

# Generalized Wong Sequences and Their Applications to Edmonds' Problems

Gábor Ivanyos\*    Marek Karpinski†    Youming Qiao‡    Miklos Santha§

## Abstract

We design two deterministic polynomial time algorithms for variants of a problem introduced by Edmonds in 1967: determine the rank of a matrix  $M$  whose entries are homogeneous linear polynomials over the integers. Given a linear subspace  $\mathcal{B}$  of the  $n \times n$  matrices over some field  $\mathbb{F}$ , we consider the following problems: *symbolic matrix rank* (SMR) is the problem to determine the maximum rank among matrices in  $\mathcal{B}$ , while *symbolic determinant identity testing* (SDIT) is the question to decide whether there exists a nonsingular matrix in  $\mathcal{B}$ . The constructive versions of these problems are asking to find a matrix of maximum rank, respectively a nonsingular matrix, if there exists one.

Our first algorithm solves the constructive SMR when  $\mathcal{B}$  is spanned by unknown rank one matrices, answering an open question of Gurvits. Our second algorithm solves the constructive SDIT when  $\mathcal{B}$  is spanned by triangularizable matrices, but the triangularization is not given explicitly. Both algorithms work over finite fields of size at least  $n + 1$  and over the rational numbers, and the first algorithm actually solves (the non-constructive) SMR independently from the field size. Our main tool to obtain these results is to generalize Wong sequences, a classical method to deal with pairs of matrices, to the case of pairs of matrix spaces.

## 1 Introduction

In [Edm67] Edmonds introduced the following problem: Given a matrix  $M$  whose entries are homogeneous linear polynomials over the integers, determine the rank of  $M$ . The problem is the same as determining the maximum rank of a matrix in a linear space of matrices over the rationals. In this paper we consider the same question and certain of its variants over more general fields.

Let us denote by  $M(n, \mathbb{F})$  the linear space of  $n \times n$  matrices over a field  $\mathbb{F}$ . We call a linear subspace  $\mathcal{B} \leq M(n, \mathbb{F})$  a *matrix space*. We define the *symbolic matrix rank* problem (SMR) over  $\mathbb{F}$  as follows: given  $\{B_1, \dots, B_m\} \subseteq M(n, \mathbb{F})$ , determine the maximum rank among matrices in  $\mathcal{B} = \langle B_1, \dots, B_m \rangle$ , the matrix space spanned by  $B_i$ 's. The *constructive* version of SMR is to find a matrix of maximum rank in  $\mathcal{B}$  (this is called the maximum rank matrix completion problem in [Gee99] and in [IKS10]). We refer to the weakening of SMR, when the question is to decide whether there exists a nonsingular matrix in  $\mathcal{B}$ , as the *symbolic determinant identity testing problem* (SDIT),

---

\*Institute for Computer Science and Control, Hungarian Academy of Sciences, Budapest, Hungary (Gabor.Ivanyos@sztaki.mta.hu).

†Department of Computer Science, University of Bonn, Bonn, Germany (marek@cs.uni-bonn.de).

‡Centre for Quantum Technologies, National University of Singapore, Singapore 117543. (cqqtq@nus.edu.sg)

§LIAFA, Univ. Paris 7, CNRS, 75205 Paris, France; and Centre for Quantum Technologies, National University of Singapore, Singapore 117543 (miklos.santha@liafa.jussieu.fr).

the name used by [KI04] (in [Gur04] this variant is called Edmonds' problem). The *constructive* version in that case is to find a nonsingular matrix, if there is one in  $\mathcal{B}$ . We will occasionally refer to any of the above problems as *Edmonds' problem*.

The complexity of the SDIT depends crucially on the size of the underlying field  $\mathbb{F}$ . When  $|\mathbb{F}|$  is a constant then it is NP-hard [BFS99], on the other hand if the field size is large enough (say  $\geq 2n$ ) then by the Schwartz-Zippel lemma [Sch79, Zip79] it admits an efficient randomized algorithm [Lov79]. Obtaining a deterministic polynomial-time algorithm for the SDIT would be of fundamental importance, since Kabanets and Impagliazzo [KI04] showed that such an algorithm would imply strong circuit lower bounds which seem beyond current techniques.

Previous works on Edmonds' problems mostly dealt with the case when the given *matrices*  $B_1, \dots, B_m$  satisfy certain *property*. For example, Lovász [Lov89] considered several cases of SMR, including when the  $B_i$ 's are of rank 1, and when they are skew symmetric matrices of rank 2. These classes were then shown to have deterministic polynomial-time algorithms [Gee99, Mur00, HKM05, GIM03, GI05, IKS10], see Section 1.1 for more details.

Another direction also studied is when instead of the given matrices, the generated *matrix space*  $\mathcal{B} = \langle B_1, \dots, B_m \rangle$  satisfies certain *property*. Since such a property is just a subset of all matrix spaces, we also call it a *class* of matrix spaces. Gurvits [Gur04] has presented an efficient deterministic algorithm for the SDIT over  $\mathbb{Q}$ , when the matrix space satisfies the so called *Edmonds-Rado property*, whose definition we shall review in Section 1.1. For now we only note that this class includes  $\mathbf{R}_1$ , the class of *rank-1 spanned* matrix spaces, where a matrix space  $\mathcal{B}$  is in  $\mathbf{R}_1$  if and only if  $\mathcal{B}$  has a basis consisting of rank-1 matrices over some extension field  $\mathbb{F}'$  of the underlying field  $\mathbb{F}$ .<sup>1</sup> This fact was first shown by Lovász [Lov89] via a theorem of Rado and Edmonds [Rad42, Edm70, Wel70]. Gurvits stated as an open question the complexity of the SMR for  $\mathbf{R}_1$  over finite fields [Gur04, page 456].

The difference between properties of matrices and properties of matrix spaces is critical for Edmonds' problems. For example, given matrices  $B_1, \dots, B_m$ , it is hard to determine whether  $\mathcal{B} = \langle B_1, \dots, B_m \rangle$  is in  $\mathbf{R}_1$ , and to find generating rank-1 matrices for  $\mathcal{B}$ . Thus the existence of algorithms for SMR when the  $B_i$ 's are rank-1 does not immediately imply algorithms for matrix spaces in  $\mathbf{R}_1$ .

Our results are in line with Gurvits' work, namely we present algorithms for two classes of matrix spaces. To be specific, we consider  $\mathbf{R}_1$ , the class of rank-1 spanned matrix spaces, and the class of (upper-)triangularizable matrix spaces, where a matrix space  $\mathcal{B} \leq M(n, \mathbb{F})$  is *triangularizable*, if there exist nonsingular  $C, D \in M(n, \mathbb{F}')$  where  $\mathbb{F}'$  is an extension field of  $\mathbb{F}$ , such that for all  $B \in \mathcal{B}$ , the matrix  $DBC^{-1}$  is upper-triangular.

To ease the description of our results, we make a few definitions and notations. We denote by  $\text{rank}(B)$  the rank of a matrix  $B$ , and we set  $\text{corank}(B) = n - \text{rank}(B)$ . For a matrix space  $\mathcal{B}$  we set  $\text{rank}(\mathcal{B}) = \max\{\text{rank}(B) \mid B \in \mathcal{B}\}$  and  $\text{corank}(\mathcal{B}) = n - \text{rank}(\mathcal{B})$ . We say that  $\mathcal{B}$  is *singular* if  $\text{rank}(\mathcal{B}) < n$ , that is if  $\mathcal{B}$  does not contain a nonsingular element, and *nonsingular* otherwise. For a subspace  $U \leq \mathbb{F}^n$ , we set  $\mathcal{B}(U) = \langle B(u) \mid B \in \mathcal{B}, u \in U \rangle$ . Let  $c$  be a positive integer. We say that  $U$  is a *c-singularity witness* of  $\mathcal{B}$ , if  $\dim(U) - \dim(\mathcal{B}(U)) \geq c$ , and  $U$  is a *singularity witness* of  $\mathcal{B}$  if for some  $c > 0$ , it is a *c-singularity witness*.

Note that if there exists a singularity witness of  $\mathcal{B}$  then  $\mathcal{B}$  can only be singular. Let us define the *discrepancy* of  $\mathcal{B}$  as  $\text{disc}(\mathcal{B}) = \max\{c \in \mathbb{N} \mid \exists \text{ c-singularity witness of } \mathcal{B}\}$ . Then it is also clear

---

<sup>1</sup>See [Gur02] for an example of a matrix space defined over  $\mathbb{Q}$ , s.t. it has a rank-1 basis over an extension field, but no rank-1 basis over  $\mathbb{Q}$ .

that  $\text{corank}(\mathcal{B}) \geq \text{disc}(\mathcal{B})$ .

We now state our main theorems.

**Theorem 1.** *Let  $\mathbb{F}$  be either  $\mathbb{Q}$  or a finite field. There is a deterministic polynomial-time algorithm which solves the SMR if  $\mathcal{B}$  is spanned by rank-1 matrices. Furthermore, if the size of the field  $\mathbb{F}$  is at least  $n + 1$ , the algorithm solves the constructive SMR, and it also outputs a  $\text{corank}(\mathcal{B})$ -singularity witness.*

**Theorem 2.** *Let  $\mathbb{F}$  be either  $\mathbb{Q}$  or a finite field of size at least  $n + 1$ . There is a deterministic polynomial-time algorithm which solves the constructive SDIT if  $\mathcal{B}$  is triangularizable. Furthermore, over finite fields, when  $\mathcal{B}$  is singular it also outputs a singularity witness.*

We remark that Theorem 1 remains true if we weaken the assumptions by only requiring that  $\mathcal{B}$  is rank-1 spanned over some extension field of  $\mathbb{F}$  rather than over  $\mathbb{F}$ . Also, instead of assuming that the whole space  $\mathcal{B}$  is rank-1 spanned it is actually sufficient to suppose that a subspace of  $\mathcal{B}$  of co-dimension one is spanned by rank one matrices.

## 1.1 Comparison with previous works

The idea of singularity witnesses was already present in Lovász's work [Lov89]. Lovász showed that for the rank-1 spanned case, the equality  $\text{corank}(\mathcal{B}) = \text{disc}(\mathcal{B})$  holds, by reducing it to Edmonds' Matroid Intersection theorem [Edm70], which in turn can be deduced from Rado's matroidal generalization of Hall's theorem [Rad42] (see also [Wel70]). Inspired by this fact, Gurvits defined the *Edmonds-Rado property* as the class of matrix spaces which are either nonsingular, or have a singularity witness. He has listed several subclasses of the Edmonds-Rado class, including  $\mathbf{R}_1$  and triangularizable matrices. A well-known example of a matrix space without the Edmonds-Rado property is the linear space of skew symmetric matrices of size 3 [Lov89].

