On rank-critical matrix spaces

Yinan Li [*] Youming Qiao [†]

March 2, 2017

Abstract

A matrix space of size $m \times n$ is a linear subspace of the linear space of $m \times n$ matrices over a field $\mathbb{F}$. The rank of a matrix space is defined as the maximal rank over matrices in this space. A matrix space $\mathcal{A}$ is called rank-critical, if any matrix space which properly contains it has rank strictly greater than that of $\mathcal{A}$.

In this note, we first exhibit a necessary and sufficient condition for a matrix space $\mathcal{A}$ to be rank-critical, when $\mathbb{F}$ is large enough. This immediately implies the sufficient condition for a matrix space to be rank-critical by Draisma (Bull. Lond. Math. Soc. 38(5):764–776, 2006), albeit requiring the field to be slightly larger.

We then study rank-critical spaces in the context of compression and primitive matrix spaces. We first show that every rank-critical matrix space can be decomposed into a rank-critical compression matrix space and a rank-critical primitive matrix space. We then prove, using our necessary and sufficient condition, that the block-diagonal direct sum of two rank-critical matrix spaces is rank-critical if and only if both matrix spaces are primitive, when the field is large enough.

1 Results

1.1 A necessary and sufficient condition for a matrix space to be rank-critical

Let $\mathbb{F}$ be a field, and let $M(m\times n,\mathbb{F})$ be the linear space of $m\times n$ matrices over $\mathbb{F}$. A *matrix space* $\mathcal{A}$ is a linear subspace of $M(m\times n,\mathbb{F})$, denoted as $\mathcal{A} \leq M(m\times n,\mathbb{F})$. For $A \in M(m\times n,\mathbb{F})$ we denote its rank, kernel, and image, by $\mathrm{rk}(A)$, $\ker(A)$, and $\mathrm{im}(A)$, respectively. The *rank of a matrix space* $\mathcal{A}$, denoted as $\mathrm{rk}(\mathcal{A})$, is defined as $\max\{\mathrm{rk}(A) : A \in \mathcal{A}\}$. $\mathcal{A}$ is *singular*, if $\mathrm{rk}(\mathcal{A}) < \min\{m,n\}$. $\mathcal{A}$ is called *rank-critical*, if for any $\mathcal{B} \leq M(m\times n,\mathbb{F})$ with $\mathcal{B} \supsetneq \mathcal{A}$, $\mathrm{rk}(\mathcal{B}) > \mathrm{rk}(\mathcal{A})$. Every $(g,h) \in GL(m,\mathbb{F}) \times GL(n,\mathbb{F})$ has a natural action on matrix spaces in $M(m\times n,\mathbb{F})$, by sending $\mathcal{A}$ to $g\mathcal{A}h^{-1}$. Two matrix spaces are equivalent if they are in the same orbit of this action.

Our first result is a necessary and sufficient condition for a matrix space to be rank-critical. To state it, we introduce some notation. For $\mathcal{A} \leq M(m\times n,\mathbb{F})$, $\mathcal{A}_{\mathrm{reg}} := \{A \in \mathcal{A} : \mathrm{rk}(A) = \mathrm{rk}(\mathcal{A})\}$. For two subspaces $U \leq \mathbb{F}^m$, $V \leq \mathbb{F}^n$ and $A \in M(m\times n,\mathbb{F})$, $A(V) = \{A(v) : v \in V\} \leq \mathbb{F}^m$ and $A^{-1}(U) = \{v \in \mathbb{F}^n : A(v) \in U\} \leq \mathbb{F}^n$. Note that the A^{-1} as in $A^{-1}(\cdot)$ does not refer to the inverse of A and A is not necessarily invertible.

The central notion in our condition is the following. Define the *rank neutral set* of $\mathcal{A} \leq M(m\times n,\mathbb{F})$ as

$$\mathrm{RNS}(\mathcal{A}) := \{B \in M(m\times n,\mathbb{F}) : \forall A \in \mathcal{A}_{\mathrm{reg}}, \forall k \in \{0,1,\ldots,m\}, B(A^{-1}B)^k \ker(A) \subseteq \mathrm{im}(A)\}. \tag{1}$$

[*]Centre for Quantum Software and Information, University of Technology Sydney, Australia (liyinan9252@gmail.com).

[†]Centre for Quantum Software and Information, University of Technology Sydney, Australia (jimmyqiao86@gmail.com).

The elements of $\mathrm{RNS}(\mathcal{A})$ are called the *rank neutral elements* of $\mathcal{A}$. Note that for $(g,h) \in GL(m,\mathbb{F}) \times GL(n,\mathbb{F})$, $\mathrm{RNS}(g\mathcal{A}h^{-1}) = g\mathrm{RNS}(\mathcal{A})h^{-1}$.

Theorem 1. *Let $\mathcal{A} \leq M(m \times n, \mathbb{F})$ and suppose $|\mathbb{F}| \geq 2 \cdot \min(m,n)$. Then $\mathrm{RNS}(\mathcal{A}) \supseteq \mathcal{A}$, and $\mathcal{A}$ is rank-critical if and only if $\mathrm{RNS}(\mathcal{A}) = \mathcal{A}$. Furthermore, given $G \leq GL(m,\mathbb{F}) \times GL(n,\mathbb{F})$ with the natural action on matrix spaces, if $\mathcal{A}$ is stable under G, then $\mathrm{RNS}(\mathcal{A})$ is also stable under G.*

We deduce the sufficient condition for a matrix space to be rank-critical by Draisma [2006], which plays a key role there to prove that the images of certain Lie algebra representations are rank-critical. The key notion in Draisma's condition is the set of *rank neural directions* of $\mathcal{A} \leq M(m \times n, \mathbb{F})$,

$$\mathrm{RND}(\mathcal{A}) := \{B \in M(m \times n, \mathbb{F}) : \forall A \in \mathcal{A}_{\mathrm{reg}}, B\ker(A) \subseteq \mathrm{im}(A)\}.$$

Clearly, $\mathrm{RND}(\mathcal{A}) \supseteq \mathrm{RNS}(\mathcal{A})$. Furthermore if a group action is present as described in Theorem 1, then $\mathrm{RND}(\mathcal{A})$ is also a stable set under the action of G. Therefore the following result by Draisma follows immediately from Theorem 1.

