Generalized Shemesh criterion, common invariant subspaces and irreducible completely positive superoperators

Andrzej Jamiołkowski\textsuperscript{a} and Grzegorz Pastuszak\textsuperscript{b}\textsuperscript{*}

\textsuperscript{a}Faculty of Physics, Astronomy and Informatics, Nicolaus Copernicus University, Toruń, Poland; \textsuperscript{b}Center for Theoretical Physics of the Polish Academy of Sciences, Warszawa, Poland

Communicated by K. Audenaert

(Received 1 June 2013; accepted 8 November 2013)

Assume that $A_1, \ldots, A_s$ are complex $n \times n$ matrices. We give a computable criterion for existence of a common eigenvector of $A_i$ which generalize the result of D. Shemesh established for two matrices. We use this criterion to prove some necessary and sufficient condition for $A_i$ to have a common invariant subspace of dimension $d$, $2 \leq d < n$, if every $A_i$ has pairwise different eigenvalues. Since the set of all matrices having multiple eigenvalues has Lebesgue measure 0, the condition is sufficient in practical applications. Being motivated by quantum information theory, we give a flavour of such applications for irreducible completely positive superoperators.

Keywords: Shemesh criterion; common eigenvectors; common invariant subspaces; irreducible operators; completely positive superoperators

AMS Subject Classifications: 15A18; 47A15

1. Introduction and the main results

Quantum theory, in its nonrelativistic formulation, is built on the theory of Hilbert spaces and operators. Assume that $\mathcal{H}$ is a fixed Hilbert space associated with a given quantum system $S$. We denote by $B(\mathcal{H})$, the set of all linear continuous operators on $\mathcal{H}$. Then the set of states of the system $S$ is, by definition, represented by all semipositive elements of $B(\mathcal{H})$ with trace equal to one. This set of states will be denoted by $S(\mathcal{H})$.

In the beginning of seventies, it appeared that some natural questions connected with fundamentals of quantum mechanics (more precisely, with the theory of open quantum systems) lead to investigations of linear maps in a real Banach space of self-adjoint operators on a fixed Hilbert space (for details we refer to [1,2]). The concept of a Banach space with the partial order defined by a specific cone, namely, the cone of positive semidefinite operators, constitutes a basic idea in the description of open quantum systems and in the quantum information theory ([1], cf. also the last section of this paper).

In this paper, we consider finite dimensional Hilbert spaces – such spaces are the current focus in quantum computing and quantum information theory for experimental reasons. This means we assume $\mathcal{H} \cong \mathbb{C}^n$ and $B(\mathcal{H}) \cong M_n(\mathbb{C})$. It should be stressed that to describe all

\textsuperscript{*}Corresponding author. Email: past@mat.umk.pl

© 2014 Taylor & Francis
possible changes of quantum states, one has to consider some specific linear operators in \( B(\mathcal{H}) \). Very often, at least in physical literature, they are called superoperators. The general form of such maps is well known. Namely, for a given superoperator \( \Phi : B(\mathcal{H}) \to B(\mathcal{H}) \), \( \dim \mathcal{H} < \infty \), there always exists an operator-sum representation given by

\[
\Phi(X) = \sum_{i=1}^{s} A_i XB_i,
\]

where \( A_i, B_i \) are elements of \( B(\mathcal{H}) \), for all \( i = 1, \ldots, s \). A particular class of such maps, the so-called completely positive maps (or in physical terminology quantum operations or quantum channels), plays a prominent role in formulations of evolution of open quantum systems and in the theory of quantum measurements.

It is obvious from the above considerations that properties of superoperators \( \Phi : B(\mathcal{H}) \to B(\mathcal{H}) \) are connected with properties of the sets \( \{A_1, \ldots, A_s\} \) and \( \{B_1, \ldots, B_s\} \) of matrices. In particular, in case of completely positive maps, we have \( B_i = A_i^* \) for \( i = 1, \ldots, s \), where \( A_i^* \) denotes matrix adjoint to \( A_i \), and thus quantum channels are described by maps of the form

\[
\Phi(X) = \sum_{i=1}^{s} A_i X A_i^*.
\]

The matrices \( A_i \) occuring in the expression above are called the Kraus coefficients of \( \Phi \) and the \(*\)-matrix algebra generated by them is called the interaction algebra.

Motivated by the main results of [3], we discuss in the paper some properties of a completely positive map \( \Phi \) of the form \((**\) in terms of common invariant subspaces of its Kraus coefficients \( A_i \). Namely, it turns out that \( \Phi \) is irreducible (see [3] or the last section of the paper) if and only if the matrices \( A_i \) do not have a nontrivial common invariant subspace.