As we stated already, Gurvits has presented a polynomial-time deterministic algorithm for the SDIT over  $\mathbb{Q}$  for matrix spaces with the Edmonds-Rado property. Therefore over  $\mathbb{Q}$ , his algorithm covers the SDIT for  $\mathbf{R}_1$  and for triangularizable matrices. Our algorithms are valid not only over  $\mathbb{Q}$  but also over finite fields. In the triangularizable case we also deal with the SDIT, but for  $\mathbf{R}_1$  we solve the SMR. In fact, it is not hard to reduce SMR for the general to SMR for the triangularizable case (see Proposition 24), so we do not expect to solve SMR for the triangularizable case at present. In both cases the algorithms solve the constructive version of the problems, and they also construct singularity witnesses, except for the SDIT over the rationals. Finally they work in polynomial time when the field size is at least  $n + 1$ . Moreover, for  $\mathbf{R}_1$  the algorithm solves the non constructive SMR in polynomial time regardless of the field size, settling the open problem of Gurvits.

Over fields of constant size, the SMR has certain practical implications [HKM05, HKY06], but is shown to be NP-hard [BFS99] in general. Some special cases have been studied, mostly in the form of the *mixed matrices*, that is linear matrices where each entry is either a variable or a field element. Then by restricting the way variables appear in the matrices some cases turn out to have efficient deterministic algorithms, including when every variable appears at most once ([HKM05], building on [Gee99, Mur00]), and when the mixed matrix is skew-symmetric and every variable appears at most twice ([GIM03, GI05]). Finally in [IKS10], Ivanyos, Karpinski and Saxena present a deterministic polynomial-time algorithm for the case when among the input matrices  $B_1, \dots, B_m$  all but  $B_1$  are of rank 1.

As a computational model of polynomials, determinants with affine polynomial entries turn out to be equivalent to algebraic branching programs (ABPs) [Val79, Ber84] up to a polynomial

overhead. Thus the identity test for ABPs is the same as SDIT. For restricted classes of ABPs, (quasi)polynomial-time deterministic identity test algorithms have been devised (cf. [FS12] and the references therein). Note that identity test results for SDIT and ABPs are generally incomparable. An interesting application of SDIT to quantum information processing can be found in [CDS10].

Let us comment briefly on the main technical tool we use in our algorithms. We generalize the first and second Wong sequences for matrix pencils (essentially two-dimensional matrix spaces) which have turned out to be useful among others in the area of linear differential-algebraic equations (see the recent survey [Tre13]). These were originally defined in [Won74] for a pair of matrices  $(A, B)$ , and were recently used to compute the Kronecker normal form in a numerical stable way [BT12, BT13]. We generalize Wong sequences to the case  $(\mathcal{A}, \mathcal{B})$  where  $\mathcal{A}$  and  $\mathcal{B}$  are matrix spaces, and show that they have analogous basic properties to the original ones. We relate the generalized Wong sequences to Edmonds' problems via singularity witnesses. Essentially this connection allows us to design the algorithm for  $\mathbf{R}_1$  using the second Wong sequence, and the algorithm for triangularizable matrix spaces using the first Wong sequence. We remark that techniques similar to the second Wong sequence were already used in [IKS10].

**Organization.** In Section 2 we define Wong sequences of a pair of matrix spaces, and present their basic properties. In Section 3 the connection between the second Wong sequence and singularity witnesses is shown. Based on this connection we introduce the power overflow problem, and reduce the SMR problem to it. We also prove here Theorem 1 under the hypothesis that there is a polynomial time algorithm for the power overflow problem. In Section 4 we show an algorithm for the power overflow problem that works in polynomial time for rank-1 spanned matrix spaces. In Section 5 the algorithm for Theorem 2 is described, which works for triangularizable matrix spaces. In Section 6 we propose and investigate some natural subclasses of the Edmonds-Rado class.

## 2 Wong sequences for pairs of matrix spaces

For  $n \in \mathbb{N}$ , we set  $[n] = \{1, \dots, n\}$ . We use  $0$  to denote the zero vector space. In this section we generalize the classical Wong sequences of matrix pencils to the situation of pairs of matrix subspaces. This is the main technical tool in this work. Let  $V$  and  $V'$  be finite dimensional vector spaces over a field  $\mathbb{F}$ , and let  $\text{Lin}(V, V')$  be the vector space of linear maps from  $V$  to  $V'$ . We set  $n = \dim(V)$  and  $n' = \dim(V')$ . For  $A \in \text{Lin}(V, V')$ , and linear subspaces  $\mathcal{A} \leq \text{Lin}(V, V')$ ,  $U \leq V$  and  $W \leq V'$ , we define:

- $A(U) = \{A(u) \mid u \in U\}$ , and  $\mathcal{A}(U) = \langle \{A(u) \mid A \in \mathcal{A}, u \in U\} \rangle$ ;
- $A^{-1}(W) = \{v \in V \mid A(v) \in W\}$ , and  $\mathcal{A}^{-1}(W) = \{v \in V \mid \forall A \in \mathcal{A}, A(v) \in W\}$ .

Observe that  $A(U)$ ,  $\mathcal{A}(U)$  are linear subspaces of  $V'$ , whereas  $A^{-1}(W)$  and  $\mathcal{A}^{-1}(W)$  are subspaces of  $V$ . Also note that  $\mathcal{A}(U) = \langle \cup_{A \in \mathcal{A}} A(U) \rangle$  and  $\mathcal{A}^{-1}(W) = \cap_{A \in \mathcal{A}} A^{-1}(W)$ . Moreover, if  $\mathcal{A}$  is spanned by  $\{A_1, \dots, A_m\}$ , then  $\mathcal{A}(U) = \langle \cup_{i \in [m]} A_i(U) \rangle$ , and  $\mathcal{A}^{-1}(W) = \cap_{i \in [m]} A_i^{-1}(W)$ .

Some easy and useful facts are the following.

**Fact 3.** For  $\mathcal{A}, \mathcal{B} \leq \text{Lin}(V, V')$ , and  $U, S \leq V$ ,  $W, T \leq V'$ , we have:

1. If  $U \subseteq S$  and  $W \subseteq T$ , then  $\mathcal{A}(U) \subseteq \mathcal{A}(S)$  and  $\mathcal{A}^{-1}(W) \subseteq \mathcal{A}^{-1}(T)$ ;
2. If  $\mathcal{B}(U) \subseteq \mathcal{A}(U)$  and  $\mathcal{B}(S) \subseteq \mathcal{A}(S)$ , then  $\mathcal{B}(\langle U \cup S \rangle) \subseteq \mathcal{A}(\langle U \cup S \rangle)$ ;

3. If  $\mathcal{B}^{-1}(W) \supseteq \mathcal{A}^{-1}(W)$  and  $\mathcal{B}^{-1}(T) \supseteq \mathcal{A}^{-1}(T)$ , then  $\mathcal{B}^{-1}(W \cap T) \supseteq \mathcal{A}^{-1}(W \cap T)$ ;
4.  $\mathcal{A}^{-1}(\mathcal{A}(U)) \supseteq U$ , and  $\mathcal{A}(\mathcal{A}^{-1}(W)) \subseteq W$ .

We now define the two Wong sequences for a pair of matrix subspaces.

**Definition 4.** Let  $\mathcal{A}, \mathcal{B} \leq \text{Lin}(V, V')$ . The sequence of subspaces  $(U_i)_{i \in \mathbb{N}}$  of  $V$  is called the first Wong sequence of  $(\mathcal{A}, \mathcal{B})$ , where  $U_0 = V$ , and  $U_{i+1} = \mathcal{B}^{-1}(\mathcal{A}(U_i))$ . The sequence of subspaces  $(W_i)_{i \in \mathbb{N}}$  of  $V'$  is called the second Wong sequences of  $(\mathcal{A}, \mathcal{B})$ , where  $W_0 = 0$ , and  $W_{i+1} = \mathcal{B}(\mathcal{A}^{-1}(W_i))$ .

When  $\mathcal{A} = \langle A \rangle$  and  $\mathcal{B} = \langle B \rangle$  are one dimensional matrix spaces, the first Wong sequence corresponds to the classical first Wong sequence for the matrix pencil  $Ax - B$ , and  $(\mathcal{A}^{-1}(W_i))_{i \in \mathbb{N}}$  corresponds to the classical second Wong sequence for the matrix pencil  $Ax - B$  [Won74, BT12].

The following properties are straightforward generalizations of those for classical Wong sequences. We start by considering the first Wong sequence.

**Proposition 5.** Let  $(U_i)_{i \in \mathbb{N}}$  be the first Wong sequence of  $(\mathcal{A}, \mathcal{B})$ . Then for all  $i \in \mathbb{N}$ , we have  $U_{i+1} \subseteq U_i$ . Furthermore,  $U_{i+1} = U_i$  if and only if  $\mathcal{B}(U_i) \subseteq \mathcal{A}(U_i)$ .

*Proof.* Firstly we show that  $U_{i+1} \subseteq U_i$ , for every  $i \in \mathbb{N}$ . For  $i = 0$ , this holds trivially. For  $i > 0$ , by Fact 3 (1) we get  $U_{i+1} = \mathcal{B}^{-1}(\mathcal{A}(U_i)) \subseteq \mathcal{B}^{-1}(\mathcal{A}(U_{i-1})) = U_i$ , since  $U_i \subseteq U_{i-1}$ .

Suppose now that  $\mathcal{B}(U_i) \subseteq \mathcal{A}(U_i)$ , for some  $i$ . Then  $U_i \subseteq \mathcal{B}^{-1}(\mathcal{B}(U_i)) \subseteq \mathcal{B}^{-1}(\mathcal{A}(U_i))$  respectively by Fact 3 (4) and (1), which gives  $U_{i+1} = U_i$ . On the other hand, if  $\mathcal{B}(U_i) \not\subseteq \mathcal{A}(U_i)$  then there exist  $B \in \mathcal{B}$  and  $v \in U_i$  such that  $B(v) \notin \mathcal{A}(U_i)$ . Thus  $v \notin \mathcal{B}^{-1}(\mathcal{A}(U_i)) = U_{i+1}$ , which gives  $U_{i+1} \subset U_i$ .  $\square$

Given Proposition 5, we see that the first Wong sequence stabilizes after at most  $n$  steps at some subspace. That is, for any  $(\mathcal{A}, \mathcal{B})$ , there exists  $\ell \in \{0, \dots, n\}$ , such that  $U_0 \supset U_1 \supset \dots \supset U_\ell = U_{\ell+1} = \dots$ . In this case we call the subspace  $U_\ell$  the *limit* of  $(U_i)_{i \in \mathbb{N}}$ , and we denote it by  $U^*$ .