Corollary 2 ([Draisma, 2006, Proposition 3])**.** *Let $\mathcal{A} \leq M(m \times n, \mathbb{F})$ and suppose $|\mathbb{F}| \geq 2 \cdot \min(n,m)$. Then $\mathrm{RND}(\mathcal{A}) \supseteq \mathcal{A}$, and if $\mathrm{RND}(\mathcal{A}) = \mathcal{A}$ then $\mathcal{A}$ is rank-critical. Furthermore, given $G \leq GL(m,\mathbb{F}) \times GL(n,\mathbb{F})$ with the natural action on matrix spaces, if $\mathcal{A}$ is stable under under G, then $\mathrm{RND}(\mathcal{A})$ is also stable under G.*

We note the following differences between Corollary 2 and [Draisma, 2006, Prop. 3], though such differences are mostly superficial. On one hand, Corollary 2 requires the field to be slightly larger than needed in [Draisma, 2006, Prop. 3]: there it only requires $|\mathbb{F}| > \mathrm{rk}(\mathcal{A})$. On the other hand, Corollary 2 deals with matrix spaces that are not necessarily square, and handles a more general group action.

In [Draisma, 2006], Draisma asked the question to investigate the "discrepancy between rank-criticality and $\mathcal{A} = \mathrm{RND}(\mathcal{A})$." Our result may be used as a guide to answer this question: it is now enough to investigate the discrepancy between $\mathrm{RNS}(\mathcal{A})$ and $\mathrm{RND}(\mathcal{A})$. Of course, since the condition in the definition of $\mathrm{RND}(\mathcal{A})$ is linear, in practice it is usually easier to work with $\mathrm{RND}(\mathcal{A})$. In fact, we are not aware of an explicit example of rank-critical spaces for which the $\mathrm{RND}(\mathcal{A}) = \mathcal{A}$ fails.

1.2 Rank-critical matrix spaces and primitive matrix spaces

Atkinson and Lloyd [1981] introduced the notion of primitive matrix spaces. Recall that a matrix space of size $m \times n$ is non-degenerate, if $\cap_{A\in\mathcal{A}} \ker(A) = \{0\}$ and $\mathrm{span}\{\cup_{A\in\mathcal{A}}\mathrm{im}(A)\} = \mathbb{F}^m$. A matrix space $\mathcal{A} \leq M(m \times n, \mathbb{F})$ is

- row-primitive, if $\cap_{A\in\mathcal{A}_{\mathrm{reg}}}\mathrm{im}(A) = 0$;
- column-primitive, if $\mathrm{span}\{\cup_{A\in\mathcal{A}_{\mathrm{reg}}} \ker(A)\} = \mathbb{F}^n$;
- pre-primitive, if $\mathcal{A}$ is row-primitive and column-primitive;
- primitive, if $\mathcal{A}$ is non-degenerate, row-primitive, and column-primitive.

Note that the zero space in $M(m \times n, \mathbb{F})$ is also a pre-primitive matrix space.

Another interesting family of matrix spaces is the following. Given $U \leq \mathbb{F}^m$ and $V \leq \mathbb{F}^n$, let $p = \dim(U)$, $q = \mathrm{codim}(V) = n - \dim(V)$, and $\mathcal{C}^{m,n}_{U\leftarrow V} = \{A \in M(m \times n, \mathbb{F}) : A(V) \leq U\}$. When $p + q < \min(m,n)$, $\mathrm{rk}(\mathcal{C}^{m,n}_{U\leftarrow V}) = \dim(U) + \mathrm{codim}(V)$. We call $\mathcal{C}^{m,n}_{U\leftarrow V}$ a maximal compression matrix space of parameter (p,q,m,n). A matrix space is called a compression matrix space, if it is a subspace of a maximal compression matrix space of parameter (p,q,m,n), and its rank is $p+q$. The standard maximal compression matrix space of parameter (p,q,m,n) is $\mathcal{C}^{m,n}_{U'\leftarrow V'}$ where U' is spanned by the first p standard basis vector of $\mathbb{F}^m$ and V' is spanned by the last $(n-q)$ standard basis vector of $\mathbb{F}^n$. We shall denote it $\mathcal{C}^{m,n}_{p,q}$ for short. Clearly, $\mathcal{C}^{m,n}_{p,q} = \{A \in M(m\times n,\mathbb{F}) : \forall p < i \le m, q < j \le n, A(i,j) = 0\}$, where $A(i,j)$ denotes the (i,j)th entry of A. The standard complement of $\mathcal{C}^{m,n}_{p,q}$ is $\overline{\mathcal{C}^{m,n}_{p,q}} := \{A \in M(m\times n,\mathbb{F}) : \forall 1 \le i \le p, 1 \le k \le n, A(i,k) = 0, \text{ and } \forall 1 \le k \le m, 1 \le j \le q, A(k,j) = 0\}$. Note that $\mathcal{C}^{m,n}_{0,0}$ is the zero matrix space.

The following structural result regarding matrix spaces of rank bounded from above was first observed by Atkinson and Lloyd [1981].

Theorem 3 ([Atkinson and Lloyd, 1981, Theorem 1])**.** *Given a singular matrix space $\mathcal{A} \le M(m\times n,\mathbb{F})$, there exist integers $p,q \ge 0$ satisfying $p+q < \min(m,n)$, and a primitive matrix space $\mathcal{P} \le M(r\times s,\mathbb{F})$, $0 \le r \le m-p$ and $0 \le s \le n-q$, such that $\mathrm{rk}(\mathcal{A}) = \mathrm{rk}(\mathcal{P}) + p + q$. Moreover, $\mathcal{A}$ is equivalent to a matrix space $\mathcal{B}$ in which each matrix is of the form*

$$\left[\begin{array}{c|cc} p\times q & & \\ \hline & P & 0 \\ & 0 & 0 \end{array}\right], \tag{2}$$

where $P \in \mathcal{P}$.

Some remarks are due for this theorem. Firstly, the parameters p, q, and $\mathcal{P}$ are not unique for a given $\mathcal{A}$. Secondly, the existence of some p, q, and $\mathcal{P}$ is easy to prove by induction. The main contribution of Atkinson and Lloyd [1981] was to obtain strong restrictions on the size of a primitive matrix space in terms of its rank. Thirdly, when $p=q=0$, then $\mathcal{A}$ is pre-primitive. On the other hand, if $r=s=0$, then $\mathcal{A}$ is a compression matrix space.

We then study rank-critical matrix spaces in the context of Theorem 3. We first observe that a compression matrix space is rank-critical, if and only if it is a maximal compression matrix space (see e.g. [Draisma, 2006, Example 10]). In general, for any rank-critical matrix space we have the following.

