Numerical method for finding decoherence-free subspaces and its applications

Xiaoting Wang, Mark Byrd, and Kurt Jacobs

Phys. Rev. A **87**, 012338 — Published 31 January 2013

DOI: 10.1103/PhysRevA.87.012338

Numerical method for finding decoherence-free subspaces and its applications

Xiaoting Wang[1], Mark Byrd[2], and Kurt Jacobs[1,3,4]
[1]*Department of Physics, University of Massachusetts at Boston, Boston, MA 02125, USA*
[2]*Physics Department & Computer Science Department, Southern Illinois University, Carbondale, Illinois 62901*
[3] *Advanced Science Institute, RIKEN, Wako-shi 351-0198, Japan*
[4]*Hearne Institute for Theoretical Physics, Louisiana State University, Baton Rouge, LA 70803, USA*
(Dated: December 20, 2012)

In this work, inspired by the study of semidefinite programming for block-diagonalizing matrix *-algebras, we propose an algorithm that can find the algebraic structure of decoherence-free subspaces (DFS's) for a given noisy quantum channel. We prove that this algorithm will work for all cases with probability one, and it is more efficient than the algorithm proposed by Holbrook, Kribs, and Laflamme [Quant. Inf. Proc. **80**, 381 (2003)]. In fact, our results reveal that this previous algorithm only works for special cases. As an application, we discuss how this method can be applied to increase the efficiency of an optimization procedure for finding an approximate DFS.

PACS numbers: 03.65.Yz, 03.67.-a, 03.67.Pp

I. INTRODUCTION

Decoherence and other noises cause errors in quantum information processing. Several methods have been proposed to significantly reduce these errors [1], such as quantum error correcting codes [2–8], decoherence-free/noiseless subsystems (DFS's) [9–19], and dynamical decoupling (DD) [20–26]. However, dynamical decoupling controls often do not satisfy the strict experimental requirements and quantum error correcting codes, while possibly protecting against any error, require a large resource overhead. Decoherence-free subspaces, or noiseless subsystems, can reduce overhead since they do not require detecting and correcting errors but are difficult to identify and use.

In terms of the (Krauss) operator-sum representation, the noisy quantum evolution can be fully characterized by a set of operators that generate a noise algebra $\mathcal{A}$. The structure of a DFS can be recovered by studying the algebraic structure of $\mathcal{A}$, or its commutant algebra $\mathcal{A}'$, both of which are special examples of a so-called $\mathbb{C}^*$-algebra, or matrix $*$-algebra [27]. Although DFS's can be obtained analytically for certain noisy systems, this is not possible in general. In [28] a numerical algorithm is proposed in which the noise algebra $\mathcal{A}$ is used to calculate the commutant algebra $\mathcal{A}'$ and decompose it into the algebraic form which gives the structure of all DFS's if any exist. However, we find that this algorithm is incomplete although useful for the special solutions of the basis of $\mathcal{A}'$ as chosen in [28]. In practice, in most of the cases, computers will pick up other solutions in which their algorithm does not give the complete decomposition. Because of this we were motivated to find a new algorithm that provides a general algorithm which can be explicitly implemented to give the required decomposition.

In fact, since $\mathcal{A}$ and $\mathcal{A}'$ are special examples of a matrix $*$-algebra, we can try to solve the more general problem of how to decompose an arbitrary matrix $*$-algebra. We find that this problem is equivalent to that of simultaneously block-diagonalizing a matrix $*$-algebra, and this has been well-studied in research on semidefinite programming [29, 30]. In particular, in [29], a numerical method was proposed to find the finest block-diagonalization of the algebra generated by real symmetric matrices. Their method consists of two steps. First, decompose the algebra into simple components, and second, decompose each simple component into irreducible components (the details of this procedure will be clarified in the following). In this work, we will show that such a two-step algorithm can also be applied to the algebra generated by Hermitian matrices, such as $\mathcal{A}$ and $\mathcal{A}'$. We will also give analysis and proofs to show the validity of this algorithm. As applications, we apply our new algorithm to the collective-noise model in [28], and compare the numerical results with the algorithm proposed there. We find that our improved algorithm is not only *valid in general*, but is also more *efficient*: it requires fewer conditional loops, and requires only $\mathcal{A}$ or $\mathcal{A}'$ alone, rather than both [28].

The paper is organized as follows: in Section II, we introduce the matrix *-algebra $\mathcal{A}$ generated by noise operators for a given quantum channel, and the Wedderburn decomposition for a DFS. In Section III, we present an algorithm to transform $\mathcal{A}$ into the Wedderburn form using two steps. Finally in Section IV, for the collective-noise model, we numerically implement and compare our algorithm with the one proposed in [28]. We will also briefly discuss how our algorithm can be used to find a good initial point for the optimization process in searching for an approximate DFS.

