Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

COMMON REDUCING UNITARY SUBSPACES AND DECOHERENCE IN QUANTUM SYSTEMS*

GRZEGORZ PASTUSZAK† AND ANDRZEJ JAMIOŁKOWSKI‡

Abstract. Maps of the form $\Phi(X) = \sum_{i=1}^{s} A_i X A_i^*$, where $A_1, \ldots, A_s$ are fixed complex $n \times n$ matrices and X is any complex $n \times n$ matrix, are used in quantum information theory as representations of quantum channels. This article deals with computable conditions for the existence of decoherence-free subspaces for Φ. Since the definition of decoherence-free subspace for quantum channels relies only on the matrices $A_1, \ldots, A_s$, the term of common reducing unitary subspace is used instead of the original one. Among the main results of the paper, there are computable conditions for the existence of common eigenvectors. These are related to common reducing unitary subspaces of dimension one. The new results on common eigenvectors provide new effective condition for the existence of common invariant subspaces of arbitrary dimensions.

Key words. Decoherence-free subspaces, Quantum channels, Common eigenvectors, Common eigenspaces, Common invariant subspaces.

AMS subject classifications. 15A18, 47A15.

1. Introduction and preliminary facts.

Quantum information theory is one of the central topics of study in quantum mechanics [15]. Quantum information may be understood as physical information that is held in the state of a quantum system, see [8] for basic concepts and terminology of quantum theory. The smallest possible unit of quantum information is the *qubit*. Qubits may be transmited through *quantum channels*.

There are many fundamental differences between qubits and bits that are used to store classical information. For example, a classical bit of information takes the value 0 or 1 whereas a qubit can take the the values 0 and 1 and all intermediate ones. This is a consequence of a fundamental property of quantum states. We can construct linear superpositions of a state in which qubit has the value 0 and of a state in which it has the value 1. In this sense, qubits are able to convey classical bits and

*Received by the editors on December 16, 2014. Accepted for publication on April 28, 2015. Handling Editor: Michael Tsatsomeros.

†Faculty of Mathematics and Computer Science, Nicolaus Copernicus University, Toruń, Poland (past@mat.umk.pl). Supported by grant no. DEC-2011/02/A/ST1/00208 of National Science Center of Poland.

‡Faculty of Physics, Astronomy and Informatics, Nicolaus Copernicus University, Toruń, Poland (jam@fizyka.umk.pl). Supported by grant no. DEC-2011/02/A/ST1/00208 of National Science Center of Poland.

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

are more capacious. Furthermore, a qubit cannot be copied or destroyed, which is obviously not the case for a classical bit.

The above comparison suggests that storing and processing information in quantum systems is safer and more economic than in the classical way. This justifies huge efforts already put in the construction of a large scale quantum computer.

Unfortunately, quantum information may be easily corrupted by a number of factors [13]. We have among them various random driving forces from the environment, possible interactions between the system and the environment, and statistical imprecision as well (i.e., timing errors). Any such a factor that can affect a quantum system is described as *decoherence*. Decoherence is an obstacle which must be overcome and managed before quantum computers can be built.

One way to overcome the effects of quantum decoherence is to "hide" quantum information from the environment in some "quiet corner". This quiet corner is called the *decoherence-free subspace* (DFS). Decoherence-free subspace is a part of the quantum system's Hilbert space where the system is decoupled from the environment and its evolution is completely unitary. Although this definition is commonly used, it is not fully precise. This resulted in the developement of few different mathematical definitions of DFS in the literature, see [10] for the details.

Regardless of this ambiguity, it seems that the definition of a decoherence-free subspace for a quantum channel, which is a very special quantum system, is already settled and takes the form studied in [18], see also [12] and Chapter 3 of [13].

Recall that a *quantum channel* is a trace preserving completely positive map $\Phi : \mathbb{M}_n(\mathbb{C}) \to \mathbb{M}_n(\mathbb{C})$ (see [8], [2] for definitions of these notions), where $\mathbb{M}_n(\mathbb{C})$ denotes the vector space of all $n \times n$ complex matrices. This implies that there are matrices $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ such that

$$\Phi(X) = \sum_{i=1}^{s} A_i X A_i^*$$

for any $X \in \mathbb{M}_n(\mathbb{C})$, and $\sum_{i=1}^{s} A_i^* A_i = I_n$ where A^* denotes matrix adjoint to A and I_n is the $n \times n$ identity matrix, see [8, 5.2.3] for details on operator sum decomposition of quantum channels. The latter condition is known as the *normalization rule*.

Before we state the definition of a decoherence-free subspace for a quantum channel, let us recall some terminology.

Assume that $A \in \mathbb{M}_n(\mathbb{C})$ and W is a subspace of $\mathbb{C}^n$. We say that W is an *invariant* subspace of A (or *A-invariant*) if and only if $Aw \in W$ for any $w \in W$. We say that W is a *reducing* subspace of A (or *A-reducing*) if and only if W is an invariant subspace of both A and A^*.

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

Assume that $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ and W is a subspace of $\mathbb{C}^n$. We say that W is a *common invariant subspace* of all A_i if and only if W is A_i-invariant for any $i = 1, \ldots, s$. We say that W is a *common reducing subspace* of all A_i if and only if W is A_i-reducing for any $i = 1, \ldots, s$.

The definition below is a precise formulation of the one taken from [12] and [13].

DEFINITION 1.1. Assume that $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ and $\Phi(X) = \sum_{i=1}^{s} A_i X A_i^*$ is a quantum channel. A nonzero subspace W of $\mathbb{C}^n$ is a *decoherence-free subspace* for Φ if and only if W is a common reducing subspace of $A_1, \ldots, A_s$ and there exists a unitary operator $U : W \to W$ and complex numbers $g_1, \ldots, g_s$ such that $A_i w = (g_i U)w$ for any $w \in W$ and $i = 1, \ldots, s$.

This paper is devoted to present some computable conditions for the existence of decoherence-free subspaces for quantum channels. By a *computable condition* (or a *computable criterion*) we mean any procedure employing only finite number of arithmetic operations. We emphasize that in applications of mathematics to physics and other sciences it is often crucial to have rather computable than purely theoretical conditions since the latter ones can be hard in verification.

It follows from the definition that decoherence-free subspaces for quantum channels may be studied without any reference to concrete examples taken from quantum mechanics. Indeed, the formulation of Definition 1.1 depends only on the matrices $A_1, \ldots, A_s$. This is the reason why we rather use the term of *common reducing unitary subspace* than the original one. We thus propose the following definition.

DEFINITION 1.2. Assume that $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ and W is a nonzero common reducing subspace of A_i. We say that W is a *common reducing unitary subspace* of A_i if and only if there exists a unitary operator $U : W \to W$ and complex numbers g_i such that $A_i w = (g_i U)w$ for any $w \in W$ and $i = 1, \ldots, s$.

It is clear that W is a common reducing unitary subspace of $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ if and only if W is a decoherence-free subspace for a quantum channel $\Phi(X) = \sum_{i=1}^{s} A_i X A_i^*$, as long as the condition $\sum_{i=1}^{s} A_i^* A_i = I_n$ holds. However, it is convenient to study the general problem of common reducing unitary subspaces, i.e., without assuming the normalization rule.

The paper is organized as follows. In Section 2, we give and compare two computable conditions for the existence of a common eigenvector of s complex matrices. One of these conditions is already known from [9], but here we obtain its new applications.