This paper is devoted to give a computable criterion for a completely positive superoperator \( \Phi \) to be irreducible. By computable criterion (or computable condition), we mean a procedure employing only finite number of arithmetic operations. Note that in various applications of mathematics, it is very often crucial to have rather computable conditions than more theoretical ones.

To establish the criterion, we give at first a computable condition for the matrices \( A_1, \ldots, A_s \) to have a common invariant subspace of a fixed dimension \( d \).

In what follows, we consequently assume that \( B(\mathcal{H}) \cong \mathbb{M}_n(\mathbb{C}) \) is the vector space of all \( n \times n \) complex matrices.

Assume that \( x \in \mathbb{C}^n, x \neq 0 \). We say that \( x \) is a common eigenvector of \( A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C}) \) if and only if \( x \) is an eigenvector of every \( A_i \), that is, \( A_i x = \mu_i x \) for some \( \mu_i \in \mathbb{C} \).

Assume that \( W \) is a subspace of \( \mathbb{C}^n \). We say that \( W \) is a common invariant subspace of \( A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C}) \) if and only if \( W \) is \( A_i \)-invariant for all \( i = 1, \ldots, s \), that is, \( A_i w \in W \) for all \( w \in W \). It is clear that \( A_i \) have a common eigenvector if and only if \( A_i \) have a common invariant subspace of dimension 1.

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 [4] Shemesh proved the following criterion for existence of common eigenvector of two complex matrices \( A \) and \( B \).
Theorem 1.1 ([4, Theorem 3.1]) Assume that \(A, B \in \mathbb{M}_n(\mathbb{C})\) and
\[
\mathcal{N}(A, B) := \bigcap_{k,l=1}^{n-1} \ker[A^k, B^l].
\]
Then \(A\) and \(B\) have a common eigenvector if and only if \(\mathcal{N}(A, B) \neq 0\).

It is observed in [4] that \(\mathcal{N}(A, B) = \ker K\), where
\[
K = \sum_{k,l=1}^{n-1} [A^k, B^l]^*[A^k, B^l]
\]
and \(X^*\) denotes matrix adjoint to \(X\). It follows that the condition
\[
\mathcal{N}(A, B) = \bigcap_{k,l=1}^{n-1} \ker[A^k, B^l] \neq 0
\]
is computable since a finite number of arithmetic operations allows us to check if \(\det K = 0\) or not.

In view of Theorem 1.1, it is natural to consider the following problem: Is there a computable condition verifying the existence of common invariant subspace of dimension \(d\) of \(s\) complex \(n \times n\) matrices \(A_1, \ldots, A_s\), where \(1 \leq d < n\) and \(s \geq 2\)?

Partial solutions to this problem are given in [5–7] and [8], where it is mainly assumed that \(s = 2\). In [5] and [6], the authors study the case when algebra generated by two complex matrices is semisimple and use the concept of a standard polynomial, see [9], Section 20.4. In [7] and [8], the authors reduce the general problem to the question of existence of common eigenvector of suitable compound matrices, see [10].

The general version of the problem with arbitrary \(d\) and \(s\) is solved completely in [11], where some techniques of Gröbner bases theory and algebraic geometry are used.

In this paper, we present a different approach to the problem discussed. Namely, for \(d = 1\) we prove the following computable generalization of the Shemesh criterion.

Theorem 1.2 Assume that \(A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})\) and
\[
\mathcal{M}(A_1, \ldots, A_s) = \bigcap_{k_i,l_i \geq 0, k_1+k_2+\ldots+k_s \neq 0, l_1+l_2+\ldots+l_s \neq 0} \ker[A_1^{k_1} \ldots A_s^{k_s}, A_1^{l_1} \ldots A_s^{l_s}].
\]

(1) Matrices \(A_i\) have a common eigenvector if and only if
\[
\mathcal{M}(A_1, \ldots, A_s) \neq 0.
\]
(2) We have $\mathcal{M}(A_1, \ldots, A_s) = \ker K$ where

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

If $d > 1$ and each of $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ has pairwise different eigenvalues, we apply Theorem 1.2 to establish a computable criterion for existence of common invariant subspace of $A_i$ of dimension $d$. In this approach, we make use of some methods presented in [7] and [8].

Observe that our criterion may be considered as sufficient for practical applications. Indeed, the set of all matrices having at least one multiple eigenvalue is Lebesgue-measurable, and its measure is equal to zero, see for example [12, Lemma 3.1]. This yields that when matrices $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ are random it is reasonable to expect that none of them has multiple eigenvalues.

In the final section of the paper, we give a flavour of such practical applications presenting a computable method of verifying whether a completely positive superoperator defined by its Kraus coefficients is irreducible.