Theorem 4. *Let $\mathcal{A} \le M(m\times n,\mathbb{F})$ be a matrix space and let $\mathcal{B}$, $\mathcal{P}$ be matrix spaces as in Theorem 3. Let $\mathcal{B}_c$ be the projection of $\mathcal{B}$ to $\mathcal{C}^{m,n}_{p,q}$ along $\overline{\mathcal{C}^{m,n}_{p,q}}$, and $\mathcal{B}_p$ the projection of $\mathcal{B}$ to $\overline{\mathcal{C}^{m,n}_{p,q}}$ along $\mathcal{C}^{m,n}_{p,q}$. Then $\mathcal{A}$ is rank-critical, if and only if the following hold: (1) $\mathcal{B}_c = \mathcal{C}^{m,n}_{p,q}$, (2) $\mathcal{P}$ is rank-critical, and (3) $\mathcal{B} = \mathcal{B}_p \oplus \mathcal{B}_c$, where $\oplus$ denotes the direct sum of two subspaces in $M(m\times n,\mathbb{F})$.*

When $\mathbb{F}$ is large enough, in Theorem 4, we may replace "rank-critical" with the condition $\mathrm{RNS}(*) = *$. It is then interesting to consider an analogous statement with RND instead of RNS.

Theorem 5. *Suppose $|\mathbb{F}| \ge 2\cdot\min(m,n)$, and let $\mathcal{A} \le M(m\times n,\mathbb{F})$ be a matrix space and let $\mathcal{B}$, $\mathcal{P}$ be matrix spaces as in Theorem 3. Let $\mathcal{B}_c$ be the projection of $\mathcal{B}$ to $\mathcal{C}^{m,n}_{p,q}$ along $\overline{\mathcal{C}^{m,n}_{p,q}}$, and $\mathcal{B}_p$ the projection of $\mathcal{B}$ to $\overline{\mathcal{C}^{m,n}_{p,q}}$ along $\mathcal{C}^{m,n}_{p,q}$. Then $\mathrm{RND}(\mathcal{A}) = \mathcal{A}$, if and only if the following hold: (1) $\mathcal{B}_c = \mathcal{C}^{m,n}_{p,q}$, (2) $\mathrm{RND}(\mathcal{P}) = \mathcal{P}$, and (3) $\mathcal{B} = \mathcal{B}_p \oplus \mathcal{B}_c$, where $\oplus$ denotes the direct sum of two subspaces in $M(m\times n,\mathbb{F})$.*

Theorem 5 confirms the common wisdom that to find a rank-critical matrix space $\mathcal{A}$ with $\mathcal{A} \ne \mathrm{RND}(\mathcal{A})$, it is enough to focus on primitive matrix spaces.

Finally, we apply the necessary and sufficient condition from Theorem 1 to prove the following result concerning direct sums of rank-critical matrix spaces. Given two matrix spaces $\mathcal{A}_1 \le M(m_1\times n_1,\mathbb{F})$ and $\mathcal{A}_2 \le M(m_2\times n_2,\mathbb{F})$, the (block-diagonal) direct sum of $\mathcal{A}_1$ and $\mathcal{A}_2$ is a matrix space in $M((m_1+m_2)\times(n_1+n_2),\mathbb{F})$, defined as $\{\begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix} \in M((m_1+m_2)\times(n_1+n_2),\mathbb{F}) : A_1 \in \mathcal{A}_1, A_2 \in \mathcal{A}_2\}$. By abuse of notation we also denote this by $\mathcal{A}_1 \oplus \mathcal{A}_2$.

Theorem 6. *Suppose we are given two rank-critical matrix spaces $\mathcal{A}_1 \leq M(m_1 \times n_1, \mathbb{F})$ and $\mathcal{A}_2 \leq M(m_2 \times n_2, \mathbb{F})$, and suppose $|\mathbb{F}| \geq 2\min(m_1 + m_2, n_1 + n_2)$. $\mathcal{A}_1 \oplus \mathcal{A}_2$ is rank-critical if and only if $\mathcal{A}_1$ and $\mathcal{A}_2$ are primitive.*

2 Proofs

2.1 On Theorem 1

2.1.1 The Wong sequences, and some digression

Our condition is achieved via a perspective that is different from Draisma's as in [Draisma, 2006]. Draisma arrived at the sufficient condition $\mathrm{RND}(\mathcal{A}) = \mathcal{A}$ from a geometric perspective, by considering tangent spaces at regular points in a linear subspace contained in an affine variety. On the other hand, our condition, $\mathrm{RNS}(\mathcal{A}) = \mathcal{A}$, was obtained from an algorithmic perspective. We now introduce some previous results from Ivanyos et al. [2015a] that support the proof of Theorem 1, together with some background information. Some of the material here is more general than strictly needed to prove Theorem 1, as we want to take this chance to advocate a connection between the geometry of matrix spaces and a key algorithmic problem in computational complexity theory.

A central problem in computational complexity theory is the *symbolic determinant identity testing* (SDIT) problem, which asks to decide whether a matrix space, given by a linear basis, contains a full-rank matrix. When the underlying field is large enough, SDIT admits a randomized efficient algorithm Lovász [1979]. The goal then is to devise a deterministic efficient algorithm, as this implies an arithmetic circuit lower bound that is believed to be beyond current techniques [Carmosino et al., 2015].

In fact, for the purpose of [Carmosino et al., 2015], it is enough to exhibit a polynomial-size witness for the singularity of a matrix space. This problem is wide open, while some helpful structures are known. One such structure is the following. For $\mathcal{A} \leq M(m \times n, \mathbb{F})$, and $V \leq \mathbb{F}^n$, it is easy to verify that $\mathrm{rk}(\mathcal{A}) \leq n - (\dim(V) - \dim(\mathcal{A}(V))) = \mathrm{codim}(V) + \dim(\mathcal{A}(V))$. So $\mathrm{rk}(\mathcal{A}) \leq n - \max\{\dim(V) - \dim(\mathcal{A}(V)) : V \leq \mathbb{F}^n\}$. Lovász [1989] observed that if $\mathcal{A}$ has a basis consisting of rank-1 matrices, then this upper bound can be achieved at some $V \leq \mathbb{F}^n$. This follows from the matroid intersection theorem for linear matroids [Edmonds, 1970].

