Symbolic determinant identity testing and non-commutative ranks of matrix Lie algebras

Gábor Ivanyos
Institute for Computer Science and Control, Eötvös Loránd Research Network (ELKH), Budapest, Hungary

Tushant Mittal
Department of Computer Science, University of Chicago, Chicago, USA

Youming Qiao
Centre for Quantum Software and Information, University of Technology Sydney, Australia

Abstract

One approach to make progress on the symbolic determinant identity testing (SDIT) problem is to study the structure of singular matrix spaces. After settling the non-commutative rank problem (Garg–Gurvits–Oliveira–Wigderson, *Found. Comput. Math.* 2020; Ivanyos–Qiao–Subrahmanyam, *Comput. Complex.* 2018), a natural next step is to understand singular matrix spaces whose non-commutative rank is full. At present, examples of such matrix spaces are mostly sporadic, so it is desirable to discover them in a more systematic way.

In this paper, we make a step towards this direction, by studying the family of matrix spaces that are closed under the commutator operation, that is, matrix Lie algebras. On the one hand, we demonstrate that matrix Lie algebras over the complex number field give rise to singular matrix spaces with full non-commutative ranks. On the other hand, we show that SDIT of such spaces can be decided in deterministic polynomial time. Moreover, we give a characterization for the matrix Lie algebras to yield a matrix space possessing singularity certificates as studied by Lovász (*B. Braz. Math. Soc.*, 1989) and Raz and Wigderson (*Building Bridges II*, 2019).

2012 ACM Subject Classification Theory of computation → Algebraic complexity theory; Theory of computation → Pseudorandomness and derandomization

Keywords and phrases derandomization, polynomial identity testing, symbolic determinant, non-commutative rank, Lie algebras

Digital Object Identifier 10.4230/LIPIcs.ITCS.2022.29

Related Version A full version of the paper is available at [17], `https://arxiv.org/abs/2109.06403`.

Funding *Youming Qiao*: Australian Research Council DP200100950

Acknowledgements T. M. would like to thank Pallav Goyal for helping him understand Lie algebras. The authors would like to thank Visu Makam for communicating [7] to them, and the anonymous reviewers for their detailed and helpful feedback.

1 Introduction

1.1 Background and motivations

Matrix spaces.

Let $\mathbb{F}$ be a field. We use $\mathrm{M}(\ell \times n, \mathbb{F})$ to denote the linear space of $\ell \times n$ matrices over $\mathbb{F}$, and let $\mathrm{M}(n, \mathbb{F}) := \mathrm{M}(n \times n, \mathbb{F})$. The general linear group of degree n over $\mathbb{F}$ is denoted by $\mathrm{GL}(n, \mathbb{F})$. A subspace $\mathcal{B}$ of $\mathrm{M}(\ell \times n, \mathbb{F})$ is called a *matrix space*, denoted by $\mathcal{B} \leq \mathrm{M}(\ell \times n, \mathbb{F})$. Given $B_1, \ldots, B_m \in \mathrm{M}(n, \mathbb{F})$, $\langle B_1, \ldots, B_m \rangle$ is the linear span of the B_i's. In algorithms, $\mathcal{B} \leq \mathrm{M}(n, \mathbb{F})$ is naturally represented by a linear basis $B_1, \ldots, B_m \in \mathrm{M}(n, \mathbb{F})$.

Two major algorithmic problems about matrix spaces are as follows.

The symbolic determinant identity testing problem.

For $\mathcal{B} \leq \mathrm{M}(n, \mathbb{F})$, let $\mathrm{mrk}(\mathcal{B})$ be the maximum rank over all matrices in $\mathcal{B}$. We say that $\mathcal{B}$ is *singular*, if $\mathrm{mrk}(\mathcal{B}) < n$. To decide whether $\mathcal{B}$ is singular is known as the *symbolic determinant identity testing* (SDIT) problem. The *maximum rank problem* for $\mathcal{B}$ then asks to compute $\mathrm{mrk}(\mathcal{B})$. The complexity of SDIT depends on the underlying field $\mathbb{F}$. When $|\mathbb{F}| = O(1)$, SDIT is coNP-complete [3]. When $|\mathbb{F}| = \Omega(n)$, by the polynomial identity testing lemma [23, 25], SDIT admits a randomized efficient algorithm. To present a deterministic polynomial-time algorithm for SDIT is a major open problem in computational complexity, as that would imply strong circuit lower bounds by the seminal work of Kabanets and Impagliazzo[18].

