need to subtract $|c\rangle\langle c|$ in order to obtain a traceless operator.

3. Mixing T- and B-states

Next we use a lemma proved in Appendix C:

Mixing Lemma: Given is a Hilbert space $\mathcal{H}=\mathcal{H}_1\oplus\mathcal{H}_2$ where $\dim\mathcal{H}_j=n_j$. Let $\{|i_1\rangle\}$ and $\{|i_2\rangle\}$ be orthonormal bases for $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. If one can implement the operators $\mathbf{X}_{i_1i_2}=|i_1\rangle\langle i_2|+|i_2\rangle\langle i_1|$, $\mathbf{Y}_{i_1i_2}=i|i_1\rangle\langle i_2|-i|i_2\rangle\langle i_1|$, and $\mathbf{Z}_{i_1i_2}=|i_1\rangle\langle i_1|-|i_2\rangle\langle i_2|$, then one can implement $\mathrm{su}(n_1+n_2)$ on $\mathcal{H}$.

Above we have explicitly shown that we can obtain every $\mathbf{X}_{i_1i_2}$, $\mathbf{Y}_{i_1i_2}$, and $\mathbf{Z}_{i_1i_2}$ acting independently on $\mathrm{DFS}_n(J)$. Thus direct application of the Mixing Lemma tells us that we can perform $\mathrm{su}(n_J)$ independently on this DFS.

Special case of $J=n/2-1$: We have neglected $\mathrm{DFS}_n(n/2-1)$ because it did not contain two different BT-states (nor a TT-state). The dimension of this DFS is $n-1$. We now show how to perform $\mathrm{su}(n-1)$ on this DFS using the fact that we have already established $\mathrm{su}(n_{J=n/2-2})$ on $\mathrm{DFS}_n(n/2-2)$. First, note that by the induction hypothesis we can perform $\mathrm{su}(n_{J=n/2-3/2})$ independently on $\mathrm{DFS}_{n-1}(n/2-3/2)$. As above, this action simultaneously affects $\mathrm{DFS}_n(n/2-1)$ and $\mathrm{DFS}_n(n/2-2)$. However, since we can perform $\mathrm{su}(n_{J=n/2-2})$ on $\mathrm{DFS}_n(n/2-2)$, we can subtract out the action of $\mathrm{su}(n_{J=n/2-3/2})$ on $\mathrm{DFS}_n(n/2-2)$. Thus we can obtain $\mathrm{su}(n_{J=n/2-3/2})$ on all of the B-states of $\mathrm{DFS}_n(n/2-1)$. But the exchange operator $\mathbf{E}_{n,n-1}$ acts to mix the B-states with the single T-state of $\mathrm{DFS}_n(n/2-1)$. Thus we can construct an su(2) algebra between that single-T state and a single B-state in a manner directly analogous to the above proof for $J<n/2-1$. Finally, by the enlarging lemma it follows that we can obtain $\mathrm{su}(n-1)$ on $\mathrm{DFS}_n(n/2-1)$.

This concludes the proof that the exchange interaction is independently universal on each of the different strong-collective-decoherence DFSs.

E. State preparation and measurement on the strong collective decoherence DFS

At first glance it might seem difficult to prepare pure states of a SCD-DFS, because these states are nontrivially entangled. However, it is easy to see that every DF subspace contains a state which is a tensor product of singlet states:

$$|0_D\rangle=\left(\frac{1}{\sqrt{2}}\right)^{n/2}\otimes_{j=1}^{n/2}(|01\rangle-|10\rangle), \tag{87}$$

because these states have zero total angular momentum. Thus a supply of singlet states is sufficient to prepare DF subspace states. Further, DF subsystems always contain a state which is a tensor product of a DF subspace and a pure state of the form $|1\rangle\otimes\cdots\otimes|1\rangle$. This can be seen from Fig. 4, where the lowest path leading to a specific $\mathrm{DFS}_n(J)$ is composed of a segment passing through a DF subspace (and is thus of the form $|0_D\rangle$), and a segment going straight up from there to $\mathrm{DFS}_n(J)$. The corresponding state is equivalent to adding a spin-0 (DF subspace) and a spin-J DF subsystem (the $|J,m_J=J\rangle$ state of the latter is seen to be made up entirely of $|1\rangle\otimes\cdots\otimes|1\rangle$). In general, addition of a spin-0 DFS and a spin-J DFS simply corresponds to tensoring the two states. Note, however, that addition of two arbitrary DF subsystems into a larger DFS is not nearly as simple: concatenation of two $J\neq0$ DFSs does not correspond to tensoring.