2. The generalized Shemesh criterion

This section is devoted to the proof of Theorem 1.2 which we shall call the generalized Shemesh criterion.

Observe that the following commonly known result holds, see for example [13].

**Proposition 2.1** Assume that $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ and $X$ is a nonzero $A_i$-invariant subset of $\mathbb{M}_n(\mathbb{C})$ such that $(A_i A_j)x = (A_j A_i)x$ for any $x \in X$. Then there is a common eigenvector $u$ of $A_i$ such that $u \in X$.

The following theorem generalizes [4, Theorem 3.1].

**Theorem 2.2** Assume that $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ and

$$\mathcal{M}(A_1, \ldots, A_s) := \bigcap_{k_i, l_j \geq 0}^{\infty} \ker \left[ A_1^{k_1} \ldots A_s^{k_s}, A_1^{l_1} \ldots A_s^{l_s} \right].$$

(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

$$\mathcal{M}(A_1, \ldots, A_s) \neq 0.$$ 

**Proof** (1) If $\mathcal{M}(A_1, \ldots, A_s) = 0$ then clearly $\mathcal{M}(A_1, \ldots, A_s)$ is $A_i$-invariant. Hence assume that $\mathcal{M}(A_1, \ldots, A_s) \neq 0$ and let $v \in \mathcal{M}(A_1, \ldots, A_s)$. We set

$$\mathcal{P}_v := \{ p(A_1, \ldots, A_s)v | p \in \mathbb{C}(x_1, \ldots, x_s) \}. $$
We will show that $P \subseteq M(A_1, \ldots, A_s)$ for any $v \in M(A_1, \ldots, A_s)$.

Assume that $k_1, \ldots, k_s, l_1, \ldots, l_s \geq 0$. If $k_2 + \ldots + k_s \neq 0$ and $l_1 + \ldots + l_s \neq 0$, then

$$\left( A_1^{k_1} \ldots A_s^{k_s} \right) \left( A_1^{l_1} \ldots A_s^{l_s} \right) v = A_1^{k_1} \left[ \left( A_2^{k_2} \ldots A_s^{k_s} \right) \left( A_1^{l_1} \ldots A_s^{l_s} \right) \right] v$$

$$= A_1^{k_1} \left[ \left( A_1^{l_1} \ldots A_s^{l_s} \right) \left( A_2^{k_2} \ldots A_s^{k_s} \right) \right] v = A_1^{k_1+l_1} \left[ \left( A_2^{l_2} \ldots A_s^{l_s} \right) \left( A_2^{k_2} \ldots A_s^{k_s} \right) \right] v$$

since $v \in \ker[A_2^{k_2} \ldots A_s^{k_s}, A_1^{l_1} \ldots A_s^{l_s}]$.

If $k_2 + \ldots + k_s = 0$ or $l_1 + \ldots + l_s = 0$, then also

$$\left( A_1^{k_1} \ldots A_s^{k_s} \right) \left( A_1^{l_1} \ldots A_s^{l_s} \right) v = A_1^{k_1+l_1} \left[ \left( A_2^{l_2} \ldots A_s^{l_s} \right) \left( A_2^{k_2} \ldots A_s^{k_s} \right) \right] v.$$

Therefore, a simple induction argument implies that

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

for any $k_1, \ldots, k_s, l_1, \ldots, l_s \geq 0$. It follows that if $q \in \mathbb{C}(x_1, \ldots, x_s)$, then

$$q( A_1 \ldots A_s ) v = \left( \sum_{0 \leq t_1 \leq \deg(q)} a_{t_1}^q A_1^{l_1} \ldots A_s^{l_s} \right) v$$

for some $a_{t_1}^q, \ldots, a_{t_s}^q \in \mathbb{C}$.

Moreover,

$$\left( A_1^{k_1} \ldots A_s^{k_s} \right) \left( A_1^{l_1} \ldots A_s^{l_s} \right) q( A_1 \ldots A_s ) v$$

$$= \left( A_1^{k_1} \ldots A_s^{k_s} \right) \left( A_1^{l_1} \ldots A_s^{l_s} \right) \left( \sum_{0 \leq t_1 \leq \deg(q)} a_{t_1}^q A_1^{l_1} \ldots A_s^{l_s} \right) v$$

$$= \sum_{0 \leq t_1 \leq \deg(q)} a_{t_1}^q \left( A_1^{k_1} \ldots A_s^{k_s} \right) \left( A_1^{l_1} \ldots A_s^{l_s} \right) A_1^{l_1} \ldots A_s^{l_s} v$$

$$= \sum_{0 \leq t_1 \leq \deg(q)} a_{t_1}^q \left( A_1^{t_1} A_1^{l_1} \ldots A_1^{l_s} A_s^{k_2} \ldots A_s^{k_s} + k_1 \ldots k_s \right) v$$

and thus $q( A_1, \ldots, A_s ) v \in \ker[A_1^{k_1} \ldots A_s^{k_s}, A_1^{l_1} \ldots A_s^{l_s}]$ for any $q \in \mathbb{C}(x_1, \ldots, x_s)$ and $k_1, \ldots, k_s, l_1, \ldots, l_s \geq 0$.