**Proposition 6.**  $U^*$  is the largest subspace  $T \leq V$  such that  $\mathcal{B}(T) \subseteq \mathcal{A}(T)$ .

*Proof.* By Proposition 6 we know that  $U^*$  satisfies  $\mathcal{B}(U^*) \subseteq \mathcal{A}(U^*)$ . Consider an arbitrary  $T \leq V$  such that  $\mathcal{B}(T) \subseteq \mathcal{A}(T)$ , we show by induction that  $T \subseteq U_i$ , for all  $i$ . When  $i = 0$  this trivially holds. Suppose that  $T \subseteq U_i$ , for some  $i$ . Then by repeated applications of Fact 3 we have  $T \subseteq \mathcal{B}^{-1}(\mathcal{B}(T)) \subseteq \mathcal{B}^{-1}(\mathcal{A}(T)) \subseteq \mathcal{B}^{-1}(\mathcal{A}(U_i)) = U_{i+1}$ .  $\square$

Analogous properties hold for the second Wong sequence  $(W_i)_{i \in \mathbb{N}}$ . In particular the sequence stabilizes after at most  $n'$  steps, and there exists a *limit* subspace  $W^*$  of  $(W_i)_{i \in \mathbb{N}}$ . We summarize them in the following proposition.

**Proposition 7.** Let  $(W_i)_{i \in \mathbb{N}}$  be the second Wong sequence of  $(\mathcal{A}, \mathcal{B})$ . Then

1.  $W_{i+1} \supseteq W_i$ , for all  $i \in \mathbb{N}$ . Furthermore,  $W_{i+1} = W_i$  if and only if  $\mathcal{B}^{-1}(W_i) \supseteq \mathcal{A}^{-1}(W_i)$ .
2. The limit subspace  $W^*$  is the smallest subspace  $T \leq V'$  s.t.  $\mathcal{B}^{-1}(T) \supseteq \mathcal{A}^{-1}(T)$ .

It is worth to note that the second Wong sequence can be viewed as the dual of the first one in the following sense. Assume that  $V$  and  $V'$  are equipped with nonsingular symmetric bilinear forms, both denoted by  $\langle, \rangle$ . For a linear map  $A : V \rightarrow V'$  let  $A^T : V' \rightarrow V$  stand for the transpose

of  $A$  with respect to  $\langle, \rangle$ . This is the unique map with the property  $\langle \mathcal{A}^T(u), v \rangle = \langle u, \mathcal{A}(v) \rangle$ , for all  $u \in V'$  and  $v \in V$ . For a matrix space  $\mathcal{A}$ , let  $\mathcal{A}^T$  be the space  $\{A^T | A \in \mathcal{A}\}$ . For  $U \leq V$ , the orthogonal subspace of  $U$  is defined as  $U^\perp = \{v \in V \mid \langle v, u \rangle = 0 \text{ for all } u \in U\}$ . Similarly we define  $W^\perp$  for  $W \leq V'$ . Then we have  $((\mathcal{A}^T)^{-1}(U))^\perp = \mathcal{A}(U^\perp)$ , and  $(\mathcal{A}^T(U))^\perp = \mathcal{A}^{-1}(U^\perp)$ . It can be verified that if  $(W_i)_{i \in \mathbb{N}}$  is the second Wong sequence of  $(\mathcal{A}, \mathcal{B})$  and  $(U_i)_{i \in \mathbb{N}}$  the first Wong sequence of  $(\mathcal{A}^T, \mathcal{B}^T)$ , then  $W_i = U_i^\perp$ .

For a matrix space  $\mathcal{A}$  and a subspace  $U \leq V$  given in terms of a basis we can compute  $\mathcal{A}(U)$  by applying the basis elements for  $\mathcal{A}$  to those of  $U$  and then selecting a maximal set of linearly independent vectors. A possible way of computing  $\mathcal{A}^{-1}(U)$  for  $U \leq V'$  is to compute first  $U^\perp$ , then  $\mathcal{A}^T(U^\perp)$  and finally  $\mathcal{A}^{-1}(U) = (\mathcal{A}^T(U^\perp))^\perp$ . Therefore we have

**Proposition 8.** *Wong sequences can be computed using  $(n + n')^{O(1)}$  arithmetic operations.*

Unfortunately, we are unable to prove that over the rationals the bit length of the entries of the bases describing the Wong sequences remain polynomially bounded in the length of the data for  $\mathcal{A}$  and  $\mathcal{B}$ . However, in Section 3.1 we will show that if  $\mathcal{A} = \langle A \rangle$ , then the first few members of the second Wong sequence which happen to be contained in  $\text{im} A$  can be computed in polynomial time using an iteration of multiplying vectors by matrices from a basis for  $\mathcal{B}$  and by a pseudo-inverse of  $A$ .

We also observe that if we consider the bases for  $\mathcal{A}$  and  $\mathcal{B}$  as matrices over an extension field  $\mathbb{F}'$  of  $\mathbb{F}$  then the members of the Wong sequences over  $\mathbb{F}'$  are just the  $\mathbb{F}'$ -linear spaces spanned by the corresponding members of the Wong sequences over  $\mathbb{F}$ . In particular, the limit of the first Wong sequence over  $\mathbb{F}$  is nontrivial if and only if the limit of the first Wong sequence over  $\mathbb{F}'$  is nontrivial.

## 3 The second Wong sequence and singularity witnesses

### 3.1 The connection

As in Section 2, let  $V$  and  $V'$  be finite dimensional vector spaces over a field  $\mathbb{F}$ , of respective dimensions  $n$  and  $n'$ . Let  $\mathcal{B} \leq \text{Lin}(V, V')$ . We have observed that  $\text{corank}(\mathcal{B}) \geq \text{disc}(\mathcal{B})$ , and that a  $\text{corank}(\mathcal{B})$ -singularity witness of  $\mathcal{B}$  doesn't exist necessarily. Let  $A \in \mathcal{B}$ , and consider  $(W_i)_{i \in \mathbb{N}}$ , the second Wong sequence of  $(A, \mathcal{B})$ . The next Lemma states that the limit  $W^*$  is basically such a witness under the condition that it is contained in the image of  $A$ . Moreover, in this specific case the limit can be computed efficiently.

**Lemma 9.** *Let  $A \in \mathcal{B} \leq \text{Lin}(V, V')$ , and let  $W^*$  be the limit of the second Wong sequence of  $(A, \mathcal{B})$ . There exists a  $\text{corank}(A)$ -singularity witness of  $\mathcal{B}$  if and only if  $W^* \subseteq \text{im}(A)$ . If this is the case, then  $A$  is of maximum rank and  $A^{-1}(W^*)$  is a  $\text{corank}(\mathcal{B})$ -singularity witness.*

*Proof.* We prove the equivalence. Firstly suppose that  $W^* \subseteq \text{im}(A)$ . Then  $\dim(A^{-1}(W^*)) = \dim(W^*) + \dim(\ker(A))$ . Since  $W^* = \mathcal{B}(A^{-1}(W^*))$  and  $\dim(\ker(A)) = \text{corank}(A)$ , it follows that  $A^{-1}(W^*)$  is a  $\text{corank}(A)$ -singularity witness of  $\mathcal{B}$ .

Let us now suppose that some  $U \leq V$  is a  $\text{corank}(A)$ -singularity witness, that is  $\dim(U) - \dim(\mathcal{B}(U)) \geq \text{corank}(A)$ . Then  $\dim(U) - \dim(A(U)) \geq \text{corank}(A)$  because  $A \in \mathcal{B}$ . Since the reverse inequality always holds without any condition on  $U$ , we have  $\dim(U) - \dim(A(U)) = \text{corank}(A)$ . Similarly we have  $\dim(U) - \dim(\mathcal{B}(U)) = \text{corank}(A)$  which implies that  $\dim(A(U)) = \dim(\mathcal{B}(U))$ , and therefore  $A(U) = \mathcal{B}(U)$ . For a subspace  $S \leq V$  the equality  $\dim(S) - \dim(A(S)) = \text{corank}(S)$

is equivalent to  $\ker(A) \subseteq S$ , thus we have  $\ker(A) \subseteq U$  from which it follows that  $U = A^{-1}(A(U))$ . But then  $\mathcal{B}^{-1}(A(U)) = \mathcal{B}^{-1}(\mathcal{B}(U)) \supseteq U = A^{-1}(A(U))$ . Since  $W^*$  is the smallest subspace  $T \leq V'$  satisfying  $\mathcal{B}^{-1}(T) \supseteq A^{-1}(T)$ , we can conclude that  $W^* \subseteq A(U)$ .

The existence of a  $\text{corank}(A)$ -singularity witness obviously implies that  $A$  is of maximum rank, and when  $W^* \subseteq \text{im}(A)$  we have already seen that  $A^{-1}(W^*)$  is a  $\text{corank}(A)$ -singularity witness of  $\mathcal{B}$ . Since  $\text{corank}(A) = \text{corank}(\mathcal{B})$ , it is also a  $\text{corank}(\mathcal{B})$ -singularity witness.  $\square$

We would like to find an efficient way of testing whether  $W^* \subseteq \text{im}(A)$  for a given  $A \in \mathcal{B}$ . In the computation of the limit  $W^*$  of the second Wong sequence of  $(A, \mathcal{B})$  the computationally hard step is applying iteratively  $A^{-1}$ . We overcome this difficulty by introducing a pseudo-inverse of  $A$  in the computation. We describe now this method.

Let  $n = \dim(V)$  and  $n' = \dim(V')$ . First of all we can assume without loss of generality that  $n = n'$ . Indeed, in case  $n < n'$  we can add as a direct complement a suitable space to  $V$  on which  $\mathcal{B}$  acts as zero, and in case  $n > n'$ , we can embed  $V'$  into a larger space. In terms of matrices, this means augmenting the elements of  $\mathcal{B}$  by zero columns or zero rows to obtain square matrices. This procedure affects neither the ranks of the matrices in  $\mathcal{B}$  nor the singularities.

We say that a nonsingular linear map  $A' : V' \rightarrow V$  is a *pseudo-inverse* of  $A$  if the restriction of  $A'$  to  $\text{im}(A)$  is the inverse of the restriction of  $A$  to a direct complement of  $\ker(A)$ . Such a map can be efficiently constructed as follows. Choose a direct complement  $U$  of  $\ker(A)$  in  $V$  as well as a direct complement  $U'$  of  $\text{im}(A)$  in  $V'$ . Then take the map  $A'_0 : \text{im}(A) \rightarrow U$  such that  $AA'_0$  is the identity of  $\text{im}(A)$  and take an arbitrary nonsingular linear map  $A'_1 : U' \rightarrow \ker(A)$ . Finally let  $A'$  be the direct sum of  $A'_0$  and  $A'_1$ .

**Lemma 10.** *Let  $A \in \mathcal{B} \leq \text{Lin}(V, V')$  and let  $A'$  be a pseudo-inverse of  $A$ . There exists a  $\text{corank}(A)$ -singularity witness if and only if*

$$(\mathcal{B}A')^i(\ker(AA')) \subseteq \text{im}(A),$$

for  $i \in [n]$ . This can be tested in polynomial time, and if the condition holds then  $A$  is of maximum rank and  $A'(W^*)$  is a  $\text{corank}(\mathcal{B})$ -singularity witness which also can be computed in polynomial time.