Pure state preparation for a SCD-DFS can thus be as simple as the ability to produce singlet states and $|1\rangle$ states (it is also possible to use the $|J,m_J=-J\rangle=|0\rangle\otimes\cdots\otimes|0\rangle$ or any of the other $|J,m_J\rangle$ states plus singlets). Other, more complicated pure state preparation procedures are also conceivable, and the decision as to which procedure to use is clearly determined by the available resources to manipulate quantum states. The pure state preparation of singlets and computational basis states has the distinct advantage that verification of these states should be experimentally achievable. Such verification is necessary for fault-tolerant preparation [51].

Measurements on the SCD-DFS can be performed by using the conjoined measurement scheme detailed in the WCD-DFS discussion [Sec. VI D]. In particular, by attaching a SCD-DF subspace ancilla via such conjunction, one can construct any conjoined measurement scenario. All that remains to be shown is how to perform a destructive measurement on such an ancilla. In [40,62] such schemes are presented for the $n=4$ SCD-DF subspace which encodes a single qubit of information. We will not repeat the details of these schemes here, but note that they involve measurements of single physical-qubit observables and thus are experimentally very reasonable. Further, we note that the ability to perform a conjoined measurement scenario by conjoining an ancilla DFS composed of a single encoded-qubit can be used to perform any possible conjoined DFS measurement scenario. As mentioned in the WCD case, the conjoined measurement procedures are fault-tolerant. Thus we have shown how to perform fault-tolerant preparation and decoding on the SCD-DFS.

VIII. UNIVERSAL FAULT-TOLERANT COMPUTATION ON CONCATENATED CODES

So far we have shown how to implement universal computation with local Hamiltonians on a DFS corresponding to a single block of qubits. This construction assumes that the only errors are collective. This is a very stringent symmetry requirement, which obviously becomes less realistic as the number of particles n increases significantly. It is thus desirable to be able to deal with perturbations that break the collective-decoherence (permutation) symmetry. To this end we have previously studied the effect of symmetry-breaking perturbations on decoherence-free subspaces [27], and have proposed a concatenation method to make DFSs robust in the presence of such perturbations. The method embeds DFS blocks of four particles (each block constituting a single encoded qubit) into a QECC [25]. The QECC in the outer layer then takes care of any single encoded-qubit errors on each of its constituent DFS-blocks. In fact, such a code can correct for any ''leakage'' error taking a state outside of the DFS by transforming this into a single encoded qubit error on the outer QECC. By choosing an appropriate QECC it is thus

possible to deal with any type of noncollective error on the encoded DFS-qubits. In particular, by using the ''perfect'' 5-qubit code [63] it is possible to correct all independent errors between blocks of four particles. In general, if one can robustly perform all of the operations needed to implement a fault-tolerant quantum error correcting code on an encoded subsystem, then concatenation of this subsystem into such a fault-tolerant quantum error correcting code will naturally produce fault-tolerance. Therefore concatenation can be quite generally used with DFSs to deal with symmetry breaking errors and to obtain fully fault-tolerant quantum computation, and is not limited to just the 4-qubit DFS proposed in [25].

One problem with this construction to date was that, in order to correct on the outer QECC, it is necessary to perform encoded operations on the constituent DFSs in a fault-tolerant way, using (realistic) local interactions. Specifically, it is necessary to be able to implement all single encoded-qubit operations on the DFS-qubits of the outer QECC, as well as operations between two DFS-blocks (see [51] for details). Consequently, given that one can perform single qubit (or ''qupit'' for higher-dimensional DFSs) operations on each DFS-block as we have shown earlier in this paper (Secs. VI and VII), the only additional gate necessary to implement both error-correction and universal quantum computation on a concatenated QECC-DFS is any nonseparable two-encoded-qubit gate **K** between any four states in the two DFS-blocks. One such gate is provided by a controlled-phase operation which gives a phase of -1 to $|0_L 0_L\rangle$ and leaves all other states unchanged. In fact, it is sufficient to be able to perform this gate **K** between neighboring blocks only [11,12,64]. To construct such an encoded **K** between two neighboring blocks, we assume that the corresponding physical qubits are spatially close together during the switching time of the gate. Since the symmetry of collective decoherence arises from the spatial correlation of the decoherence process, we can further assume that during this switching time, both DFS-blocks couple to the same bath mode. This assumption is physically motivated by the expectation that collective decoherence occurs in the analog of the Dicke limit of quantum optics, where the qubits have small spatial separations relative to the bath correlation length [60]. Then the two DFS-clusters temporarily form a bigger DFS and we can use the universal operations we have constructed previously on this big DFS to implement the desired gate **K**.

Another issue arising with concatenation is the ability to fault-tolerantly detect leakage errors on a DFS. Concatenation resulting in in unreliable leakage detection would be useless. However, this is not a problem here, since detection can easily be performed when one has the ability to make some fault-tolerant measurements on the DFS and also to perform universal manipulations over any combination of DFS states. Both of these are valid with the DFS-QECC concatenation, as we have summarized above. In particular, it is always possible to measure the relevant observables for leakage by (i) attaching ancilla encoded DFS states, (ii) performing the leakage syndrome detection routine onto the ancilla states, and (iii) fault-tolerantly measuring this ancilla.

