Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 32, pp. 343-356, August 2017.

THE COMMON INVARIANT SUBSPACE PROBLEM AND TARSKI'S THEOREM*

GRZEGORZ PASTUSZAK†

Abstract. This article presents a computable criterion for the existence of a common invariant subspace of $n \times n$ complex matrices $A_1, \ldots, A_s$ of a fixed dimension $1 \leq d \leq n$. The approach taken in the paper is model-theoretic. Namely, the criterion is based on a constructive proof of the renowned Tarski's theorem on quantifier elimination in the theory ACF of algebraically closed fields. This means that for an arbitrary formula φ of the language of fields, a quantifier-free formula φ' such that $\varphi \leftrightarrow \varphi'$ in ACF is given explicitly. The construction of φ' is elementary and based on the effective Nullstellensatz. The existence of a common invariant subspace of $A_1, \ldots, A_s$ of dimension d can be expressed in the first-order language of fields, and hence, the constructive version of Tarski's theorem yields the criterion. In addition, some applications of this criterion in quantum information theory are discussed.

Key words. Common invariant subspaces, Common eigenvectors, Quantifier elimination, Effective Nullstellensatz, Quantum information theory.

AMS subject classifications. 15A18, 03C10, 03C98, 81P05, 81P45.

1. Introduction.

Throughout the paper, $\mathbb{C}$ is the field of complex numbers and $\mathbb{M}_n(\mathbb{C})$ the vector space of $n \times n$ matrices over $\mathbb{C}$.

Assume that $A, A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ and V is a subspace of $\mathbb{C}^n$. We say that V is *A-invariant* (or *invariant subspace of A*) if and only if $Av \in V$ for any $v \in V$. We say that V is a *common invariant subspace* of $A_1, \ldots, A_s$ if and only if V is A_i-invariant for any $i = 1, \ldots, s$. Assume that $x \in \mathbb{C}^n$, $x \neq 0$. We say that x is a *common eigenvector* of $A_1, \ldots, A_s$ if and only if x is an eigenvector of every A_i, that is, $A_i x = \mu_i x$ for some $\mu_i \in \mathbb{C}$, for any $i = 1, \ldots, s$. The vector $x \in \mathbb{C}^n$ is a common eigenvector of $A_1, \ldots, A_s$ if and only if the one-dimensional subspace $\langle x \rangle \subseteq \mathbb{C}^n$ generated by x is a common invariant subspace of $A_1, \ldots, A_s$.

A *computable criterion* (or *computable condition*) is a procedure employing only finite number of arithmetic operations. The problem of providing a computable criterion for the existence of d-dimensional common invariant subspace of $s \geq 2$ matrices $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$, for $d \leq n$, is known as the *common invariant subspace problem* or the CIS *problem*.

There are many partial solutions of the CIS problem. In [32], D. Shemesh shows that the matrices $A, B \in \mathbb{M}_n(\mathbb{C})$ have a common eigenvector (i.e., a common invariant subspace of dimension one) if and only if $\mathcal{L}(A, B) \neq 0$ where

$$\mathcal{L}(A, B) = \bigcap_{k,l=1}^{n-1} \ker[A^k, B^l] \neq 0.$$

Here, $\ker X = \{v \in \mathbb{C}^n | Xv = 0\}$ is the *kernel* of X and $[X, Y] = XY - YX$ the *commutator* of X and Y,

*Received by the editors on November 14, 2016. Accepted for publication on August 12, 2017. Handling Editor: Michael Tsatsomeros.

†Faculty of Mathematics and Computer Science, Nicholaus Copernicus University, Toruń, Poland (past@mat.uni.torun.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 32, pp. 343-356, August 2017.

for any $X, Y \in \mathbb{M}_n(\mathbb{C})$. The author observes that $\mathcal{L}(A,B) = \ker K$, where

$$K = \sum_{k,l=1}^{n-1} [A^k, B^l]^*[A^k, B^l]$$

and X^* is the matrix adjoint to X, for any $X \in \mathbb{M}_n(\mathbb{C})$. It follows that the condition $\mathcal{L}(A,B) \neq 0$ is computable.

The result of Shemesh is generalized in [16]. Indeed, we show in [16, Corollary 2.3] that the matrices $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ have a common eigenvector if and only if $\mathcal{M}(A_1, \ldots, A_s) \neq 0$, where

$$\mathcal{M}(A_1, \ldots, A_s) = \bigcap_{\substack{k_i, l_j \geq 0 \\ k_1+k_2+\cdots+k_s \neq 0 \\ l_1+l_2+\cdots+l_s \neq 0}}^{n-1} \ker[A_1^{k_1} \cdots A_s^{k_s}, A_1^{l_1} \cdots A_s^{l_s}].$$

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

$$K = \sum_{\substack{k_i, l_j \geq 0 \\ k_1+k_2+\cdots+k_s \neq 0 \\ l_1+l_2+\cdots+l_s \neq 0}}^{n-1} [A_1^{k_1} \cdots A_s^{k_s}, A_1^{l_1} \cdots A_s^{l_s}]^*[A_1^{k_1} \cdots A_s^{k_s}, A_1^{l_1} \cdots A_s^{l_s}],$$

and thus, the condition $\mathcal{M}(A_1, \ldots, A_s) \neq 0$ is computable.

In [25], we simplified the above condition in the following way. Assume that $H, A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ and H has pairwise different eigenvalues. Then matrices $H, A_1, \ldots, A_s$ have a common eigenvector if and only if $\mathcal{N}(H, A_1, \ldots, A_s) \neq 0$, where

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

Similarly as in the previous cases, $\mathcal{N}(H, A_1, \ldots, A_s) = \ker K$, where

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

The papers [1], [2], [11] and [35] are devoted to common invariant subspaces of dimensions higher than one. In [1] and [2], the authors study the case when algebra generated by two complex matrices is semisimple and use the concept of a *standard polynomial*, see [27]. In [11] and [35], the authors reduce the general CIS problem to the question of existence of a common eigenvector of suitable *compound matrices*, see [20]. This is done for the case of two complex matrices. Some methods of [11] and [35] are used in [16] and [25] to obtain generalized results for arbitrary number of matrices. The cited papers generally assume that given matrices have pairwise different eigenvalues. Hence, they do not give a complete solution of the CIS problem.

The general version of the CIS problem, with arbitrary number of matrices and arbitrary dimension of common invariant subspaces, is solved in [3]. In the solution the authors use techniques of Gröbner bases theory and algebraic geometry.

In this paper, we present another complete solution of the common invariant subspace problem. Our approach has a model-theoretic nature. Namely, we observe that the existence of a common invariant

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 32, pp. 343-356, August 2017.

subspace of $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ of dimension $d \leq n$ can be expressed in the first-order language of fields. Denote this first-order formula by φ. Then it follows from the renowned theorem of A. Tarski on quantifier elimination in the theory of algebraically closed fields (denoted by ACF) that there exists a quantifier-free formula φ' (a formula in which quantifiers do not occur) such that $\varphi \leftrightarrow \varphi'$ in ACF. Quantifier-free formulas can be viewed as computable criteria, and hence, Tarski's theorem directly implies that the solution of the CIS problem exists. We prove in the paper a *constructive version* of Tarski's theorem to get an explicit form of the solution. Our proof is short and elementary. We base it on the *effective Nullstellensatz*.

A. Tarski showed that the theory of algebraically closed fields admits quantifier elimination in 1948. Tarski has never published his proof, but one can find it implicitly in [29], see also [34] and [36] for more information. Tarski's proof is inductive with respect to the degree of a formula, see [21] for the definition. In the second step of induction the author eliminates one existential quantifier from a given formula. This leads to a formula of lower degree.

By a *constructive proof* (or *constructive version*) of Tarski's theorem, we mean a proof of Tarski's theorem which yields a *concrete* quantifier-free form of a given formula. In some sense, the original proof given by Tarski is already constructive.

Tarski's theorem has a number of proofs. Proofs which are constructive are part of *algorithmic* quantifier elimination theory. There is an extensive literature on this topic. The reader is reffered to [22] for some review of important results in the field. Here, we only mention [12] by J. Heintz, where the author presents a detailed and comprehensive analysis of the complexity of quantifier elimination in ACF. In the paper Heintz gives a concrete algorithm for quantifier elimination. He obtains a doubly-exponential degree bound for the complexity of quantifier-free formula, see Section 4 of [12].