*Proof.* By Lemma 9 a  $\text{corank}(A)$ -singularity witness exists if and only if  $W_i \subseteq \text{im}(A)$ , for  $i = 1, \dots, n$ . We claim that for  $i = 1, \dots, n$ , if  $W_{i-1} \subseteq \text{im}(A)$  then  $W_i = (\mathcal{B}A')^i(\ker(AA'))$ , from which the equivalence follows. The proof is by induction. For  $i = 1$  the claim  $W_1 = \mathcal{B}A'(\ker(AA'))$  holds since  $\ker(AA') = A'^{-1}(\ker(A))$ . For  $i > 1$ , by definition  $W_i = \mathcal{B}A^{-1}(W_{i-1})$ . Since every subspace  $W \subseteq \text{im}(A)$  satisfies  $A^{-1}W = A'W$ , we get  $W_i = \mathcal{B}A'(W_{i-1})$ , and can conclude by the inductive hypothesis using  $\ker(AA') = A'^{-1}\ker(A)$ .

Based on this equivalence, testing the existence of a  $\text{corank}(A)$ -singularity witness can be accomplished by the following simple algorithm. First compute a basis for  $\mathcal{B}$ , and then multiply it by  $A'$  to obtain a basis for  $\mathcal{B}A'$ . Compute also a basis for  $\ker(AA')$ . We now describe how to compute bases for the subspaces in the second Wong sequence until either we find  $i$  such that  $W_i \not\subseteq \text{im}(A)$  or we compute  $W^*$ . A basis for  $W_1$  can be obtained by applying the basis elements of  $\mathcal{B}A'$  to the basis elements of  $\ker(AA')$  and then selecting a maximal set of linearly independent vectors. Having computed a basis for  $W_i$ , we stop if it contains an element outside  $\text{im}(A)$ . Otherwise we apply the basis elements of  $\mathcal{B}A'$  to the basis elements of  $W_i$ , and select a maximal set of linearly independent vectors to obtain a basis for  $W_{i+1}$ . When  $W_{i+1} = W_i$  we can stop since  $W^* = W_i$ .

If we find that the condition holds than  $A'(W^*)$  by Lemma 9 is a  $\text{corank}(\mathcal{B})$ -singularity witness, and it can be easily computed from  $W^*$ .  $\square$

### 3.2 The power overflow problem

For  $A \in \mathcal{B} \leq \text{Lin}(V, V')$ , we would like to know whether  $A$  is of maximum rank in  $\mathcal{B}$ . With the help of the limit  $W^*$  of the second Wong sequence of  $(A, \mathcal{B})$  we have established a sufficient condition: we know that if  $W^* \subseteq \text{im}(A)$  then  $A$  is indeed of maximum rank. Our results until now don't give a sufficient condition for the maximum rank. Now we show that the second Wong sequence actually allows to translate this question to the *power overflow* problem (PO) which we define below. As a consequence an efficient solution of the PO guarantees an efficient solution for the SMR. The reduction is mainly based on a theorem of Atkinson and Stephens which essentially says that over big enough fields, in 2-dimensional matrix spaces  $\mathcal{B}$ , the equality  $\text{corank}(\mathcal{B}) = \text{disc}(\mathcal{B})$  holds.

**Proposition 11** ([AS78]). *Assume that  $|\mathbb{F}| > n$ , and let  $A, B \in \text{Lin}(V, V')$ . If  $A$  is a maximum rank element of  $\langle A, B \rangle$  then there exists a  $\text{corank}(A)$ -singularity witness of  $\langle A, B \rangle$ .*

Combining Lemma 10 and Proposition 11 we get also a sufficient (actually equivalent) condition for  $A$  being of maximum rank.

**Lemma 12.** *Assume that  $|\mathbb{F}| > n$ . Let  $A \in \mathcal{B} \leq \text{Lin}(V, V')$ , and let  $A'$  be a pseudo-inverse of  $A$ . Then  $A$  is of maximum rank in  $\mathcal{B}$  if and only if for every  $B \in \mathcal{B}$  and for all  $i \in [n]$ , we have*

$$(BA')^i(\ker(AA')) \subseteq \text{im}(A).$$

*Proof.* First observe that  $A$  is of maximum rank in  $\mathcal{B}$  if and only if for every  $B \in \mathcal{B}$ , it is of maximum rank in  $\langle A, B \rangle$ . For a fixed  $B$ , by Proposition 11 and Lemma 10,  $A$  is of maximum rank in  $\langle A, B \rangle$  exactly when  $((B, A)A')^i(\ker(AA')) \subseteq \text{im}(A)$ , for all  $i \in [n]$ . From that we can conclude since  $A'$  is the inverse of  $A$  on  $\text{im}(A)$ .  $\square$

This lemma naturally leads us to reduce the problems of deciding if  $A$  is of the maximum rank, and finding a matrix of rank larger than  $A$  when this is not the case, to the following question.

**Problem 13** (The power overflow problem). *Given  $\mathcal{D} \leq M(n, \mathbb{F})$ ,  $U \leq \mathbb{F}^n$  and  $U' \leq \mathbb{F}^n$ , output  $D \in \mathcal{D}$  and  $\ell \in [n]$  such that  $D^\ell(U) \not\subseteq U'$ , if there exists such  $(D, \ell)$ . Otherwise say **no**.*

The power overflow problem admits an efficient randomized algorithm when  $|\mathbb{F}| = \Omega(n)$ . For the rank-1 spanned case we show a deterministic solution regardless of the field size.

**Theorem 14.** *Let  $\mathcal{D} \leq M(n, \mathbb{F})$  be spanned by rank-1 matrices. Then there exists  $D \in \mathcal{D}$  and  $\ell \in [n]$  such that  $D^\ell(U) \not\subseteq U'$  if and only if there exists  $\ell \in [n]$  such that  $\mathcal{D}^\ell(U) \not\subseteq U'$ . The power overflow problem for  $\mathcal{D}$  can be solved in polynomial time.*

Using this result we are now ready to prove Theorem 1.

**Proof of Theorem 1.** First we suppose that  $|\mathbb{F}| \geq n + 1$ . Let  $A$  be an arbitrary matrix in  $\mathcal{B}$ . The algorithm iterates the following process until  $A$  becomes of maximum rank.

We run the algorithm of Lemma 10 to test whether  $(\mathcal{B}A')^i(\ker(AA')) \subseteq \text{im}(A)$  for  $i \in [n]$ . If this condition holds then  $A$  is of maximum rank, and the algorithm also gives a  $\text{corank}(\mathcal{B})$ -singularity witness. Otherwise we know by Theorem 14 that there exists  $B \in \mathcal{B}$  and  $i \in [n]$  such that  $(BA')^i(\ker(AA')) \not\subseteq \text{im}(A)$ . We apply the algorithm of Theorem 14 with input  $\mathcal{B}A'$ ,  $\ker(AA')$  and  $\text{im}(A)$ , which finds such a couple  $(B, i)$ . Lemma 12 applied to  $\langle A, B \rangle$  implies that  $A$  is not

of maximum rank in  $\langle A, B \rangle$ . If  $A$  has rank  $r \leq n - 1$  which is not maximal in  $\langle A, B \rangle$ , then the determinant of an appropriate  $(r + 1) \times (r + 1)$  minor is a nonzero polynomial of degree at most  $r + 1$  which has at most  $r + 1 \leq n$  roots. We then pick  $n + 1$  arbitrary field elements  $\lambda_1, \dots, \lambda_{n+1}$ , and we know that for some  $1 \leq j \leq n + 1$  we have  $\text{rank}(A + \lambda_j B) > \text{rank}(A)$ . We replace  $A$  by  $A + \lambda_j B$  and restart the process from the beginning.

At the end each iteration we can achieve by a reduction procedure described in [dGIR96] that the matrix  $A$ , written as a linear combination of  $B_1, \dots, B_m$  has coefficients form a fixed subset  $K \subseteq \mathbb{F}$  of size  $n + 1$ . In fact, if  $A = \alpha_1 B_1 + \alpha_2 B_2 \dots + \alpha_m B_m$  has rank  $r$  then for at least one  $\kappa_1 \in \Lambda$  the matrix  $\lambda_1 B_1 + \alpha_2 B_2 \dots + \alpha_m B_m$  has rank at least  $r$ . This way all the coefficients  $\alpha_j$  can be replaced with an appropriate element from  $K$ .

The number of iterations is at most  $n$ , and each iteration takes polynomial many steps since the processes of Lemma 10 and Theorem 1 are polynomial. Therefore the overall running time is also polynomial.  $\square$

We can compute the maximum rank over a field of size less than  $n + 1$  by running the above procedure over a sufficiently large extension field. The maximum rank will not grow if we go over an extension. This follows from the fact that the equality  $\text{corank}(\mathcal{B}) = \text{disc}(\mathcal{B})$  holds over any field if  $\mathcal{B}$  is spanned by an arbitrary matrix and by rank one matrices, see [IKS10].

## 4 The power overflow problem for rank-1 spanned matrix spaces

In this section we prove Theorem 14. Suppose we are given subspaces  $U, U'$  of  $\mathbb{F}^n$  as well as a basis  $\{D_1, \dots, D_m\}$  for a matrix space  $\mathcal{D} \leq M(n, \mathbb{F})$ . We will show is that in polynomial time we can decide if  $\mathcal{D}^\ell(U) \not\subseteq U'$  for some  $\ell$ , and if this holds then find  $D \in \mathcal{D}$  such that  $D^\ell(U) \not\subseteq U'$ .

Formally we define  $\ell = \ell(\mathcal{D})$  as the smallest integer  $j$  such that  $\mathcal{D}^j(U) \not\subseteq U'$  if such an integer exists, and  $n$  otherwise. We start with computing  $\ell$  and for  $1 \leq j \leq \ell$ , bases  $\mathcal{T}_j$  for  $\mathcal{D}^j$ . We set  $\mathcal{T}_1 = \{D_1, \dots, D_m\}$ . If  $\mathcal{D}^j(U) \not\subseteq U'$  then we set  $\ell = j$  and stop constructing further bases. If  $j = n$  and  $\mathcal{D}^n(U) \subseteq U'$  then we stop the algorithm and output **no**. Otherwise we compute  $\mathcal{T}_{j+1}$  by selecting a maximal linearly independent set form the products of elements in  $\mathcal{T}_j$  and  $\mathcal{T}_1$ .