We reemphasize that the fault-tolerance in our proposed scheme is not solely a result of properties of decoherence-free subsystems. Decoherence-free subsystems must be combined with quantum error correcting codes to achieve full fault tolerant quantum computation. However, until recent results [25,27], as well as the results presented in this paper, it was not clear that the methods needed to perform the operations on the decoherence-free subsystem level would not destroy the higher threshold results of the fault-tolerant quantum error correcting methods. This paper, along with previous results, demonstrates how measurements, concatenation, and computation can all be done with relative ease on a DFS in order to aid in the construction of a fully workable QECC-DFS scheme.

IX. SUMMARY AND CONCLUSIONS

In this paper we have settled the issue of quantum computation with realistic (few-body) means on both decoherence-free subspaces and decoherence-free (noiseless) subsystems (DFSs) for two important forms of decoherence: collective phase damping (''weak collective decoherence'') and collective phase damping plus collective dissipation (''strong collective decoherence''). This resolves an outstanding question as to whether universal computation on these physically relevant DFSs by using just one- and two-body Hamiltonians is possible. The answer is affirmative.

The implications of this result for the usefulness of DFSs are drastic. They put the theory of DFSs on an equal footing with the theory of quantum error correction, in that the full repertoire of universal fault tolerant quantum computation is now available on DFSs for collective decoherence which is the most important pertinent decoherence process. Moreover, the strict assumption of collective decoherence can be lifted by allowing for perturbing independent qubit errors. As we proposed earlier it is possible to stabilize DFSs against such errors by concatenation with a quantum error correcting code (QECC). However, to be able to implement error-correction and fault-tolerant universal computation on these concatenated codes a crucial (and so far missing) ingredient was the ability to perform encoded operations on the DFS-blocks fault-tolerantly. This paper settles that matter, showing constructively that DFSs can be made robust.

Furthermore, this paper reports on a general framework incorporating both DFSs and QECCs, and generalizes the theory of stabilizer codes to the (non-Abelian) DFS-case. This framework enabled us to identify the allowed operations on a DFS and to show that these operations can be performed while maintaining a very strong form of fault-tolerance: the states remain within the DFS during the entire switching time of the gate. Our formalism should be readily applicable for other nonadditive codes.

There is an interesting duality between QECCs which are designed to correct single (or greater) qubit errors and DFSs. In QECC the errors are all single body interactions. The QECC condition therefore implies that any one- or two-body Hamiltonian must take code words outside of the code space because these interactions themselves look like errors. QECCs must leave their code space in order to perform quantum computation on the encoded operations. This means

that QECCs must have gates which act much faster than the decoherence mechanism so that a perturbative treatment can be carried out. QECC can correct small errors but the price paid for this is that gates must be executed quickly (not to mention that fault-tolerant gates must also be used). DFSs on the other hand do not have the requirement of correcting single qubit errors and we have found that a single two-body interaction (exchange) is sufficient to generate universal quantum computation fault-tolerantly. DFSs have larger errors but this allows for an economy of Hamiltonians.

As corollaries to our results on weak and strong collective decoherence two additional properties of the corresponding DFS encodings appear:

(1) One can work on all DFSs in parallel: Since we are able to implement SU(d_n) on each DFS$_n$ (n=number of particles) independently, we can in principle work on all DFSs in parallel. This means that we can encode quantum information into each of the DFSs and perform calculations (possibly different) on all of them at once.

(2) For the strong collective decoherence case the exchange gate is asymptotically universal: It is well-known that the encoding efficiency of the singlet space of the strong collective decoherence-DFS for large n approaches unity [21]. More precisely, let k be the number of encoded qubits in the singlet ($J=0$) sector of a Hilbert space of n qubits, then

$$\lim_{n\to\infty}\frac{k}{n}=1-\frac{3}{2}\frac{\log_2 n}{n}. \tag{88}$$

We have established that the exchange gate alone (with an irrational phase) implements universal computation on each DFS, and on the singlet space in particular. Thus we find that, for large n, in order to achieve universal computation with nearly perfect efficiency, all we need to be able to perform is the exchange interaction. This result is very promising from an experimental point of view, since the exchange interaction is prevalent whenever there is a Heisenberg coupling between systems [28,40]. We emphasize that regardless of the decoherence mechanism, this implies that universal quantum computation can be achieved ''asymptotically'' using a single gate [62]. We conjecture that there are many more such two-body interactions which similarly provide such ''asymptotic universality'' on their own.