This implies that $P \subseteq M(A_1, \ldots, A_s)$ for any $v \in M(A_1, \ldots, A_s)$ and hence

$$M(A_1, \ldots, A_s) = \bigcup_{v \in M(A_1, \ldots, A_s)} P_v.$$
This shows that the subspace $\mathcal{M}(A_1, \ldots, A_s)$ is $A_i$-invariant since clearly $P_v$ is $A_i$-invariant, for any $i = 1, \ldots, s$.

(2) Assume that $x \in \mathbb{C}^n$ is a common eigenvector of $A_i$ such that $A_ix = \mu_ix$ for some $\mu_i \in \mathbb{C}$. Then

$$\left( A_1^{k_1} \ldots A_s^{k_s} \right) \left( A_1^{l_1} \ldots A_s^{l_s} \right) x = \mu_1^{k_1+l_1} \ldots \mu_s^{k_s+l_s} x = \left( A_1^{l_1} \ldots A_s^{l_s} \right) \left( A_1^{k_1} \ldots A_s^{k_s} \right) x$$

hence, $x \in \ker[A_1^{k_1} \ldots A_s^{k_s}, A_1^{l_1} \ldots A_s^{l_s}]$ for any $k_i, l_j \geq 0$. It follows that $x \in \mathcal{M}(A_1, \ldots, A_s)$ and $\mathcal{M}(A_1, \ldots, A_s) \neq 0$.

$\Leftarrow$ The subspace $\mathcal{M}(A_1, \ldots, A_s)$ is $A_i$-invariant by (1). Moreover, if $x \in \mathcal{M}(A_1, \ldots, A_s)$, then $x \in \ker[A_i, A_j]$ for any $i, j = 1, \ldots, s$ and thus $A_i$ commute on $\mathcal{M}(A_1, \ldots, A_s)$. Since $\mathcal{M}(A_1, \ldots, A_s) \neq 0$, it follows by Proposition 2.1 that $A_i$ have a common eigenvector $v \in \mathcal{M}(A_1, \ldots, A_s)$.

In the following corollary, we show that the condition

$$\mathcal{M}(A_1, \ldots, A_s) \neq 0$$

is computable, i.e. it can be checked in finite number of arithmetic operations.

**Corollary 2.3** Assume that $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$. Then the following equalities hold for $\mathcal{M}(A_1, \ldots, A_s)$ defined in Theorem 2.2.

(1) $\mathcal{M}(A_1, \ldots, A_s) = \bigcap_{k_1, l_1 \geq 0} \ker \left[ A_1^{k_1} \ldots A_s^{k_s}, A_1^{l_1} \ldots A_s^{l_s} \right].$

(2) $\mathcal{M}(A_1, \ldots, A_s) = \ker K$, where

$$K = \sum_{k_1, l_1 \geq 0} \left[ A_1^{k_1} \ldots A_s^{k_s}, A_1^{l_1} \ldots A_s^{l_s} \right] \left[ A_1^{k_1} \ldots A_s^{k_s}, A_1^{l_1} \ldots A_s^{l_s} \right]^*.$$

**Proof** (1) Assume that $t_1, \ldots, t_s \geq 0$. It follows easily by the renowned theorem of Cayley and Hamilton that $A_1^{l_1} \ldots A_s^{l_s}$ is a linear combination of $A_1^{k_1} \ldots A_s^{k_s}$ for some $0 \leq k_i \leq n - 1$. Moreover, observe that

$$[A + B, C + D] = [A, C] + [A, D] + [B, C] + [B, D]$$

and hence,

$$\ker[A, C] \cap \ker[A, D] \cap \ker[B, C] \cap \ker[B, D] \subseteq \ker[A + B, C + D]$$

for any $A, B, C, D \in \mathbb{M}_n(\mathbb{C})$. This implies what is required.

(2) 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 semidefinite. Hence, the equality follows by (1). \qed
Proof of Theorem 1.2 (1) is a consequence of Theorem 2.2 (2) and Corollary 2.3 (1) whereas (2) of Corollary 2.3 (2).