Recall that a nonzero vector $v \in \mathbb{C}^n$ is a *common eigenvector* of $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ if and only if v is an eigenvector of every A_i, that is, $A_i v = \alpha_i v$ for some

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

$\alpha_i \in \mathbb{C}$. Obviously, v is a common eigenvector of A_i if and only if the one-dimensional subspace V generated by v is A_i-invariant.

In the section, we also prove that the general problem of the existence of common reducing unitary subspaces is equivalent, in some sense, to the problem of the existence of common eigenspaces. A *common eigenspace* is a common reducing unitary subspace with the unitary operator being equal to identity.

Section 3 is devoted to present main results of the paper, which we derive from the results of Section 2. Among other things, we show there is a computable criterion for the existence of a common reducing unitary subspace of $A_i \in \mathbb{M}_n(\mathbb{C})$ of dimension one. Observe that such a subspace exists if and only if there exists a common eigenvector of $A_1, \ldots, A_s, A_1^*, \ldots, A_s^*$.

We first formulate the results of Section 3 in the language of common reducing unitary subspaces and then in the language of decoherence-free subspaces for quantum channels. As we shall see, both formulations are useful.

In Section 4, we give some additional comments on the problems discussed. For example, we apply our results from Section 2 concerning common eigenvectors to the problem of common invariant subspaces of arbitrary dimensions. This is done in the spirit of [9]. Note that common invariant subspaces of arbitrary dimensions have an application in quantum information theory as well, see for example [4].

In the final section of the paper, we illustrate our computable criterions with a concrete numerical example. In this example, we verify the existence of a common reducing unitary subspace of dimension one for three complex 3×3 matrices randomly generated in a computer algebra system.

Let us now introduce some notation and recall few basic facts that we use in the paper. Assume that $B(\mathbb{C}^n)$ is the vector space of all linear operators on $\mathbb{C}^n$. If we fix a basis of $\mathbb{C}^n$, then $B(\mathbb{C}^n)$ is isomorphic with the vector space $\mathbb{M}_n(\mathbb{C})$ of all $n \times n$ complex matrices. From now on we identify $B(\mathbb{C}^n)$ with $\mathbb{M}_n(\mathbb{C})$, and thus, we call an element A of $\mathbb{M}_n(\mathbb{C})$ an *operator* or a *matrix*.

Assume that $A \in \mathbb{M}_n(\mathbb{C})$ and W is an invariant subspace of A. A *restriction* of A on W is the operator $A|W : W \to W$ defined by $(A|W)w = Aw \in W$ for any $w \in W$. Observe that if W is A-reducing, then $(A|W)^* = A^*|W$.

Assume that $A \in \mathbb{M}_n(\mathbb{C})$ and W is a subspace of $\mathbb{C}^n$. Then W is A-reducing if and only if W is A^*-reducing. Moreover, W is reducing for A if and only if both W and $\mathbb{C}^n \ominus W$ are A-invariant where $\mathbb{C}^n \ominus W$ denotes the unique subspace V of $\mathbb{C}^n$ such that $W \oplus V = \mathbb{C}^n$.

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

Assume that W is a common reducing unitary subspace of $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ such that $A_i w = (g_i U)w$ for some complex numbers g_i and a unitary operator $U : W \to W$, for any $w \in W$. We call W *trivial*, if $g_i = 0$ for any i. If W is not trivial, we call W *nontrivial*.

Note that if W is a common reducing unitary subspace as above, then we have $A_i^* w = (\overline{g_i} U)w$, where $\overline{g_i}$ denotes the complex conjugate of $g_i \in \mathbb{C}$.

2. Common eigenvectors, common eigenspaces and common reducing unitary subspaces. This section is devoted to show and compare two computable conditions for the existence of a common eigenvector. It is easy to see that there is a common reducing unitary subspace of $A_1, \ldots, A_s$ of dimension one if and only if there exists a common eigenvector of $A_1, \ldots, A_s, A_1^*, \ldots, A_s^*$. Thus, the problem of the existence of a common reducing unitary subspace of dimension one comes down to the problem of the existence of a common eigenvector.

The notion of a common eigenspace is a natural generalization of a common eigenvector. Assume that W is a nonzero subspace of $\mathbb{C}^n$. We call W a *common eigenspace* of $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ if and only if there exist complex numbers $\alpha_1, \ldots, \alpha_s$ such that $A_i w = \alpha_i w$ for any $w \in W$. We prove in Theorem 2.5 that the general problem of the existence of common reducing unitary subspaces is equivalent to the problem of the existence of common eigenspaces.

Assume that $A, B \in \mathbb{M}_n(\mathbb{C})$. We denote by $[A, B] = AB - BA$ the *commutator* of A and B, and by $\ker A = \{v \in \mathbb{C}^n; Av = 0\}$ the *kernel* of A.

In [9], we proved the following computable criterion for the existence of a common eigenvector of $s \geq 2$ complex square matrices. This is the generalized version of [16, Theorem 3.1].

THEOREM 2.1. *Assume that* $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ *and*

$$\mathcal{M}(A_1, \ldots, A_s) = \bigcap_{k_i, l_j \geq 0}^{n-1} \ker[A_1^{k_1} \cdots A_s^{k_s}, A_1^{l_1} \cdots A_s^{l_s}]$$

where $k_1 + k_2 + \cdots + k_s \neq 0$ *and* $l_1 + l_2 + \cdots + l_s \neq 0$.

(1) *The subspace* $\mathcal{M}(A_1, \ldots, A_s)$ *is* A_i*-invariant for any* $i = 1, \ldots, s$.
(2) *Matrices* A_i *have a common eigenvector if and only if* $\mathcal{M}(A_1, \ldots, A_s) \neq 0$.
(3) *We have* $\mathcal{M}(A_1, \ldots, A_s) = \ker K$ *where*

$$K = \sum_{k_i, l_j \geq 0}^{n-1} [A_1^{k_1} \cdots A_s^{k_s}, A_1^{l_1} \cdots A_s^{l_s}]^* [A_1^{k_1} \cdots A_s^{k_s}, A_1^{l_1} \cdots A_s^{l_s}]$$

and $k_1 + k_2 + \cdots + k_s \neq 0$, $l_1 + l_2 + \cdots + l_s \neq 0$.

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

We show in the proposition below that the subspace $\mathcal{M}(A_1,\ldots,A_s)$ has other interesting properies. These properties are related to the subject of our study.

PROPOSITION 2.2. *Assume $A_1,\ldots,A_s \in \mathbb{M}_n(\mathbb{C})$ and let $\mathcal{M} = \mathcal{M}(A_1,\ldots,A_s)$.*

(1) *We have $(A_iA_j)w = (A_jA_i)w$ for any i,j and any $w \in \mathcal{M}$. Moreover, if $V \subseteq \mathbb{C}^n$ is A_i-invariant and $(A_iA_j)v = (A_jA_i)v$ for any i,j and any $v \in V$, then $V \subseteq \mathcal{M}$.*
(2) *If $v \in \mathbb{C}^n$ is a common eigenvector of A_i, then $v \in \mathcal{M}$. Consequently, any common eigenspace of A_i is contained in $\mathcal{M}$.*

Proof. (1) Obviously, if $w \in \mathcal{M}$, then $w \in \ker[A_i, A_j]$ and so $(A_iA_j)w = (A_jA_i)w$ for any i,j.