Assume that K is an algebraically closed field and $K[x_1, \ldots, x_m]$ is the polynomial ring over K in m variables $x_1, \ldots, x_m$. Our constructive proof of Tarski's theorem is based on the *effective Nullstellensatz*. Assume that $m, d, s \geq 1$ are some natural numbers. Effective Nullstellensatz yields a natural number $\gamma(m, d, s)$ satisfying the following condition: for any polynomials $F_1, \ldots, F_s \in K[x_1, \ldots, x_m]$ such that $\deg(F_i) \leq d$ we have $1 \in \langle F_1, \ldots, F_s \rangle$ if and only if there exist polynomials $H_1, \ldots, H_s \in K[x_1, \ldots, x_m]$ such that $1 = H_1F_1 + \cdots + H_sF_s$ and $\deg(H_i) \leq \gamma(m, d, s)$, for any $i = 1, \ldots, s$ ($\deg(F)$ denotes the degree of a polynomial $F \in K[x_1, \ldots, x_m]$). The numbers $\gamma(m, d, s)$ are calculated in [14] (with corrections in [31]), [8], [18], [33], [17] and [24] (see also [4] for more general considerations). Any value from these papers suffices for our proof of Tarski's theorem, but the results of [18] and [17] are optimal, that is, the lowest possible.

The significance of knowing the values $\gamma(m, d, s)$ is fundamental in our constructive proof. Indeed, this enables to write the condition $1 \in \langle F_1, \ldots, F_s \rangle$ in the first-order language of fields. Such a strategy for the proof appears implicitly in the literature and may already be known. For example, Heintz makes somewhat similar use of the effective Nullstellensatz in his algorithm, see Section 4 of [12].

The paper is organized as follows. In Section 2, we recall for convenience some basic facts and terminology from model theory (we base on [21] and [28]). We also introduce the notation which is, in most cases, the standard one.

In Section 3, we recall the aforementioned results concernig effective Nullstellensatz. We concentrate on our recent construction of $\gamma(m, d, s)$ obtained in [24]. It was developed exclusively for the constructive proof of Tarski's theorem. Although the construction is far from optimal, it suffices for the proof, because any value of $\gamma(m, d, s)$ is sufficient. Results of [18] and [17] yield the optimal construction.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 32, pp. 343-356, August 2017.

Section 4 is devoted to the constructive proof of Tarski's theorem. The main result is Theorem 4.2. In Corollary 4.3 we give a computable criterion for the existence of a common root of multivariate polynomials. This is a direct consequence of Theorem 4.2.

In Section 5, we give a solution of the CIS problem, based on the results of Section 4. We define a first-order formula CIS_d of the language of fields that expresses the existence of a common invariant subspace of dimension d of complex $n \times n$ matrices. Thus, Theorem 4.2 yields the desired solution. Finally, we discuss some applications of common invariant subspaces in quantum information theory. In that sense, we continue our research from [16] and [25], see also [15] and [26] for similar concepts.

Section 6 is the last section of the paper. In this section, we apply our results to give a computable criterion for the existence of a 2-dimensional common invariant subspace of two general 3×3 matrices. This is the first non-trivial example since the CIS problem for common eigenvectors is solved completely in [16].

2. First-order languages and formulas. In this section, we recall for convenience some facts and terminology from model theory. All the details can be found in [21], [28] or any other textbook in model theory. Among other things, we give a precise formulation of Tarski's theorem. We also introduce the notation.

A *first-order language* $\mathcal{L}$ is a quadruple (Ω, R, C, X), where Ω is the set of *operation symbols*, R the set of *relation symbols*, C the set of *constant symbols* and X the set of *variables*. If $\mathcal{L}$ is a language, then $\mathrm{Form}(\mathcal{L})$ is the set of all *first-order $\mathcal{L}$-formulas* (or *first-order formulas over* $\mathcal{L}$).

Assume that $\mathcal{L}$ is a language and $\varphi_1, \ldots, \varphi_n$ are $\mathcal{L}$-formulas. Then $\bigwedge_{i=1}^n \varphi_i$ and $\bigvee_{i=1}^n \varphi_i$ denote the formulas $\varphi_1 \wedge \cdots \wedge \varphi_n$ and $\varphi_1 \vee \cdots \vee \varphi_n$, respectively. If $\underline{x} = (x_1, \ldots, x_m)$ is a sequence of variables and Q is a quantifier, then $Q_{\underline{x}}$ is the abbreviation of $Q_{x_1} \cdots Q_{x_m}$. Generally, if $A = \{a_1, \ldots, a_s\}$ is a set of variables, then Q_A is the abbreviation of $Q_{b_1} \cdots Q_{b_s}$, where $b_1, \ldots, b_s$ is any permutation of $a_1, \ldots, a_s$. This is consistent since the formulas $Q_{b_1} \cdots Q_{b_s} \varphi$ and $Q_{a_1} \cdots Q_{a_s} \varphi$ are equivalent, for any $\mathcal{L}$-formula φ.

A variable x occurring in a formula $\varphi \in \mathrm{Form}(\mathcal{L})$ is *bound* if and only if there is a subformula ψ of φ such that x occurs in ψ and $\exists_x \psi$ or $\forall_x \psi$ is a subformula of φ. If x occurs in φ and x is not bound, then x is *free*. For example, if $\varphi = \exists_x (x^2 + y = 1)$, then x is bound and y is free. If φ is an $\mathcal{L}$-formula and $a_1, \ldots, a_n$ are all free variables of φ, then we write $\varphi(\underline{a})$ instead of φ, where $\underline{a} = (a_1, \ldots, a_n)$. A formula $\varphi \in \mathrm{Form}(\mathcal{L})$ is *atomic* if and only if φ is of the form $r(\underline{a})$ or $t_1 = t_2$, where r is a relation symbol of $\mathcal{L}$ and t_1, t_2 are terms over $\mathcal{L}$. For example, a formula $x^2 + y = 1$ is atomic and $(x^2 + y = 1) \wedge (x + y + z = 0)$ is not. A formula $\varphi \in \mathrm{Form}(\mathcal{L})$ is *quantifier-free* if and only if it has no subformula of the form $\exists_x \psi$ or $\forall_x \psi$. Hence, quantifier-free formulas are boolean combinations of atomic formulas. For example, a formula $(x^2 + y = 1) \wedge (x + y + z = 0)$ is quantifier-free and $\exists_x (x^2 + y = 1)$ is not.

Assume that $\mathcal{L}$ is a language. A formula $\varphi \in \mathrm{Form}(\mathcal{L})$ is a *sentence* if and only if φ has no free variables. For example, a formula $\forall_y \exists_x (x^2 + y = 1)$ is a sentence. A formula $\exists_x (x^2 + y = 1)$ is not a sentence. The set of all sentences over $\mathcal{L}$ is denoted by $\mathrm{Sent}(\mathcal{L})$. An *$\mathcal{L}$-theory* (or *theory* over $\mathcal{L}$) is any subset of $\mathrm{Sent}(\mathcal{L})$. If T is an $\mathcal{L}$-theory and a formula $\varphi \in \mathcal{L}$ is provable in T, then we write $T \vdash \varphi$. We denote by $\mathrm{Mod}(\mathcal{L})$ the set of all *models of* $\mathcal{L}$. If $\varphi \in \mathrm{Form}(\mathcal{L})$ and φ is satisfied in a model M, then we write $M \models \varphi$. If T is a $\mathcal{L}$-theory, M is a model of $\mathcal{L}$ and $M \models \varphi$ for any $\varphi \in \mathrm{Sent}(\mathcal{L})$, then we say that M is a *model of* T. We denote by $\mathrm{Mod}(T)$ the set of all models of T. The following fundamental theorem states that the first-order logic is sound and complete.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 32, pp. 343-356, August 2017.

THEOREM 2.1. *Assume that $\mathcal{L}$ is a language, T is an $\mathcal{L}$-theory and $\varphi \in \mathrm{Sent}(\mathcal{L})$. Then $T \vdash \varphi$ if and only if $M \models \varphi$ for any $M \in \mathrm{Mod}(T)$.*

Assume that $\mathcal{L}$ is a language and φ is a formula over $\mathcal{L}$. It is well known that φ can be written in the *prenex normal form*. It follows from De Morgan's laws that φ is equivalent with the formula $\bigvee_{i=1}^{t} \exists_{\underline{x}} (\bigwedge_{j=1}^{s_i} \varphi_{ij})$, where φ_{ij} are atomic formulas or negations of atomic formulas. An $\mathcal{L}$-formula is a *conjunctive prenex normal formula* if it has the form $\exists_{\underline{x}} (\bigwedge_{i=1}^{s} \varphi_i)$, where each φ_i is an atomic $\mathcal{L}$-formula or a negation of such. We say that an $\mathcal{L}$-theory T admits *quantifier elimination* if and only if for any conjunctive prenex normal $\mathcal{L}$-formula φ there is a quantifier-free $\mathcal{L}$-formula φ' such that $T \vdash \varphi \leftrightarrow \varphi'$. It is clear that we can replace conjunctive prenex normal $\mathcal{L}$-formula by any $\mathcal{L}$-formula in this condition.