Note that Theorem 1.2 provide us a computable condition verifying the existence of a common eigenvector of \( s \geq 2 \) complex matrices \( A_1, \ldots, A_s \in M_n(\mathbb{C}) \). The condition is a generalization of [4, Theorem 3.1] since \( \mathcal{N}(A, B) = \mathcal{N}(A, B) \) for all \( A, B \in M_n(\mathbb{C}) \), see Theorem 1.1.

Indeed, it is easy to see from the proof of [4, Theorem 3.1] that if \( v \in \mathcal{N}(A, B) \), then
\[
(A^{p_1}B^{p_2})(A^{q_1}B^{q_2})v = (A^{p_1+q_1}B^{p_2+q_2})v = (A^{q_1}B^{q_2})(A^{p_1}B^{p_2})v
\]
for all \( p_1, p_2, q_1, q_2 \geq 0 \) and hence \( v \in \ker[A^{p_1}B^{p_2}, A^{q_1}B^{q_2}] \). This implies that \( \mathcal{N}(A, B) \subseteq \mathcal{M}(A, B) \) and since clearly \( \mathcal{M}(A, B) \subseteq \mathcal{N}(A, B) \), we get \( \mathcal{N}(A, B) = \mathcal{M}(A, B) \).

3. Common invariant subspaces of higher dimensions

In Section 2, we proved a computable criterion that allows one to check whether there exists a common eigenvector of \( s \geq 2 \) complex matrices \( A_1, \ldots, A_s \in M_n(\mathbb{C}) \), or equivalently, a common invariant subspace of dimension 1.

In this section, we apply the above result to show a computable criterion for existence of a common invariant subspace of dimension \( d \geq 2 \) of matrices \( A_1, \ldots, A_s \in M_n(\mathbb{C}) \), if any \( A_i \) has pairwise different eigenvalues. Our approach bases on methods from [7] and [8].

Recall that by [12, Lemma 3.1] the set of all \( n \times n \) complex matrices having at least one multiple eigenvalue is Lebesgue-measurable, and of measure zero (observe that the result follows easily from [14, Chapter I, Corollary 10]). This can be understood in the following way: if all matrices \( A_1, \ldots, A_s \in M_n(\mathbb{C}) \) are random then it should be expected that each one of them has pairwise different eigenvalues. In consequence, this assumption seems not to be so strong in practical applications.

First we recall the definition of \( k \)-\textit{th compound} of a matrix, see [10].

Assume that \( n \geq 1 \) and \( \alpha, \beta \subseteq \langle n \rangle \), where \( \langle s \rangle := \{1, \ldots, s\} \) for any \( s \in \mathbb{N} \). If \( A \in M_n(\mathbb{C}) \), we denote by \( A[\alpha|\beta] \) a submatrix of \( A \) composed from rows of \( A \) indexed by \( \alpha \) and columns of \( A \) indexed by \( \beta \).

Assume that \( k \leq n \) and
\[
Q_{k,n} := \{(i_1, \ldots, i_k) \in \mathbb{N}^k | 1 \leq i_1 < i_2 < \ldots < i_k \leq n\}
\]
is the set of all \( k \)-tuples of elements from \( \langle n \rangle \) ordered lexicographically.

The \( k \)-\textit{th compound} of \( A \in M_n(\mathbb{C}) \) is defined to be the matrix
\[
C_k(A) := [\det A[\alpha|\beta]]_{\alpha,\beta \in Q_{k,n}} \in M_{(\langle n \rangle)^k}(\mathbb{C}).
\]

The following theorem is implicitly contained in [8]. It generalizes [7, Theorem 2.2] and [7, Theorem 3.1] for the case of \( s \) complex matrices where \( s \geq 2 \).

**Theorem 3.1** Assume that \( A_1, \ldots, A_s \in M_n(\mathbb{C}) \) are nonsingular, \( k \in \mathbb{N}, 2 \leq k < n \) and \( C_k(A_1), \ldots, C_k(A_s) \) have pairwise different eigenvalues. Then \( A_i \) have a common invariant subspace of dimension \( k \) if and only if \( C_k(A_i) \) have a common eigenvector.
Proof Theorem follows easily from the proof of [8, Theorem 2.2].

We can exchange assumptions of Theorem 3.1 for the assumption that \( A_1, \ldots, A_s \) have pairwise different eigenvalues. It can be easily concluded from the proposition below which is essentially the same as [7, Lemma 2.4].

**Proposition 3.2** Assume that \( A \in \mathbb{M}_n(\mathbb{C}) \) has pairwise different eigenvalues, \( k \in \mathbb{N} \) and \( 2 \leq k < n \). Then there is \( t \in \{0, \ldots, p\} \), where

\[
p = \frac{\binom{n}{k}}{2} \left( \binom{n}{k} - 1 \right) (k - 1)
\]

such that \( A - t1_n \) is nonsingular and \( C_k(A - t1_n) \) has pairwise different eigenvalues.