II. ALGEBRAIC STRUCTURE OF A NOISE ALGEBRA

A. Noise Algebra for a Noisy Quantum Channel

Let ρ be the density operator of an n-dimensional quantum system with Hilbert space $\mathcal{H}$. In real physical

systems, the evolution of ρ suffers from noise due to its interaction with the environment. Such noisy evolution can be represented as a quantum channel $\mathcal{E}$: $\rho \to \mathcal{E}(\rho)$, where $\mathcal{E}$ is characterized by a set of operators $\{A_k\}$, $j = 1, \ldots, p$:

$$\mathcal{E}(\rho) = \sum_{k=1}^{p} A_k \rho A_k^\dagger = p_0 \rho + \sum_{k=2}^{p} A_k \rho A_k^\dagger, \quad \sum_k A_k^\dagger A_k = \mathbb{I}.$$

This is often referred to as the Kraus operator-sum representation [31], where $\{A_k\}$ can include a Hamiltonian as well as irreversible coupling to a Markovian bath. In the following, we will assume the Hamiltonian $H = 0$ and only focus on the noise effect on ρ. In this case the $\{A_k\}$ contain information purely about the noise, and are known as noise operators. For many channels, we have $A_1 = \sqrt{p_0}\mathbb{I}$, where p_0 represents the probability that no error occurs. The noisy channel is referred to as *unital* if $\mathcal{E}(\mathbb{I}) = \sum_k A_k A_k^\dagger = \mathbb{I}$. Define the *noise algebra* $\mathcal{A}$ to be the $\mathbb{C}^*$-algebra, or the matrix $*$-algebra generated by $\{A_k\}$. The definition of a matrix $*$-algebra simply implies that $\mathcal{A}$ is closed under matrix summation, multiplication and $\dagger$-operation. The reason why we introduce the concept of a matrix $*$-algebra is that it can be decomposed into a nice algebraic structure, with details in the following.

B. Wedderburn Decomposition for a DFS

For a general ρ, $\mathcal{E}(\rho) \neq \rho$, and thus the quantum information stored in ρ will not be preserved by the noise. It may be possible, however, find a subspace or subsystem in some space $\mathcal{H}_1 \in \mathcal{H}$ such that for $\rho \in \mathcal{H}_1$, $\mathcal{E}(\rho) = \rho$. If so $\mathcal{H}_1$ is called a decoherence free subspace or subsystem (DFS). Notice that for a unital channel $\mathcal{E}$, if $[\rho, A_k] = 0$, for all k, then $\mathcal{E}(\rho) = \rho$. Hence to locate a DFS it is enough to study the commutant of $\mathcal{A}$, which is defined to be

$$\mathcal{A}' = \{B | [B, A] = 0,\ A \in \mathcal{A}\},$$

and is also a matrix $*$-algebra. Applying the Wedderburn-Artin theorem[27, 32] to a special case, it can be shown that every matrix $*$-algebra with an identity has the following fundamental structure decomposition [32, 33]:

Theorem 1. *(Wedderburn decomposition) Let $\mathcal{A} \subseteq \mathbb{C}^{n\times n}$ be a matrix $*$-algebra with an identity. Then there exists a unitary transformation U such that $U^\dagger \mathcal{A} U$ has a block-diagonal structure:*

$$U^\dagger \mathcal{A} U = \mathrm{diag}(\mathcal{N}_1, \mathcal{N}_2, \cdots, \mathcal{N}_\ell)$$

where each $\mathcal{N}_i$ corresponds to a simple subalgebra component. Moreover, $\mathcal{N}_i$ has the following block-diagonal structure:

$$\mathcal{N}_i = \{\mathrm{diag}(M_i, \cdots, M_i),\ M_i \in \mathcal{M}_{n_i}\} = \mathcal{M}_{n_i} \otimes \mathbb{I}_{m_i} \tag{1}$$

where $\mathcal{M}_{n_i}$ denotes the $n_i \times n_i$ matrix $*$-algebra over the complex field $\mathbb{C}$.

Here $\mathcal{N}_i = \mathcal{M}_{n_i} \otimes \mathbb{I}_{m_i}$ is an algebra different from $\mathcal{M}_{n_i} \oplus \cdots \oplus \mathcal{M}_{n_i}$. Applying Theorem 1 to the conjugates $\mathcal{A}$ and $\mathcal{A}'$, we can find some unitary U such that:

$$U^\dagger \mathcal{A} U = \bigoplus_i^\ell \mathcal{N}_i = \bigoplus_i^\ell \mathcal{M}_{n_i} \otimes \mathbb{I}_{m_i}, \tag{2a}$$

$$U^\dagger \mathcal{A}' U = \bigoplus_i^\ell \mathcal{N}_i' = \bigoplus_i^\ell \mathbb{I}_{n_i} \otimes \mathcal{M}_{m_i}. \tag{2b}$$

Mathematically, each $\mathcal{N}_i$, $i = 1, \cdots, \ell$, corresponds to a simple component of $\mathcal{A}$, while the subblock M_i at each diagonal position corresponds to an irreducible component.

Assume that there exists some $m_i > 1$, and call this m_k. We can encode an arbitrary m_k-dimensional state $\bar{\rho}$ into $\rho = \mathbb{I}_{n_k} \otimes \bar{\rho} \oplus 0_{res} \in \mathcal{A}'$ such that $\mathcal{E}(\rho) = \rho$, where 0_{res} represents the zero density operator on the rest of the Hilbert space with respect to $\mathbb{I}_{n_i} \otimes \bar{\rho}$. Hence, if we find the Wedderburn decomposition for $\mathcal{A}$ or $\mathcal{A}'$, then each $\mathcal{N}_i$ with $m_i > 1$ corresponds to a decoherence-free subsystem (which reduces to a decoherence-free subspace if $n_i = 1$). Moreover, since $\mathcal{A}$ and $\mathcal{A}'$ obey the commutant relation given in Eq.(2), we do not need both the decompositions for $\mathcal{A}$ and $\mathcal{A}'$; one will suffice.