We are now looking for  $D$  such that  $D^\ell(U) \not\subseteq U'$ . For  $i \in [\ell]$ , we define subspaces  $\mathcal{H}_i$  of  $\mathcal{D}$ , which play a crucial role in the algorithm:

$$\mathcal{H}_i = \{X \in \mathcal{D} \mid \mathcal{D}^{\ell-j} X \mathcal{D}^{j-1}(U) \subseteq U', j = 1, \dots, i - 1, i + 1, \dots, \ell\}.$$

That is,  $X \in \mathcal{H}_i$  if and only if whenever  $X$  appears in a place other than the  $i$ th in a product  $P$  of  $\ell$  elements from  $\mathcal{D}$  then  $P(U) \subseteq U'$ . The subspaces  $\mathcal{H}_i$  can be computed as follows. Let  $x_1, \dots, x_m$  be formal variables, a generic element in  $\mathcal{D}$  can be written as  $X = \sum_{k \in [m]} x_k D_k$ . The condition

$$\mathcal{D}^{\ell-j} X \mathcal{D}^{j-1}(U) \subseteq U'$$

is equivalent to the set of the following homogeneous linear equations in the variables  $x_k$ :

$$\langle Z \left( \sum_{k \in [m]} x_k D_k \right) Z' u, v \rangle = 0,$$

where  $Z$  is from  $\mathcal{T}_{\ell-j}$ ,  $Z'$  is from  $\mathcal{T}_{j-1}$ ,  $u$  is from a basis for  $U$  and  $v$  is from a basis for  $U'^\perp$ . Thus  $\mathcal{H}_i$  can be computed by solving a a system of polynomially many homogeneous linear equations.

Note that the coefficients of the equations are scalar products of vectors from a basis for  $U'^\perp$  by vectors obtained as applying products of  $\ell$  matrices from  $\{D_1, \dots, D_m\}$  to basis elements for  $U$ . The definition of  $\mathcal{H}_i$  implies the following.

**Lemma 15.** *For a matrix  $X = X_1 + \dots + X_\ell$  with  $X_i \in \mathcal{H}_i$ , we have  $X^\ell(U) \subseteq U'$  if and only if  $X_\ell \cdots X_2 X_1(U) \subseteq U'$ .*

*Proof.* We have  $X^m = \sum_\sigma X_{\sigma(\ell)} \cdots X_{\sigma(1)}$ , where the summation is over the maps  $\sigma : [\ell] \rightarrow [\ell]$ . When  $\sigma$  is not the identity map then there exists an index  $j$  such that  $\sigma(j) \neq j$ . Then  $X_{\sigma(\ell)} \cdots X_{\sigma(1)}(U) \subseteq U'$  by the definition of  $\mathcal{H}_{\sigma(j)}$ .  $\square$

In general,  $\mathcal{H}_i$  can be zero. However, the existence of rank one generators implies that this is not the case. Recall that  $\ell$  is the smallest integer such that  $\mathcal{D}^\ell(U) \not\subseteq U'$ .

**Lemma 16.** *We have  $\mathcal{H}_\ell \cdots \mathcal{H}_1(U) \not\subseteq U'$ .*

*Proof.* Assume that  $\mathcal{D}$  is spanned by the rank one matrices  $C_1, \dots, C_m$ . Then there exist indices  $k_1, \dots, k_\ell$  such

$$C_{k_\ell} \cdots C_{k_1}(U) \not\subseteq U'.$$

We show that  $C_{k_i} \in \mathcal{H}_i$ , for  $i \in [\ell]$ , this implies immediately  $\mathcal{H}_\ell \cdots \mathcal{H}_1(U) \not\subseteq U'$ . Assume by contradiction that  $C_{k_i} \notin \mathcal{H}_i$ , for some  $i \in [\ell]$ . Then

$$\mathcal{D}^{\ell-j} C_{k_i} \mathcal{D}^{j-1}(U) \not\subseteq U'$$

for some  $j \neq i$ . On the other hand  $C_{k_i}$  satisfies that

$$\mathcal{D}^{\ell-i} C_{k_i} \mathcal{D}^{i-1}(U) \not\subseteq U'.$$

Since  $C_{k_i}$  is of rank 1 we have that

$$C_{k_i} \mathcal{D}^{j-1}(U) = C_{k_i} \mathcal{D}^{i-1}(U),$$

which yields that neither  $\mathcal{D}^{\ell-i} C_{k_i} \mathcal{D}^{j-1}(U)$  nor  $\mathcal{D}^{\ell-j} C_{k_i} \mathcal{D}^{i-1}(U)$  is contained in  $U'$ . However one of these products is shorter than  $\ell$ , contradicting the minimality of  $\ell$ .  $\square$

To finish the algorithm, we compute bases for products  $\mathcal{H}_i \cdots \mathcal{H}_1$ , for  $i \in [n]$ , in a way similar to computing bases for  $\mathcal{D}^i$ . Then we search the basis of  $\mathcal{H}_\ell$  for an element  $Z$  such that  $Z \mathcal{H}_{\ell-1} \cdots \mathcal{H}_1(U) \not\subseteq U'$ . We put  $X_\ell = Z$  and continue searching the basis of  $\mathcal{H}_{\ell-1}$  for an element  $Z$  such that  $X_\ell Z \mathcal{H}_{\ell-2} \cdots \mathcal{H}_1(U) \not\subseteq U'$ . Continuing the iteration, Lemma 16 ensures that eventually we find  $X_i \in \mathcal{H}_i$ , for  $i \in [\ell]$ , such that  $X_\ell \cdots X_1(U) \not\subseteq U'$ . We set  $D = X_1 + \dots + X_\ell$ , then by Lemma 15 we have  $D^\ell(U) \not\subseteq U'$ . We return  $D$  and  $\ell$ .  $\square$

## 5 The first Wong sequence and triangularizable matrix spaces

### 5.1 An algorithm over finite and black box fields

Suppose we are given a basis  $\{B_1, \dots, B_m\}$  for  $\mathcal{B} \leq M(n, \mathbb{F})$  which is triangularizable over an extension field  $\mathbb{F}'$  of  $\mathbb{F}$ , i. e.,  $B_i = DB'_i C^{-1}$  for some nonsingular  $C, D \in M(n, \mathbb{F}')$ , and  $B'_i \in M(n, \mathbb{F}')$  is upper triangular for every  $i \in [m]$ . Our problem is to determine whether there exists a nonsingular matrix in  $\mathcal{B}$  or not and finding such a matrix if exists.

Our starting point is to observe the following lemma, which connects first Wong sequences with singular witnesses.

**Lemma 17.** *Let  $A \in \mathcal{B} \leq M(n, \mathbb{F})$ , and let  $U^*$  be the limit of the first Wong sequence of  $(A, \mathcal{B})$ . Set  $d = \dim(U^*)$ . Then either  $U^*$  is a singularity witness of  $\mathcal{B}$ , or there exist nonsingular matrices  $P, Q \in M(n, \mathbb{F})$ , such that  $\forall B \in \mathcal{B}$ ,  $QBP^{-1}$  is of the form  $\begin{bmatrix} X & Y \\ 0 & Z \end{bmatrix}$ , where  $X$  is of size  $d \times d$ , and  $\mathcal{B}$  is nonsingular in the  $X$ -block.*

*Proof.* If  $\dim(U^*) > \dim(\mathcal{B}(U^*))$  then  $U^*$  is a singularity witness. If  $\dim(U^*) = \dim(\mathcal{B}(U^*))$  then the choice of  $P$  and  $Q$  corresponds to an appropriate basis change transformation. To see that  $\mathcal{B}$  is nonsingular in the  $X$ -block, note that  $A \in \mathcal{B}$  and  $A(U^*) = \mathcal{B}(U^*)$ .  $\square$

Lemma 17 suggests a recursive algorithm: take an arbitrary  $A \in \mathcal{B}$  and compute  $U^*$ , the limit of the first Wong sequence of  $(A, \mathcal{B})$ . If we get a singular witness, we are done. Otherwise, if  $U^* \neq 0$  we can focus on the nonsingularity of  $Z$ -block which is of smaller size. To make this idea work, we have to satisfy essentially two conditions. We must find some  $A$  such that  $U^* \neq 0$ , and to allow for recursion the specific property of the matrix space  $\mathcal{B}$  we are concerned with has to be inherited by the subspace corresponding to the  $Z$ -block. It turns out that in the triangularizable case these two problems can be taken care of by the following lemma.

**Lemma 18.** *Let  $\mathcal{B} \leq M(n, \mathbb{F})$  given by a basis  $\{B_1, \dots, B_m\}$ , and suppose that there exist nonsingular matrices  $C, D \in M(n, \mathbb{F})$  such that  $B_i = DB'_iC^{-1}$  and  $B'_i \in M(n, \mathbb{F})$  is upper triangular for every  $i \in [m]$ . Then we have the following.*

1. *Either  $\bigcap_{i \in [m]} \ker(B_i) \neq 0$ , or there exists  $j \in [m]$  and  $0 \neq U \leq \mathbb{F}^n$  such that  $B_j(U) = \mathcal{B}(U)$ .*
2. *Suppose that there exists  $U \leq \mathbb{F}^n$  such that  $\dim(\mathcal{B}(U)) = \dim(U)$ . For  $i \in [m]$ , let  $B'_i : \mathbb{F}^n/U \rightarrow \mathbb{F}^n/\mathcal{B}(U)$  be the linear map induced by  $B_i$ . Then  $\mathcal{B}^* = \langle B'_1, \dots, B'_m \rangle$  is triangularizable.*

*Proof.* 1. Let  $\{e_i \mid i \in [n]\}$  be the standard basis of  $\mathbb{F}^n$ , and  $c_i = C(e_i)$  and  $d_i = D(e_i)$  for  $i \in [n]$ . If  $B'_i(1, 1) = 0$  for all  $i \in [m]$  then  $c_1$  is in the kernel of every  $B_i$ 's. If there exists  $j$  such that  $B'_j(1, 1) \neq 0$ , we set  $U' = \langle c_1 \rangle \leq \mathbb{F}^n$ . Then it is clear that  $\langle d_1 \rangle = B_j(U') = \mathcal{B}(U')$ . It follows that the first Wong sequence of  $(B_j, \mathcal{B})$  over  $\mathbb{F}'$  has nonzero limit, and therefore the same holds over  $\mathbb{F}$ . We can choose for  $U$  this limit.

2. First we recall that for a vector space  $V$  of dimension  $n$ , a complete flag of  $V$  is a nested sequence of subspaces  $0 = V_0 \subset V_1 \subset \dots \subset V_n = V$ . For  $\mathcal{A} \leq \text{Lin}(V, V')$  with  $\dim(V) = \dim(V') = n$ , the matrix space  $\mathcal{A}$  is triangularizable if and only if there exist complete flags  $0 = V_0 \subset V_1 \subset \dots \subset V_n = V$  and  $0 = V'_0 \subset V'_1 \subset \dots \subset V'_n = V'$  such that  $\mathcal{A}(V_i) \subseteq V'_i$  for  $i \in [n]$ .