ACKNOWLEDGMENTS

This material is based upon work supported by the U. S. Army Research Office under Contract/Grant No. DAAG55-98-1-0371 and No. NSF DMS-9971169 (J.K.). It is a pleasure to acknowledge helpful discussions with Dr. Dorit Aharonov and Dr. Alexei Kitaev.

APPENDIX A: THE PARTIAL COLLECTIVE ANGULAR MOMENTUM OPERATORS ARE A SET OF COMMUTING OBSERVABLES

We prove here that the partial collective operators $\mathbf{S}_\alpha^k \equiv \mathbf{S}_\alpha^{(1,2,\ldots,k)}=\Sigma_{i=1}^k \sigma_\alpha^i$ form a commuting set and hence, a good operator basis. Note first that

$$(\mathbf{S}^k)^2=\sum_{i,j=1}^{k}\sum_{\alpha=x,y,z}\sigma_\alpha^i\sigma_\alpha^j. \tag{A1}$$

Thus

$$[(\mathbf{S}^k)^2,(\mathbf{S}^l)^2]=\left[\sum_{i,j=1}^{k}\sum_{\alpha=x,y,z}\sigma_\alpha^i\sigma_\alpha^j,\sum_{m,n=1}^{l}\sum_{\beta=x,y,z}\sigma_\beta^m\sigma_\beta^n\right]. \tag{A2}$$

Terms with $\alpha=\beta$ obviously commute. Further, terms with $(m=i,n=j)$, $(m=j,n=i)$, or $(i\neq m,n,j\neq m,n)$, commute, so we need only consider $(i=m,j\neq n)$, $(i=n,j\neq m)$ or $(i\neq m,j=n)$, $(i\neq n,j=m)$. In addition, assuming without loss of generality that $l\geqslant k$, terms with $m,n>k$ also commute. Thus we are left with

$$\begin{aligned}[(\mathbf{S}^k)^2,(\mathbf{S}^l)^2]=&2\sum_{i,j=1}^{k}\sum_{n(\neq j)=1}^{k}\sum_{\beta\neq\alpha=x,y,z}[\sigma_\alpha^i\sigma_\alpha^j,\sigma_\beta^i\sigma_\beta^n]\\&+2\sum_{i,j=1}^{k}\sum_{m(\neq i)=1}^{k}\sum_{\beta\neq\alpha=x,y,z}[\sigma_\alpha^i\sigma_\alpha^j,\sigma_\beta^m\sigma_\beta^j].\end{aligned} \tag{A3}$$

Using the fact that $[\sigma_\alpha^i\sigma_\alpha^j,\sigma_\beta^i\sigma_\beta^n]=i\Sigma_\gamma\varepsilon_{\alpha\beta\gamma}\sigma_\gamma^i\sigma_\alpha^j\sigma_\beta^n$ and $[\sigma_\alpha^i\sigma_\alpha^j,\sigma_\beta^m\sigma_\beta^j]=i\Sigma_\gamma\varepsilon_{\alpha\beta\gamma}\sigma_\alpha^i\sigma_\beta^m\sigma_\gamma^j$:

$$\begin{aligned}[(\mathbf{S}^k)^2,(\mathbf{S}^l)^2]=&2\sum_{i,j=1}^{k}\sum_{n(\neq j)=1}^{k}\sum_{\alpha,\beta,\gamma=\{x,y,z\}}\varepsilon_{\alpha\beta\gamma}\sigma_\gamma^i\sigma_\alpha^j\sigma_\beta^n\\&+2\sum_{i,j=1}^{k}\sum_{m(\neq i)=1}^{k}\sum_{\alpha,\beta,\gamma=\{x,y,z\}}\varepsilon_{\alpha\beta\gamma}\sigma_\alpha^i\sigma_\beta^m\sigma_\gamma^j,\end{aligned}$$

and both sums vanish due to the antisymmetric property of $\varepsilon_{\alpha\beta\gamma}$.

APPENDIX B: MAXIMAL-m_J STATES OF THE STRONG COLLECTIVE DECOHERENCE DFS

We show how to recursively express the n-particle total spin-J states in terms of $(n-1)$-particle states. Let us focus on DFS$_n(J)$ and in particular on the maximal-m_J state in it:

$$|\psi\rangle=|J_1,\ldots,J_{n-1},J;m_J=J\rangle. \tag{B1}$$

In general ($J\neq 0,n/2$) there are two kinds of states: bottom ($|\psi\rangle_{\mathrm{B}}$) and top ($|\psi\rangle_{\mathrm{T}}$) ones. The angular momentum addition rule that must be satisfied for adding a single spin-$\frac{1}{2}$ particle is that

$$m_{J_{n-1}}\pm\frac{1}{2}=m_J.$$

The B-state comes from adding a particle to the maximal m_J state in DFS$_{n-1}(J-1/2)$, which is

$$|\mathrm{B}\rangle = \left| J_1, \ldots, J_{n-2}, J-\frac{1}{2}; m_{J_{n-1}} = J-\frac{1}{2} \right\rangle. \tag{B2}$$