We denote the language of fields $(0, 1, +, -, \cdot)$ by $\mathcal{F}$. The theory of algebraically closed fields over the language $\mathcal{F}$ is denoted by ACF. The axioms forming ACF are well known. Recall that if $\varphi(\underline{a})$ is an atomic $\mathcal{F}$-formula, then $\varphi(\underline{a})$ has the form $F = 0$, where F is a mutivariate polynomial in $\mathbb{Z}[a_1, \ldots, a_n]$. This yields the general form of quantifier-free $\mathcal{F}$-formulas. We introduce some notation for multivariate polynomials over the ring $\mathbb{Z}$.

Assume that $\underline{a} = (a_1, \ldots, a_n)$ and $\underline{x} = (x_1, \ldots, x_m)$. Then $\mathbb{Z}[\underline{a}]$ denotes the ring $\mathbb{Z}[a_1, \ldots, a_n]$ and $\mathbb{Z}[\underline{a}][\underline{x}]$ the ring of polynomials in m variables $x_1, \ldots, x_m$ over the ring $\mathbb{Z}[\underline{a}]$. Generally, if C is a set of variables, then $\mathbb{Z}[C][\underline{x}]$ is the ring of polynomials in m variables $x_1, \ldots, x_m$ over the ring $\mathbb{Z}[C]$ of polynomials in variables from C. A polynomial F in $\mathbb{Z}[\underline{a}][\underline{x}]$ has the form $\sum_{\alpha \in \mathbb{N}^m} f_\alpha \cdot \underline{x}^\alpha$, where $f_\alpha \in \mathbb{Z}[\underline{a}]$ for any $\alpha \in \mathbb{N}^m$ and $f_\alpha = 0$ for almost all $\alpha \in \mathbb{N}^m$. Here $\underline{x}^\alpha$ denotes $x_1^{\alpha_1} \cdots x_m^{\alpha_m}$, where $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m$. If $\alpha \in \mathbb{N}^m$ and $\alpha = (a_1, \ldots, a_m)$, then we set $|\alpha| = a_1 + \cdots + a_m$. If $F = \sum_{\alpha \in \mathbb{N}^m} f_\alpha \cdot \underline{x}^\alpha$, then the *degree* of F with respect to $x_1, \ldots, x_m$ is a maximal element of the set $\{|\alpha|; f_\alpha \neq 0\}$. The degree of F with respect to $x_1, \ldots, x_m$ is denoted by $\deg(F)$.

The following is a precise statement of Tarski's theorem on quantifier elimination in the theory of algebraically closed fields.

THEOREM 2.2. *Assume that $\underline{a} = (a_1, \ldots, a_n)$ and $\varphi(\underline{a})$ is a conjunctive prenex normal $\mathcal{F}$-formula. The following equivalent assertions hold.*

(1) *There exists a quantifier-free $\mathcal{F}$-formula $\varphi'(\underline{a})$ such that* $\mathrm{ACF} \vdash \varphi(\underline{a}) \leftrightarrow \varphi'(\underline{a})$.

(2) *There exists a quantifier-free $\mathcal{F}$-formula $\varphi'(\underline{a})$ such that for any algebraically closed field K and any tuple $\underline{a} \in K^n$ we have $K \models \varphi(\underline{a})$ if and only if $K \models \varphi'(\underline{a})$.*

Note that the equivalence of conditions (1) and (2) from the above theorem follows directly from Theorem 2.1.

3. Effective Nullstellensatz. We recall in this section some results concerning the effective Nullstellensatz. First we introduce the terminology.

We denote by $\mathbb{N}_1$ the set $\mathbb{N} \setminus \{0\}$. Assume that K is an algebraically closed field and $m, d, s \in \mathbb{N}_1$. A number $\gamma(m, d, s) \in \mathbb{N}$ is *K-bounding* if and only if the following condition is satisfied: for any $F_1, \ldots, F_s \in K[x_1, \ldots, x_m]$ such that $\deg(F_i) \leq d$ we have $1 \in \langle F_1, \ldots, F_s \rangle$ if and only if there exist $H_1, \ldots, H_s \in K[x_1, \ldots, x_m]$ such that $1 = H_1F_1 + \cdots + H_sF_s$ and $\deg(H_i) \leq \gamma(m, d, s)$, for any $i = 1, \ldots, s$. A number $\gamma(m, d, s) \in \mathbb{N}$ is *bounding* if and only if it is K-bounding for any algebraically closed field K. A function $\gamma : (\mathbb{N}_1)^3 \to \mathbb{N}$ is *K-bounding* (*bounding*, respectively) if and only if the number $\gamma(m, d, s)$ is K-bounding (bounding, respectively) for any $m, d, s \in \mathbb{N}_1$.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 32, pp. 343-356, August 2017.

Effective Nullstellensatz yields a bounding function or a K-bounding function for some concrete K. The first result on effective Nullstellensatz is proved by G. Hermann in [14], with some corrections made by A. Seidenberg in [31]. They showed that the function $\gamma(m,d,s) = (2d)^{2^m}$, for any $m,d,s \in \mathbb{N}_1$, is a bounding function. Functions of this form are called doubly-exponential. In [8], W. D. Brownawell shows that the function

$$\gamma(m,d,s) = m \cdot \min(s,m) \cdot d^{\min(s,m)} + \min(s,m) \cdot d,$$

for any $m,d,s \in \mathbb{N}_1$, is a $\mathbb{C}$-bounding function. J. Kollar shows in [18] that the number $\gamma(m,d,s) = d^m$ is a bounding number for any $m,s \in \mathbb{N}_1$ and $d \geq 3$. In [33], M. Sombra gets that the function $\gamma(m,d,s) = 2d^m$, for any $m,d,s \in \mathbb{N}_1$, is a bounding function. The result of Z. Jelonek given in [17] shows that the function $\gamma(m,d,s) = d^m$ for $s \leq m$ and $\gamma(m,d,s) = 2d^m - 1$ for $s > m$ is a bounding function. We note that the analysis of effective Nullstellensatz given in [18], [21] and [17] is more detailed than the approach we take in the section. The results of [18] and [17] give optimal, or nearly optimal, single-exponential values of $\gamma(m,d,s)$, see Section 1 of [17] for the details. Here by *optimal* we mean the *lowest possible*.

A construction of a bounding function is also given in our recent paper [24]. In that paper we set a bound on the length of ascending chains of ideals in $K[x_1,\ldots,x_m]$ which are generated by polynomials of degrees less or equal to fixed natural numbers, see [24, Theorem 4.2]. Similar problems are studied in [23] and [5], see also [30]. We derive a bounding function from results of Section 3 of [24] and [24, Theorem 4.2] by applying some basic techniques of Gröbner bases theory. In fact, we get a more general function, see Corollary 4.5 in [24] for details. The main results of [24] are proved in elementary way, using mainly combinatorial arguments.

The bounding function obtained in [24] is not optimal, but we got it exclusively for the constructive proof of Tarski's theorem. Since any concrete bounding function is sufficient for this proof (and hence, for solution of the CIS problem), we recall our construction below.

Denote by $\mathbb{F}$ the set of all non-decreasing functions $\mathbb{N}_1 \to \mathbb{N}_1$. If $f \in \mathbb{F}$ and $s \in \mathbb{N}$, then ${}^sf : \mathbb{N}_1 \to \mathbb{N}_1$ is a function such that ${}^sf(n) = f(s+n)$ for any $n \in \mathbb{N}_1$. Observe that ${}^sf \in \mathbb{F}$. The elements of the set $\mathbb{N}^m$ are treated as sequences of natural numbers, for any $m \in \mathbb{N}$.

We define a sequence $(\mathcal{B}_m)_{m\in\mathbb{N}_1}$ of functions such that $\mathcal{B}_m : \mathbb{F} \to \mathbb{N}$ for any $m \in \mathbb{N}$ as follows. The definition is inductive with respect to the number m. It is given in two main steps, but the second step is divided in three parts.