Assume that $V \subseteq \mathbb{C}^n$ is A_i-invariant, and $(A_iA_j)v = (A_jA_i)v$ for any i,j and $v \in V$. Let $t \geq 2$, $X_1,\ldots,X_t \in \{A_1,\ldots,A_s\}$ and $1 \leq i < t-1$. We set $X_1\cdots X_{i-1} = I_n$, if $i = 1$ and $X_{i+2}\cdots X_t = I_n$, if $i = t-1$. Then

$$\begin{aligned}(X_1\cdots X_t)v &= (X_1\cdots X_{i-1})(X_iX_{i+1})(X_{i+2}\cdots X_t)v\\ &= (X_1\cdots X_{i-1})(X_{i+1}X_i)(X_{i+2}\cdots X_t)v\end{aligned}$$

for any $v \in V$ since $(X_{i+2}\cdots X_t)v \in V$ and all the matrices A_i commute on V. This easily implies that $(X_1\cdots X_t)v = (X_{\sigma(1)}\cdots X_{\sigma(t)})v$ for any permutation σ of the set $\{1,\ldots,t\}$, and thus,

$$(A_1^{k_1}\cdots A_s^{k_s})(A_1^{l_1}\cdots A_s^{l_s})v = (A_1^{k_1+l_1}\cdots A_s^{k_s+l_s})v = (A_1^{l_1}\cdots A_s^{l_s})(A_1^{k_1}\cdots A_s^{k_s})v$$

for any $k_i, l_j \geq 0$ and $v \in V$. Hence, $v \in \ker[A_1^{k_1}\cdots A_s^{k_s}, A_1^{l_1}\cdots A_s^{l_s}]$ and so $V \subseteq \mathcal{M}$.

(2) Assume that $v \in \mathbb{C}^n$ is a common eigenvector of A_i and V is the one-dimensional vector space generated by v. Then there are complex numbers α_i such that $A_iv = \alpha_iv$ for any i. Observe that $(A_iA_j)v = \alpha_i\alpha_jv = (A_jA_i)v$ and so $(A_iA_j)v = A_i(A_jv) \in V$. Hence, the subspace V is A_i-invariant and the matrices A_i commute on V. Therefore it follows by (1) that $V \subseteq \mathcal{M}$, and so $v \in \mathcal{M}$. This yields any common eigenspace W of A_i is contained in $\mathcal{M}$, because W is a set of common eigenvectors of A_i. □

Now we define another subspace related to the problem of the existence of a common eigenvector. This subspace allows us to formulate a computable criterion analogous to the one presented in Theorem 2.1. The criterion requires less computation than the first one, but needs an additional assumption. We start with the following general observation.

PROPOSITION 2.3. *Assume that $H, A_1,\ldots,A_s \in \mathbb{M}_n(\mathbb{C})$ and H has pairwise different eigenvalues. If the subspace $X \subseteq \mathbb{C}^n$ is nonzero H-invariant and $(HA_i)x =$*

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

$(A_iH)x$ for any i and any $x \in X$, then there exists a common eigenvector $v \in X$ of the matrices $H, A_1, \ldots, A_s$.

Proof. Assume that $0 \neq X \subseteq \mathbb{C}^n$ is H-invariant and $(HA_i)x = (A_iH)x$ for any $x \in X$. Since X is H-invariant and H is a matrix over an algebraically closed field $\mathbb{C}$ of complex numbers, there exists $\alpha \in \mathbb{C}$ and a nonzero vector $v \in X$ such that $Hv = \alpha v$. Moreover,

$$H(A_iv) = (HA_i)v = (A_iH)v = A_i(Hv) = \alpha(A_iv)$$

for any i since $v \in X$ and the matrix H commutes with A_i on the subspace X. This yields that A_iv is an eigenvector of H corresponding to the eigenvalue α. Because H does not have multiple eigenvalues, the space of all eigenvectors corresponding to α is one-dimensional. This implies that the vectors v and A_iv are linearly dependent and so $A_iv = \beta_iv$ for some complex numbers β_i. Consequently, $Hv = \alpha v$, $A_iv = \beta_iv$ and so v is a common eigenvector of $H, A_1, \ldots, A_s$. □

The following theorem gives an interesting alternative to Theorem 2.1.

THEOREM 2.4. *Assume that $H, A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ and define*

$$\mathcal{N}(H, A_1, \ldots, A_s) := \bigcap_{k=1}^{\infty} \bigcap_{i=1}^{s} \ker[H^k, A_i].$$

(1) *The subspace $\mathcal{N}(H, A_1, \ldots, A_s)$ is H-invariant and $(HA_i)x = (A_iH)x$ for any $x \in \mathcal{N}(H, A_1, \ldots, A_s)$.*
(2) *Assume that H has pairwise different eigenvalues. Then the matrices H, $A_1, \ldots, A_s$ have a common eigenvector if and only if $\mathcal{N}(H, A_1, \ldots, A_s) \neq 0$.*
(3) *We have*

$$\mathcal{N}(H, A_1, \ldots, A_s) = \bigcap_{k=1}^{n-1} \bigcap_{i=1}^{s} \ker[H^k, A_i]$$

and consequently $\mathcal{N}(H, A_1, \ldots, A_s) = \ker K$ where

$$K = \sum_{k=1}^{n-1} \sum_{i=1}^{s} [H^k, A_i]^*[H^k, A_i].$$

Proof. (1) We show that the subspace $\mathcal{N}(H, A_1, \ldots, A_s)$ is H-invariant. The second condition follows from the fact that $\mathcal{N}(H, A_1, \ldots, A_s) \subseteq \bigcap_{i=1}^{s} \ker[H, A_i]$.

If $\mathcal{N}(H, A_1, \ldots, A_s) = 0$ then $\mathcal{N}(H, A_1, \ldots, A_s)$ is H-invariant. Hence, assume that $\mathcal{N}(H, A_1, \ldots, A_s) \neq 0$ and let $v \in \mathcal{N}(H, A_1, \ldots, A_s)$. Then $(H^kA_i)v = (A_iH^k)v$ for any k and $i = 1, \ldots, s$ which implies that

$$(H^kA_i)Hv = H^k(A_iH)v = H^k(HA_i)v = (H^{k+1}A_i)v = (A_iH^{k+1})v = (A_iH^k)Hv$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

for any $k \in \mathbb{N}$ and any $i = 1, \ldots, s$. Hence, we get $Hv \in \ker[H^k, A_i]$ for any k and i, and thus, $Hv \in \mathcal{N}(H, A_1, \ldots, A_s)$. Consequently, the subspace $\mathcal{N}(H, A_1, \ldots, A_s)$ is H-invariant.

(2) Assume that the matrices $H, A_1, \ldots, A_s$ have a common eigenvector. Then there are complex numbers $\alpha_H, \alpha_1, \ldots, \alpha_s$ and a nonzero vector $v \in \mathbb{C}^n$ such that $Hv = \alpha_H v$ and $A_i v = \alpha_i v$ for any i. Observe that $(H^k A_i)v = \alpha_H^k \alpha_i v = (A_i H^k)v$, and hence, $v \in \ker[H^k, A_i]$ for any $k \in \mathbb{N}$ and any $i = 1, \ldots, s$. This implies that $v \in \mathcal{N}(H, A_1, \ldots, A_s)$ and so $\mathcal{N}(H, A_1, \ldots, A_s) \neq 0$.

Conversely, it follows by (1) that the subspace $\mathcal{N}(H, A_1, \ldots, A_s)$ is H-invariant and $(HA_i)x = (A_i H)x$ for any $x \in \mathcal{N}(H, A_1, \ldots, A_s)$. Hence, it follows by Proposition 2.2 that if $\mathcal{N}(H, A_1, \ldots, A_s) \neq 0$, then the matrices $H, A_1, \ldots, A_s$ have a common eigenvector.