For  $U \leq \mathbb{F}^n$  and  $\mathbb{F}'$  an extension field of  $\mathbb{F}$ , let  $\mathbb{F}'U$  be the linear span of  $U$  in  $\mathbb{F}'^n$ . We think of  $B_i$ 's and  $B'_i$ 's as linear maps over  $\mathbb{F}'$  in a natural way. Let  $\ell = \dim(\mathbb{F}'^n/\mathbb{F}'U)$ . For  $0 \leq i \leq n$  set  $S_i = \langle c_1, \dots, c_i \rangle$  and  $T_i = \langle d_1, \dots, d_i \rangle$ . Obviously  $\mathcal{B}(S_i) \subseteq T_i$  for  $0 \leq i \leq n$ . Let  $S_i^* = S_i/\mathbb{F}'U$  and  $T_i^* = T_i/\mathcal{B}(\mathbb{F}'U)$ , and consider  $S_0^* \subseteq \dots \subseteq S_n^*$  and  $T_0^* \subseteq \dots \subseteq T_n^*$ . As  $\mathcal{B}^*(S_i^*) \subseteq T_i^*$ ,  $\dim(S_{i+1}^*) - \dim(S_i^*) \leq 1$ , and  $\dim(T_{i+1}^*) - \dim(T_i^*) \leq 1$ , there must be a pair of complete flags  $S_0^* \subset S_{j_1}^* \subset \dots \subset S_{j_\ell}^* = S_n^*$  and  $T_0^* \subset T_{k_1}^* \subset \dots \subset T_{k_\ell}^* = T_n^*$ , such that  $\mathcal{B}^*(S_{j_h}^*) \subseteq T_{k_h}^*$  for all  $h \in [\ell]$ . It follows that  $\mathcal{B}^*$  is triangularizable over  $\mathbb{F}'$ .  $\square$

We expand the above idea into a rigorous algorithm, called TRIALGO and present it in Algorithm 1. This algorithm requires polynomially many arithmetic operations, and therefore of polynomial complexity in finite fields. The input of the algorithm can be an arbitrary matrix space

(not necessarily triangularizable), but it may fail in certain cases. For triangularizable matrix spaces the algorithm would not fail due to Lemma 18. Note that though the algorithm works assuming triangularizability over some extension field, the algorithm itself does not need to deal with the field extension explicitly by Lemma 18, given that  $\mathbb{F}$  is large enough. To allow for recursion, the output of the algorithm can be one of the following: the first is an explicit linear combination of the given matrices, which gives a nonsingular matrix. The second is a singular subspace witness. The third one is **Fail**.

Regarding implementation, it might be needed to comment on Line 13. At this point we have that  $\dim(U^*) \leq \dim(\mathcal{B}(U^*)) \leq \dim(B_j(U^*)) \leq \dim(U^*)$ . Thus  $\dim(\mathcal{B}(U^*)) = \dim(U^*)$ , and note that  $B_i(U^*) \subseteq \mathcal{B}(U^*)$ , for all  $i \in [m]$ . Then two bases of  $\mathbb{F}^n$  can be formed by extending bases of  $U^*$  and  $\mathcal{B}(U^*)$  respectively, and w.r.t. these two bases the induced action  $B_i$  from  $\mathbb{F}^n/U^*$  to  $\mathbb{F}^n/\mathcal{B}(U^*)$  can be read off easily.

For correctness we distinguish among the types of output of the algorithm, and show that they indeed have the required property.

If  $(\alpha_1, \dots, \alpha_m)$  is returned: This case occurs in Line 2 and Line 20. Line 2 is trivial. If the algorithm reaches Line 20, we claim that there exists  $(\lambda, \mu) \in \Lambda \times \Lambda$  s.t.  $\lambda B_j + \mu E$  is nonsingular. Let  $P$  and  $Q$  be the matrices from Lemma 17. Thus  $\forall i \in [m]$ ,  $QB_iP^{-1}$  is of the form:  $\begin{bmatrix} X_i & Y_i \\ 0 & Z_i \end{bmatrix}$ , where  $X_i$  is of size  $(n - \ell) \times (n - \ell)$  and  $Z_i$  is of size  $\ell$  by  $\ell$ . As  $X_j$  is nonsingular and  $\sum_{i \in [m]} \alpha_i Z_i$  is nonsingular,  $\det(xB_j + yE)$  is a nonzero polynomial, thus from Schwartz-Zippel lemma the existence of  $(\lambda, \mu)$  in  $\Lambda \times \Lambda$  is ensured.

If a subspace of  $\mathbb{F}^n$  is returned: This case occurs in Line 2, 4, 8 and 16. All are straightforward.

The case of **Fail**: After Line 3  $\bigcap_{i \in [m]} \ker(B_i) = 0$ . Then Lemma 18 ensures that **Fail** cannot be returned for triangularizable matrix spaces.

## 5.2 An algorithm over rationals

To obtain a polynomial-time algorithm over rationals, we give first a characterization of triangularizability of a nonsingular matrix space.

**Lemma 19.** *Assume  $\mathcal{B} \leq M(n, \mathbb{F})$  contains a nonsingular matrix  $S$ . Then  $\mathcal{B}$  is triangularizable over  $\mathbb{F}$  if and only if there exists a nonsingular matrix  $D \in M(n, \mathbb{F})$  such that  $D^{-1}\mathcal{B}S^{-1}D$  consists of upper triangular matrices.*

*Proof.*  $\Rightarrow$ : Assume that  $D^{-1}\mathcal{B}C$  consists of upper triangular matrices. Then  $C^{-1}S^{-1}D = (D^{-1}SC)^{-1}$  is upper triangular as well, whence – as products of upper triangular matrices remain upper triangular –  $D^{-1}\mathcal{B}S^{-1}D = (D^{-1}\mathcal{B}C)(C^{-1}S^{-1}D)$  also consists of upper triangular matrices.

$\Leftarrow$ : Assume that  $D^{-1}\mathcal{B}S^{-1}D$  consists of upper triangular matrices. Put  $C = S^{-1}D$ .  $\square$

We have the following criterion of triangularizability:

**Lemma 20.** *Let  $\mathcal{A} \leq M(n, \mathbb{F})$  containing the identity matrix and let  $\mathbb{F}'$  be the algebraic closure of  $\mathbb{F}$ . Then there exists  $D \in M(n, \mathbb{F}')$  such that  $D^{-1}\mathcal{A}D$  consists of upper triangular matrices (over  $\mathbb{F}'$ ) if and only if*

$$(\mathcal{A}^{n^2}[\mathcal{A}, \mathcal{A}]\mathcal{A}^{n^2})^n = (0).$$

Here  $[\mathcal{A}, \mathcal{A}]$  is the space spanned by the commutators  $[X, Y] = XY - YX$  ( $X, Y \in \mathcal{A}$ ).

---

**Algorithm 1:** TRIALGO( $B_1, \dots, B_m$ )

---

**Input:**  $\mathcal{B} = \langle B_1, \dots, B_m \rangle \subseteq M(n, \mathbb{F})$ .

**Output:** One of the following: (1)  $(\alpha_1, \dots, \alpha_m) \in \mathbb{F}^m$  s.t.  $\sum_{i \in [m]} \alpha_i B_i$  is nonsingular. (2) A singular subspace witness  $U \leq \mathbb{F}^n$ . (3) **Fail**.

// Base case

1 **if**  $n = 1$  **then**

2   | If  $\exists$  nonzero  $B_i$ , **return**  $(0, \dots, 1, \dots, 0)$  where 1 is at the  $i$ th position. Otherwise  
2   |   **return**  $\mathbb{F}^n$ .

// Start of the recursive step.

// If  $\cap_{i \in [m]} \ker(B_i) \neq 0$  then  $\cap_{i \in [m]} \ker(B_i)$  is a singular witness itself.

3 **if**  $\cap_{i \in [m]} \ker(B_i) \neq 0$  **then**

4   |   **return**  $\cap_{i \in [m]} \ker(B_i)$ .

5 **forall** the  $i \in [m]$  **do**

6   |  $U_i^* \leftarrow$  the limit of the first Wong sequence of  $(B_i, \mathcal{B})$ .

7 **if**  $\exists i \in [m]$ ,  $\dim(\mathcal{B}(U_i^*)) < \dim(U_i^*)$  **then**

8   |   **return**  $U_i^*$

9 **if**  $\nexists j$  s.t.  $\dim(U_j^*) > 0$  **then**

10   |   **return** **Fail**

11  $U^* \leftarrow U_j^*$  where  $U_j^*$  satisfies that  $\dim(U_j^*) > 0$ ;

12 **forall** the  $i \in [m]$  **do**

13   |  $B_i^* \leftarrow$  the induced linear map of  $B_i$  from  $\mathbb{F}^n/U^*$  to  $\mathbb{F}^n/\mathcal{B}(U^*)$ .

// Recursive call.

14  $X \leftarrow$  TRIALGO( $B_1^*, \dots, B_m^*$ );

15 **if**  $X$  is a singular subspace witness  $W/U^*$  **then**

16   |   **return** the full preimage of  $W/U^*$  in the canonical projection  $\mathbb{F}^n \rightarrow \mathbb{F}^n/U^*$ .

17 **else if**  $X$  is  $(\alpha_1, \dots, \alpha_m)$  **then**

18   |  $\Lambda \leftarrow$  a set of field element of size  $n + 1$ ;

19   |  $E \leftarrow \sum_{i \in [m]} \alpha_i B_i$ ;

20   | Choose  $(\lambda, \mu) \in \Lambda \times \Lambda$ , s.t.  $\lambda B_j + \mu E$  is nonsingular;

21   |   **return**  $(\mu\alpha_1, \dots, \mu\alpha_{j-1}, \mu\alpha_j + \lambda, \mu\alpha_{j+1}, \dots, \mu\alpha_m)$

22 **else if**  $X = \text{Fail}$  **then**

23   |   **return** **Fail**

---

*Proof.* Put  $\mathcal{D} = (\mathcal{A})^{n^2}$ . Then  $\mathcal{D}$  is the matrix algebra generated by  $\mathcal{A}$ . The formula expresses that the two-sided ideal of  $\mathcal{D}$  generated by the commutators from  $\mathcal{A}$  is nilpotent. Let  $\mathcal{D}' = \mathbb{F}' \otimes \mathcal{D}$ . Then the formula is also equivalent to that the ideal of  $\mathcal{D}'$  generated by the commutators is nilpotent. This is further equivalent to that the factor algebra  $\mathcal{D}'/Rad(\mathcal{D}')$  is commutative. However, over an algebraically closed field a matrix algebra is nilpotent if it is a conjugate of a subalgebra of the upper triangular matrices. (To see one direction, observe that the whole algebra of the upper triangular matrices and hence every subalgebra of it has this property. As for reverse implication, note that all the irreducible representations of an algebra over an algebraically closed field which is commutative by its radical are one-dimensional and hence a composition series gives a complete flag consisting of invariant subspaces.)  $\square$

**Corollary 21.** *Let  $\mathbb{F}$  be either a finite field or  $\mathbb{Q}$ . Assume that we are given a nonsingular  $S \in \mathcal{B}$ . Then there is a polynomial time algorithm which decides whether or not there exists an extension of  $\mathbb{F}$  over which  $\mathcal{B}$  is triangularizable.*

Again, we actually have an algorithm using a polynomial number of arithmetic operations and equality tests in the black box model for  $\mathbb{F}$ .