III. NUMERICAL ALGORITHM TO OBTAIN THE WEDDERBURN DECOMPOSITION

To find the Wedderburn decomposition for a quantum channel given by a group of noise operators $\{A_k\}$, it is sufficient to find the unitary transform U such that $\mathcal{A}$ and $\mathcal{A}'$ are simultaneously block-diagonalized into the decomposition in Eq. (2). An algorithm to do this for real symmetric A_k is given in [29]. Here we construct an equivalent algorithm that we prove works for Hermitian A_k. This is sufficient for our purposes, because while the noise operators A_k need not be Hermitian, we can always replace a non-Hermitian operator A_j with the two Hermitian operators $A_j^{(1)} = A_j + A_j^\dagger$ and $A_j^{(2)} = i(A_j - A_j^\dagger)$ and still have a generating set for the algebra $\mathcal{A}$. For simplicity we simply assume that all the A_k are Hermitian and form a basis for $\mathcal{A}$. The advantage of choosing an Hermitian basis will be clear in the following analysis.

The algorithm breaks into two steps:

Algorithm 1. *(Wedderburn decomposition) Let $\mathcal{A} \subseteq \mathbb{C}^{n\times n}$ be a matrix $*$-algebra with an identity, and A a "generic" element of $\mathcal{A}$ ("generic" is defined below).*
Step 1: *Find the unitary transform V such that*

$$V^\dagger A V = \mathrm{diag}(\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_\ell), \tag{3}$$

where each $\mathcal{C}_i$ corresponds to some representation of the simple component $\mathcal{N}_i$ in (2).

Step 2: *Find the local unitary transform P such that within each $\mathcal{C}_i$, $P^\dagger V^\dagger A V P$ is equal to $\mathcal{N}_i = \mathcal{M}_{n_i} \otimes \mathbb{I}_{m_i}$. Then $U \equiv VP$ is the required unitary transform for the Wedderburn decomposition.*

To implement the two steps above one picks a single operator $A \in \mathcal{A}$, and diagonalizes A to find the required decompositions. Due to the decomposition in Eq. (2), we know that there exists a unitary transformation $\bar{V}$ such that for $A \in \mathcal{A}$,

$$\bar{V}^\dagger A \bar{V} = \bigoplus_i^\ell (\mathbb{I}_{m_i} \otimes D_i), \tag{4}$$

where the D_i are diagonal matrices whose elements are the eigenvalues of A. To obtain the spaces spanned by the simple algebras from this eigenvalue decomposition, we need to pick an A such that the $D_1, \ldots, D_\ell$ do not share any eigenvalues, and the eigenvalues in each D_i are distinct. Note that A will have this property if it has the maximum possible number of distinct eigenvalues. It can be shown [29] that the set of operators that have this maximum number of distinct eigenvalues is topologically dense in $\mathcal{A}$, and so we will refer to such A as being *generic*. If we randomly choose A from $\mathcal{A}$ using a suitable measure, it will be generic with probability 1. A simple way to generate a generic A is to choose a random vector $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_k)$ and generate $A = \sum_{j=1}^k \alpha_j A_j$.

After picking a generic A, we diagonalize A and obtain the distinct eigenvalues, λ_j, and their multiplicities, k_j, $j = 1, \ldots, q$. We then group these eigenvalues and write down the eigenspace decomposition according to their multiplicities in a non-decreasing order:

$$V^\dagger A V = \mathrm{diag}(\lambda_1 \mathbb{I}_{k_1}, \lambda_2 \mathbb{I}_{k_2}, \cdots, \lambda_q \mathbb{I}_{k_q}) \tag{5}$$

with $V = (V_1, V_2, \ldots, V_q)$ where each V_j is composed of the eigenvectors corresponding to the eigenspace of λ_j. We can further define a new division of V: $V = (K^{(1)}, K^{(2)}, \cdots, K^{(s)})$ where each $K^{(r)}$ is the union of all eigenspaces V_j with the same multiplicity p_r:

$$K^{(r)} = \bigoplus_{k_j = p_r} V_j$$

where $p_1 < p_2 < \cdots < p_s$ are the distinct multiplicities of the eigenvalue α_j's.

By Theorem 1, each V_j will lie in some simple component $\mathcal{N}_i$, $i = 1, \ldots, \ell$. Due to the form of $\mathcal{N}_i = \mathcal{M}_{n_i} \otimes \mathbb{I}_{m_i}$, we immediately know that only V_j's within the same $K^{(r)}$ can belong to the same $\mathcal{N}_i$, and V_j's in different $K^{(r)}$'s must belong to different $\mathcal{N}_i$'s. Hence, each $K^{(r)}$ must either be some $\mathcal{N}_i$, or a direct sum of a few $\mathcal{N}_i$'s, in which case $K^{(r)}$ can be further decomposed. In either case $\mathcal{A}$ is block-diagonalized over the division $V = (K^{(1)}, K^{(2)}, \cdots, K^{(s)})$.

There is a simple method to check whether $K^{(r)}$ can be further decomposed: we choose another randomly generated $\bar{A} = \sum_{j=1}^k \beta_j A_j \in \mathcal{A}$. Since $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are independent, with probability 1, A and $\bar{A}$ will generate the whole algebra $\mathcal{A}$. As we have pointed out, both A and $\bar{A}$ are block-diagonalized over the division $(K^{(1)}, K^{(2)}, \cdots, K^{(s)})$. If there exist V_j and $V_{j'}$ within some $K^{(r)}$ such that $V_j^\dagger \bar{A} V_{j'} = 0$, then $\bar{A}$ can be further block-diagonalized on $K^{(r)}$ over the division between V_j and $V_{j'}$. In this way, by checking the value of $V_j^\dagger \bar{A} V_{j'}$ between all different j and j' on each $K^{(r)}$, we can identify the structure of each $\mathcal{N}_i$ in each $K^{(r)}$, and finally make both A and $\bar{A}$ simultaneously block-diagonalized over $\oplus_i \mathcal{N}_i$. Since A and $\bar{A}$ will generate $\mathcal{A}$ with probability 1, we can claim that the whole algebra $\mathcal{A}$ has been simultaneously block-diagonalized over $\oplus_i \mathcal{N}_i$. However, we should notice that within each sub-block $\mathcal{N}_i$, $\mathcal{A}$ may not be the same as $\mathcal{M}_{n_i} \otimes \mathbb{I}_{m_i}$, but some representation of it, so we will instead denote the sub-block by $\mathcal{C}_i$. Thus we have obtained a V that transforms $\mathcal{A}$ into the form of Eq. (3). In particular this V has already transformed the generic A into the Wedderburn form:

$$V^\dagger A V = \bigoplus_i^\ell (D_i \otimes \mathbb{I}_{m_i}), \tag{6}$$

where D_i is a diagonal matrix with all distinct eigenvalues of A on each $\mathcal{C}_i$.

Now we note that $V^\dagger \bar{A} V$ is usually not in the form of $\mathcal{N}_i$ on $\mathcal{C}_i$. In the next step, we are looking for a further unitary transform that leaves $V^\dagger A V$ invariant but transforms $V^\dagger \bar{A} V$ into the form of $\mathcal{N}_i$ on each $\mathcal{C}_i$. Without loss of generality, let us focus on a simple component $\mathcal{C}_i$ which is composed of a few eigenspaces V_j of A:

$$\mathcal{C}_i = V_1^{(i)} \oplus V_2^{(i)} \oplus \cdots \oplus V_{m_i}^{(i)}$$

If according to the division $\oplus_i \mathcal{C}_i$, we define a local unitary transform P to be:

$$P \equiv \mathrm{diag}(P^{(1)}, P^{(1)}, \cdots, P^{(\ell)}) \tag{7}$$

$$P^{(i)} \equiv \mathrm{diag}(P_1^{(i)}, P_2^{(i)}, \cdots, P_{m_i}^{(i)}) \tag{8}$$

where $P_j^{(i)}$ is a unitary matrix on the subspace $V_j^{(i)}$, then such P will leave $V^\dagger \bar{A} V$ invariant. Moreover, the following result is proved in Proposition 3.7 in [29]:

Theorem 2. *For A and V satisfying (6), there exists a local unitary transform P as in (7) such that $P^\dagger V^\dagger \mathcal{A} V P = \oplus_i (\mathcal{M}_{n_i} \otimes \mathbb{I}_{m_i})$.*

Hence, it is possible to construct a local unitary Q (which may not be equal to P) in the form of Eq. (7) such that $\bar{Q}^\dagger V^\dagger \mathcal{A} V \bar{Q}$ is in the Wedderburn form. Before we design the required Q, we would like to find out what the matrix of $V^\dagger \bar{A} V$ looks like on $\mathcal{C}_i$ after the transform V. Notice that since Theorem 2 only claims the existence of such P, the local transform Q we finally construct may look either the same as, or different from P.

A matrix is called a *scalar matrix* if it is equal to a scalar times an identity matrix. On each $\mathcal{C}_i$, as a corollary of Theorem 2, we have

$$\bar{A}_{j,j'} \equiv (V^\dagger \bar{A} V)^{(i)}_{j,j'} = V_j^{(i)\dagger} \bar{A} V_{j'}^{(i)} = k_{j,j'} P_j^{(i)} P_{j'}^{(i)\dagger} \quad (9)$$

For $j = j'$, $\bar{A}_{j,j'}$ is equal to $k_{j,j}\mathbb{I}_{m_i}$ (that is, the diagonal sub-blocks of $(V^\dagger \bar{A} V)^{(i)}$ are already in scalar-matrix form). For $j \neq j'$ the off-diagonal sub-blocks $\bar{A}_{j,j'}$ may or may not be in this form. Our next goal is to find a local transform Q in the form of (7) such that $(Q^{(i)\dagger}(V^\dagger \bar{A} V)^{(i)} Q^{(i)})_{j,j'}$ are in scalar-matrix form for all j and j'.

On each $\mathcal{C}_i$, we can sequentially construct each $Q_j^{(i)}$ in $Q^{(i)} \equiv \mathrm{diag}(Q_1^{(i)}, Q_2^{(i)}, \cdots, Q_{m_i}^{(i)})$. First, choose $Q_1^{(i)} = \mathbb{I}_{m_i}$. Then for $j \geq 2$ define

$$\hat{Q}_j^{(i)} = \left(V_1^{(i)\dagger} \bar{A} V_j^{(i)}\right)^{-1} Q_1^{(i)}, \quad (10a)$$

$$Q_j^{(i)} = \frac{1}{||q_j||} \hat{Q}_j^{(i)}, \quad (10b)$$

where q_j is the first row of $\hat{Q}_j^{(i)}$. We now prove that this $Q^{(i)}$ is the required unitary transform.