Furthermore, for $\mathcal{A} \leq M(m \times n, \mathbb{F})$ and $s \in \mathbb{Z}^+$, we call $V \leq \mathbb{F}^n$ an s-shrunk subspace of $\mathcal{A}$, if $\dim(V) - \dim(\mathcal{A}(V)) \geq s$. It is then an interesting question to decide whether a given matrix space possesses an s-shrunk subspace for a given $s \in \mathbb{Z}^+$. Recently, deterministic polynomial-time algorithms were devised in Garg et al. [2016] over $\mathbb{Q}$, and Ivanyos et al. [2015b, 2016] over any field. The key algorithmic technique in Ivanyos et al. [2015b, 2016] is the (second generalized) Wong sequences, first used in Fortin and Reutenauer [2004] and then rediscovered in Ivanyos et al. [2015a]. They can be viewed as a linear algebraic analogue of the augmenting paths, which were developed to solve the perfect matching problem on bipartite graphs. Given $A \in \mathcal{A} \leq M(m \times n, \mathbb{F})$, the Wong sequence of $(A, \mathcal{A})$ is the following sequence of subspaces of $\mathbb{F}^m$: $W_0 = \{0\}, W_1 = \mathcal{A}(A^{-1}(W_0)), W_2 = \mathcal{A}(A^{-1}(W_1)), \dots, W_{i+1} = \mathcal{A}(A^{-1}(W_i)), \dots$. It is known that for some $\ell \in \{0, 1, \dots, m\}$, $W_0 < W_1 < \dots < W_\ell = W_{\ell+1} = \dots$ [Ivanyos et al., 2015a, Prop. 7], and $\mathcal{A}$ has a $\dim(\ker(A))$-shrunk subspace if and only if $W_\ell \subseteq \mathrm{im}(A)$ [Ivanyos et al., 2015a, Lemma 9].

2.1.2 Proof of Theorem 1

We now turn to prove Theorem 1. The reader probably has noticed the similarity between the formulation of the rank neutral set, and Wong sequences introduced above. One more ingredient is to relate Wong sequences to 2-dimensional matrix spaces. For $\mathcal{A} \leq M(m \times n, \mathbb{F})$ of dimension 2 with $|\mathbb{F}| > \min(m, n)$, it is known that $\mathrm{rk}(\mathcal{A}) = n - \max\{\dim(V) - \dim(\mathcal{A}(V)) : V \leq \mathbb{F}^n\}$

(see e.g. Atkinson and Stephens [1978]). Combining with the Wong sequences, Ivanyos et al. [2015a] showed the following:

Lemma 7 ([Ivanyos et al., 2015a, Lemma 12]). *Suppose we are given $A \in \mathcal{A} = \text{span}\{A, B\} \leq M(m \times n, \mathbb{F})$, and $|\mathbb{F}| > \min(m, n)$. Then A is of maximal rank in $\mathcal{A}$, if and only if for $i \in \{0, 1, \ldots, m\}$, $B(A^{-1}B)^i \ker(A) \leq \text{im}(A)$.*

Given Lemma 7 it is easy to prove Theorem 1.

Theorem 1, restated Let $\mathcal{A} \leq M(m \times n, \mathbb{F})$ and suppose $|\mathbb{F}| \geq 2 \cdot \min(m, n)$. Then $\text{RNS}(\mathcal{A}) \supseteq \mathcal{A}$, and $\mathcal{A}$ is rank-critical if and only if $\text{RNS}(\mathcal{A}) = \mathcal{A}$. Furthermore, given $G \leq GL(m, \mathbb{F}) \times GL(n, \mathbb{F})$ with the natural action on matrix spaces, if $\mathcal{A}$ is stable under G, then $\text{RNS}(\mathcal{A})$ is also stable under G.

Proof. To start with, note that Lemma 7 immediately implies that $\text{RNS}(\mathcal{A}) \supseteq \mathcal{A}$.

We first show that $\text{RNS}(\mathcal{A}) = \mathcal{A}$ implies that $\mathcal{A}$ is rank-critical. By contradiction suppose there exists a matrix $B \notin \mathcal{A}$ s.t. $\text{rk}(\text{span}\{\mathcal{A}, B\}) = \text{rk}(\mathcal{A})$. Then for any $A \in \mathcal{A}_{\text{reg}}$, $\text{rk}(\text{span}\{A, B\}) = \text{rk}(A)$. Lemma 7 tells us that $B \in \text{RNS}(\mathcal{A})$, so $\mathcal{A}$ is a proper subset of $\text{RNS}(\mathcal{A})$, a contradiction.

We then prove that if $\mathcal{A}$ is rank-critical then $\text{RNS}(\mathcal{A}) = \mathcal{A}$. Suppose not, then there exists $B \in \text{RNS}(\mathcal{A}) \setminus \mathcal{A}$. Let $r = \text{rk}(\mathcal{A})$, and $\mathcal{A}' = \text{span}\{B, \mathcal{A}\}$. Note that $r < \min(m, n)$. Because $\mathcal{A}$ is rank-critical, $\text{rk}(\mathcal{A}') > r$, so there exists $A \in \mathcal{A}$ s.t. $\text{rk}(B + A) > r$. Since $B \in \text{RNS}(\mathcal{A})$, by Lemma 7 A cannot be from $\mathcal{A}_{\text{reg}}$. Take any $A' \in \mathcal{A}_{\text{reg}}$, and consider $B + A + xA'$, where x is a formal variable. As $\text{rk}(B+A) > r$, for all but at most $(r+1)$ $\lambda \in \mathbb{F}$, $\text{rk}(B+A+\lambda A') = \text{rk}(B+A) > r$. As $\text{rk}(A') = r$, for all but at most r $\mu \in \mathbb{F}$, $\text{rk}(A+\mu A') = r$. Since $|\mathbb{F}| \geq 2\min(m, n) > 2r+1$, there exists some $\nu \in \mathbb{F}$, such that $\text{rk}(B + A + \nu A') > r$ and $\text{rk}(A + \nu A') = r$. In this case, $A + \nu A' \in \mathcal{A}_{\text{reg}}$, so by Lemma 7 again, this suggests that $B \notin \text{RNS}(\mathcal{A})$, a contradiction.