With these preparations we are now ready to prove Theorem 2.

**Proof of Theorem 2.** Over finite fields Algorithm 1 is all we need. Over rationals we shall perform a reduction to finite fields via Lemma 20.

We assume that  $\mathcal{B}$  is given by matrices  $B_1, \dots, B_m$  over  $\mathbb{Q}$ . Multiplying by a common denominator for the entries, we can achieve the situation when the entries of  $B_1, \dots, B_m$  are integers. Let  $b$  be a bound on the of absolute values of the entries of  $B_1, \dots, B_m$ . Then a polynomial-time algorithm should run in time polynomial in  $n$  and  $\log b$ . If  $\mathcal{B}$  is nonsingular then there exist integers  $\lambda_1, \dots, \lambda_m$ , each between 0 and  $n$  such that  $S = \lambda_1 B_1 + \dots + \lambda_m B_m$  is nonsingular. The absolute value of the determinant of  $S$  is a nonzero integer whose logarithm is bounded by a polynomial in  $\log b$  and  $n$ . It follows that there is a prime  $p$  of size bounded by an (explicit) polynomial in  $b$  and  $n$  that does not divide the determinant of  $S$ .

Let  $S' = \det(S)S^{-1}$ . We reduce the problem modulo  $p$ . We see that  $S$  and  $S'$  are integral matrices and both are invertible modulo  $p$ . Furthermore, if  $\mathcal{B}$  is triangularizable over an extension of  $\mathbb{Q}$ , then all the products of the form  $B_{i_1} S' \cdots B_{i_{n_2}} S' [B_{j_1} S', B_{j_2} S'] B_{k_1} S' \cdots B_{k_{n_2}} S'$  vanish, and this will be the case modulo  $p$  as well. It follows that the subspace of matrices over  $\mathbb{F}_p$ , spanned by the matrices  $B_i S'$ , reduced modulo  $p$ , can be triangularized over an extension field of  $\mathbb{F}_p$ . But then the space spanned by  $B_i$  is also triangularizable.

Thus if  $\mathcal{B}$  is nonsingular and triangularizable over an extension of  $\mathbb{Q}$  then there is a prime  $p$  greater than  $n$  but smaller than the value of an explicit polynomial function in  $\log b$  and  $n$ , such that the reduction modulo  $p$  gives a nonsingular matrix space which is triangularizable over an extension field of  $\mathbb{F}_p$ . The algorithm consists of taking the primes  $p$  up the the polynomial limit and applying the generic method over  $\mathbb{F}_p$  to the reduced setting. The method either finds a  $p$  and an integer combination of  $B_1, \dots, B_m$  which is nonsingular even modulo  $p$  or, concludes that  $\mathcal{B}$  cannot be nonsingular and triangularizable at the same time.  $\square$

## 6 On the Edmonds-Rado class and some subclasses

### 6.1 Matrix spaces not in the Edmonds-Rado class

Recall that  $\mathcal{B} \leq M(n, \mathbb{F})$  is in the Edmonds-Rado class if either (1)  $\mathcal{B}$  contains nonsingular matrices, or (2)  $\mathcal{B}$  is singular and there exist singular witnesses of  $\mathcal{B}$ . Recall that in Section 1.1 we defined  $\text{disc}(\mathcal{B}) = \max(c \in \mathbb{N} \mid \exists c\text{-discrepancy subspace witness})$ , and it is clear that  $\text{corank}(\mathcal{B}) \geq \text{disc}(\mathcal{B})$ . In terms of  $\text{disc}$ ,  $\mathcal{B}$  is in the Edmonds-Rado class, if  $\text{disc}(\mathcal{B}) = 0 \iff \text{corank}(\mathcal{B}) = 0$ .

A well-known example of matrix spaces not in the Edmonds-Rado class is the following

$$\text{sk}_3 := \left\langle \left[ \begin{array}{ccc} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{array} \right], \left[ \begin{array}{ccc} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{array} \right], \left[ \begin{array}{ccc} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{array} \right] \right\rangle.$$

Consider the following problem: if a matrix space  $\mathcal{B}$  has a basis consisting of matrices with certain property (e.g. triangular, positive semidefinite, projections, positive<sup>2</sup> etc.), does it imply that  $\mathcal{B}$  is in the Edmonds-Rado class? The triangular and positive semidefinite properties indeed put  $\mathcal{B}$  in the Edmonds-Rado class as observed by Gurvits. We now show that the other two properties, namely projection and positive matrices, do not necessarily imply that  $\mathcal{B}$  is in the Edmonds-Rado class.

Given  $\mathcal{B} = \langle B_1, \dots, B_m \rangle \leq M(n, \mathbb{F})$ . Let  $A \in M(n, \mathbb{F})$  be an arbitrary nonsingular matrix. Define  $Y'_i, Z' \in M(2n, \mathbb{F})$  by  $Y'_i = \begin{bmatrix} A & B_i + A \\ 0 & 0 \end{bmatrix}$ , and let  $Z' = \begin{bmatrix} 0 & 0 \\ A & A \end{bmatrix}$ . Form  $\mathcal{A}' = \langle Y'_1, \dots, Y'_m, Z' \rangle$ . Note that if  $A = I$ , then  $Y'_i$ 's and  $Z'$  are projections. If  $A$  is a positive matrix with entries no less than the absolute values of entries in  $B_i$ 's, then  $Y'_i$ 's and  $Z'$  are positive matrices.

Via simultaneous row and column operations, from  $Y'_i$ 's and  $Z'$  we get  $Y_i = \begin{bmatrix} A & B_i \\ 0 & 0 \end{bmatrix}$ , and  $Z = \begin{bmatrix} 0 & 0 \\ A & 0 \end{bmatrix}$ . Let  $\mathcal{A} = \langle Y_1, \dots, Y_m, Z \rangle$ . Note that simultaneous row and column operations do not change  $\text{corank}$  nor  $\text{disc}$ ; that is  $\text{corank}(\mathcal{A}') = \text{corank}(\mathcal{A})$  and  $\text{disc}(\mathcal{A}') = \text{disc}(\mathcal{A})$ . Observe that  $\text{corank}(\mathcal{A}) = \text{corank}(\mathcal{B})$ , and suppose we could show that  $\text{disc}(\mathcal{A}) = \text{disc}(\mathcal{B})$ . Then taking some  $\mathcal{B}$  not in the Edmonds-Rado class (e.g.  $\text{sk}_3$ ) and plugging into the construction above, it would follow that  $\mathcal{A}$  and  $\mathcal{A}'$  are not in the Edmonds-Rado class. Finally recall that  $\mathcal{A}'$  can be generated by projections or positive matrices depending on the choice of  $A$ .

**Proposition 22.**  $\text{disc}(\mathcal{A}) = \text{disc}(\mathcal{B})$ .

*Proof.* Let  $E_1 \leq \mathbb{F}^{2n}$  be the coordinate subspace generated by the first  $n$  coordinates, and  $E_2 \leq \mathbb{F}^{2n}$  be the coordinate subspace generated by the last  $n$  coordinates.

To show that  $\text{disc}(\mathcal{A}) \geq \text{disc}(\mathcal{B})$ , we take a  $\text{disc}(\mathcal{B})$ -discrepancy witness  $(U, U')$  of  $\mathcal{B}$ , and embed  $U$  and  $U'$  into  $E_2$ . Then  $(\langle E_1 \cup U \rangle, \langle E_1 \cup U' \rangle)$  is a  $\text{disc}(\mathcal{B})$ -discrepancy witness of  $\mathcal{A}$ .

To show that  $\text{disc}(\mathcal{A}) \leq \text{disc}(\mathcal{B})$ , let  $(W, W')$  be  $\text{disc}(\mathcal{A})$ -discrepancy witness of  $\mathcal{A}$ , and w.l.o.g. assume  $W' = \mathcal{A}(W)$ . Let  $W'_1 = W' \cap E_1$  and  $W'_2 = W' \cap E_2$ . Due to the form of  $Y_i$ 's and  $Z$ ,  $W' = W'_1 \oplus W'_2$ . In particular note that  $W'_2 = Z(W)$ , and  $A$  is nonsingular. So letting  $R \leq W$  be  $\{w \in W \mid Z(w) = 0\}$ , we have  $R \leq E_2$ ,  $\dim(R) = \dim(W) - \dim(W'_2)$ , and  $\dim(W'_1) \geq \dim(\mathcal{B}(R))$ .

<sup>2</sup>Recall that a matrix over  $\mathbb{R}$  is positive if every entry in it is positive.

Thus  $\text{disc}(\mathcal{A}) = \dim(W) - \dim(W') = (\dim(W) - \dim(W'_2)) - \dim(W'_1) \leq \dim(R) - \dim(\mathcal{B}(R)) \leq \text{disc}(\mathcal{B})$ .  $\square$

## 6.2 The quantitative Edmonds-Rado class

If  $\text{rank}(\mathcal{B})$  is of primary interest, in analogous to the Edmonds-Rado class we have the following. Here we allow non-square matrices from  $M(n \times n', \mathbb{F})$ , and recall that for  $A \in M(n \times n', \mathbb{F})$ , its rank is  $\dim(\text{im}(A))$ , co-rank is  $\dim(\ker(A))$ , and  $A$  is nonsingular if  $\text{rank}(A) = \min(n, n')$ .

**Definition 23.** *Let  $\mathcal{B} \leq M(n \times n', \mathbb{F})$ .  $\mathcal{B}$  is in the quantitative Edmonds-Rado class if  $\mathcal{B}$  possesses  $\text{corank}(\mathcal{B})$ -discrepancy subspace witnesses.*

For brevity we call it q-Edmonds-Rado class in the following. In terms of  $\text{disc}$ ,  $\mathcal{B}$  is in the q-Edmonds-Rado class if  $\text{corank}(\mathcal{B}) = \text{disc}(\mathcal{B})$ . As to Wong sequences, from Lemma 9 we immediately have: if  $\mathcal{B} \leq M(n \times n', \mathbb{F})$  is in the q-Edmonds-Rado class, then for  $A \in \mathcal{B}$ ,  $A$  is of maximum rank if and only if the limit of the second Wong sequence of  $(A, \mathcal{B})$  is contained in  $\text{im}(A)$ .