Proof It follows by [7, Lemma 2.4] that there is \( t \in \{0, \ldots, p\} \) where

\[
p = \frac{\binom{n}{k}}{2} \left( \binom{n}{k} - 1 \right) (k - 1)
\]

such that \( C_k(A - t1_n) \) has pairwise different eigenvalues. All eigenvalues of \( C_k(A - t1_n) \) are of the form \((t - \lambda_{i_1})(t - \lambda_{i_2})\ldots(t - \lambda_{i_k})\) where \( 1 \leq i_1 < i_2 < \ldots < i_k \leq n \) and \( \lambda_1, \lambda_2, \ldots, \lambda_n \) are eigenvalues of \( A \), see [7, Theorem 2.1 (7)]. This implies that \( t \) is not an eigenvalue of \( A \) since otherwise it is clear that 0 is a multiple eigenvalue of \( C_k(A - t1_n) \). Hence, \( \det(A - t1_n) \neq 0 \) and \( A - t1_n \) is nonsingular.

In the following theorem, we present a necessary and sufficient condition for complex matrices with pairwise different eigenvalues to have a common invariant subspace of a fixed dimension. The result applies Theorem 1.2.

**Corollary 3.3** Assume that \( A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C}) \) have pairwise different eigenvalues and \( k \in \mathbb{N}, 2 \leq k < n \).

1. There are \( t_1, \ldots, t_s \in \{0, \ldots, p\} \) where

\[
p = \frac{\binom{n}{k}}{2} \left( \binom{n}{k} - 1 \right) (k - 1)
\]

such that \( \tilde{A}_i := A_i - t_i1_n \) are nonsingular and \( C_k(\tilde{A}_i) \) have pairwise different eigenvalues.

2. The matrices \( A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C}) \) have a common invariant subspace of dimension \( k \) if and only if \( C_k(\tilde{A}_i) \) have a common eigenvector.

3. The matrices \( A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C}) \) have a common invariant subspace of dimension \( k \) if and only if \( \ker K \neq 0 \) where

\[
K = \sum_{k_i, l_j \geq 0 \atop k_1 + k_2 + \ldots + k_s \neq 0 \atop l_1 + l_2 + \ldots + l_s \neq 0} \left[ X_1^{k_1} \ldots X_s^{k_s}, X_1^{l_1} \ldots X_s^{l_s} \right]^* \left[ X_1^{k_1} \ldots X_s^{k_s}, X_1^{l_1} \ldots X_s^{l_s} \right]
\]

and \( X_i := C_k(\tilde{A}_i) \) for \( i = 1, \ldots, s \).
Proof. (1) follows by Proposition 3.2. (2) follows by (1), Theorem 3.1 and a simple fact that $A_i$ have a common invariant subspace $W$ if and only if $A_i - q_i 1_n$ have a common invariant subspace $W$, for any $W \subseteq \mathbb{C}^n$ and $q_i \in \mathbb{C}$. (3) follows by (2) and Theorem 1.2. □

Now, we propose a finite and deterministic algorithm verifying the existence of a common invariant subspace of $A_1, \ldots, A_s \in M_n(\mathbb{C})$ of a fixed dimension $d$ provided every $A_i$ has pairwise different eigenvalues.

Recall first that the discriminant $\text{disc}(f)$ of a polynomial $f \in \mathbb{C}[x]$ is, by the definition, the resultant of $f$ and $f'$ where $f'$ denotes the formal derivative of $f$, see [15, Chapter IV, Section 8].

It is commonly known that $\text{disc}(f) = 0$, if and only if $f$ has a multiple root. Obviously, the condition $\text{disc}(f) = 0$ is computable.

**Algorithm.** Input: $A_1, \ldots, A_s \in M_n(\mathbb{C})$ having pairwise different eigenvalues and $d \in \{1, \ldots, n - 1\}$. Output: ‘yes’ if there is a common invariant subspace of dimension $d$ and ‘no’ otherwise.

1. If $d = 1$, compute $\mathcal{M}(A_1, \ldots, A_s)$ and check whether $\mathcal{M}(A_1, \ldots, A_s) \neq 0$ using Theorem 1.2. If $\mathcal{M}(A_1, \ldots, A_s) \neq 0$, print ‘yes’, otherwise print ‘no’.
2. If $d \geq 2$, compute $p = \binom{n}{d} (d-1)$ and $t_i \in \{0, \ldots, p\}$ such that $\det(\tilde{A}_i) \neq 0$ and $\text{disc}(f_i) \neq 0$ where $\tilde{A}_i := A - t_i 1_n$ and $f_i$ denotes the characteristic polynomial of $C_d(\tilde{A}_i)$. Go to the step 3.
3. Compute $\ker K$, where the matrix $K$ is the matrix from Corollary 3.3 (3). If $\ker K \neq 0$, print ‘yes’, otherwise print ‘no’. □

The correctness of the above algorithm follows from Theorem 1.2 and Corollary 3.3.