There is only one way to go from $|\mathrm{B}\rangle$ to $|\psi\rangle_{\mathrm{B}}$, namely to add 1/2 to $m_{J_{n-1}} = J-\frac{1}{2}$ in order to obtain $m_J = J$. Thus

$$|\psi\rangle_{\mathrm{B}} = |\mathrm{B}\rangle \left| \frac{1}{2}, \frac{1}{2} \right\rangle, \tag{B3}$$

where $|\frac{1}{2}, \frac{1}{2}\rangle$ is the single-particle spin-up state. The situation is different for the T-state, which is constructed by adding a particle to

$$|\mathrm{T}_{\pm}\rangle = \left| J_1, \ldots, J_{n-2}, J+\frac{1}{2}; m_{J_{n-1}} = J \pm \frac{1}{2} \right\rangle. \tag{B4}$$

These two possibilities give:

$$|\psi\rangle_{\mathrm{T}} = \alpha |\mathrm{T}_+\rangle \left| \frac{1}{2}, -\frac{1}{2} \right\rangle + \beta |\mathrm{T}_-\rangle \left| \frac{1}{2}, \frac{1}{2} \right\rangle. \tag{B5}$$

To find the coefficients α and β, we use the collective raising operator $\mathbf{s}_+ = \mathbf{s}_x + i\mathbf{s}_y$, where we recall that $\mathbf{s}_\alpha^{(k)} = \frac{1}{2}\Sigma_{i=1}^{k} \sigma_\alpha^i$. Since $|\psi\rangle$ is a maximal-m_J state it is annihilated by $\mathbf{s}_+ \equiv \mathbf{s}_\alpha^{(n)}$. Similarly, $|\mathrm{T}_+\rangle$ is annihilated by $\mathbf{s}_+^{(n-1)}$. Therefore since $\mathbf{s}_+ = \mathbf{s}_+^{(n-1)} + \frac{1}{2}\sigma_+^n$:

$$\mathbf{s}_+ |\mathrm{T}_+\rangle \left| \frac{1}{2}, -\frac{1}{2} \right\rangle = |\mathrm{T}_+\rangle \left| \frac{1}{2}, \frac{1}{2} \right\rangle$$

$$\mathbf{s}_+ |\mathrm{T}_-\rangle \left| \frac{1}{2}, \frac{1}{2} \right\rangle = \sqrt{2J+1} |\mathrm{T}_+\rangle \left| \frac{1}{2}, \frac{1}{2} \right\rangle,$$

where in the second line we used the elementary raising operator formula $\mathbf{J}_+ |j,m\rangle = [j(j+1) - m(m+1)]^{1/2} |j, m+1\rangle$ with $j = J + \frac{1}{2}$ and $m = J - \frac{1}{2}$. Application of $\mathbf{s}_+$ to Eq. (B5) thus yields:

$$\alpha + \sqrt{2J+1}\,\beta = 0. \tag{B6}$$

Hence up to an arbitrary phase choice, we find that

$$\alpha = -\sqrt{\frac{2J+1}{2J+2}}; \quad \beta = \frac{1}{\sqrt{2J+2}}. \tag{B7}$$

The special cases of $J = 0, n/2$ differ only in that the corresponding DFSs support just T- and B-states, respectively. The calculation of the coefficients, therefore, remains the same.

In a similar manner one can carry the calculation one particle deeper. Doing this we find for the maximal-m_J states (provided they exist):

$$\begin{aligned}
|\mathrm{TT}\rangle \equiv & \left| J_1, \ldots, J_{n-3}, J+1, J+\frac{1}{2}, J; m_J = J \right\rangle \\
= & \sqrt{\frac{2J+1}{2J+3}} |J_1, \ldots, J_{n-3}, J+1; m_{J_{n-2}} = J+1\rangle \\
& \times \left| \frac{1}{2}, -\frac{1}{2} \right\rangle \left| \frac{1}{2}, -\frac{1}{2} \right\rangle - \sqrt{\frac{2J+1}{(2J+2)(2J+3)}} \\
& \times |J_1, \ldots, J_{n-3}, J+1; m_{J_{n-2}} = J\rangle \\
& \times \left(\left| \frac{1}{2}, \frac{1}{2} \right\rangle \left| \frac{1}{2}, -\frac{1}{2} \right\rangle + \left| \frac{1}{2}, -\frac{1}{2} \right\rangle \left| \frac{1}{2}, \frac{1}{2} \right\rangle \right) \\
& + \sqrt{\frac{2}{(2J+2)(2J+3)}} \\
& \times |J_1, \ldots, J_{n-3}, J+1; m_{J_{n-2}} = J-1\rangle \left| \frac{1}{2}, \frac{1}{2} \right\rangle \left| \frac{1}{2}, \frac{1}{2} \right\rangle;
\end{aligned}$$