Theorem 3. *$Q_j^{(i)}$ as defined in (10) are unitary matrices, and $Q^{(i)} \equiv \mathrm{diag}(Q_1^{(i)}, Q_2^{(i)}, \cdots, Q_{m_i}^{(i)})$ is the unitary transform such that ${Q_j^{(i)}}^\dagger (V^\dagger \bar{A} V)^{(i)}_{j,j'} Q_{j'}^{(i)}$ are scalar matrices.*

Proof. To show $Q_j^{(i)}$ is a unitary matrix, it is sufficient to show $\hat{Q}_j^{(i)} \hat{Q}_j^{(i)\dagger}$ is in scalar-matrix form. For $j \geq 2$, from (9), we have:

$$\begin{aligned} \hat{Q}_j^{(i)} \hat{Q}_j^{(i)\dagger} &= (k_{1,j} P_1^{(i)} P_j^{(i)\dagger})^{-1} (k_{1,j}^* P_j^{(i)} P_1^{(i)\dagger})^{-1} \\ &= |k_{1,j}|^{-2} \left(P_j^{(i)} P_1^{(i)\dagger} P_1^{(i)} P_j^{(i)\dagger}\right)^{-1} = |k_{1,j}|^{-2} \mathbb{I}_{m_i} \end{aligned}$$

Hence, after normalization, $Q_j^{(i)}$ becomes a unitary matrix. In addition,

$$\begin{aligned} &{Q_j^{(i)}}^\dagger (V^\dagger \bar{A} V)^{(i)}_{j,j'} Q_{j'}^{(i)} = {Q_j^{(i)}}^\dagger k_{j,j'} P_j^{(i)} P_{j'}^{(i)\dagger} Q_{j'}^{(i)} \\ =& k_{j,j'} / (k_{1,j}^* k_{1,j'}) P_1^{(i)} P_j^{(i)\dagger} P_j^{(i)} P_{j'}^{(i)\dagger} P_{j'}^{(i)} P_1^{(i)\dagger} \\ =& k_{j,j'} / (k_{1,j}^* k_{1,j'}) \mathbb{I}_{m_i}, \end{aligned}$$

and so all sub-blocks are in the scalar-matrix form. □

Numerically, following Eq. (10), we can construct the local unitary transform Q in the form of Eq. (7) that leave A invariant but transforms $\bar{A}$ into the form $\oplus_i (M_{n_i} \otimes \mathbb{I}_{m_i})$. Since $\mathcal{A}$ is generated by A and $\bar{A}$, we can claim that the whole algebra $\mathcal{A}$ is in the Wedderburn form after the unitary transform $U \equiv VQ$. We summarize the full algorithm in Table I.

When implementing the algorithm for a given noisy channel, we can calculate the Wedderburn form for either $\mathcal{A}$ or $\mathcal{A}'$, depending on which one is easier to derive.

Step 1:	(a) from $\mathcal{A}$, pick two generic matrices A and $\bar{A}$
	(b) diagonalize A and $\bar{A}$ to get V as in Eq. (5)
	(c) find the structure of $\mathcal{N}_i$ in $K^{(r)}$, getting Eq. (6)
Step 2:	(d) build the local transform Q using Eq. (10)
	(e) $U = VQ$ is the required unitary in Eq. (2)

TABLE I. Algorithm to find U in the decomposition Eq. (2).

Notice that for special cases when $\mathcal{N}_i = \mathcal{M}_k \otimes \mathbb{I}_1$, or $N_i = \mathbb{I}_k$, after Step 1 in Algorithm 1, $\mathcal{C}_i$ will already be the same as $\mathcal{N}_i$. For such cases, there is no need to implement Step 2, and we can simply choose $Q^{(i)} = \mathbb{I}$ on $\mathcal{N}_i$.

IV. APPLICATIONS

A. Finding the DFS Structure of a Channel

The primary application for the above algorithm is deriving the DFS structure for a given noisy quantum channel, and finding the corresponding unitary transform U in Eq. (2). First of all, let's reinvestigate the collective noise model calculated in [28]. For a system with n_q qubits, we say a quantum channel $\mathcal{E}$ is under collective noise if

$$\begin{aligned} \mathcal{E}(\rho) &= A_x \rho A_x^\dagger + A_y \rho A_y^\dagger + A_z \rho A_z^\dagger, \\ A_k &= \frac{1}{\sqrt{3}} e^{iS_k}, \quad k = x, y, z, \end{aligned}$$

where

$$S_x = \sum_{i=1}^{n_q} X_i, \quad S_y = \sum_{i=1}^{n_q} Y_i, \quad S_z = \sum_{i=1}^{n_q} Z_i$$

are sums of local Pauli operators on each qubit. For such a noisy channel, we can define the algebra generated by the noise operators by

$$\begin{aligned} \mathcal{A} &\equiv \mathrm{span}\{A_x, A_y, A_z\} = \mathrm{span}\{S_x, S_y, S_z\}, \\ &= \mathrm{span}\{S_x, S_y\} = \mathrm{span}\{S_y, S_z\} = \mathrm{span}\{S_x, S_z\}, \end{aligned}$$

We would like to find the Wedderburn decomposition of $\mathcal{A}$ or $\mathcal{A}'$ in the form of Eq. (2). Notice that since the collective noise channel is a special type of noisy channel, we can actually derive the the fundamental decomposition by using Young diagrams for the addition of angular momentum for any value of n_q [34]. For example, for $n_q = 3$, $\mathcal{A} = (\mathcal{M}_2 \otimes \mathbb{I}_2) \oplus \mathcal{M}_4$; for $n_q = 4$, $\mathcal{A} = \mathbb{I}_2 \oplus (\mathcal{M}_3 \otimes \mathbb{I}_3) \oplus \mathcal{M}_5$. However, theory does not give a specific basis for the operators $\mathcal{A}$, and must identify one numerically. In the following, we shall apply both the algorithm suggested in [28] and the above Algorithm 1 to the collective noise channel and compare the numerical results.