(3) The first identity follows easily by the Cayley-Hamilton theorem. For the proof of the second one, observe that $\ker(A^*A + B^*B) = \ker A \cap \ker B$ for any $A, B \in \mathbb{M}_n(\mathbb{C})$, because the matrices A^*A, B^*B are positive semi-definite. □

In the final theorem of this section, we show a relation between common reducing unitary subspaces, common eigenspaces and the subspace $\mathcal{M}$ introduced in Theorem 2.1 and studied for the first time in [9].

THEOREM 2.5. *Assume that $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ and W is a subspace of $\mathbb{C}^n$. The subspace W is a common reducing unitary subspace of $A_1, \ldots, A_s$ if and only if W is an A_i-reducing common eigenspace of $A_i^* A_j$ such that $W \subseteq \mathcal{M}(A_1, \ldots, A_s, A_1^*, \ldots, A_s^*)$.*

Proof. $\Rightarrow$ Assume that W is a common reducing unitary subspace of $A_1, \ldots, A_s$. Then W is A_i-reducing and there are complex numbers g_i and a unitary operator $U : W \to W$ such that $A_i w = (g_i U)w$ for any $w \in W$. Hence,

$$(A_i^* A_j)w = A_i^*(A_j w) = A_i^*(g_j U)w = g_j A_i^*(Uw) = (g_j \overline{g_i} U^* U)w = g_j \overline{g_i} w$$

for any $w \in W$, because $Uw \in W$. Thus, W is a common eigenspace of $A_i^* A_j$.

Similar calculations show that $(A_j A_i^*)w = \overline{g_i} g_j w$, $(A_i A_j)w = (g_i g_j U^2)w$ and $(A_i^* A_j^*)w = (\overline{g_i g_j} U^{*2})w$, and thus, all the matrices $A_1, \ldots, A_s, A_1^*, \ldots, A_s^*$ commute on W. It follows from Proposition 2.2 (1) that $W \subseteq \mathcal{M}(A_1, \ldots, A_s, A_1^*, \ldots, A_s^*)$.

$\Leftarrow$ Assume that W is an A_i-reducing common eigenspace of $A_i^* A_j$ such that $W \subseteq \mathcal{M}(A_1, \ldots, A_s, A_1^*, \ldots, A_s^*)$.

Since W is a common eigenspace of $A_i^* A_j$, there are complex numbers α_{ij} such that $(A_i^* A_j)w = \alpha_{ij} w$ for any $w \in W$ and $i, j = 1, \ldots, s$. Moreover, $(A_i^* A_i)w = (A_i A_i^*)w$ for any $w \in W$ by Proposition 2.2 (1).

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

Consequently, $(A_i^*A_i)w = (A_iA_i^*)w = \alpha_i w$ for any $w \in W$ where $\alpha_i = \alpha_{ii}$. Because the operators $A_i^*A_i$ are positive semi-definite, the numbers α_i are real non-negative.

Assume that $\alpha_k = 0$ for some k. Then $(A_k^*A_k)w = 0$, and thus, $0 = \langle w|(A_k^*A_k)w\rangle = \langle A_kw|A_kw\rangle = ||A_kw||^2$, where $\langle\cdot|\cdot\rangle$ and $||\cdot||$ denote the standard scalar product and the standard norm in $\mathbb{C}^n$, respectively. This implies that $A_kw = 0$ for any $w \in W$, and hence, $A_kw = (0 \cdot U)w$ for any unitary operator $U : W \to W$.

Assume that $\alpha_k > 0$ for some k and take any $r_k \in \mathbb{C}$ such that $r_k\overline{r_k} = \frac{1}{\alpha_k}$. Then $(\overline{r_k}A_k^*)(r_kA_k)w = (r_kA_k)(\overline{r_k}A_k^*)w = w$, and hence, the operator $r_kA_k : W \to W$ is unitary. This implies that there is a nonzero complex number $s_k = \frac{1}{r_k}$ and a unitary operator $U_k : W \to W$ such that $A_kw = (s_kU_k)w$ for any $w \in W$.

Assume that $\alpha_k > 0$ and $\alpha_l > 0$ for some k, l. Then there are nonzero complex numbers s_k, s_l and unitary operators $U_k, U_l : W \to W$ such that

$$\alpha_{kl}w = (A_k^*A_l)w = A_k^*(A_lw) = \overline{s_k}U_k^*(A_lw) = (\overline{s_k}U_k^*s_lU_l)w = (\overline{s_k}s_lU_k^*U_l)w$$

and hence

$$(\alpha_{kl}U_k)w = U_k(\alpha_{kl}w) = U_k(\overline{s_k}s_lU_k^*U_l)w = (\overline{s_k}s_lU_kU_k^*U_l)w = (\overline{s_k}s_lU_l)w$$

for any $w \in W$. Therefore $U_lw = (\frac{\alpha_{kl}}{\overline{s_k}s_l}U_k)w$ since $\overline{s_k}, s_l \neq 0$ and so U_l and U_k are linearly dependent. Obviously $\alpha_{kl} \neq 0$, because U_l is nonzero as a unitary operator.

The above arguments yield the existence of a unitary operator $U : W \to W$ and complex numbers g_i such that $A_iw = (g_iU)w$ for any $w \in W$.

Indeed, if there is k such that $\alpha_k > 0$, then $U = U_k$, where $U_k : W \to W$ is the unique unitary operator satisfying $A_kw = (s_kU_k)w$ for some nonzero complex number s_k. We set $g_i = 0$ if and only if $\alpha_i = 0$. Thus, in the case $\alpha_i = 0$ for any i, we may assume U is an arbitrary unitary operator, for example an identity. We conclude that W is a common reducing unitary subspace of $A_1, \ldots, A_s$. □

Theorem 2.5 implies that the problem of the existence of common reducing unitary subspaces is equivalent, in the above sense, to the problem of the existence of common eigenspaces. The latter problem comes down to the existence of d linearly independent common eigenvectors $w_1, \ldots, w_d$ associated to a fixed sequence of eigenvalues, where d is an arbitrary natural number. It is thus interesting to ask whether the results of Theorem 2.1 and Theorem 2.4 are somehow sufficient to solve the general problem of common reducing unitary subspaces.

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

Since the subspaces $\mathcal{M}$ and $\mathcal{N}$ considered in the section are crucial in Theorem 2.1 and Theorem 2.4, respectively, we make a comparison of these two subspaces, pointing out similarities and differences between them.

REMARK 2.6. Assume that $H, A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ and set $\mathcal{M} = \mathcal{M}(H, A_1, \ldots, A_s)$ and $\mathcal{N} = \mathcal{N}(H, A_1, \ldots, A_s)$.

1. It is easy to see that $\mathcal{M} \subseteq \mathcal{N}$, so $\mathcal{M} \neq 0$ implies $\mathcal{N} \neq 0$. The converse implication does not hold in general.
2. The condition $\mathcal{N} \neq 0$ requires much less computation than the condition $\mathcal{M} \neq 0$. From the other hand, the subspace $\mathcal{N}$ is related to common eigenvectors only if we assume that H do not have multiple eigenvalues. This assumption is unimportant if we consider the subspace $\mathcal{M}$.
3. The subspace $\mathcal{M}$ is a common invariant subspace of $H, A_1, \ldots, A_s$ by Theorem 2.1 (1). The subspace $\mathcal{N}$ is, in general, only H-invariant, see Theorem 2.4 (1).
4. The subspace $\mathcal{M}$ is the biggest common invariant subspace of $H, A_1, \ldots, A_s$ on which all these matrices commute, by Proposition 2.2 (1). It can be shown similarly as in Proposition 2.2 (1) that the subspace $\mathcal{N}$ is the biggest H-invariant subspace on which the matrix H commutes with A_i, for any i. In general, the matrices A_i do not commute with each other on $\mathcal{N}$.
5. Since $\mathcal{M} \subseteq \mathcal{N}$ and $\mathcal{M}$ contains any common eigenvector of $H, A_1, \ldots, A_s$ by Proposition 2.2 (2), this is also the case for $\mathcal{N}$.