To see that the statement regarding the group action holds, recall that $\text{RNS}(g\mathcal{A}h^{-1}) = g\text{RNS}(\mathcal{A})h^{-1}$. ☐

2.2 Proof of Theorem 4

Theorem 4, restated Let $\mathcal{A} \leq M(m \times n, \mathbb{F})$ be a matrix space and let $\mathcal{B}$, $\mathcal{P}$ be matrix spaces as in Theorem 3. Let $\mathcal{B}_c$ be the projection of $\mathcal{B}$ to $\mathcal{C}_{p,q}^{m,n}$ along $\overline{\mathcal{C}_{p,q}^{m,n}}$, and $\mathcal{B}_p$ the projection of $\mathcal{B}$ to $\overline{\mathcal{C}_{p,q}^{m,n}}$ along $\mathcal{C}_{p,q}^{m,n}$. Then $\mathcal{A}$ is rank-critical, if and only if the following hold: (1) $\mathcal{B}_c = \mathcal{C}_{p,q}^{m,n}$, (2) $\mathcal{P}$ is rank-critical, and (3) $\mathcal{B} = \mathcal{B}_p \oplus \mathcal{B}_c$, where $\oplus$ denotes the direct sum of two subspaces in $M(m \times n, \mathbb{F})$.

Proof. As $\mathcal{A}$ is rank-critical if and only if $\mathcal{B}$ is rank-critical, we focus on $\mathcal{B}$ in the following.

We first examine the necessary direction. Recall that from Theorem 3, we have $p, q \in \mathbb{N}$ satisfying $p + q < \min(m, n)$, and a primitive matrix space $\mathcal{P} \leq M(r \times s, \mathbb{F})$ where $r \leq m - p$ and $s \leq n - q$, such that (1) $\text{rk}(\mathcal{B}) = p + q + \text{rk}(\mathcal{P})$, and (2) every $B \in \mathcal{B}$ is of the form

$$B = \begin{bmatrix} & \overbrace{\begin{matrix} * & \cdots & * \end{matrix}}^{q} & \begin{matrix} * & \cdots & \cdots & * \end{matrix} \\ p\left\{\begin{matrix} \\ \\ \end{matrix}\right. & \begin{matrix} \vdots & & \vdots \\ * & \cdots & * \end{matrix} & \begin{matrix} \vdots & & & \vdots \\ * & \cdots & \cdots & * \end{matrix} \\ & \begin{matrix} * & \cdots & * \\ \vdots & & \vdots \\ \vdots & & \vdots \\ * & \cdots & * \end{matrix} & \begin{matrix} P_{r \times s} & 0 \\ 0 & 0 \end{matrix} \end{bmatrix}_{m \times n}, \tag{3}$$

where $P \in \mathcal{P}$.

Now $\mathcal{B}$ is rank-critical. We first show that $\mathcal{C}_{p,q}^{m,n} \leq \mathcal{B}$, which will then establish (1) and (3). Take any $C \in \mathcal{C}_{p,q}^{m,n}$, and let $\mathcal{B}' = \operatorname{span}(C, \mathcal{B})$. Any $B' \in \mathcal{B}$ is also of the form as in Equation 3, as C only adds to the $*$ entries. But this gives that $\operatorname{rk}(B') \leq p+q+\operatorname{rk}(P) \leq p+q+\operatorname{rk}(\mathcal{P}) = \operatorname{rk}(\mathcal{B})$. Then by the rank criticality of $\mathcal{B}$, $C \in \mathcal{B}$.

We then turn to (2) $\mathcal{P}$ is rank-critical. Suppose $\mathcal{P}$ is not, then there exists some $P' \notin \mathcal{P}$ satisfying $\operatorname{rk}(\operatorname{span}(\mathcal{P}, P')) = \operatorname{rk}(\mathcal{P})$. Then let $C \in M(m \times n, \mathbb{F})$ be

$$C = \begin{bmatrix} \mathrm{p}\left\{ \overbrace{\begin{matrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{matrix}}^{\mathrm{q}} \right. & \begin{matrix} 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \end{matrix} \\ \begin{matrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{matrix} & \begin{matrix} P' & 0 \\ 0 & 0 \end{matrix} \end{bmatrix}_{m \times n}.$$

Clearly, $C \notin \mathcal{B}$. Now consider $\mathcal{B}' = \operatorname{span}(C, \mathcal{B})$. We then have $\operatorname{rk}(\mathcal{B}') \leq p+q+\operatorname{rk}(\operatorname{span}(P', \mathcal{P})) = p+q+\operatorname{rk}(\mathcal{P}) = \operatorname{rk}(\mathcal{B}')$. This contradicts the rank-criticality of $\mathcal{B}$, proving that $\mathcal{P}$ is rank-critical.

To show the sufficiency, our strategy is the following. Let $\mathcal{B}_{\mathrm{ur}} \leq M((p+r) \times (n-q), \mathbb{F})$ be the matrix space that consists of those submatrices of size $(p+r) \times (n-q)$ in the upper-right corner of $B \in \mathcal{B}$. We first prove that $\mathcal{B}_{\mathrm{ur}}$ is rank-critical, using only the row primitivity of $\mathcal{P}$. We then show that as $\mathcal{P}$ is column-primitive, $\mathcal{B}_{\mathrm{ur}}$ is also column-primitive. This allows us to conclude that $\mathcal{B}$ is rank-critical, by applying the column version of the argument which proved the rank criticality of $\mathcal{B}_{\mathrm{ur}}$.