It is clear that if  $\mathcal{B}$  is in the Edmonds-Rado class then it is in the q-Edmonds-Rado class. The converse is not true.

**Proposition 24.** *Rank maximization of matrix spaces can be reduced to rank maximization of matrix spaces with a basis of pairwise commuting, and strictly upper triangular matrices.*

*Proof.* For  $\mathcal{B} = \langle B_1, \dots, B_m \rangle \leq M(n \times n', \mathbb{F})$  we first pad 0's to make it a matrix space of  $M(\max(n, n'), \mathbb{F})$ . Then consider the matrix space in  $M(2 \cdot \max(n, n'), \mathbb{F})$  generated by  $C_1, \dots, C_m$  where  $C_i = \begin{bmatrix} 0 & B_i \\ 0 & 0 \end{bmatrix}$ .  $\square$

This explains why we do not expect to achieve rank maximization for upper triangular matrices in Theorem 1. Then recall that if a matrix space is spanned by upper-triangular matrices then it is in the Edmonds-Rado class. Apply the construction in Proposition 24 with  $\text{sk}_3$ , we have the following:

**Corollary 25.** *There exists a matrix space in the Edmonds-Rado class, but not in the q-Edmonds-Rado class.*

## 6.3 The black-box Edmonds-Rado class

**Definition 26.** *Let  $\mathcal{B} \leq M(n \times n', \mathbb{F})$ .  $\mathcal{B}$  is in the black-box Edmonds-Rado class if the following conditions hold: (1) there exists a  $\text{corank}(\mathcal{B})$ -discrepancy witness; (2) for any  $A \in \mathcal{B}$ , either  $A$  is of maximum rank, or  $\mathcal{B}(\ker(A)) \not\subseteq \text{im}(A)$ .*

By the first condition, the black-box Edmonds-Rado class is a subclass of the q-Edmonds-Rado class. Also note that  $\mathcal{B}(\ker(A))$  is just the first item in the second Wong sequence of  $(A, \mathcal{B})$ . The second condition says that if  $A$  is non-maximum rank then already the first item in the second Wong sequence excludes existence of  $\text{corank}(A)$ -discrepancy witnesses. In this case for any matrix  $B$  from  $\mathcal{B}$  with  $B \ker(A) \not\subseteq \text{im}(A)$  we have  $\text{rank} B > \text{rank} A$ . Therefore in matrix spaces in this class the following simple algorithm finds an element of maximum rank over sufficiently large base fields.

Compute the rank of  $A + \lambda B$  where  $\lambda$  is from a subset of  $\mathbb{F}$  of size  $\text{rank} A + 1$  and  $B$  is from a basis of  $\mathcal{B}$ . If none of these matrices have rank larger than  $A$ , conclude that  $A$  is of maximum rank. Otherwise replace  $A$  with an  $A + \lambda B$  of larger rank.

As a justification of the name of the subclass, observe that this algorithm does not make use of any properties of matrices other than their rank. It even works in the setting that instead of inputting the basis  $B_1, \dots, B_m$  explicitly, we only know  $m$  and have an oracle which, on input  $(\alpha_1, \dots, \alpha_m)$  returns the rank of  $\alpha_1 B_1, \dots, \alpha_m B_m$ .

While this class seems quite restrictive, it contains some interesting cases. A first example is when  $\mathcal{B}$  has a basis of positive semidefinite matrices. Suppose  $\mathcal{B} = \langle B_1, \dots, B_m \rangle \leq M(n, \mathbb{R})$ , where  $B_i$ 's are positive semidefinite. Then it is seen easily that  $A$  is of maximum rank if and only if  $\ker(A) = \bigcap_{i \in [m]} \ker(B_i)$ . In particular if  $A$  is not of maximum rank then there exists  $v \in \ker(A)$  s.t.  $B_j(v) \notin \text{im}(A)$  for some  $j \in [m]$ .

Another more interesting scenario is from [CIK97] (see also [IKS10], Lemma 4.2). Let  $G$  be a finite dimensional associative algebra over  $\mathbb{F}$  and let  $V, V'$  be semisimple  $G$ -modules,  $\mathcal{B} = \text{Hom}_G(V, V')$ . Recall that a semisimple module is the direct sum of simple modules and in a semisimple module every submodule has a direct complement.  $A \in \mathcal{B}$  is of maximum rank if and only if for every isomorphism type  $S$  of simple modules for  $A$ , the multiplicity of  $S$  in  $\text{im}(A)$  is the minimum of the multiplicities of  $S$  in  $U$  and  $V$ .

If  $A$  is not of maximum rank, then for some simple module  $S$  there is an isomorphic copy  $S_1$  of  $S$  in  $\ker(A)$  and there is a copy  $S_2$  of  $S$  in  $V'$  intersecting  $\text{im}(A)$  trivially. And there are nontrivial homomorphisms mapping the first copy of  $S$  to the second one. (For instance, any isomorphism  $S_1 \rightarrow S_2$  can be extended to a homomorphism  $V \rightarrow V'$  by the zero map on a direct complement of  $S_1$ .)

On the other hand, if  $A$  is of maximum rank then for every simple submodule in  $\ker(A)$ , the copies in  $V'$  isomorphic to it are in  $\text{im}(A)$ , therefore no simple constituent can be moved out of  $\text{im}(A)$  via the second Wong sequence.

## References

- [AS78] M. D. Atkinson and N. M. Stephens. Spaces of matrices of bounded rank. *The Quarterly Journal of Mathematics*, 29(2):221–223, 1978.
- [Ber84] Stuart J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Information Processing Letters*, 18(3):147–150, 1984.
- [BFS99] Jonathan F. Buss, Gudmund S. Frandsen, and Jeffrey O. Shallit. The computational complexity of some problems of linear algebra. *Journal of Computer and System Sciences*, 58(3):572–596, 1999.
- [BT12] T. Berger and S. Trenn. The quasi-Kronecker form for matrix pencils. *SIAM Journal on Matrix Analysis and Applications*, 33(2):336–368, 2012.
- [BT13] Thomas Berger and Stephan Trenn. Addition to “the quasi-Kronecker form for matrix pencils”. *SIAM Journal on Matrix Analysis and Applications*, 34(1):94–101, 2013.
- [CDS10] Eric Chitambar, Runyao Duan, and Yaoyun Shi. Multipartite-to-bipartite entanglement transformations and polynomial identity testing. *Physical Review A*, 81(5):052310, 2010.
- [CIK97] Alexander L. Chistov, Gábor Ivanyos, and Marek Karpinski. Polynomial time algorithms for modules over finite dimensional algebras. In *ISSAC*, pages 68–74, 1997.

- [dGIR96] Willem A. de Graaf, Gábor Ivanyos, and Lajos Rónyai. Computing Cartan subalgebras of Lie algebras. *Applicable Algebra in Engineering, Communication and Computing*, 7(5):339–349, 1996.
- [Edm67] Jack Edmonds. Systems of distinct representatives and linear algebra. *J. Res. Nat. Bur. Standards Sect. B*, 71:241–245, 1967.
- [Edm70] Jack Edmonds. Submodular functions, matroids, and certain polyhedra. In N. Sauer R. K. Guy, H. Hanani and J. Schönheim, editors, *Combinatorial Structures and their Appl.*, pages 69–87, New York, 1970. Gordon and Breach.
- [FS12] Michael A. Forbes and Amir Shpilka. Quasipolynomial-time identity testing of non-commutative and read-once oblivious algebraic branching programs. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:115, 2012.
- [Gee99] James F. Geelen. Maximum rank matrix completion. *Linear Algebra and its Applications*, 288:211–217, 1999.
- [GI05] James Geelen and Satoru Iwata. Matroid matching via mixed skew-symmetric matrices. *Combinatorica*, 25(2):187–215, 2005.
- [GIM03] James F. Geelen, Satoru Iwata, and Kazuo Murota. The linear delta-matroid parity problem. *Journal of Combinatorial Theory, Series B*, 88(2):377–398, 2003.
- [Gur02] Leonid Gurvits. Quantum matching theory (with new complexity theoretic, combinatorial and topological insights on the nature of the quantum entanglement), 2002.
- [Gur04] Leonid Gurvits. Classical complexity and quantum entanglement. *J. Comput. Syst. Sci.*, 69(3):448–484, 2004.
- [HKM05] Nicholas J. A. Harvey, David R. Karger, and Kazuo Murota. Deterministic network coding by matrix completion. In *Proceedings of the sixteenth annual ACM-SIAM symposium on Discrete algorithms*, pages 489–498. Society for Industrial and Applied Mathematics, 2005.
- [HKY06] Nicholas J. A. Harvey, David R. Karger, and Sergey Yekhanin. The complexity of matrix completion. In *Proceedings of the seventeenth annual ACM-SIAM symposium on Discrete algorithm*, pages 1103–1111. ACM, 2006.
- [IKS10] Gábor Ivanyos, Marek Karpinski, and Nitin Saxena. Deterministic polynomial time algorithms for matrix completion problems. *SIAM J. Comput.*, 39(8):3736–3751, 2010.
- [KI04] Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004.
- [Lov79] László Lovász. On determinants, matchings, and random algorithms. In *FCT*, pages 565–574, 1979.
- [Lov89] László Lovász. Singular spaces of matrices and their application in combinatorics. *Boletim da Sociedade Brasileira de Matemática-Bulletin/Brazilian Mathematical Society*, 20(1):87–99, 1989.

- [Mur00] Kazuo Murota. *Matrices and matroids for systems analysis*. Springer, 2000.
- [Rad42] Richard Rado. A theorem on independence relations. *The Quarterly Journal of Mathematics, Oxford Ser.*, 13(1):83–89, 1942.
- [Sch79] Jacob T. Schwartz. Probabilistic algorithms for verification of polynomial identities. In Edward W. Ng, editor, *Symbolic and Algebraic Computation*, volume 72 of *Lecture Notes in Computer Science*, pages 200–215. Springer Berlin Heidelberg, 1979.
- [Tre13] Stephan Trenn. Solution concepts for linear DAEs: A survey. In Achim Ilchmann and Timo Reis, editors, *Surveys in Differential-Algebraic Equations I*, Differential-Algebraic Equations Forum, pages 137–172. Springer Berlin Heidelberg, 2013.
- [Val79] Leslie G. Valiant. Completeness classes in algebra. In *STOC*, pages 249–261, 1979.
- [Wel70] D. J. A. Welsh. On matroid theorems of Edmonds and Rado. *Journal of the London Mathematical Society*, 2(2):251–256, 1970.
- [Won74] Kai-Tak Wong. The eigenvalue problem  $\lambda Tx + Sx$ . *Journal of Differential Equations*, 16(2):270 – 280, 1974.
- [Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In Edward W. Ng, editor, *Symbolic and Algebraic Computation*, volume 72 of *Lecture Notes in Computer Science*, pages 216–226. Springer Berlin Heidelberg, 1979.