We shall now present an application of the above algorithm to three concrete $3 \times 3$ matrices $A$, $B$ and $C$. 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 presented below without details were done in the same computer algebra system and can be easily repeated in any other one.

Assume that

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

Then $\mathcal{M}(A, B, C) = \ker K$, where

$$K = \sum_{x,y,z,a,b,c \geq 0 \atop x+y+z \neq 0 \atop a+b+c \neq 0} [A^x B^y C^z, A^a B^b C^c]^* [A^x B^y C^z, A^a B^b C^c] = \begin{bmatrix} 318093544828 & 344449876 & 2439397518 \\ 344449876 & 93442719998 & -53853796564 \\ 2439397518 & -53853796564 & 312435993812 \end{bmatrix}.$$
Since the matrix $K$ is nonsingular, we get $\mathcal{M}(A, B, C) = 0$ and hence the matrices $A$, $B$ and $C$ do not have a common eigenvector, or equivalently, a common invariant subspace of dimension 1.

Observe that

$$C_2(A) = \begin{bmatrix} 9 & -9 & -3 \\ 9 & -9 & 0 \\ 3 & -6 & -2 \end{bmatrix}, \quad C_2(B) = \begin{bmatrix} 1 & -6 & 2 \\ 8 & -6 & 2 \\ 3 & -4 & 6 \end{bmatrix}, \quad C_2(C) = \begin{bmatrix} -4 & 6 & -1 \\ 1 & -9 & 4 \\ 6 & -9 & 9 \end{bmatrix}.$$

Moreover, the matrices $A$, $B$, $C$ are nonsingular and have pairwise different eigenvalues. Since $C_2(A)$, $C_2(B)$ and $C_2(C)$ also have pairwise different eigenvalues, the matrices $A$, $B$ and $C$ have a common invariant subspace of dimension 2 if and only if $\mathcal{M}(X, Y, Z) = \ker K' \neq 0$ where $X = C_2(A)$, $Y = C_2(B)$, $Z = C_2(C)$ and

$$K' = \sum_{x, y, z, a, b, c \geq 0} \sum_{x+y+z \neq 0} \sum_{a+b+c \neq 0} [X^xY^yZ^z, X^aY^bZ^c]^* [X^xY^yZ^z, X^aY^bZ^c] = \begin{bmatrix} 953052882412686980 & -1200501514572913728 & 1748291455051463970 \\ -1200501514572913728 & 13205493879907762240 & -6658460582311823052 \\ 1748291455051463970 & -6658460582311823052 & 8278709434752866020 \end{bmatrix}.$$  

Since the matrix $K'$ is nonsingular, we get $\mathcal{M}(X, Y, Z) = 0$ and hence the matrices $A$, $B$ and $C$ do not have a common invariant subspace of dimension 2.

Observe that the result of our algorithm applied to the above example should not surprise. Indeed, it follows easily from [14, Chapter I, Corollary 10] that the set of all $s$-tuples $(A_1, \ldots, A_s)$ of $n \times n$ complex matrices (without multiple eigenvalues) having a nontrivial common invariant subspace is Lebesgue-measurable, and of measure zero.

4. An application to completely positive superoperators

This section is devoted to show an application of our results in the theory of completely positive superoperators defined on a finite-dimensional complex Hilbert space, see [1,2].

Assume that $\mathcal{H}$ is a complex Hilbert space and $B(\mathcal{H})$ is the set of all linear continuous operators on $\mathcal{H}$. It is commonly known that $B(\mathcal{H})$ is equipped with the structure of a Banach space. As it was mentioned in Section 1, a linear and continuous map $\Phi : B(\mathcal{H}) \to B(\mathcal{H})$ on $B(\mathcal{H})$ is called a superoperator.

Assume that $\mathcal{H}$ is a complex finite-dimensional Hilbert space and $\dim(\mathcal{H}) = n$. A superoperator $\Phi : B(\mathcal{H}) \to B(\mathcal{H})$ on $B(\mathcal{H})$ of the form

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

where $K_i \in B(\mathcal{H})$ is completely positive. Such operators play a prominent role in quantum information theory, see [1,16,17] for details.