3. Main results and applications to quantum channels. In this section, we deduce the main results of the paper. First, we formulate them in the language of common reducing unitary subspaces and then in the language of decoherence-free subspaces for quantum channels. We apply here the results of the Section 2.

We distinguish the case of nontrivial and the case of arbitrary common reducing unitary subspaces, see Section 1 for the definitions. Both of these cases seem to be important, as we demonstrate in Section 4. Assume that $X_1, \ldots, X_s \in \mathbb{M}_n(\mathbb{C})$ and define

$$\mathcal{K}(X_1, \ldots, X_s) = \{v \in \mathbb{C}^n; X_i v = 0 \text{ for any } i\}.$$

We set $\mathcal{K} = \mathcal{K}(X_1, \ldots, X_s)$, $\mathcal{M} = \mathcal{M}(X_1, \ldots, X_s)$ and $\mathcal{N} = \mathcal{N}(X_1, \ldots, X_s)$. It follows from Proposition 2.2 (1) that $\mathcal{K} \subseteq \mathcal{M}, \mathcal{N}$ since $\mathcal{K}$ is X_i-invariant and all the matrices $X_1, \ldots, X_s$ commute on $\mathcal{K}$.

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

We define $\mathcal{M}' = \mathcal{M}'(X_1, \ldots, X_t)$ and $\mathcal{N}' = \mathcal{N}'(X_1, \ldots, X_t)$ as the unique subspaces of $\mathcal{M}$ and $\mathcal{N}$, respectively, such that $\mathcal{K} \cap \mathcal{M} = \mathcal{K} \cap \mathcal{N} = 0$ and $\mathcal{K} \oplus \mathcal{M}' = \mathcal{M}$, $\mathcal{K} \oplus \mathcal{N}' = \mathcal{N}$. Observe that $\mathcal{M}' = (\mathbb{C}^n \ominus \mathcal{K}) \cap \mathcal{M}$ and $\mathcal{N}' = (\mathbb{C}^n \ominus \mathcal{K}) \cap \mathcal{N}$.

THEOREM 3.1. *Assume that* $H, A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ *and set*

$$\mathcal{M} = \mathcal{M}(H, A_1, \ldots, A_s, H^*, A_1^*, \ldots, A_s^*),$$
$$\mathcal{N} = \mathcal{N}(H, A_1, \ldots, A_s, H^*, A_1^*, \ldots, A_s^*),$$
$$\mathcal{K} = \mathcal{K}(H, A_1, \ldots, A_s, H^*, A_1^*, \ldots, A_s^*).$$

Assume that $\mathcal{M}'$ *and* $\mathcal{N}'$ *are defined according to the notation introduced above.*

(1) *Matrices* $H, A_1, \ldots, A_s$ *have a common reducing unitary subspace of dimension one if and only if* $\mathcal{M} \neq 0$.
(1') *Matrices* $H, A_1, \ldots, A_s$ *have a nontrivial common reducing unitary subspace of dimension one if and only if* $\mathcal{M}' \neq 0$.
(2) *Assume that* H *has pairwise different eigenvalues. Then* $H, A_1, \ldots, A_s$ *have a common reducing unitary subspace of dimension one if and only if* $\mathcal{N} \neq 0$.
(2') *Assume that* H *has pairwise different eigenvalues. Then* $H, A_1, \ldots, A_s$ *have a nontrivial common reducing unitary subspace of dimension one if and only if* $\mathcal{N}' \neq 0$.
(3) *The conditions* $\mathcal{M} \neq 0$, $\mathcal{M}' \neq 0$, $\mathcal{N} \neq 0$, $\mathcal{N}' \neq 0$ *are computable.*

Proof. (1) and (2) Assume that $X_1, \ldots, X_t$ are arbitrary $n \times n$ complex matrices. It is easy to see that there exists a common reducing unitary subspace of X_i of dimension one if and only if there exists a common eigenvector of $X_1, \ldots, X_t, X_1^*, \ldots, X_t^*$. Hence, the assertion of (1) follows from Theorem 2.1 (2) and that of (2) follows from Theorem 2.4 (2).

(1') ($\Rightarrow$) Assume that V is a nontrivial one-dimensional common reducing unitary subspace of $H, A_1, \ldots, A_s$. Then there is a nonzero common eigenvector $v \in V$ of $H, A_1, \ldots, A_s, H^*, A_1^*, \ldots, A_s^*$. Hence, $v \in \mathcal{M}$ by Proposition 2.2 (2) and there are complex numbers $\alpha_H, \alpha_1, \ldots, \alpha_s$ such that $Hv = \alpha_H v$, $H^*v = \overline{\alpha_H} v$, $A_i v = \alpha_i v$, $A_i^* v = \overline{\alpha_i} v$. Since V is nontrivial, we get $\alpha_H \neq 0$ or $\alpha_t \neq 0$ for some t, and thus, $Hv = \alpha_H v \neq 0$ or $A_t v = \alpha_t v \neq 0$. It follows that $v \notin \mathcal{K}$, so $v \in \mathcal{M}'$ and $\mathcal{M}' \neq 0$.

($\Leftarrow$) Observe that the subspace $\mathcal{M}'$ is $H, A_1, \ldots, A_s$-reducing. Indeed, we have that $\mathcal{M}' = (\mathbb{C}^n \ominus \mathcal{K}) \cap \mathcal{M}$, $\mathcal{M}$ is $H, A_1, \ldots, A_s$-reducing by Theorem 2.1 (1) and $\mathbb{C}^n \ominus \mathcal{K}$ is $H, A_1, \ldots, A_s$-reducing, because $\mathcal{K}$ is $H, A_1, \ldots, A_s$-reducing. Moreover, $\mathcal{M}' \subseteq \mathcal{M}$ and so the matrices $H, A_1, \ldots, A_s, H^*, A_1^*, \ldots, A_s^*$ commute on $\mathcal{M}'$ by Proposition 2.2 (1).

Since the subspace $\mathcal{M}'$ is nonzero $H, A_1, \ldots, A_s, H^*, A_1^*, \ldots, A_s^*$-invariant and all these matrices commute on $\mathcal{M}'$, we get by a known result that there exists a common

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

eigenvector $v \in \mathcal{M}'$ of $H, A_1, \ldots, A_s, H^*, A_1^*, \ldots, A_s^*$, see for example [6]. Hence, the subspace V generated by v is a one-dimensional common reducing unitary subspace of $H, A_1, \ldots, A_s$. This subspace is nontrivial, because $V \subseteq \mathcal{M}' \subseteq \mathbb{C}^n \ominus \mathcal{K}$.

(2') ($\Rightarrow$) This follows by (1') since $\mathcal{M}' \subseteq \mathcal{N}'$.