Step 1. Assume that $m = 1$. We define $\mathcal{B}_1 : \mathbb{F} \to \mathbb{N}$ to be a function such that $\mathcal{B}_1(f) = f(1) + 1$ for any $f \in \mathbb{F}$.

Step 2. Assume that $m \geq 2$ and the function $\mathcal{B}_{m-1} : \mathbb{F} \to \mathbb{N}$ is defined. In order to define $\mathcal{B}_m : \mathbb{F} \to \mathbb{N}$, we construct a sequence of functions $(\mathcal{B}_m^k)_{k=0}^m$, $\mathcal{B}_m^k : \mathbb{F} \times \mathbb{N}^k \to \mathbb{N}$. This is done by the backward induction with respect to the number k. We give the construction in three steps.

Step 2.1. Assume that $k = m$. We define $\mathcal{B}_m^m : \mathbb{F}\times\mathbb{N}^m \to \mathbb{N}$ to be a function such that $\mathcal{B}_m^m(f,b_1,\ldots,b_m) = (b_1+1)\cdots(b_m+1)$ for any $f \in \mathbb{F}$ and $(b_1,\ldots,b_m) \in \mathbb{N}^m$.

Step 2.2. Assume that $k \in \{0,\ldots,m-1\}$ and the function $\mathcal{B}_m^{k+1} : \mathbb{F} \times \mathbb{N}^{k+1} \to \mathbb{N}$ is defined. Suppose $f \in \mathbb{F}$, $\beta \in \mathbb{N}^k$ and let $g : \mathbb{N}_1 \to \mathbb{N}_1$ be a function such that $g(1) = 1$ and

$$g(n+1) = 1 + g(n) + \mathcal{B}_m^{k+1}({}^{g(n)}f, \beta, f(g(n)))$$

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 32, pp. 343-356, August 2017.

for any $n \geq 1$. We have $g \in \mathbb{F}$, and hence, there is a function $\mathcal{F}_m^k : \mathbb{F} \times \mathbb{N}^k \to \mathbb{F}$ such that $(f, \beta) \mapsto g$. We set $\mathcal{B}_m^k(f, \beta) = g(\mathcal{B}_{m-1}(f \circ g) + 1)$ for any $f \in \mathbb{F}$, $\beta \in \mathbb{N}^k$ and $g = \mathcal{F}_m^k(f, \beta)$.

Step 2.3. We identify $\mathcal{B}_m$ with $\mathcal{B}_m^0$.

Let $d \in \mathbb{N}_1$ and denote the function $f : \mathbb{N}_1 \to \mathbb{N}_1$ such that $f(n) = 3^n d$ by a string $3^n d$. Then [24, Corollary 3.5] yields that the function

$$\gamma(m, d, s) = (3^{\mathcal{B}_m(3^n d)-1} - 1)d,$$

for any $m, d, s \in \mathbb{N}_1$, is a bounding function. This function is rather Ackermannian (see [10] for some information on such functions) and hence far from optimal.

4. Tarski's theorem. This section is devoted to present the constructive proof of Tarski's theorem. The proof uses an arbitrary bounding function, so any version of the effective Nullstellensatz fits for our purpose. We recall from Section 2 that it suffices to give the proof for conjunctive prenex normal $\mathcal{F}$-formulas. We show below that these formulas have some special form.

Assume that $\underline{a} = (a_1, \ldots, a_n)$, $\underline{x} = (x_1, \ldots, x_m)$ and $F_1, \ldots, F_s \in \mathbb{Z}[\underline{a}][\underline{x}]$. Assume that $F_i = \sum_{\alpha \in \mathbb{N}^m} f_{i,\alpha} \cdot \underline{x}^\alpha$, where $f_{i,\alpha} \in \mathbb{Z}[\underline{a}]$ for any $i = 1, \ldots, s$, $\alpha \in \mathbb{N}^m$ and $f_\alpha = 0$ for almost all $\alpha \in \mathbb{N}^m$. A formula of the form $\exists_{\underline{x}}(F_1(\underline{x}) = 0 \wedge \cdots \wedge F_s(\underline{x}) = 0)$ is a *common root formula*.

Proposition 4.1. *Any conjunctive prenex normal $\mathcal{F}$-formula is equivalent with some common root formula.*

Proof. Assume that $\underline{a} = (a_1, \ldots, a_n)$ and $\varphi(\underline{a})$ is a conjunctive prenex normal $\mathcal{F}$-formula. Then

$$\varphi(\underline{a}) = \exists_{\underline{x}}(F_1(\underline{x}) = 0 \wedge \cdots \wedge F_r(\underline{x}) = 0 \wedge G_1(\underline{x}) \neq 0 \wedge \cdots \wedge G_t(\underline{x}) \neq 0),$$

where each F_i, G_j is a polynomial of the form $\sum_{\alpha \in \mathbb{N}^m} f_\alpha \cdot \underline{x}^\alpha$, where $f_\alpha \in \mathbb{Z}[\underline{a}]$ and $f_\alpha = 0$ for almost all $\alpha \in \mathbb{N}^m$. Since the formula $G_1(\underline{x}) \neq 0 \wedge \cdots \wedge G_t(\underline{x}) \neq 0$ is equivalent with $(G_1 \cdots G_t)(\underline{x}) \neq 0$, the formula $\varphi(\underline{a})$ is equivalent with

$$\varphi'(\underline{a}) = \exists_{\underline{x},z}(F_1(\underline{x}) = 0 \wedge \cdots \wedge F_r(\underline{x}) = 0 \wedge zG(\underline{x}) - 1 = 0),$$

where $G = G_1 \cdots G_t$. This shows the assertion. ∎

Proposition 4.1 implies that it suffices to give the proof of Tarski's theorem only for common root formulas. Thus, we aim to give an equivalent quantifier-free form of common root formulas. Note that the proof of Proposition 4.1 shows a procedure of getting a common root formula equivalent with a given conjunctive prenex normal formula.

We introduce some special quantifier-free $\mathcal{F}$-formulas. Assume that $m \in \mathbb{N}_1$. We view the set $\mathbb{N}^m$ as a monoid with respect to the pointwise addition, denoted by $+$. If $\alpha, \beta \in \mathbb{N}^m$ and $\alpha + \gamma = \beta$ for some $\gamma \in \mathbb{N}^m$, then we write $\alpha \parallel \beta$. If $\alpha \in \mathbb{N}^m$ and $\alpha = (a_1, \ldots, a_m)$, then we set $|\alpha| = a_1 + \cdots + a_m$.

Assume that $d, d' \geq 1$ are fixed natural numbers. Let $F_1, \ldots, F_s \in \mathbb{Z}[\underline{a}][\underline{x}]$ be polynomials such that $\deg(F_i) \leq d$ and $F_i = \sum_{|\alpha| \leq d} f_{i,\alpha} \cdot \underline{x}^\alpha$, where $f_{i,\alpha} \in \mathbb{Z}[\underline{a}]$ for any $i = 1, \ldots, s$ and $\alpha \in \mathbb{N}^m$. Let $A^{d,d'}_{F_1,\ldots,F_s} = A$ be a matrix with rows indexed by elements of the set $X = \{\delta \in \mathbb{N}^m | d + d' \geq |\delta|\}$, columns indexed by elements of $\{1, \ldots, s\} \times X$ and

$$A(\delta, (i, \beta)) = \begin{cases} f_{i,\delta-\beta} & \text{if } \beta \parallel \delta, \\ 0 & \text{otherwise,} \end{cases}$$

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 32, pp. 343-356, August 2017.

where $\delta, \beta \in X$ and $i \in \{1, \ldots, s\}$. Let $\widehat{A}^{d,d'}_{F_1,\ldots,F_s} = \widehat{A}$ be an augmented matrix $(A|B)$, where B is a column with $\{1, \ldots, s\} \times X$ rows such that $B = \begin{bmatrix} 0 & \ldots & 0 & 1 \end{bmatrix}^T$. Assume that $S(A)$ and $S(\widehat{A})$ are the sets of all square submatrices of A and $\widehat{A}$, respectively. Moreover, assume that $S(\widehat{A}, n)$ is the subset of $S(\widehat{A})$ consisting of the matrices of order greater than n. We define a quantifier-free formula

$$\Delta^{d,d'}_{F_1,\ldots,F_s}(\underline{a}) = \bigwedge_{M \in S(A)} (\det M \neq 0 \to (\bigvee_{N \in S(\widehat{A}, o_M)} \det N \neq 0)),$$

where o_M denotes the order of the matrix M. Assuming that $\underline{a}$ is a tuple of elements of some field, the formula $\Delta^{d,d'}_{F_1,\ldots,F_s}(\underline{a})$ holds if and only if the rank of the matrix $\widehat{A}$ is greater than the rank of A.