We first prove that $\mathcal{B}_{\mathrm{ur}}$ is rank-critical. To start with, note that $\operatorname{rk}(\mathcal{B}_{\mathrm{ur}}) = p + \operatorname{rk}(\mathcal{P})$, $p+\operatorname{rk}(\mathcal{P}) < p+r$ (by $\operatorname{rk}(\mathcal{P}) < r$), and $p+\operatorname{rk}(\mathcal{P}) < n-q$ (by $p+q+\operatorname{rk}(\mathcal{P}) < \min\{m, n\}$). So $\mathcal{B}_{\mathrm{ur}}$ is singular. Suppose we have $C \in M((p+r) \times (n-q), \mathbb{F})$, $C \notin \mathcal{B}_{\mathrm{ur}}$, such that $\operatorname{rk}(\mathcal{B}_{\mathrm{ur}}) = \operatorname{rk}(\mathcal{B}'_{\mathrm{ur}})$ where $\mathcal{B}'_{\mathrm{ur}} = \operatorname{span}(C, \mathcal{B}_{\mathrm{ur}})$. As the first p rows are free in $\mathcal{B}_{\mathrm{ur}}$, w.l.o.g. we can assume the first p rows of C are 0. Write C as $C = \begin{bmatrix} 0 & 0 \\ C_1 & C_2 \end{bmatrix}_{(p+r)\times(n-q)}$ where C_1 is of size $r \times s$. We observe that $C_1 \in \mathcal{P}$. If not, by the rank-criticality of $\mathcal{P}$, we would have $\operatorname{rk}(\mathcal{B}_{\mathrm{ur}}) = \operatorname{rk}(\mathcal{P}) + p < \operatorname{rk}(\operatorname{span}(C_1, \mathcal{P})) + p \leq \operatorname{rk}(\mathcal{B}'_{\mathrm{ur}})$, a contradiction. Therefore we can further assume C to be of the form $C = \begin{bmatrix} 0 & 0 \\ 0 & C_2 \end{bmatrix}_{(p+r)\times(n-q)}$. Consider the matrix space $\mathcal{C} = \operatorname{span}(\begin{bmatrix} 0 & C_2 \end{bmatrix}, \begin{bmatrix} \mathcal{P} & 0 \end{bmatrix}) \leq M(r \times (n-q), \mathbb{F})$. As before, since $\operatorname{rk}(\mathcal{B}_{\mathrm{ur}}) = \operatorname{rk}(\mathcal{B}'_{\mathrm{ur}})$, it is necessary that $\operatorname{rk}(\mathcal{C}) = \operatorname{rk}(\mathcal{P})$. It follows that every column of C_2 is in $\cap_{P \in \mathcal{P}_{\mathrm{reg}}} \operatorname{im}(P)$. By the row-primitivity of $\mathcal{P}$, C_2 has to be the zero matrix. Therefore the whole C is the zero matrix, proving that $\mathcal{B}_{\mathrm{ur}}$ is rank-critical.

We now prove that $\mathcal{B}_{\mathrm{ur}}$ is column-primitive. As $\mathcal{P}$ is column-primitive, $\begin{bmatrix} \mathcal{P} & 0 \end{bmatrix}$ is also column primitive. Take any $B \in (\mathcal{B}_{\mathrm{ur}})_{\mathrm{reg}}$. B is of the form $\begin{bmatrix} D_1 & D_2 \\ P & 0 \end{bmatrix}$, and $\ker(B) = \ker(\begin{bmatrix} D_1 & D_2 \end{bmatrix}) \cap \ker(\begin{bmatrix} P & 0 \end{bmatrix})$. $\ker(B) \neq 0$ since $\mathcal{B}_{\mathrm{ur}}$ is singular. As the first p rows are free, by choosing appropriate $\begin{bmatrix} D_1 & D_2 \end{bmatrix}$ we can go through all codimension-p subspaces of $\ker(\begin{bmatrix} P & 0 \end{bmatrix})$. Now the column-primitivity of $\mathcal{B}_{\mathrm{ur}}$ follows from that of $\begin{bmatrix} \mathcal{P} & 0 \end{bmatrix}$. $\square$

2.3 Proof of Theorem 5

Theorem 5, restated Let $\mathcal{A} \leq M(m \times n, \mathbb{F})$ be a matrix space and let $\mathcal{B}, \mathcal{P}$ be matrix spaces as in Theorem 3. Let $\mathcal{B}_c$ be the projection of $\mathcal{B}$ to $\mathcal{C}_{p,q}^{m,n}$ along $\overline{\mathcal{C}_{p,q}^{m,n}}$, and $\mathcal{B}_p$ the projection of $\mathcal{B}$ to $\overline{\mathcal{C}_{p,q}^{m,n}}$ along $\mathcal{C}_{p,q}^{m,n}$. Then $\operatorname{RND}(\mathcal{A}) = \mathcal{A}$, if and only if the following hold: (1) $\mathcal{B}_c = \mathcal{C}_{p,q}^{m,n}$,

(2) $\mathrm{RND}(\mathcal{P}) = \mathcal{P}$, and (3) $\mathcal{B} = \mathcal{B}_p \oplus \mathcal{B}_c$, where $\oplus$ denotes the direct sum of two subspaces in $M(m \times n, \mathbb{F})$.

Proof. To start with, note that when $\mathcal{A}$ and $\mathcal{B}$ are equivalent, then $\mathrm{RND}(\mathcal{A}) = \mathcal{A}$ if and only if $\mathrm{RND}(\mathcal{B}) = \mathcal{B}$. The proof strategy is similar to the proof of Theorem 4, while some changes are required to deal with $\mathrm{RND}(\mathcal{B})$.

For the sufficiency direction, let $\mathcal{B}_{\mathrm{ur}} \leq M((p+r)\times(n-q), \mathbb{F})$ be a matrix space that consists of those submatrices of size $(p+r)\times(n-q)$ in the upper-right corner of $B \in \mathcal{B}$. We will first show that $\mathrm{RND}(\mathcal{B}_{\mathrm{ur}}) = \mathcal{B}_{\mathrm{ur}}$, using only the row primitivity of $\mathcal{P}$. Then by the column version of the argument, we can conclude that $\mathrm{RND}(\mathcal{B}) = \mathcal{B}$, as $\mathcal{B}_{\mathrm{ur}}$ is also column-primitive as shown in the proof of Theorem 4.

It remains to prove that $\mathrm{RND}(\mathcal{B}_{\mathrm{ur}}) = \mathcal{B}_{\mathrm{ur}}$. Take any $B \in (\mathcal{B}_{\mathrm{ur}})_{\mathrm{reg}}$. B is of the form $B = \begin{bmatrix} D_1 & D_2 \\ P & 0 \end{bmatrix}_{(p+r)\times(n-q)}$, where $D_1 \in M(p \times s, \mathbb{F})$, $D_2 \in M(p\times(n-q-s), \mathbb{F})$, and $P \in \mathcal{P}$. Clearly, $\ker(B) = \ker(\begin{bmatrix} D_1 & D_2 \end{bmatrix}) \cap \ker(\begin{bmatrix} P & 0 \end{bmatrix})$. Since $\mathrm{rk}(B) = p + \mathrm{rk}(P)$, $\ker(B)$ is a codimension-p subspace in $\ker(\begin{bmatrix} P & 0 \end{bmatrix})$, which implies that $\mathrm{im}(B) = \mathbb{F}^p \oplus \mathrm{im}(P)$. Now let C be a rank neutral direction of $\mathcal{B}_{\mathrm{ur}}$, and put it in the block form $C = \begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix}$, where $C_{11} \in M(p \times s, \mathbb{F})$, $C_{12} \in M(p\times(n-q-s), \mathbb{F})$, $C_{21} \in M(r \times s, \mathbb{F})$ and $C_{22} \in M(r\times(n-q-s), \mathbb{F})$. By the definition of rank neutral directions, we have