$$\begin{aligned}
|\mathrm{BT}\rangle \equiv & \left| J_1, \ldots, J_{n-3}, J, J+\frac{1}{2}, J; m_J = J \right\rangle \\
= & -\sqrt{\frac{2J+1}{2J+2}} |J_1, \ldots, J_{n-3}, J; m_{J_{n-2}} = J\rangle \\
& \times \left| \frac{1}{2}, \frac{1}{2} \right\rangle \left| \frac{1}{2}, -\frac{1}{2} \right\rangle + \frac{1}{\sqrt{(2J+2)(2J+1)}} \\
& \times |J_1, \ldots, J_{n-3}, J; m_{J_{n-2}} = J\rangle \left| \frac{1}{2}, -\frac{1}{2} \right\rangle \left| \frac{1}{2}, \frac{1}{2} \right\rangle \\
& + \sqrt{\frac{2J}{(2J+1)(2J+2)}} \\
& \times |J_1, \ldots, J_{n-3}, J; m_{J_{n-2}} = J-1\rangle \left| \frac{1}{2}, \frac{1}{2} \right\rangle \left| \frac{1}{2}, \frac{1}{2} \right\rangle;
\end{aligned}$$

$$\begin{aligned}
|\mathrm{TB}\rangle \equiv & \left| J_1, \ldots, J_{n-3}, J, J-\frac{1}{2}, J; m_J = J \right\rangle \\
= & -\sqrt{\frac{2J}{2J+1}} |J_1, \ldots, J_{n-3}, J; m_{J_{n-2}} = J\rangle \left| \frac{1}{2}, -\frac{1}{2} \right\rangle \\
& \times \left| \frac{1}{2}, \frac{1}{2} \right\rangle + \frac{1}{\sqrt{2J+1}} \\
& \times |J_1, \ldots, J_{n-3}, J; m_{J_{n-2}} = J-1\rangle \left| \frac{1}{2}, \frac{1}{2} \right\rangle \left| \frac{1}{2}, \frac{1}{2} \right\rangle,
\end{aligned}$$

$$\begin{aligned}
|\mathrm{BB}\rangle \equiv & \left| J_1, \ldots, J_{n-3}, J-1, J-\frac{1}{2}, J; m_J = J \right\rangle \\
= & |J_1, \ldots, J_{n-3}, J-1; m_{J_{n-2}} = J-1\rangle \left| \frac{1}{2}, \frac{1}{2} \right\rangle \left| \frac{1}{2}, \frac{1}{2} \right\rangle.
\end{aligned} \tag{B8}$$

Caution must be exercised in using these expressions near the boundary of Table I, where some of the states may not exist.

APPENDIX C: PROOFS OF THE LEMMAS

Enlarging Lemma: Let $\mathcal{H}$ be a Hilbert space of dimension d and let $|i\rangle \in \mathcal{H}$. Assume we are given a set of Hamiltonians H_1 that generates su$(d-1)$ on the subspace of $\mathcal{H}$ that does not contain $|i\rangle$, and another set H_2 that generates su(2) on the subspace of $\mathcal{H}$ spanned by $\{|i\rangle,|j\rangle\}$, where $|j\rangle$ is another state in $\mathcal{H}$. Then $[\mathsf{H}_1,\mathsf{H}_2]$ (all commutators) generates su(d) on $\mathcal{H}$ under closure as a Lie algebra.

Proof: We explicitly construct the Lie-algebra su(d) with the given Hamiltonians. Let $\tilde{\mathcal{H}} \subset \mathcal{H}$ be the $d-1$ dimensional subspace H_1 acts on. Let us show that we can generate su(2) between $|k\rangle \in \tilde{\mathcal{H}}$ and $|i\rangle$.

Let $\mathbf{X}_{ij} \equiv |i\rangle\langle j| + |j\rangle\langle i| \in \mathsf{H}_2$ and $\mathbf{X}_{jk} \equiv |j\rangle\langle k| + |k\rangle\langle j| \in \mathsf{H}_1$. Then

$$\mathbf{Y}_{ik} \equiv i[\mathbf{X}_{jk},\mathbf{X}_{ij}] = -i|i\rangle\langle k| + i|k\rangle\langle i| \tag{C1}$$

acts as σ_y on the states $|i\rangle,|k\rangle$. Similarly

$$\mathbf{X}_{ik} \equiv i[\mathbf{Y}_{ij},\mathbf{X}_{jk}] = |i\rangle\langle k| + |k\rangle\langle i| \tag{C2}$$

yields σ_x on the space spanned by $|i\rangle,|k\rangle$. These two operations generate su(2) on $|i\rangle,|k\rangle$ for all $|k\rangle$ in the subspace of $\mathcal{H}$ that does not contain $|i\rangle$. Now the Mixing Lemma gives the desired result together with the observation that there we only use elements in $[\mathsf{H}_1,\mathsf{H}_2]$.