In the following theorem we show that common root formulas are equivalent with quantifier-free formulas of the form $\Delta^{d,d'}_{F_1,\ldots,F_s}(\underline{a})$. This theorem is a constructive version of Tarski's theorem on quantifier elimination in the theory of ACF. Note that any $\mathcal{F}$-formula can be easily written as a disjunction of common root formulas.

THEOREM 4.2. *Assume that $\gamma : (\mathbb{N}_1)^3 \to \mathbb{N}$ is a bounding function. Assume that $\underline{a} = (a_1, \ldots, a_n)$, $\underline{x} = (x_1, \ldots, x_m)$, $F_1, \ldots, F_s \in \mathbb{Z}[\underline{a}][\underline{x}]$ and*

$$\varphi(\underline{a}) = \exists_{\underline{x}}(F_1(\underline{x}) = 0 \wedge \cdots \wedge F_s(\underline{x}) = 0).$$

Let d be the maximum of degrees of $F_1, \ldots, F_s$ and $d' = \gamma(m, d, s)$. Then $\mathrm{ACF} \vdash \varphi(\underline{a}) \leftrightarrow \Delta^{d,d'}_{F_1,\ldots,F_s}(\underline{a})$.

Proof. Assume that $F_i = \sum_{|\alpha| \leq d} f_{i,\alpha} \cdot \underline{x}^{\alpha}$, where $f_{i,\alpha} \in \mathbb{Z}[\underline{a}]$ for any $i = 1, \ldots, s$ and $\alpha \in \mathbb{N}^m$. Assume that K is an algebraically closed field and $\underline{a} \in K^n$. Then $f_{i,\alpha}(\underline{a}) \in K$ for any $i = 1, \ldots, s$, $\alpha \in \mathbb{N}^m$, and thus, it follows from Hilbert's Nullstellensatz that $\varphi(\underline{a})$ holds if and only if $1 \notin \langle F_1, \ldots, F_s \rangle$. Since $\gamma : (\mathbb{N}_1)^3 \to \mathbb{N}$ is a bounding function, the condition $1 \notin \langle F_1, \ldots, F_s \rangle$ is equivalent with non-existence of polynomials $H_1, \ldots, H_s \in K[x_1, \ldots, x_m]$ such that $1 = H_1F_1 + \cdots + H_sF_s$ and $\deg(H_i) \leq \gamma(m, d, s) = d'$ for any $i = 1, \ldots, s$. The fact that $\deg(H_i) \leq d'$ enables to write the latter condition in the first-order language of fields.

We introduce some sets of variables. Assume that $C_i = \{c_{i,\beta}\}_{|\beta| \leq d'}$, where $\beta \in \mathbb{N}^m$ and $i = 1, \ldots, s$. Let $H_i \in \mathbb{Z}[C_i][\underline{x}]$ be a polynomial of the form $H_i = \sum_{|\beta| \leq d'} c_{i,\beta} \cdot \underline{x}^{\beta}$ for $i = 1, \ldots, s$. Set $C = \bigcup_{i=1}^{s} C_i$ and consider the formula $\psi(\underline{a}) = \forall_C H_1F_1 + \cdots + H_sF_s \neq 1$ which is equivalent with $\varphi(\underline{a})$. Observe that

$$H_1F_1 + \cdots + H_sF_s = \sum_{|\delta| \leq d + d'} (\sum_{\beta + \alpha = \delta} c_{1,\beta} f_{1,\alpha} + \cdots + c_{s,\beta} f_{s,\alpha}) \underline{x}^{\delta},$$

where $\delta \in \mathbb{N}^m$, and hence, the formula $\psi(\underline{a})$ expresses the non-existence of solution of some system of linear equations with the set C as a set of variables. This system can be written in such a way that the matrices $A = A^{d,d'}_{F_1,\ldots,F_s}$ and $\widehat{A} = \widehat{A}^{d,d'}_{F_1,\ldots,F_s}$ are its coefficient matrix and augmented matrix, respectively. Then it follows from the Kronecker-Capelli theorem that $\psi(\underline{a})$ holds if and only if $\mathrm{rk}(\widehat{A}) > \mathrm{rk}(A)$, where $\mathrm{rk}(M)$ denotes the rank of the matrix M. This is equivalent with $\Delta^{d,d'}_{F_1,\ldots,F_s}(\underline{a})$. Hence, we get $\mathrm{ACF} \vdash \varphi(\underline{a}) \leftrightarrow \Delta^{d,d'}_{F_1,\ldots,F_s}(\underline{a})$ by Theorem 2.1. ∎

Note that in the proof of Theorem 4.2, any bounding function suffices. Bounding functions obtained in [18] and [17] are optimal (see Section 2), so they yield formulas $\Delta^{d,d'}_{F_1,\ldots,F_s}(\underline{a})$ of the lowest degree.

As a direct consequence of our considerations, we get the following computable criterion for the existence of a common root of multivariate polynomials.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 32, pp. 343-356, August 2017.

COROLLARY 4.3. *Assume that $\gamma : (\mathbb{N}_1)^3 \to \mathbb{N}$ is a bounding function. Assume that K is an algebraically closed field, d is a natural number, $F_1, \ldots, F_s \in K[x_1, \ldots, x_m]$ and $F_i = \sum_{|\alpha| \leq d} a_{i,\alpha} \cdot \underline{x}^{\alpha}$ for $i = 1, \ldots, s$. Set $d' = \gamma(m, d, s)$. The polynomials $F_1, \ldots, F_s$ have a common root if and only if $\mathrm{rk}(\widehat{A}) > \mathrm{rk}(A)$, where A and $\widehat{A}$ are matrices obtained from $A^{d,d'}_{F_1,\ldots,F_s}$ and $\widehat{A}^{d,d'}_{F_1,\ldots,F_s}$, respectively, by replacing the elements $f_{i,\alpha}$ by $a_{i,\alpha}$ for any $i = 1, \ldots, s$, $\alpha \in \mathbb{N}^m$.*

Proof. The proof is a simplified version of the proof of Theorem 4.2. □

5. Common invariant subspaces. In this section, we give a computable criterion for the existence of a common invariant subspace of complex $n \times n$ matrices of dimension $d \leq n$. This is a complete solution of the CIS problem. We base the solution on the constructive proof of Tarski's theorem, see Theorem 4.2. The end of this section is devoted to some applications of common invariant subspaces in quantum information theory.

Assume that $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ and $d \leq n$ is a natural number. We show that that the existence of a common invariant subspace of $A_1, \ldots, A_s$ of dimension d can be expressed in the first-order language of fields $\mathcal{F}$. Let $A_t = [a^t_{ij}]_{i,j=1,\ldots,n}$ for any $t = 1, \ldots, s$ and $C = \{a^t_{ij} | i, j = 1, \ldots, n; t = 1, \ldots, s\}$. Define a lexicographic order on C in a natural way, that is, $a^t_{ij} < a^{t'}_{i'j'}$ if and only if (t, i, j) is smaller then (t', i', j') in the lexicographic order. We define a tuple $\underline{c}$ of coefficients of $A_1, \ldots, A_s$ as the only increasing sequence of elements of C of length $s \cdot n^2$. We call $\underline{c}$ the *coefficient tuple* of $A_1, \ldots, A_s$.