$$\begin{aligned} \begin{bmatrix} C_{11} & C_{12} \end{bmatrix} \left(\ker(\begin{bmatrix} D_1 & D_2 \end{bmatrix}) \cap \ker(\begin{bmatrix} P & 0 \end{bmatrix}) \right) &\leq \mathbb{F}^p; \\ \begin{bmatrix} C_{21} & C_{22} \end{bmatrix} \left(\ker(\begin{bmatrix} D_1 & D_2 \end{bmatrix}) \cap \ker(\begin{bmatrix} P & 0 \end{bmatrix}) \right) &\leq \mathrm{im}(P) \end{aligned} \tag{4}$$

for all D_1, D_2 and $P \in \mathcal{P}_{\mathrm{reg}}$ satisfying $\mathrm{rk}(\begin{bmatrix} D_1 & D_2 \\ P & 0 \end{bmatrix}) = p + \mathrm{rk}(P)$. The first constraint in Equation 4 puts no restriction on C_{11} and C_{12}. For the second constraint in Equation 4, as already argued in the last paragraph in the proof of Theorem 4, since the first p rows are free, by choosing appropriate $\begin{bmatrix} D_1 & D_2 \end{bmatrix}$ we can go over all codimension-p subspaces of $\ker(\begin{bmatrix} P & 0 \end{bmatrix})$. This gives that $\begin{bmatrix} C_{21} & C_{22} \end{bmatrix} \ker(\begin{bmatrix} P & 0 \end{bmatrix}) \leq \mathrm{im}(P)$. Then by $\ker(\begin{bmatrix} P & 0 \end{bmatrix}) = \ker(P) \oplus \mathbb{F}^{n-q-s}$, we have

$$C_{21} \ker(P) + C_{22}\mathbb{F}^{n-q-s} \leq \mathrm{im}(P), \tag{5}$$

for all $P \in \mathcal{P}_{\mathrm{reg}}$, from which we deduce that (a) $C_{21} \in \mathrm{RND}(\mathcal{P}) = \mathcal{P}$ for any $P \in \mathcal{P}_{\mathrm{reg}}$, and (b) $C_{22} = 0$ as $\mathrm{im}(C_{22}) \leq \cap_{P \in \mathcal{P}_{\mathrm{reg}}} \mathrm{im}(P) = \{0\}$, where the equality follows from the row primitivity of $\mathcal{P}$. That $\mathrm{RND}(\mathcal{B}_{\mathrm{ur}}) = \mathcal{B}_{\mathrm{ur}}$ then follows.

For the necessary direction, notice that $\mathrm{RND}(\mathcal{B}) = \mathcal{B}$ implies $\mathrm{RNS}(\mathcal{B}) = \mathcal{B}$, thus conditions (1) and (3) hold by Theorem 4. By contradiction, assume that $\mathrm{RND}(\mathcal{P}) \neq \mathcal{P}$, so there exists $P_0 \in \mathrm{RND}(\mathcal{P})$ but $P_0 \notin \mathcal{P}$. It is easy to see that $P_0' = \begin{bmatrix} 0 & 0 \\ P_0 & 0 \end{bmatrix} \in M((p+r)\times(n-q), \mathbb{F})$ is not an element of $\mathcal{B}_{\mathrm{ur}}$ but satisfies Equations 4 for all $P \in \mathcal{P}_{\mathrm{reg}}$, which implies $P_0' \in \mathrm{RND}(\mathcal{B}_{\mathrm{ur}})$. Consider then the matrix $P_0'' = \begin{bmatrix} 0 & 0 & 0 \\ 0 & P_0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \in M(m \times n, \mathbb{F})$, and by the column version of the argument, we have $P_0'' \in \mathrm{RND}(\mathcal{B})$ but $P_0'' \notin \mathcal{B}$, arriving at a contradiction. □

2.4 Proof of Theorem 6

Theorem 6, restated Suppose we are given two rank-critical matrix spaces $\mathcal{A}_1 \leq M(m_1 \times n_1, \mathbb{F})$ and $\mathcal{A}_2 \leq M(m_2 \times n_2, \mathbb{F})$, and suppose $|\mathbb{F}| \geq 2\min(m_1+m_2, n_1+n_2)$. $\mathcal{A}_1 \oplus \mathcal{A}_2$ is rank-critical if and only if $\mathcal{A}_1$ and $\mathcal{A}_2$ are primitive.

We point out that, by the discussion in Section 2.1.1, an equivalent formulation of $\mathrm{RNS}(\mathcal{A})$ is

$$\mathrm{RNS}(\mathcal{A}) := \{B \in M(m \times n, \mathbb{F}) : \forall A \in \mathcal{A}_{\mathrm{reg}}, \forall k \in \mathbb{N}, B(A^{-1}B)^k \ker(A) \subseteq \mathrm{im}(A)\}.$$

Proof. To see the necessity, we prove that if $\mathcal{A}_1$ is not primitive, then $\mathcal{A}_1 \oplus \mathcal{A}_2$ is not rank-critical. If $\mathcal{A}_1$ is not primitive then $\mathcal{A}_1 \oplus \mathcal{A}_2$ is not primitive. Furthermore by transforming to an equivalent space, $\mathcal{A}_1$ can be arranged to be in the form as the $\mathcal{B}$ in Theorem 3, with one of p or q being nonzero. W.l.o.g. assume $q > 0$. Then the first column is also the cause of imprimitivity of $\mathcal{A}_1 \oplus \mathcal{A}_2$; that is, the first standard basis vector is not in $\mathrm{span}\{\cup_{A \in (\mathcal{A}_1 \oplus \mathcal{A}_2)_{\mathrm{reg}}} \ker(A)\}$. Now by Theorem 4, for $\mathcal{A}_1 \oplus \mathcal{A}_2$ to be rank-critical, it is necessary that the first column is free, while every $A \in \mathcal{A}_1 \oplus \mathcal{A}_2$ would have the first column containing some 0's. This proves that $\mathcal{A}_1 \oplus \mathcal{A}_2$ is not rank-critical.