In the algorithm suggested by [28], we need to first calculate each B_j in $\mathcal{A}' = \text{span}\{B_1, \ldots, B_r\}$, where $\{B_j\}$ form a basis for $\mathcal{A}'$. Next, based on the operators $\{B_j\}$, $j = 1, \cdots, r$, we find a group of so-called minimal-reducing projectors P_j, and then block-diagonalize $\mathcal{A}'$ into the form $\text{diag}(\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_\ell)$, where $\mathcal{C}_i$ is a representation of $\mathcal{N}_i \equiv \mathcal{M}_{n_i} \otimes \mathbb{I}_{m_i}$. Then after reshuffling the order of basis vectors, all the diagonal sub-blocks are transformed into the scalar-matrix form. It is then claimed in [28] that the whole algebra $\mathcal{A}'$ is in the form of Eq. (2).

If we compare the algorithm in [28] with the algorithm in Table I, we find that the former achieves Step 1, but Step 2 is missing. Step 2 turns out to be necessary for most cases, since the solution $\{B_j\}$ as the set of basis $\mathcal{A}'$ is not unique. It is true that for the $\{B_j\}$ chosen in [28], Step 1 and reshuffling of basis vectors are enough to transform $\mathcal{A}'$ into the form of (2), but such choice of $\{B_j\}$ is very special. A different solution for the $\{B_j\}$ will be obtained it is derived numerically by solving the system of linear equations $[B_j, A_k] = 0$, $k = 1, \cdots, p$.

As an example of the necessity of step 2, consider for $n_q = 4$, and $\mathcal{A}' = \mathcal{M}_2 \oplus (\mathcal{M}_3 \otimes \mathbb{I}_3) \oplus \mathbb{I}_5$. Following the algorithm in [28] and using Matlab, we derive a group of 14 orthonormal basis matrices in $\mathcal{A}'$ ($\{B_j\}$, $j = 1, \cdots, 14$) which are different from those in [28]. Then we find the corresponding minimal-reducing projectors P_m, $m = 1, \cdots, 6$, in which $\text{rank}(P_1) = \text{rank}(P_2) = 1$ corresponding to the $\mathcal{N}_1 = \mathcal{M}_2$ subspace, $\text{rank}(P_6) = 5$ corresponding to the $\mathcal{N}_3 = \mathbb{I}_5$ subspace, and $\text{rank}(P_i) = 3$, $i = 3, 4, 5$, corresponding to the $\mathcal{N}_2 = \mathcal{M}_3 \otimes \mathbb{I}_3$ subspace. Hence, $\{P_m\}$ induces a unitary transform V such that $V^\dagger \mathcal{A}' V$ is in the form $\text{diag}(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$, where $\mathcal{C}_1 = \mathcal{N}_1$, $\mathcal{C}_3 = \mathcal{N}_3$, and $\mathcal{C}_2$ is some representation of $\mathcal{N}_2$. After reshuffling the basis vectors we can make the three diagonal sub-blocks of $V^\dagger B_j V$ on $\mathcal{C}_2$ in the scalar-matrix form.

Specifically, if we still denote $V^\dagger B_1 V$ as B_1, then after reshuffling, on $\mathcal{C}_2$ we have

$$B_1 = \begin{pmatrix} -0.167\mathbb{I}_3 & B_{1,2} & B_{1,3} \\ B_{1,2}^\dagger & 0.233\mathbb{I}_3 & B_{2,3} \\ B_{1,3}^\dagger & B_{2,3}^\dagger & 0.308\mathbb{I}_3, \end{pmatrix}$$

where

$$B_{1,2} = \begin{pmatrix} -0.180 + 0.089i & -0.120 - 0.242i & -0.042 + 0.063i \\ 0.097 + 0.169i & 0.103 - 0.001i & -0.259 + 0.059i \\ 0.193 - 0.060i & -0.100 - 0.159i & -0.051 - 0.200i \end{pmatrix},$$

$$B_{1,3} = \begin{pmatrix} -0.074 + 0.136i & 0.055 + 0.047i & 0.072 + 0.055i \\ -0.003 + 0.087i & -0.094 + 0.080i & -0.074 - 0.095i \\ -0.066 + 0.039i & 0.087 - 0.0960i & -0.114 - 0.041i \end{pmatrix},$$

$$B_{2,3} = \begin{pmatrix} -0.030 - 0.078i & -0.020 - 0.068i & -0.067 + 0.180i \\ -0.118 + 0.099i & 0.139 + 0.050i & -0.037 + 0.045i \\ -0.133 - 0.023i & -0.016 - 0.147i & -0.009 - 0.093i \end{pmatrix}.$$

Therefore, we see that for a general solution $\{B_j\}$ for $\mathcal{A}'$, such as the solution derived from the matlab routine, the algorithm suggested by [28] fails to give the Wedderburn decomposition, although it does give the the correct form for the particularly chosen $\{B_j\}$ in [28]. Hence, in practice, the algorithm in [28] is sometimes insufficient, which motivated us to develop the modified algorithm presented here. Next, we would like to continue with this example for $n_q = 4$, and following our algorithm to find the local unitary transform $Q = \text{diag}(Q_1, Q_2, Q_3)$ such that all the sub-blocks of $Q^\dagger B_j Q$ are in the scalar matrix form. Strictly speaking, we should use the random combination method in the last section to pick up a generic $\bar{B}$ for Step 2. However, for this particular example, the above B_1 is already a generic matrix, so we will instead based on B_1 to construct Q.