Assume that $V = \{v^j_i | i = 1, \ldots, d; j = 1, \ldots, n\}$ is a set of variables and $\underline{v}$ is a tuple of elements of V defined similarly as the coefficient tuple. Set $\underline{v}_i = \begin{bmatrix} v^1_i & \ldots & v^n_i \end{bmatrix}^T$ for $i = 1, \ldots, d$ and denote by M_V the augmented matrix $(\underline{v}_1 | \ldots | \underline{v}_d)$. Assume that $S_d(M_V)$ is the set of all square submatrices of the matrix M_V of order d and denote by $\mathrm{rk}(M_V) = d$ the first-order $\mathcal{F}$-formula

$$\bigvee_{M \in S_d(M_V)} (\det M \neq 0).$$

The formula $\mathrm{rk}(M_V) = d$ states that the vectors $\underline{v}_1, \ldots, \underline{v}_d$ are linearly independent. Assume that $W = \{\alpha^t_{ij} | i = 1, \ldots, s; j, t = 1, \ldots, d\}$ is a set of variables and $\underline{\alpha}$ is a tuple of elements of W defined similarly as the coefficient tuple. Denote by $I_V(A_i)$, for $i = 1, \ldots, s$, the first-order $\mathcal{F}$-formula

$$\bigwedge_{j=1}^{d} (A_i \underline{v}_j = \alpha^1_{ij} \underline{v}_1 + \cdots + \alpha^d_{ij} \underline{v}_d).$$

The formula $I_V(A_i)$ states that the vector space spanned by $\underline{v}_1, \ldots, \underline{v}_d$ is A_i-invariant. Thus, the first-order $\mathcal{F}$-formula

$$\varphi(\underline{c}) = \exists_{\underline{v}} (\mathrm{rk}(M_V) = d \wedge \exists_{\underline{\alpha}} (\bigwedge_{i=1}^{s} I_V(A_i)))$$

expresses the existence of a common invariant subspace of $A_1, \ldots, A_s$ of dimension d. This formula is equivalent with the formula

$$\bigvee_{M \in S_d(M_V)} (\exists_{(\underline{v}, \underline{\alpha})} (\det M \neq 0 \wedge \bigwedge_{i=1}^{s} I_V(A_i))),$$

and finally, we get that $\varphi(\underline{c})$ is equivalent with the formula

$$\bigvee_{M \in S_d(M_V)} (\exists_{(\underline{v}, \underline{\alpha}, z_M)} (z_M \cdot \det M = 1) \wedge \bigwedge_{i=1}^{s} \bigwedge_{j=1}^{d} (A_i \underline{v}_j = \alpha^1_{ij} \underline{v}_1 + \cdots + \alpha^d_{ij} \underline{v}_d)).$$

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 32, pp. 343-356, August 2017.

We denote the above formula by $\mathrm{CIS}_d(\underline{c})$ and call it the CIS-*formula*. Observe that $\mathrm{CIS}_d(\underline{c})$ is a logical disjunction of common root formulas which are indexed by the elements of $S_d(M_V)$. We denote these common root formulas by $\mathrm{CIS}_d(\underline{c}, M)$, for $M \in S_d(M_V)$, that is,

$$\mathrm{CIS}_d(\underline{c}) = \bigvee_{M \in S_d(M_V)} \mathrm{CIS}_d(\underline{c}, M).$$

The formula $\mathrm{CIS}_d(\underline{c}, M)$ has the form $\exists_{\underline{w}}(F_1(\underline{w}) = 0 \wedge \cdots \wedge F_{r(\underline{c},d)}(\underline{w}) = 0)$, where $\underline{w} = (\underline{v}, \underline{\alpha}, z_M)$, $r(\underline{c}, d) = sdn + 1$ and $F_i \in \mathbb{Z}[\underline{c}][\underline{w}]$ for any $i = 1, \ldots, r(\underline{c}, d)$. We denote the sequence $F_1, \ldots, F_{r(\underline{c},d)}$ by $\sigma_d(\underline{c}, M)$.

The following theorem yields a computable criterion for the existence of a common invariant subspace of $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ of dimension d.

THEOREM 5.1. *Assume that $\gamma : (\mathbb{N}_1)^3 \to \mathbb{N}$ is a bounding function. Assume that $A_1, \ldots, A_s \in \mathbb{M}_n(\mathbb{C})$ and $d \leq n$ is a natural number. Assume that $\underline{c}$ is the coefficient tuple of $A_1, \ldots, A_s$ and let*

$$\mathrm{CIS}_d(\underline{c}) = \bigvee_{M \in S_d(M_V)} \mathrm{CIS}_d(\underline{c}, M).$$

Set $t = d + 1$ and $t' = \gamma(d(n + sd) + 1, d + 1, sdn + 1)$. The matrices $A_1, \ldots, A_s$ have a common invariant subspace of dimension d if and only if there exists $M \in S_d(M_V)$ such that the quantifier-free formula $\Delta^{t,t'}_{\sigma_d(\underline{c},M)}$ holds.

Proof. The matrices $A_1, \ldots, A_s$ have a common invariant subspace of dimension d if and only if there exists $M \in S_d(M_V)$ such that the common root formula $\mathrm{CIS}_d(\underline{c}, M)$ holds. This formula has the form $\exists_{\underline{w}}(F_1(\underline{w}) = 0 \wedge \cdots \wedge F_{r(\underline{c},d)}(\underline{w}) = 0)$, where $r(\underline{c}, d) = sdn + 1$ and $F_i \in \mathbb{Z}[\underline{c}][\underline{w}]$ for any $i = 1, \ldots, r(\underline{c}, d)$. The tuple $\underline{w}$ has $d(n + sd) + 1$ elements and the maximum of degrees of polynomials F_i equals the degree of the polynomial $z_M \cdot \det M - 1$ which is $d + 1 \geq 2$. Hence, the assertion follows from Theorem 4.2. ∎

Observe that the polynomials $F_i(\underline{w})$, for $i = 1, \ldots, r(\underline{c}, M)$, can be viewed as elements of $\mathbb{C}[\underline{w}]$, because $\underline{c}$ is a tuple of complex numbers. Hence, Corollary 4.3 also yields a computable condition for the existence of a common invariant subspace.

We note that the formula $\mathrm{CIS}_d(\underline{c})$ is equivalent with a single common root formula of the form

$$\exists_{(\underline{v},\underline{\alpha},\underline{z})}((\prod_{M \in S_d(M_V)} (z_M \cdot \det M - 1)) = 0 \wedge \bigwedge_{i=1}^{s} \bigwedge_{j=1}^{d} (A_i \underline{v}_j = \alpha^1_{ij} \underline{v}_1 + \cdots + \alpha^d_{ij} \underline{v}_d)),$$

where the tuple $\underline{z}$ contains all elements of the set $\{z_M | M \in S_d(M_V)\}$, ordered in a fixed way. Indeed, this follows from the fact that $G_1(\underline{x}) = 0 \vee \cdots \vee G_n(\underline{x}) = 0$ is equivalent with $(G_1 \cdots G_n)(\underline{x}) = 0$, for any polynomials $G_1, \ldots, G_n$. The required computable criterion can be obtained by applying Theorem 4.2 to the above single common root formula. Nevertheless, we usually prefer to view the formula $\mathrm{CIS}_d(\underline{c})$ as in Theorem 5.1, where it is a logical disjunction of less complex common root formulas (note that the degree of $\prod_{M \in S_d(M_V)}(z_M \cdot \det M - 1)$ equals $\binom{n}{d}(d + 1)$). It is hard to say which way is better from the point of view of computational complexity.

REMARK 5.2. We can consider the *generalized* CIS problem where the field $\mathbb{C}$ of complex numbers is replaced by any algebraically closed field K. The formula $\mathrm{CIS}_d(\underline{c})$, where $\underline{c}$ is a coefficient tuple of $A_1, \ldots, A_s \in \mathbb{M}_n(K)$, expresses the existence of a d-dimensional common invariant subspace of these matrices. Hence, Theorem 4.2 yields the solution to the generalized CIS problem.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 32, pp. 343-356, August 2017.

Common invariant subspaces, sometimes satisfying additional conditions, play a prominent role in quantum information theory. We show this role on two examples concerning quantum channels: irreducible quantum channels and decoherence-free subspaces. In these examples, we apply Theorem 5.1 and Theorem 4.2 to generalize some results from [16] and [25]. We give this part of the section an expository character and leave the details. We recommend [7] and [13] as comprehensive monographs on quantum information theory and quantum mechanics in general.

A *quantum channel* is a completely positive map $\Phi : \mathbb{M}_n(\mathbb{C}) \to \mathbb{M}_n(\mathbb{C})$ which preserves the trace. It follows from [13, 5.2.3] 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 $X \in \mathbb{M}_n(\mathbb{C})$, where A^* denotes the matrix adjoint to A.

An important subclass of the class of all quantum channels is formed by *irreducible* quantum channels. It is proved in [9] that a quantum channel $\Phi(X) = \sum_{i=1}^{s} A_i X A_i^*$ is irreducible if and only if the matrices $A_1, \ldots, A_s$ do not have a nontrivial common invariant subspace. Hence, Theorem 5.1 provides a computable criterion for irreducibility of Φ. This generalizes the main results of [16], see especially Sections 3 and 4 of [16].