For the sufficiency direction, by Theorem 1, we turn to prove $\mathcal{A}_1 \oplus \mathcal{A}_2 = \mathrm{RNS}(\mathcal{A}_1 \oplus \mathcal{A}_2)$. That is, for any $X \in \mathrm{RNS}(\mathcal{A}_1 \oplus \mathcal{A}_2)$ satisfying $\forall A \in (\mathcal{A}_1 \oplus \mathcal{A}_2)_{\mathrm{reg}}, \forall k \in \mathbb{N}$,

$$X(A^{-1}X)^k \ker(A) \leq \mathrm{im}(A), \tag{6}$$

we need to show $X \in \mathcal{A}_1 \oplus \mathcal{A}_2$. Noticing $(\mathcal{A}_1 \oplus \mathcal{A}_2)_{\mathrm{reg}} = (\mathcal{A}_1)_{\mathrm{reg}} \oplus (\mathcal{A}_2)_{\mathrm{reg}}$, we denote a given $A \in (\mathcal{A}_1 \oplus \mathcal{A}_2)_{\mathrm{reg}}$ by $A = A_1 \oplus A_2$, where $A_1 \in (\mathcal{A}_1)_{\mathrm{reg}}$ and $A_2 \in (\mathcal{A}_2)_{\mathrm{reg}}$. Moreover, we have $\mathrm{im}(A) = \mathrm{im}(A_1) \oplus \mathrm{im}(A_2)$ and $\ker(A) = \ker(A_1) \oplus \ker(A_2)$.

Now, let $X = \begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix} \in \mathrm{RNS}(\mathcal{A}_1 \oplus \mathcal{A}_2)$, where $X_{ij} \in M(m_i \times n_j, \mathbb{F})$, $i, j = 1, 2$. By Equation 6 with $k = 0$, for any $A_1 \in (\mathcal{A}_1)_{\mathrm{reg}}$, $A_2 \in (\mathcal{A}_2)_{\mathrm{reg}}$, X_{ij}'s satisfy:

$$X_{11} \ker(A_1) + X_{12} \ker(A_2) \leq \mathrm{im}(A_1);$$

$$X_{21} \ker(A_1) + X_{22} \ker(A_2) \leq \mathrm{im}(A_2).$$

Therefore, $X_{12} \ker(A_2) \leq \mathrm{im}(A_1)$ and $X_{21} \ker(A_1) \leq \mathrm{im}(A_2)$ hold for any $A_1 \in (\mathcal{A}_1)_{\mathrm{reg}}$, $A_2 \in (\mathcal{A}_2)_{\mathrm{reg}}$. So we have

$$X_{12}(\mathrm{span}\{\cup_{A_2 \in (\mathcal{A}_2)_{\mathrm{reg}}} \ker(A_2)\}) \leq \cap_{A_1 \in (\mathcal{A}_1)_{\mathrm{reg}}} \mathrm{im}(A_1);$$

$$X_{21}(\mathrm{span}\{\cup_{A_1 \in (\mathcal{A}_1)_{\mathrm{reg}}} \ker(A_1)\}) \leq \cap_{A_2 \in (\mathcal{A}_2)_{\mathrm{reg}}} \mathrm{im}(A_2).$$

Now by the primitivity of $\mathcal{A}_1$ and $\mathcal{A}_2$, we obtain $X_{12} = 0$ and $X_{21} = 0$.

We then need to show that for $i = 1, 2$, $X_{ii} \in \mathcal{A}_i$. By the assumption $\mathcal{A}_i = \mathrm{RNS}(\mathcal{A}_i)$, we turn to show that for $i = 1, 2$, $X_{ii} \in \mathrm{RNS}(\mathcal{A}_i)$, that is, $\forall k \in \mathbb{N}$, and $i = 1, 2$, $X_{ii}(A_i^{-1} X_{ii})^k \ker(A_i) \leq \mathrm{im}(A_i)$. This can be seen by an induction on k, once we notice the following: if $U = U_1 \oplus U_2$, $U_i \in \mathrm{im}(A_i)$, then $A^{-1}(U) = A_1^{-1}(U_1) \oplus A_2^{-1}(U_2)$. □

Acknowledgement

We thank Jan Draisma and Gábor Ivanyos for helpful discussions though email correspondences. Y. Q. was supported by the Australian Research Council DECRA DE150100720 during this research.

Bibliography

References

M. D. Atkinson and S. Lloyd. Primitive spaces of matrices of bounded rank. *Journal of the Australian Mathematical Society (Series A)*, 30(04):473–482, 1981.

M. D. Atkinson and N. M. Stephens. Spaces of matrices of bounded rank. *The Quarterly Journal of Mathematics*, 29(2):221–223, 1978.

Marco Carmosino, Russell Impagliazzo, Valentine Kabanets, and Antonina Kolokolova. Tighter connections between derandomization and circuit lower bounds. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2015, August 24-26, 2015, Princeton, NJ, USA*, pages 645–658, 2015. doi:10.4230/LIPIcs.APPROX-RANDOM.2015.645. URL `http://dx.doi.org/10.4230/LIPIcs.APPROX-RANDOM.2015.645`.

Jan Draisma. Small maximal spaces of non-invertible matrices. *Bulletin of the London Mathematical Society*, 38:764–776, 10 2006. ISSN 1469-2120. doi:10.1112/S0024609306018741. URL `http://journals.cambridge.org/article_S0024609306018741`.

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.

M. Fortin and C. Reutenauer. Commutative/noncommutative rank of linear matrices and subspaces of matrices of low rank. *Séminaire Lotharingien de Combinatoire*, 52:B52f, 2004.

Ankit Garg, Leonid Gurvits, Rafael Oliveira, and Avi Wigderson. A deterministic polynomial time algorithm for non-commutative rational identity testing. In *IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016, 9-11 October 2016, Hyatt Regency, New Brunswick, New Jersey, USA*, pages 109–117, 2016. doi:10.1109/FOCS.2016.95. URL `http://dx.doi.org/10.1109/FOCS.2016.95`.

Gábor Ivanyos, Marek Karpinski, Youming Qiao, and Miklos Santha. Generalized wong sequences and their applications to edmonds' problems. *J. Comput. Syst. Sci.*, 81(7):1373–1386, 2015a. doi:10.1016/j.jcss.2015.04.006. URL `http://dx.doi.org/10.1016/j.jcss.2015.04.006`.

Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Constructive non commutative rank computation in deterministic polynomial time over fields of arbitrary characteristics. preprint arXiv:1512.03531, 2015b.

Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Non-commutative Edmonds' problem and matrix semi-invariants. *computational complexity*, pages 1–47, 2016. ISSN 1420-8954. doi:10.1007/s00037-016-0143-x. URL `http://dx.doi.org/10.1007/s00037-016-0143-x`.

László Lovász. On determinants, matchings, and random algorithms. In *FCT*, pages 565–574, 1979.

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.