($\Leftarrow$) We show similarly as in (1') that the subspace $\mathcal{N}'$ is H-invariant, although we apply Theorem 2.4 (1). Since $\mathcal{N}' \subseteq \mathcal{N}$, we have that H commutes with $A_1, \ldots, A_s$, $H^*, A_1^*, \ldots, A_s^*$ on $\mathcal{N}'$ by Theorem 2.4 (1). Because $\mathcal{N}'$ is nonzero, it follows by Proposition 2.3 that there is a common eigenvector $v \in \mathcal{N}'$ of $H, A_1, \ldots, A_s, H^*, A_1^*, \ldots, A_s^*$. Hence, the subspace V generated by v is a one-dimensional common reducing unitary subspace of $H, A_1, \ldots, A_s$. This subspace is nontrivial, because $V \subseteq \mathcal{N}' \subseteq \mathbb{C}^n \ominus \mathcal{K}$.

(3) The fact that the conditions $\mathcal{M} \neq 0$ and $\mathcal{N} \neq 0$ are computable follows from Theorem 2.1 and Theorem 2.4, respectively.

Observe that $\ker X \cap \ker Y = \ker(X^*X + Y^*Y)$ for any matrices $X, Y \in \mathbb{M}_n(\mathbb{C})$, because X^*X, Y^*Y are positive semi-definite.

Since the subspace $\mathcal{K}$ is an intersection of kernels of the matrices $H, A_1, \ldots, A_s$, $H^*, A_1^*, \ldots, A_s^*$, the observation implies that the linear basis of $\mathcal{K}$ can be directly computed. This is also the case for $\mathcal{M}$ and $\mathcal{N}$, see Theorem 2.1 and Theorem 2.4.

Hence, we can explicitly calculate the dimensions $\dim_{\mathbb{C}}\mathcal{K}$, $\dim_{\mathbb{C}}\mathcal{M}$, $\dim_{\mathbb{C}}\mathcal{N}$, and thus, the assertion follows from the fact that $\dim_{\mathbb{C}}\mathcal{M}' = \dim_{\mathbb{C}}\mathcal{M} - \dim_{\mathbb{C}}\mathcal{K}$ and $\dim_{\mathbb{C}}\mathcal{N}' = \dim_{\mathbb{C}}\mathcal{N} - \dim_{\mathbb{C}}\mathcal{K}$. □

The above theorem solves the problem of the existence of common reducing unitary subspaces of dimension one. In the following theorem, we consider another special case of the general problem of common reducing unitary subspaces. Namely, we assume that all the numbers g_i from the definition of a common reducing unitary subspace are equal to 1.

THEOREM 3.2. *Assume that $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ and define $\mathcal{J} = \mathcal{J}(A_1, \ldots, A_s)$ as the intersection of the following subspaces:*

- $\mathcal{M}(A_1, \ldots, A_s, A_1^*, \ldots, A_s^*)$,
- $\{v \in \mathbb{C}^n; A_i v = A_j v \text{ and } A_i^* v = A_j^* v \text{ for any } i, j\}$,
- $\{v \in \mathbb{C}^n; (A_i^* A_i)v = v \text{ for any } i\}$.

(1) *The subspace $\mathcal{J}$ is a common reducing subspace of $A_1, \ldots, A_s$.*
(2) *If $\mathcal{J} \neq 0$, then there exists a unitary operator $U : \mathcal{J} \to \mathcal{J}$ such that $A_i v = Uv$ for any i and any $v \in \mathcal{J}$. Hence, $\mathcal{J}$ is a common reducing unitary subspace.*

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

(3) *If W is a common reducing unitary subspace of $A_1, \ldots, A_s$ such that $A_i w = Uw$ for some unitary operator $U : W \to W$ and any $i = 1, \ldots, s$ and $w \in W$, then $W \subseteq \mathcal{J}$.*

Proof. (1) We set $\mathcal{M} = \mathcal{M}(A_1, \ldots, A_s, A_1^*, \ldots, A_s^*)$.

Assume that $x \in \mathcal{J}$ and $k \in \{1, \ldots, s\}$. We prove that $A_k x, A_k^* x \in \mathcal{J}$. Since $x \in \mathcal{M}$ and $\mathcal{M}$ is A_i, A_i^*-invariant by Theorem 2.1 (1), we get $A_k x, A_k^* x \in \mathcal{M}$. Because $\mathcal{J} \subseteq \mathcal{M}$, it follows from Proposition 2.2 (1) that the matrices $A_1, \ldots, A_s$, $A_1^*, \ldots, A_s^*$ commute on $\mathcal{J}$. Moreover, $A_i x = A_j x$ and $A_i^* x = A_j^* x$, so

$$A_i(A_k x) = (A_i A_k)x = (A_k A_i)x = (A_k A_j)x = (A_j A_k)x = A_j(A_k x)$$

and similarly $A_i^*(A_k x) = A_j^*(A_k x)$, $A_i(A_k^* x) = A_j(A_k^* x)$, $A_i^*(A_k^* x) = A_j^*(A_k^* x)$ for any $i, j, k = 1, \ldots, s$. Therefore, we obtain

$$A_k x, A_k^* x \in \{v \in \mathbb{C}^n; A_i v = A_j v \text{ and } A_i^* v = A_j^* v \text{ for any } i, j\}.$$

Assume that $B_k = A_k$ or $B_k = A_k^*$. Because the matrices $A_1, \ldots, A_s$, $A_1^*, \ldots, A_s^*$ commute on $\mathcal{J}$, we easily get $(A_i^* A_i)B_k x = B_k(A_i^* A_i)x$. It follows that $(A_i^* A_i)B_k x = B_k x$ since $(A_i^* A_i)x = x$, and thus,

$$A_k x, A_k^* x \in \{v \in \mathbb{C}^n; (A_i^* A_i)v = v \text{ for any } i\}.$$

We conclude from the above arguments that if $x \in \mathcal{J}$, then $A_k x, A_k^* x \in \mathcal{J}$, and hence, the subspace $\mathcal{J}$ is A_i-reducing.

(2) Observe that $(A_i^* A_i)x = (A_i A_i^*)x = x$ for any $x \in \mathcal{J}$ and since $\mathcal{J} \neq 0$, all the operators $A_i|\mathcal{J} : \mathcal{J} \to \mathcal{J}$ are unitary. Moreover, $A_i|\mathcal{J} = A_j|\mathcal{J}$ for any i, j, because $A_i x = A_j x$ for any $x \in \mathcal{J}$. This proves the assertion.

(3) Assume that W is a common reducing unitary subspace of A_i such that $A_i w = Uw$ for some unitary operator $U : W \to W$. It follows from Theorem 2.5 that $W \subseteq \mathcal{M}$ and since $A_i^* w = U^* w = A_j^* w$ and $(A_i^* A_i)w = (U^* U)w = w$ for any $w \in W$, we get $W \subseteq \mathcal{J}$. □

Let us observe that the construction of the subspace $\mathcal{J}$ from the above theorem seems to be natural in view of Theorem 2.5.

The following theorem applies the results of Theorem 3.1 and Theorem 3.2 to decoherence-free subspaces for quantum channels.