Quantum channels are used to transmit quantum information. Unfortunately, quantum information may be easily corrupted by a number of factors, see [6]. Any such a factor is described as a *decoherence*. A way to overcome the effects of decoherence is to "hide" quantum information from the environment in some "quiet corner". This quiet corner is called the *decoherence-free subspace* (DFS).

There are few different mathematical definitions of DFS in the literature, see [19] for the details. In [25], we define DFS as the *common reducing unitary subspace*. We recall this definition below.

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

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 *common reducing unitary subspace* (or 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 matrix $U \in \mathbb{M}_n(\mathbb{C})$ and complex numbers $g_1, \ldots, g_s$ such that $A_i w = (g_i U)w$ for any $w \in W$ and $i = 1, \ldots, s$.

The conditions that $U \in \mathbb{M}_n(\mathbb{C})$ is a unitary matrix and $A_i w = (g_i U)w$ for any $w \in W$ and $i = 1, \ldots, s$ can be written in the first-order language of fields $\mathcal{F}$. Hence, there is a $\mathcal{F}$-formula expressing the existence of a common reducing unitary subspace of dimension d. This formula is similar to $\mathrm{CIS}_d(\underline{c})$. Consequently, Theorem 4.2 provides a computable criterion for the existence of decoherence-free subspaces. This generalizes the main results of [25], see especially Section 3 of [25].

Remark 5.3. The paper shows that there is a significant impact of quantifier elimination theory on mathematics and related fields. Indeed, Tarski's theorem shows that any problem which can be expressed in the first-order language of fields (like the CIS problem) has its equivalent reformulation as a computable criterion. Moreover, Theorem 4.2 (and algorithmic quantifier elimination theory in general) provides the exact form of this criterion. It is our opinion that this observation opens the possibility for other applications of quantifier elimination theory in mathematical sciences.

6. An example. We apply here our main results to get a computable criterion for the existence of a 2-dimensional common invariant subspace of two general 3×3 matrices. We concentrate on the construction

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 32, pp. 343-356, August 2017.

of the appropriate general CIS-formula. We stick to the notation introduced in Section 5. We do not present any calculations for concrete 3×3 matrices since the procedure given in Sections 4 and 5 is tedious. We leave the systematic treatment of this issue to further research.

We consider the existence of a common invariant subspace of dimension 2 of two 3×3 matrices A_1, A_2. Hence, $n = 3$, $s = 2$ and $d = 2$. Assume that

$$A_1 = \begin{bmatrix} a_{11}^1 & a_{12}^1 & a_{13}^1 \\ a_{21}^1 & a_{22}^1 & a_{23}^1 \\ a_{31}^1 & a_{32}^1 & a_{33}^1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} a_{11}^2 & a_{12}^2 & a_{13}^2 \\ a_{21}^2 & a_{22}^2 & a_{23}^2 \\ a_{31}^2 & a_{32}^2 & a_{33}^2 \end{bmatrix}.$$

Then the coefficient tuple $\underline{c}$ of A_1, A_2 is the following tuple

$$\underline{c} = (a_{11}^1, a_{12}^1, a_{13}^1, a_{21}^1, a_{22}^1, a_{23}^1, a_{31}^1, a_{32}^1, a_{33}^1, a_{11}^2, a_{12}^2, a_{13}^2, a_{21}^2, a_{22}^2, a_{23}^2, a_{31}^2, a_{32}^2, a_{33}^2).$$

Furthermore, let $V = \{v_i^j | i = 1, 2; j = 1, 2, 3\}$, and thus,

$$M_V = \begin{bmatrix} v_1^1 & v_2^1 \\ v_1^2 & v_2^2 \\ v_1^3 & v_2^3 \end{bmatrix}.$$

The set $S_2(V)$ is a set of all submatrices of the matrix M_V of order 2, so

$$S_2(V) = \{\begin{bmatrix} v_1^1 & v_2^1 \\ v_1^2 & v_2^2 \end{bmatrix}, \begin{bmatrix} v_1^2 & v_2^2 \\ v_1^3 & v_2^3 \end{bmatrix}, \begin{bmatrix} v_1^1 & v_2^1 \\ v_1^3 & v_2^3 \end{bmatrix}\}.$$

We denote the elements of this set by M_1, M_2, M_2, respectively, and set

$$\underline{w}_i = (v_1^1, v_2^1, v_1^2, v_2^2, v_1^3, v_2^3, \alpha_{11}^1, \alpha_{12}^1, \alpha_{21}^1, \alpha_{22}^1, \alpha_{11}^2, \alpha_{12}^2, \alpha_{21}^2, \alpha_{22}^2, z_{M_i})$$

for $i = 1, 2, 3$. Since $\det M_1 = v_1^1 v_2^2 - v_2^1 v_1^2$ we get

$$\mathrm{CIS}_2(\underline{c}, M_1) = \exists_{\underline{w}_1}((z_{M_1}(v_1^1 v_2^2 - v_2^1 v_1^2) = 1) \wedge (A_1 \begin{bmatrix} v_1^1 \\ v_1^2 \\ v_1^3 \end{bmatrix} = \alpha_{11}^1 \begin{bmatrix} v_1^1 \\ v_1^2 \\ v_1^3 \end{bmatrix} + \alpha_{11}^2 \begin{bmatrix} v_2^1 \\ v_2^2 \\ v_2^3 \end{bmatrix}) \wedge$$

$$\wedge (A_1 \begin{bmatrix} v_2^1 \\ v_2^2 \\ v_2^3 \end{bmatrix} = \alpha_{12}^1 \begin{bmatrix} v_1^1 \\ v_1^2 \\ v_1^3 \end{bmatrix} + \alpha_{12}^2 \begin{bmatrix} v_2^1 \\ v_2^2 \\ v_2^3 \end{bmatrix}) \wedge (A_2 \begin{bmatrix} v_1^1 \\ v_1^2 \\ v_1^3 \end{bmatrix} = \alpha_{21}^1 \begin{bmatrix} v_1^1 \\ v_1^2 \\ v_1^3 \end{bmatrix} + \alpha_{21}^2 \begin{bmatrix} v_2^1 \\ v_2^2 \\ v_2^3 \end{bmatrix}) \wedge$$

$$\wedge (A_2 \begin{bmatrix} v_2^1 \\ v_2^2 \\ v_2^3 \end{bmatrix} = \alpha_{22}^1 \begin{bmatrix} v_1^1 \\ v_1^2 \\ v_1^3 \end{bmatrix} + \alpha_{22}^2 \begin{bmatrix} v_2^1 \\ v_2^2 \\ v_2^3 \end{bmatrix})).$$

Note that the formula

$$A_1 \begin{bmatrix} v_1^1 \\ v_1^2 \\ v_1^3 \end{bmatrix} = \alpha_{11}^1 \begin{bmatrix} v_1^1 \\ v_1^2 \\ v_1^3 \end{bmatrix} + \alpha_{11}^2 \begin{bmatrix} v_2^1 \\ v_2^2 \\ v_2^3 \end{bmatrix},$$

and the other three similar formulas as well, is in fact a logical conjunction of 3 formulas. We get the formulas $\mathrm{CIS}_2(\underline{c}, M_2), \mathrm{CIS}_2(\underline{c}, M_3)$ by replacing the formula $z_{M_1}(v_1^1 v_2^2 - v_2^1 v_1^2) = 1$ in $\mathrm{CIS}_2(\underline{c}, M_1)$ by $z_{M_2}(v_1^2 v_2^3 - v_2^2 v_1^3) =$

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 32, pp. 343-356, August 2017.