Mixing Lemma: Consider the division of an n dimensional Hilbert space $\mathcal{H}$ into a direct sum of two subspaces $\mathcal{H}_1 \oplus \mathcal{H}_2$ of dimensions n_1 and n_2, respectively. Suppose that $|i_n\rangle$ is an orthonormal basis for $\mathcal{H}_n$. Then the Lie algebras generated by $\mathbf{X}_{i_1,i_2} = |i_1\rangle\langle i_2| + |i_2\rangle\langle i_1|$, $\mathbf{Y}_{i_1,i_2} = i|i_1\rangle\langle i_2| - i|i_2\rangle\langle i_1|$, and $\mathbf{Z}_{i_1,i_2} = |i_1\rangle\langle i_1| - |i_2\rangle\langle i_2|$ generate su(n).

Proof: We explicitly construct the elements of su(n). Consider $i[\mathbf{X}_{i_1,i_2},\mathbf{Y}_{j_1,j_2}]$. Clearly, if $i_1 \neq i_2 \neq j_1 \neq j_2$ this equals zero and if $i_1 = j_1$ and $i_2 = j_2$ then this commutator is $-\mathbf{Z}_{i_1,i_2}$. If, however, $i_1 = j_1$ and $i_2 \neq j_2$ this becomes

$$i[\mathbf{X}_{i_1,i_2},\mathbf{Y}_{i_1,j_2}] = -|i_2\rangle\langle j_2| - |j_2\rangle\langle i_2|. \tag{C3}$$

Similarly:

$$i[\mathbf{X}_{i_1,i_2},\mathbf{Y}_{j_1,i_2}] = |i_1\rangle\langle j_1| + |j_1\rangle\langle i_1|. \tag{C4}$$

Thus every $|i_k\rangle\langle j_l| + |j_l\rangle\langle i_k|$ is in the Lie algebra. Similarly, $i[\mathbf{X}_{i_1,i_2},\mathbf{X}_{j_1,j_2}]$ yields

$$i[\mathbf{X}_{i_1,i_2},\mathbf{X}_{i_1,j_2}] = i|i_2\rangle\langle j_2| - i|j_2\rangle\langle i_2|,$$

$$i[\mathbf{X}_{i_1,i_2},\mathbf{X}_{j_1,i_2}] = i|i_1\rangle\langle j_1| - i|j_1\rangle\langle i_1|. \tag{C5}$$

Thus every $i|i_k\rangle\langle j_l| - i|j_l\rangle\langle i_k|$ is in the Lie algebra. Taking the commutator of these with the $|i_k\rangle\langle j_l| + |j_l\rangle\langle i_k|$ operators finally yields every $|i_k\rangle\langle j_l| - |j_l\rangle\langle i_k|$. Since su$(n)$ can be decomposed into a sum of overlapping su(2)'s [65], the Lie algebra is the entire su(n), as claimed.

[1] P.W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1994), p. 124.

[2] L.K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[3] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[4] C.H. Bennett and P.W. Shor, IEEE Trans. Inf. Theory **44**, 2724 (1998).

[5] Abbreviations frequently used in this paper are QECC = quantum error correcting code, DFS = decoherence-free subsystem (or subspace, if no confusion can arise), WCD/SCD = weak/strong collective decoherence, and the irrep=irreducible representation.

[6] P.W. Shor, Phys. Rev. A **52**, R2493 (1995).

[7] A.M. Steane, Phys. Rev. Lett. **77**, 793 (1996).

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

[9] D. Gottesman, Phys. Rev. A **54**, 1862 (1997).

[10] P.W. Shor, in *Proceedings of the 37th Symposium on Foundations of Computing* (IEEE Computer Society Press, Los Alamitos, CA, 1996), p. 56.

[11] D. Aharonov and M. Ben-Or, in *Proceedings of the 29th Annual ACM Symposium on Theory of Computing (STOC)* (ACM, New York, 1997).

[12] D. Aharonov and M. Ben-Or, LANL Report No. quant-ph/9906129, 1999 (unpublished).

[13] A.Yu. Kitaev, Russian Math. Surveys **52**, 1191 (1996).

[14] E. Knill, R. Laflamme, and W. Zurek, Science **279**, 342 (1998).

[15] J. Preskill, Proc. R. Soc. **454**, 385 (1998).

[16] G. Palma, K. Suominen, and A. Ekert, Proc. R. Soc. London, Ser. A **452**, 567 (1996).

[17] L.-M. Duan and G.-C. Guo, Phys. Rev. Lett. **79**, 1953 (1997).

[18] L.-M. Duan and G.-C. Guo, Phys. Rev. A **57**, 737 (1998).