THEOREM 3.3. *Assume that $\Phi(X) = \sum_{i=1}^s A_i X A_i^*$ is a quantum channel.*

(1) *Any common reducing unitary subspace of A_i is nontrivial.*

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

(2) *There exists a one-dimensional decoherence-free subspace for* Φ *if and only if* $\mathcal{M}(A_1, \ldots, A_s, A_1^*, \ldots, A_s^*) \neq 0$. *This condition is computational.*

(2') *Asume that there exists* t *such that* A_t *has pairwise different eigenvalues. We interchange* A_t *with* A_1. *Then there exists a one-dimensional decoherence-free subspace for* Φ *if and only if* $\mathcal{N}(A_1, \ldots, A_s, A_1^*, \ldots, A_s^*) \neq 0$. *This condition is computational.*

(3) *Assume that* $\mathcal{J} = \mathcal{J}(\sqrt{s}A_1, \ldots, \sqrt{s}A_s)$. *If* $\mathcal{J} \neq 0$, *then* $\mathcal{J}$ *is a common reducing unitary subspace of* $A_1, \ldots, A_s$ *and consequently, a decoherence-free subspace for* Φ. *The condition* $\mathcal{J} \neq 0$ *is computable.*

Proof. (1) Assume that W is a common reducing unitary subspace of A_i such that $A_i w = (g_i U)w$ for some $g_i \in \mathbb{C}$ and a unitary operator $U : W \to W$, for any $w \in W$. Since $\sum_{i=1}^s A_i^* A_i = I_n$, we get $\sum_{i=1}^s |g_i| = 1$ and hence there is t such that $g_t \neq 0$. Thus, W is nontrivial.

(2) and (2') Assume that W is a one-dimensional decoherence-free subspace for Φ. It follows from Definition 1.1 and Definition 1.2 that W is a common reducing unitary subspace of $A_1, \ldots, A_s$ of dimension one. We know from (1) that W is nontrivial, and hence, there are equivalences (1)$\Leftrightarrow$(1') and (2)$\Leftrightarrow$(2') of the conditions from Theorem 3.1. Thus, the assertions follow from Theorem 3.1.

(3) We know from Theorem 3.2 that $(\sqrt{s}A_i)|\mathcal{J} = U$ for some unitary operator $U : \mathcal{J} \to \mathcal{J}$. Thus, $A_i|\mathcal{J} = \frac{1}{\sqrt{s}}U$, so $\mathcal{J}$ is a common reducing unitary subspace of $A_1, \ldots, A_s$ and consequently, a decoherence-free subspace for Φ. The condition $\mathcal{J} \neq 0$ is computable since the subspace $\mathcal{J}$ is an intersection of suitable kernels. □

Observe that there exist quantum channels $\Phi(X) = \sum_{i=1}^s A_i X A_i^*$ with the property $\mathcal{J}(\sqrt{s}A_1, \ldots, \sqrt{s}A_s) \neq 0$. Indeed, assume that the matrices $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ have the following block-diagonal form

$$A_i = \begin{bmatrix} \frac{1}{\sqrt{s}}U & 0 \\ 0 & E_i \end{bmatrix}$$

where $U : \mathbb{C}^k \to \mathbb{C}^k$ is an arbitrary unitary operator and the matrices $E_i \in \mathbb{M}_{n-k}(\mathbb{C})$ satisfy the condition $\sum_{i=1}^s E_i^* E_i = I_{n-k}$. Then obviously $\sum_{i=1}^s A_i^* A_i = I_n$ and $(\sqrt{s}A_i)|\mathbb{C}^k = U$. This implies that the assertion of Theorem 3.3 (3) may be useful in practical applications.

4. Remarks. This section is devoted to present some additional comments on the subject matter of the paper. In particular, we relate the results of Section 2 with the problem of the existence of common invariant subspaces of arbitrary dimensions.

4.1. The trivial and the nontrivial case. The proof of the assertions (2) and (2') of Theorem 3.3 convinces to consider general conditions for the existence of

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

common reducing unitary subspaces, i.e., not necessarily conditions only for nontrivial ones, see Section 1 for the definition. Indeed, in some important cases any common reducing unitary subspace is nontrivial, see Theorem 3.3 (1).

Despite of this fact, only the problem of the existence of nontrivial common reducing unitary subspaces is challenging. Indeed, assume that $X_1, \ldots, X_s \in \mathbb{M}_n(\mathbb{C})$. It is easy to see that the subspace $\mathcal{K} = \mathcal{K}(X_1, \ldots, X_s)$ introduced in Section 3 is a trivial common reducing unitary subspace of X_i. Moreover, any such a subspace is contained in $\mathcal{K}$. Hence, there exists a trivial common reducing unitary subspace of X_i if and only if $\mathcal{K} \neq 0$.

It may be sometimes convenient to completely eliminate the case of trivial common reducing unitary subspaces from our considerations. This can be done in the following way.

Observe that $V \cap V' = 0$ for any nontrivial common reducing unitary subspace V of X_i and any trivial one V'. Assume that $Y_i : \mathbb{C}^n \ominus \mathcal{K} \to \mathbb{C}^n \ominus \mathcal{K}$ is defined by $Y_i = X_i|(\mathbb{C}^n \ominus \mathcal{K})$ and let W be a subspace of $\mathbb{C}^n$. The observation yields that the subspace W is a nontrivial common reducing unitary subspace of X_i if and only if W is contained in $\mathbb{C}^n \ominus \mathcal{K}$ and W is a common reducing unitary subspace of Y_i. Moreover, any common reducing unitary subspace of Y_i is nontrivial. These arguments imply that we can study the matrices Y_i instead of X_i if we wish to consider only nontrivial common reducing unitary subspaces of X_i.

4.2. Common invariant subspaces. Assume that $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ have pairwise different eigenvalues. We prove in [9, Corollary 3.3] (see also [1], [5], [17]) that in this case, the matrices A_i have a common invariant subspace of dimension k if and only if the matrices $C_k(\widetilde{A_i})$ have a common eigenvector where $\widetilde{A_i} = A_i - t_i I_n$ for some $t_i \in \mathbb{N}$ and $C_k(\widetilde{A_i})$ denotes the *k-th compound* of $\widetilde{A_i}$, see [14] for the definition and main properties.

In [9, Corollary 3.3] we apply the condition $\mathcal{M} \neq 0$ for the existence of a common eigenvector of A_i, see also Theorem 2.1. The results of Section 2 show that we can suitably exchange the condition $\mathcal{M} \neq 0$ used in [9, Corollary 3.3] to the condition $\mathcal{N} \neq 0$, see Theorem 2.4. As discussed in Section 2, this condition requires less computation than the first one. Consequently, we obtain more efficient computational condition for the existence of a common invariant subspace of dimension k. Note that this condition may be applied as in Section 3 and Section 4 of [9] in checking irreducibility of a given completely positive map. Indeed, it follows by [4] that a completely positive map Φ such that $\Phi(X) = \sum_{i=1}^{s} A_i X A_i^*$ for any $X \in \mathbb{M}_n(\mathbb{C})$ and some $A_i \in \mathbb{M}_n(\mathbb{C})$ is irreducible if and only if the matrices A_i do not have a nontrivial common invariant subspace. Recall that, by the definition, a completely positive map

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

Φ is *irreducible* if and only if there is no nontrivial projector P such that $\Phi(P) \leq \lambda P$ for some $\lambda > 0$.

4.3. Pairwise different eigenvalues. The assumption that the matrix H from Theorem 2.4 has pairwise different eigenvalues seems not to be so strong in practical applications. Indeed, it follows from [3, Lemma 3.1] or [7, Chapter I, Corollary 10] that the set of all $n \times n$ complex matrices having at least one multiple eigenvalue is Lebesgue-measurable, and of measure zero. So if H is random, it should be expected that H has pairwise different eigenvalues. These arguments imply that if $\Phi(X) = \sum_{i=1}^{s} A_i X A_i^*$ is a quantum channel, then we can use the efficient condition $\mathcal{N}(A_1, \ldots, A_s, A_1^*, \ldots, A_s^*) \neq 0$ to check whether there is a decoherence-free subspace for Φ of dimension one.