Define $Q_1 = \mathbb{I}_3$, and according to Step 2 in Table I, we define $\hat{Q}_k = B_{1,k}^{-1}$ and $Q_k = 1/||q_k|| \hat{Q}_k$, $k = 2, 3$, where q_k is the first row of $\hat{Q}_k$. Then we have

$$Q^\dagger B_1 Q = \begin{pmatrix} -0.167\mathbb{I}_3 & 0.345\mathbb{I}_3 & 0.1931\mathbb{I}_3 \\ 0.345\mathbb{I}_3 & 0.233\mathbb{I}_3 & -0.033 - 0.219i\mathbb{I}_3 \\ 0.193\mathbb{I}_3 & -0.033 + 0.219i\mathbb{I}_3 & 0.308\mathbb{I}_3 \end{pmatrix}$$

We can double-check the form of $Q^\dagger B_j Q$ for other B_j and we will find that all B_j are transformed in the form of $\mathcal{M}_3 \otimes I_3$. Hence, for this particular set of $\{B_j\}$, we have explicitly constructed the unitary matrix $U = VQ$ that transforms $\mathcal{A}'$ into the Wedderburn decomposition, which is not accessible from the algorithm in [28]. Now

we know how to encode an arbitrary three-level quantum state $\bar{\rho}$ into the DFS $\mathcal{N}_2$. In the current computational basis, the encoded density operator ρ should take the form:

$$\rho = U\big(0 \oplus (\bar{\rho} \otimes \mathbb{I}_3) \oplus 0\big)U^\dagger$$

We note finally that: i) in the above implementation of our algorithm, we have skipped Step 1 since the algorithm in [28] has already transformed all B_j into 3. ii) We have applied Step 2 to B_1 instead of to a random combination of the $\{B_j\}$, so as to make it easy for comparison. In practice, we do not really have to use the two generic operators as we suggest. They are introduced primarily to guarantee the validity of the algorithm.

B. Searching for an Approximate DFS

Although for every noisy channel there exists a decomposition as in (2), not all channels have a DFS that is useful for protecting quantum information. In fact, the noisy channels with a useful DFS constitute only a very small set. For many channels the algebraic decomposition (2) looks like the following:

$$\mathcal{A}' = \bigoplus_i k_i \mathbb{I}_{m_i},$$

where $k_i \neq k_j$, for $i \neq j$, which means that all the $\mathcal{M}_{n_i}$'s are 1-dimensional and so cannot store quantum information. When this happens, we would like to ask an alternative question: does there exist a subsystem on which the noise, even if not zero, is significantly reduced? This is the concept of an *approximate* DFS (ADFS).

It is not easy to characterize an ADFS by algebraic conditions, as we have done for a perfect DFS. Rather, an ADFS should be formulated as an optimal solution such that the noise on the system is reduced as much as possible. Hence, it is possible to obtain an ADFS numerically by solving the corresponding optimization problem. Since there is more than one way to quantify the effects of noise, there is more than one way to define the function to be minimized in the optimization. For the purposes of our analysis in what follows, we simply assume that one such function has been chosen, and denote it by J. Furthermore, one must specify when the noise is "small enough" to be helpful as an ADFS.

The problem of finding an ADFS involves searching for the optimal unitary matrix U that transforms the original basis into a new basis, such that a state ρ_1, encoded in $\rho = \frac{1}{n_2}\rho_1 \otimes \mathbb{I}_{n_2} \oplus 0_{res}$, experiences the least noise under the noise operators $\{\bar{A}_k\}$, where $\bar{A}_k = UA_kU^\dagger$. That is, we want to minimize $J(U)$, where U varies over the unitary group. Numerically, we can apply the BFGS quasi Newton method for the optimization [35]. Broadly speaking this involves i) choosing an initial point $U = U^{(0)}$ in the unitary matrix space; ii) calculating the value and the gradient of the objective function $J^{(0)} = J[U^{(0)}]$; iii) using the value and the gradient to implicitly derive the Hessian information and use them all to get a new $U^{(1)}$ such that $J[U^{(1)}] < J[U^{(0)}]$. Repeating steps ii) and iii), we obtain a sequence of $\{U^{(k)}\}$ with a limit corresponding to a local minimum of J. The limiting unitary transform $\bar{U}$ is what we are looking for.

N	1	2	3	4	5	6
J_{min}	0.2195	0.2078	0.2088	0.0123	0.4788	0.0125

TABLE II. The final value of J_{min} obtained from numerical optimization, using 6 different random starting points enumerated by N.

Due to the existence of many local minima, different initial choices of $U^{(0)}$ may result in different values of the optimized J. In particular, as the dimension gets larger we may need to run the optimization many times before we obtain a value of J close to the global minimum. Hence a wise choice of $U^{(0)}$ can be very important in performing the numerical optimization. One important result in optimization theory is that any gradient-based algorithm only guarantees that the iteration sequence will converge to some local minimum; however, if the initial point of optimization iteration is very close to the global minimum, then the iteration sequence will converge to the global minimum. On the other hand, if our noisy quantum channel $\mathcal{E}$ can be considered as a perturbation of another channel $\mathcal{E}'$ that has a perfect DFS, then the ADFS of $\mathcal{E}$ should be pretty close to the DFS of $\mathcal{E}$. Hence, we can apply the DFS algorithm in Section III to first calculate the unitary matrix U_0 for the DFS of $\mathcal{E}'$, and then run the optimization for ADFS, with $U^{(0)} = U_0$. In that way, we will be able to derive the ADFS more efficiently.