[19] P. Zanardi and M. Rasetti, Mod. Phys. Lett. B **11**, 1085 (1997).

[20] P. Zanardi, Phys. Rev. A **56**, 4445 (1997).

[21] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).

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

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

[24] D.A. Lidar, I.L. Chuang, and K.B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).

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

[26] D.A. Lidar, D. Bacon, J. Kempe, and K.B. Whaley, Phys. Rev. A **63**, 022306 (2001).

[27] D. Bacon, D.A. Lidar, and K.B. Whaley, Phys. Rev. A **60**, 1944 (1999).

[28] D.A. Lidar, D. Bacon, J. Kempe, and K.B. Whaley, Phys. Rev. A **61**, 052307 (2000).

[29] M. Durdevich, H.E. Makaruk, and R. Owczarek, LANL Report No. quant-ph/0003134, 2000 (unpublished).

[30] P. Zanardi and F. Rossi, Phys. Rev. Lett. **81**, 4572 (1998).
[31] P. Zanardi and F. Rossi, Phys. Rev. B **59**, 8170 (1999).
[32] L. Viola and S. Lloyd, Phys. Rev. A **58**, 2733 (1998).
[33] L. Viola, E. Knill, and S. Lloyd, Phys. Rev. Lett. **82**, 2417 (1999).
[34] L.-M. Duan and G. Guo, LANL Report No. quant-ph/9807072, 1998 (unpublished).
[35] P. Zanardi, Phys. Lett. A **258**, 77 (1999).
[36] P. Zanardi, Phys. Rev. A **63,** 012301 (2001).
[37] P. Zanardi, Phys. Rev. A **60**, R729 (1999).
[38] A. Beige, D. Braun, and P.L. Knight, New J. Phys. **2** (2000).
[39] A. Beige, D. Braun, B. Tregenna, and P.L. Knight, Phys. Rev. Lett. **85**, 1762 (2000).
[40] D. Bacon, J. Kempe, D.A. Lidar, and K.B. Whaley, Phys. Rev. Lett. **85**, 1758 (2000).
[41] D. Deutsch, A. Barenco, and A. Ekert, Proc. R. Soc. London, Ser. A **449**, 669 (1995).
[42] A. Barenco, Proc. R. Soc. London, Ser. A **449**, 679 (1995).
[43] D. P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).
[44] S. Lloyd, Phys. Rev. A **75**, 346 (1995).
[45] T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995).
[46] D. P. DiVincenzo, D. Bacon, J. Kempe, G. Burkard, and K. B. Whaley, Nature (London) **408**, 339 (2000).
[47] L. Duan and G. Guo, Phys. Lett. A **255**, 209 (1999).
[48] E. Knill, R. Laflamme, and L. Viola, Phys. Rev. Lett. **84**, 2525 (2000).
[49] L. Viola, E. Knill, and S. Lloyd, Phys. Rev. Lett. **85**, 3520 (2000).
[50] H. Carmichael, *An Open Systems Approach to Quantum Optics*, No. m18 in Lecture Notes in Physics (Springer-Verlag, Berlin, 1993).
[51] D. Gottesman, Phys. Rev. A **57**, 127 (1997).
[52] G. Lindblad, Commun. Math. Phys. **48**, 119 (1976).
[53] R. Alicki and K. Lendi, *Quantum Dynamical Semigroups and Applications*, No. 286 in Lecture Notes in Physics (Springer-Verlag, Berlin, 1987).
[54] S. De Filippo, Phys. Rev. A **62**, 052307 (2000).
[55] N.P. Landsman, LANL Report No. math-ph/9807030, 1998 (unpublished).
[56] K. Kraus, *States, Effects and Operations*, *Fundamental Notions of Quantum Theory* (Academic, Berlin, 1983).
[57] L.-M. Duan and G.-C. Guo, Phys. Rev. A **57**, 737 (1998).
[58] J.P. Paz and W.H. Zurek, Proc. R. Soc. London, Ser. A **454**, 355 (1998).
[59] D. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[60] R.H. Dicke, Phys. Rev. **93**, 99 (1954).
[61] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, New York, 1995).
[62] D. P. DiVincenzo, G. Burkard, D. Loss, and E.V. Sukhorukov, in *Quantum Mesoscopic Phenomena and Mesoscopic Devices in Microelectronics.*, edited by I.O. Kulk and R. Ellialtioglu (NATO Advanced Study Institute, Turkey, 1999).
[63] R. Laflamme, C. Miquel, J.P. Paz, and W.H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[64] D. Gottesman, J. Mod. Opt. **47**, 333 (2000).
[65] R.N. Cahn, *Semi-Simple Lie Algebras and Their Representations* (Benjamin/Cummings, Reading, MA, 1984), available online at http://www-physics.lbl.gov/rncahn/book.html.