5. A numerical example. In the last section, we present an application of the criterion given in Theorem 3.1 to three concrete 3×3 matrices A, B and C. Specifically, we check whether A, B, C have a common reducing unitary subspace of dimension one (trivial or nontrivial). These matrices were randomly generated in a computer algebra system under the assumption that their entries belong to the set $\{-3, -2, -1, 0, 1, 2, 3\}$. All calculations given below were performed using the same software.

Assume that

$$A = \begin{bmatrix} 3 & 0 & 1 \\ 3 & 1 & -1 \\ 2 & 0 & -1 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 & -2 \\ -3 & 1 & 1 \\ -3 & -3 & -2 \end{bmatrix}, C = \begin{bmatrix} 3 & -1 & -1 \\ -3 & 2 & 3 \\ -1 & -2 & 1 \end{bmatrix}.$$

We prefer to apply the conditions (2) and (2′) of Theorem 3.1 since these are more efficient than the remaining ones. For this purpose, we check whether A, B or C has pairwise different eigenvalues.

Recall that the *discriminant* $\operatorname{disc}(f)$ of a polynomial $f \in \mathbb{C}[x]$ is the resultant of f and f' where f' denotes the formal derivative of f, see [11, Chapter IV, Section 8]. It is commonly known that $\operatorname{disc}(f) = 0$ if and only if f has a multiple root. Hence, a matrix $Y \in \mathbb{M}_n(\mathbb{C})$ has a pairwise different eigenvalues if and only if $\operatorname{disc}(\chi_Y) \neq 0$ where χ_Y denotes the characteristic polynomial of Y.

We get that $\operatorname{disc}(\chi_A) = 864$, $\operatorname{disc}(\chi_B) = -13419$ and $\operatorname{disc}(\chi_C) = -976$. Thus, all the matrices has pairwise different eigenvalues and the conditions (2) and (2′) of Theorem 3.1 are applicable. Note that this is consistent with Section 4.3.

We set $H = A$, $A_1 = B$, $A_2 = C$, $A_3 = A^*$, $A_4 = B^*$ and $A_5 = C^*$. Then

$$\mathcal{N}(A, B, C, A^*, B^*, C^*) = \mathcal{N}(H, A_1, \ldots, A_5) = \bigcap_{k=1}^{2} \bigcap_{i=1}^{5} \ker[H^k, A_i] = \ker K$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

where

$$K = \sum_{k=1}^{2}\sum_{i=1}^{5}[H^k, A_i]^*[H^k, A_i] = \begin{bmatrix} 14292 & -4376 & -1769 \\ -4376 & 5698 & 3389 \\ -1769 & 3389 & 4484 \end{bmatrix}.$$

Since $\det K = 149782564282 \neq 0$, we get $\mathcal{N}(H, A_1, \ldots, A_5) = 0$ and hence Theorem 3.1 (2) implies that the matrices A, B, C do not have a common reducing unitary subspace of dimension one. This obviously yields these matrices do not have a nontrivial common reducing unitary subspace of dimension one either.

To make the comparison of subspaces $\mathcal{M}$ and $\mathcal{N}$ from Section 2 more concrete (see Remark 2.6), we compute also $\mathcal{M}(A, B, C, A^*, B^*, C^*)$. It follows from Theorem 2.1 that $\mathcal{M}(A, B, C, A^*, B^*, C^*) = \ker K'$ where

$$K' = \sum_{k_i, l_j \in \{0,1,2\}} [B_1^{k_1} \cdots B_6^{k_6}, B_1^{l_1} \cdots B_6^{l_6}]^*[B_1^{k_1} \cdots B_6^{k_6}, B_1^{l_1} \cdots B_6^{l_6}]$$

for $k_1 + \cdots + k_6 \neq 0$, $l_1 + \cdots + l_6 \neq 0$ and $B_1 = A$, $B_2 = B$, $B_3 = C$, $B_4 = A^*$, $B_5 = B^*$, $B_6 = C^*$. We get

$$K' \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 90269511662695957111656 \\ -72804159139519208105154 \\ 2647442205609513388425 0 \end{bmatrix},$$

$$K' \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} -72804159139519208105154 \\ 8538140585480483345688 0 \\ -30062218685628270512574 \end{bmatrix},$$

$$K' \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 26474422056095 13!3884250 \\ -30062218685628270512574 \\ 20348385815244430069452 \end{bmatrix}$$

and $\det K'$ is a nonzero integer having the number of decimal digits equal to 68.

We note that it takes only 9 seconds to calculate K whereas about 165 minutes to calculate K'. This emphasizes the fact that the condition $\mathcal{N} \neq 0$ requires much less computation than the condition $\mathcal{M} \neq 0$.

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 30, pp. 253-270, June 2015

ELA

REFERENCES

[1] Yu. Alpin and Kh.D. Ikramov. Rational procedures in the problem of common invariant subspaces of a pair of matrices. *Journal of Mathematical Sciences (New York)*, 114:1757–1764, 2003.

[2] I. Bengtsson and K. Zyczkowski. *Geometry of Quantum States: An Introduction to Quantum Entanglement*. Cambridge University Press, Cambridge, 2006.

[3] C. Bordenave and D. Chafai. Around the circular law. *Probability Surveys*, 9:1–89, 2012.

[4] D.R. Farenick. Irreducible positive linear maps on operator algebras. *Proceedings of the American Mathematical Society*, 124(11):3381–3390, 1996.

[5] A. George and Kh.D. Ikramov. Common Invariant Subspaces of Two Matrices. *Linear Algebra and its Applications*, 287:171–179, 1999.

[6] I. Gohberg, P. Lancaster, and L. Rodman. *Invariant Subspaces of Matrices with Applications*. Classics in Applied Mathematics, SIAM, Philadelphia, 2006.

[7] R.C. Gunning and H. Rossi. *Analytic Functions of Several Complex Variables*. Prentice-Hall, Inc., Englewood Cliffs, NJ, 1965.

[8] T. Heinosaari and M. Ziman. *The Mathematical Language of Quantum Theory*. Cambridge University Press, Cambridge, 2012.

[9] A. Jamiołkowski and G. Pastuszak. Generalized Shemesh criterion, common invariant subspaces and irreducible completely positive superoperators. *Linear and Multilinear Algebra*, 63:314–325, 2015.

[10] R.I. Karasik, K.P. Marzlin, B.C. Sanders, and K.B. Whaley. Criteria for dynamically stable decoherence-free subspaces and incoherently generated coherences. *Physical Review. A. Third Series*, 77:052301, 2008.

[11] S. Lang. *Algebra*, third edition. Springer-Verlag, New York, 2002.

[12] D.A. Lidar. Review of Decoherence Free Subspaces, Noiseless Subsystems, and Dynamical Decoupling. In S. Kais, Ed., *Quantum Information and Computation for Chemistry: Advances in Chemical Physics*, pp. 295–354, John Wiley and Sons, Inc., Hoboken, NJ, 2014.

[13] D.A. Lidar and T.A. Brun. *Quantum Error Correction*. Cambridge University Press, New York, 2013.

[14] M. Marcus and H. Minc. *A Survey of Matrix Theory and Matrix Inequalities*. Dover Publications, Inc., New York, 1992.

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

[16] D. Shemesh. Common eigenvectors of two matrices. *Linear Algebra and its Applications*, 62:11–18, 1984.

[17] M. Tsatsomeros. A criterion for the existence of common invariant subspaces of matrices. *Linear Algebra and its Applications*, 322:51–59, 2001.

[18] P. Zanardi and D.A. Lidar. Purity and state fidelity of quantum channels. *Physical Review. A. Third Series*, 70:012315, 2004.