1 and $z_{M_3}(v_1^1v_2^3 - v_2^1v_1^3) = 1$, respectively. We also replace the tuple $\underline{w}_1$ in $\mathrm{CIS}_2(\underline{c}, M_1)$ by $\underline{w}_2$ or $\underline{w}_3$. Finally, we get

$$\mathrm{CIS}_2(\underline{c}) = \mathrm{CIS}_2(\underline{c}, M_1) \vee \mathrm{CIS}_2(\underline{c}, M_2) \vee \mathrm{CIS}_2(\underline{c}, M_3).$$

Recall also from Section 5 that $\mathrm{CIS}_2(\underline{c})$ is equivalent with the formula obtained from $\mathrm{CIS}_2(\underline{c}, z_{M_1})$ by replacing $\underline{w}_1$ by the tuple

$$\underline{w} = (v_1^1, v_2^1, v_1^2, v_2^2, v_1^3, v_2^3, alpha_{11}^1, \alpha_{12}^1, \alpha_{21}^1, \alpha_{22}^1, \alpha_{11}^2, \alpha_{12}^2, \alpha_{21}^2, \alpha_{22}^2, z_{M_1}, z_{M_2}, z_{M_3})$$

and the formula $z_{M_1}(v_1^1v_2^2 - v_2^1v_1^2) = 1$ by the formula

$$(z_{M_1}(v_1^1v_2^2 - v_2^1v_1^2) - 1) \cdot (z_{M_2}(v_1^2v_2^3 - v_2^2v_1^3) - 1) \cdot (z_{M_3}(v_1^1v_2^3 - v_2^1v_1^3) - 1) = 0.$$

Assume that $i \in \{1, 2, 3\}$. The formula $\mathrm{CIS}_d(\underline{c}, M_i)$ has the form

$$\exists_{\underline{w}_i}(F_1^i(\underline{w}_i) = 0 \wedge \cdots \wedge F_{r(\underline{c},d)}^i(\underline{w}_i) = 0),$$

where $r(\underline{c}, d) = sdn + 1 = 13$ and the tuple $\underline{w}_i$ has $d(n + sd) + 1 = 15$ elements. The maximum of degrees of polynomials $F_1^i(\underline{w}_i), \ldots, F_{13}^i(\underline{w}_i)$ equals the degree of the polynomial $z_{M_i} \cdot \det M_i - 1$ which is $d + 1 = 3$. We denote the sequence $F_1^i(\underline{w}_i), \ldots, F_{13}^i(\underline{w}_i)$ by $\sigma_2(\underline{c}, i)$.

Recall from Section 3 that the function $\gamma(m, d, s) = d^m$ for $s \leq m$ and $\gamma(m, d, s) = 2d^m - 1$ for $s > m$ is a bounding function. We set $t = d + 1 = 3$ and

$$t' = \gamma(d(n + sd) + 1, d + 1, sdn + 1) = \gamma(15, 3, 13) = 3^{15}.$$

Then Theorem 5.1 yields the matrices A_1, A_2 have a 2-dimensional common invariant subspace if and only if there is $i \in \{1, 2, 3\}$ such that the quantifier-free formula $\Delta_{\sigma_2(\underline{c},i)}^{t,t'}$ holds. These formulas are complicated since the number $t' = 3^{15}$ is very large.

Remark 6.1. In Section 4, we construct some quantifier-free formula equivalent with a given common root formula. This quantifier-free formula depends on the bounding function γ. Assume that γ is one of the optimal bounding functions, see Section 3 for the details. Then our quantifier-free formula gets the optimal complexity (this is shown implicitly in [12]). This implies that computational complexity of the CIS problem depends on the complexity of the CIS-formula (that is, on the number and degrees of polynomials that it involves). It is thus interesting and natural to seek for less complex formulas expressing the existence of a common invariant subspace of square complex matrices then the one proposed in Section 5. It is easy to observe that our proposition is the simplest one, but it seems to be far from optimal.

Acknowledgment. The author is grateful to Stanisław Kasjan for all discussions on the subject matter of paper and to the anonymous referee for valuable comments.

REFERENCES

[1] Yu. Alpin, A. George, and Kh. Ikramov. Solving the two dimensional CIS problem by a rational algorithm. *Linear Algebra Appl.*, 312:115–123, 2000.

[2] Yu. Alpin and Kh. Ikramov. Rational procedures in the problem of common invariant subspaces of two matrices. *J. Math. Sci.*, 114(6):1757–1764, 2003.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 32, pp. 343-356, August 2017.

[3] D. Arapura and Ch. Peterson. The common invariant subspace problem: an approach via Gröbner bases. *Linear Algebra Appl.*, 384:1–7, 2004.
[4] M. Aschenbrenner and A. Leykin. Degree bounds for Gröbner bases in algebras of solvable type. *J. Pure Appl. Algebra*, 213(8):1578–1605, 2009.
[5] M. Aschenbrenner and W.Y. Pong. Orderings of monomial ideals. *Fundam. Math.*, 181:27–74, 2004.
[6] D. Lidar and T. Brun. *Quantum Error Correction*. Cambridge University Press, New York, 2013.
[7] I. Bengtsson and K. Zyczkowski. *Geometry of Quantum States: An Introduction to Quantum Entanglement*. Cambridge University Press, Cambridge, 2006.
[8] W.D. Brownawell. Bounds for the degrees in Nullstellensatz. *Ann. of Math*, 126:577–592, 1987.
[9] D. Farenick Irreducible positive linear maps on operator algebras. *Proc. Amer. Math. Soc.*, 124(11):3381–3390, 1996.
[10] H. Friedman. The Ackermann function in elementary algebraic geometry. Manuscript, 1999.
[11] A. George and Kh. Ikramov Common invariant subspaces of two matrices. *Linear Algebra Appl.*, 287:171–179, 1999.
[12] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoret. Comput. Sci.*, 24(3):239–277, 1983.
[13] T. Heinosaari and M. Ziman. *The Mathematical Language of Quantum Theory*. Cambridge University Press, Cambridge, 2012.
[14] G. Hermann Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Math. Ann.*, 95:736–788, 1926.
[15] A. Jamiołkowski, T. Kamizawa, and G. Pastuszak. On invariant subspace in quantum control systems and some concepts of integrable quantum systems. *Int. J. Theor. Phys.*, 54(8):2662–2674, 2015.
[16] A. Jamiołkowski and G. Pastuszak. Generalized Shemesh criterion, common invariant subspaces and irreducible completely positive superoperators. *Linear Multilinear Algebra*, 63(2):314–325, 2015.
[17] Z. Jelonek. On the effective Nullstellensatz. *Invent. Math.*, 162(1):1–17, 2005.
[18] J. Kollar. Sharp effective Nullstellensatz. *J. Amer. Math. Soc.*, 1(4):963–975, 1988.
[19] R. Karasik, K. Marzlin, B. Sanders, and K. Whaley. Criteria for dynamically stable decoherence-free subspaces and incoherently generated coherences. *Phys. Rev. A*, 77:052301, 2008.
[20] M. Marcus and H. Minc. *A Survey of Matrix Theory and Matrix Inequalities*. Dover, Boston, 1992.
[21] D. Marker. *Model Theory: An Introduction*. Springer, Berkeley, 2002.
[22] B. Mishra. *Algorithmic Algebra*. Texts and Monographs in Computer Science, Springer-Verlag, New York, 1993.
[23] G. Moreno Socías. Length of polynomial ascending chains and primitive recursiveness. *Math. Scand.*, 71:181–205, 1992.
[24] G. Pastuszak. On ascending chains of ideals in the polynomial ring. Preprint arXiv:1605.06263, submitted, 2016.
[25] G. Pastuszak and A. Jamiołkowski. Common reducing unitary subspaces and decoherence in quantum systems. *Electron. J. Linear Algebra*, 30:253–270, 2015.
[26] G. Pastuszak, T. Kamizawa, and A. Jamiołkowski. On a criterion for simultaneous block-diagonalization of normal matrices. *Open Syst. Inf. Dyn.*, 23:1650003, 2016.
[27] R. Pierce. *Associative Algebras*. Springer-Verlag, New York, 1982.
[28] P. Rothmaler. *Introduction to Model Theory*. Algebra, Logic and Applications Series, Vol. 15, Gordon and Breach Science Publishers, Amsterdam, 2000.
[29] A. Seidenberg. A new decision method for elementary algebra. *Ann. of Math.*, 60:365–374, 1954.
[30] A. Seidenberg. On the length of a Hilbert ascending chain. *Proc. Amer. Math. Soc.*, 29:443–450, 1971.
[31] A. Seidenberg. Constructions in algebra. *Trans. Amer. Math. Soc.*, 197:273–313, 1974.
[32] D. Shemesh. Common eigenvectors of two matrices. *Linear Algebra Appl.*, 62:11–18, 1984.
[33] M. Sombra. A sparse effective Nullstellensatz. *Adv. Appl. Math.*, 22:271–295, 1999.
[34] A. Tarski. *A Decision Method for Elementary Algebra and Geometry*. RAND Corporation, Santa Monica, 1948.
[35] M. Tsatsomeros. A criterion for the existence of common invariant subspaces of matrices. *Linear Algebra Appl.*, 322:51–59, 2001.
[36] L. van den Dries. Alfred Tarski's elimination theory for real closed fields. *J. Symbolic Logic*, 53(1):7–19, 1988.