The operators $K_1, \ldots, K_s \in B(\mathcal{H})$ in the above formula are called the Kraus coefficients of $\Phi$. Clearly, they can be viewed as arbitrary $n \times n$ complex matrices and also can be treated as objects that define $\Phi$. 
Important subclass of the class of all completely positive superoperators is formed by *irreducible* completely positive superoperators. Recall that a completely positive superoperator \( \Phi : B(H) \to B(H) \) is irreducible if and only if there is no nontrivial projector \( P \) such that \( \Phi(P) \leq \lambda P \) for some \( \lambda > 0 \). Alternatively, superoperator \( \Phi \) is irreducible if no face of the positive cone in \( B(H) \) is invariant under \( \Phi \). Recall that a face \( F \) is a subcone of the positive cone in \( B(H) \) such that if \( 0 \leq B \leq A \) and \( A \in F \) then also \( B \in F \). Let us recall that every face in a finite dimensional *-matrix algebra is closed and there exists a projection \( P \) (i.e. \( P = P^* \) and \( P^2 = P \)) such that \( F \) can be represented by \( F = PAP \) where in our case \( A \) denotes the interaction algebra generated by Kraus operators.

The following theorem connects irreducible completely positive superoperators with the subject matter of the paper.

**Theorem 4.1** (see [3]) Assume that \( \mathcal{H} \) is a complex finite-dimensional Hilbert space and \( \Phi : B(H) \to B(H) \) is a completely positive superoperator on \( B(H) \) such that \( \Phi(X) = \sum_{i=1}^{s} K_i X K_i^* \). Then \( \Phi \) is irreducible if and only if the matrices \( K_i \) do not have a nontrivial common invariant subspace in \( \mathcal{H} \).

The above theorem allows to apply the algorithm presented in Section 3 in checking irreducibility of a given completely positive superoperator, if its Kraus coefficients do not have a multiple eigenvalue. As it was emphasized before, such a situation should be quite common in practical applications.

One can say even more. We will have an invariant subspace of the superoperator \( \Phi \) (quantum operation) if and only if \( K \) defined in Corollary 3.3 satisfies the inequality \( \det K > 0 \). Obviously, this property can be checked in a finite number of steps.

**Acknowledgements**
The authors are grateful to the anonymous referees for helpful comments that improved the paper enormously.

**Funding**
This research has been supported by [grant number DEC-2011/02/A/ST1/00208] of the National Science Centre of Poland.

**References**

[1] Heinosaari T, Ziman M. The mathematical language of quantum theory. Cambridge: Cambridge Univ. Press; 2012.
[2] Jamiołkowski A. Effective methods in investigation of irreducible quantum operations. Int. J. Geom. Methods Mod. Phys. 2012;9: 8p. Paper No.14.
[3] Farenick DR. Irreducible positive linear maps on operator algebras. Proc. Amer. Math. Soc. 1996;124:3381–3390.
[4] Shemesh D. Common eigenvectors of two matrices. Linear Algebra Appl. 1984;62:11–18.
[5] Alpin Yu, George A, Ikramov KhD. Solving the two dimensional CIS problem by a rational algorithm. Linear Algebra Appl. 2000;312:115–123.
[6] Alpin Yu, Ikramov KhD. Rational procedures in the problem of common invariant subspaces of two matrices. J. Math. Sci. 2003;114:1757–1764.
[7] George A, Ikramov KhD. Common invariant subspaces of two matrices. Linear Algebra Appl. 1999;287:171–179.
[8] Tsatsomeros M. A criterion for the existence of common invariant subspaces of matrices. Linear Algebra Appl. 2001;322:51–59.
[9] Pierce RS. Associative algebras. New York (NY): Springer-Verlag; 1982.
[10] Marcus M, Minc H. A survey of matrix theory and matrix inequalities. New York (NY): Dover; 1992.
[11] Arapura D, Peterson Ch. The common invariant subspace problem: an approach via Gröbner bases. Linear Algebra Appl. 2004;384:1–7.
[12] Bordenave Ch, Chafai D. Around the circular law. Probab. Surveys. 2009;9:1–89.
[13] Gohberg I, Lancaster P, Rodman L. Invariant subspaces of matrices with applications, Classics in applied mathematics. Philadelphia (PA): SIAM; 2006.
[14] Gunning RC, Rossi H. Analytic functions of several complex variables, Prentice-Hall series in modern analysis. London: Prentice-Hall; 1965.
[15] Lang S. Algebra. Revised 3rd ed. New York (NY): Springer, GTM 211; 2002.
[16] Nielsen MA, Chuang IL. Quantum computation and quantum information. Cambridge: Cambridge Univ. Press; 2010.
[17] Bengtsson I, Zyczkowski K. Geometry of quantum states: an introduction to quantum entanglement. Cambridge: Cambridge Univ. Press; 2006.