Specifically, let us take the collective noise model as an example, but this time add a perturbation to the original noise operators:

$$\tilde{A}_x = V_\epsilon A_x, \quad \tilde{A}_y = A_y, \quad \tilde{A}_z = A_z,$$

where we have defined a perturbation unitary matrix V_ϵ that is sufficiently close to the identity: $||V_\epsilon - \mathbb{I}|| < \epsilon$. Under the new noise operators $\tilde{A}_{x,y,z}$, we apply the algorithm in Section III and find that there is no useful DFS. Next we try to run optimization to this model in searching for ADFS. First we do the optimization using random initial point. For example, choosing $\epsilon = 1$ and $n_q = 4$, we run the optimization routine 6 times, starting from different initial $U^{(0)}$, and record the final minimized J_{min} in Table II. We see that among the six different runs, only two of them have obtained $J_{min} < 0.0125$. Hence we cannot guarantee that we have the best minimized J from a single run of the optimization process from an arbitrary random initial $\{U^{(0)}\}$. However, if we instead choose $U^{(0)} = U_0$, where U_0 is the unitary matrix in the Wedderburn decomposition for the perfect DFS of $\{A_{x,y,z}\}$, then the optimization generates the minimized $J_{min} = 0.0123$. For other values of n_q we find similar results. Thus our DFS-finding algorithm helps in finding

good initial points for the optimization of ADFS searching.

In addition, many local minima may also result in options for our ADFS implementation. Whereas our algorithm gives the dimensionally optimal DFS, there may be several ADFSs and the "best" one may not be the dimensionally optimal one. The "best" might be the one which has robust, experimentally available controls, or one that has the lowest error rate per unit time.

V. CONCLUSION

In this work, for a given noisy quantum channel, we have presented an algorithm to numerically calculate the unitary matrix that transforms the original noise algebra into the Wedderburn form, and this gives the structure of all DFS's if any exist. This algorithm is based on the theory of the Wedderburn decomposition of matrix *-algebras. We also compared our algorithm with the earlier algorithm proposed in [28], which we found was incomplete. The new algorithm is also more efficient, in that it requires fewer checks and evaluations, and requires only information from either the noise algebra $\mathcal{A}$ or its conjugate $\mathcal{A}'$, rather than both. As an application, we show that the DFS-finding method is helpful in locating good initial points for finding approximate DFS's, and this is likely to be a more practical use for the algorithm.

ACKNOWLEDGEMENTS

KJ is partially supported by the NSF project PHY-1005571, and KJ and XW are partially supported by the NSF project PHY-0902906 and the ARO MURI grant W911NF-11-1-0268. All the authors are partially supported by the Intelligence Advanced Research Projects Activity (IARPA) via Department of Interior National Business Center contract number D11PC20168. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon. Disclaimer: The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of IARPA, DoI/NBC, or the U.S. Government.

[1] P. Zanardi, Phys. Rev. A **57**, 3276 (1998).
[2] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[3] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[4] A. Steane, Rep. Prog. Phys. **61**, 117 (1998).
[5] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[6] D. Gottesman, "Stabilizer codes and quantum error correction," (1997), arXiv:quant-ph/9705052.
[7] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[8] F. Gaitan, *Quantum Error Correction and Fault Tolerant Quantum Computing* (CRC press, Boca Raton, 2008).
[9] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).
[10] D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).
[11] D. A. Lidar, D. Bacon, and K. B. Whaley, Phys. Rev. Lett. **82**, 4556 (1999).
[12] P. Zanardi, Physics Letters A **258**, 77 (1999).
[13] D. Bacon, J. Kempe, D. A. Lidar, and K. B. Whaley, Phys. Rev. Lett. **85**, 1758 (2000).
[14] L. Viola, E. Knill, and S. Lloyd, Phys. Rev. Lett. **85**, 3520 (2000).
[15] P. Zanardi, Phys. Rev. A **63**, 012301 (2000).
[16] L.-A. Wu and D. A. Lidar, Phys. Rev. Lett. **88**, 207902 (2002).
[17] M. Mohseni, J. S. Lundeen, K. J. Resch, and A. M. Steinberg, Phys. Rev. Lett. **91**, 187903 (2003).
[18] A. Shabani and D. A. Lidar, Phys. Rev. A **72**, 042303 (2005).
[19] C. A. Bishop and M. S. Byrd, J. Phys. A: Math. Theor. **42**, 055301 (2009).
[20] L. Viola, E. Knill, and S. Lloyd, Phys. Rev. Lett. **82**, 2417 (1999).
[21] L. Viola, S. Lloyd, and E. Knill, Phys. Rev. Lett. **83**, 4888 (1999).
[22] A. G. Kofman and G. Kurizki, Phys. Rev. Lett. **87**, 270405 (2001).
[23] L.-A. Wu, M. S. Byrd, and D. A. Lidar, Phys. Rev. Lett. **89**, 127901 (2002).
[24] G. S. Uhrig, Phys. Rev. Lett. **98**, 100504 (2007).
[25] G. S. Uhrig, Phys. Rev. Lett. **102**, 120502 (2009).
[26] A. M. Souza, G. A. Álvarez, and D. Suter, Phys. Rev. Lett. **106**, 240501 (2011).
[27] J. H. M. Wedderburn, *Lectures on Matrices* (American Mathematical Society, New York, 1934).
[28] J. A. Holbrook, D. W. Kribs, and R. Laflamme, Quantum. Inf. Proc. **80**, 381 (2003).
[29] K. Murota, Y. Kanno, M. Kojima, and S. Kojima, Japan Journal of Industrial and Applied Mathematics **27**, 125 (2010).
[30] E. de Klerk, C. Dobre, and D. Pasechnik, Mathematical Programming **129**, 91 (2011).
[31] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[32] D. Gijswijt, "Matrix algebras and semidefinite programming techniques for codes," (2010), arXiv:math/1007.0906.
[33] G. P. Barker, L. Q. Eifler, and T. P. Kezlan, Linear Algebra and its Applications **20**, 95 (1978).
[34] M. Byrd, Phys. Rev. A **73**, 032330 (2006).
[35] J. Nocedal and S. J. Wright, *Numerical Optimization* (Springer, New York, 2006).