The shrunk subspace problem.

For $\mathcal{B} \leq \mathrm{M}(n, \mathbb{F})$ and $U \leq \mathbb{F}^n$, the image of U under $\mathcal{B}$ is $\mathcal{B}(U) := \{Bu : B \in \mathcal{B}, u \in U\}$. We say that U is a *shrunk subspace* of $\mathcal{B}$, if $\dim(U) > \dim(\mathcal{B}(U))$. The problem of deciding whether $\mathcal{B}$ admits a shrunk subspace is *the shrunk subspace problem*. The *non-commutative rank problem*[1] [11, 16] asks to compute $\mathrm{ncrk}(\mathcal{B}) := \max\{\dim(U) - \dim(\mathcal{B}(U)) : U \leq \mathbb{F}^n\}$. That is, $\mathcal{B}$ admits a shrunk subspace if and only if its non-commutative rank is not full, i.e. $< n$. This problem is known for its connections to invariant theory, linear algebra, graph theory, and quantum information. Major progress in the past few years lead to deterministic efficient algorithms for the shrunk subspace problem, one by Garg, Gurvits, Oliveira, and Wigderson over fields of characteristic 0 [11], and the other by Ivanyos, Qiao, and Subrahmanyam over any field [15, 16].

Motivations of our investigation.

Note that if a matrix space admits a shrunk subspace, then it has to be singular. However, there exist singular matrix spaces without shrunk subspaces. After settling the shrunk subspace problem [11, 16], such matrix spaces form a bottleneck for further progress on SDIT. Moreover, ideas from these works are not expected to directly generalize as it was recently shown that the space of singular matrices cannot be seen as the null-cone of any reductive group action [21]

Two classical examples of such subspaces are as follows [20].

▶ **Example 1.** **1.** Let $\Lambda(n, \mathbb{F})$ be the linear space of alternating matrices, namely matrices satisfying $\forall v \in \mathbb{F}^n$, $v^t A v = 0$.[2] When n is odd, $\Lambda(n, \mathbb{F})$ is singular, as every alternating matrix is of even rank. Furthermore, it is easy to verify that $\Lambda(n, \mathbb{F})$ does not admit shrunk subspaces.

2. Let $C_1, \ldots, C_n \in \Lambda(n, \mathbb{F})$, and let $\mathcal{C} \leq \mathrm{M}(n, \mathbb{F})$ consist of all the matrices of the form $[C_1 v, C_2 v, \ldots, C_n v]$, over $v \in \mathbb{F}^n$. As C_i's are alternating, we have

$$v^t[C_1 v, C_2 v, \ldots, C_n v] = [v^t C_1 v, v^t C_2 v, \ldots, v^t C_n v] = 0,$$

so $\mathcal{C}$ is singular. In [10], it is shown that when $n = 4$, certain choices of C_i ensure that $\mathcal{C}$ does not have shrunk subspaces.

[1] The name "non-commutative" rank comes from a natural connection between matrix spaces and symbolic matrices over skew fields; see [11, 16] for details.

[2] When $\mathbb{F}$ is of characteristic not 2, a matrix is alternating if and only if it is skew-symmetric.

While there are further examples in [1, 6], the above two examples (and their certain subspaces) have been studied most in theoretical computer science and combinatorics, such as by Lovász [20] and Raz and Wigderson [22], due to their connections to matroids and graph rigidity.

As far as we see from the above, examples of singular matrix spaces without shrunk subspaces in the literature are sporadic. Therefore, it is desirable to discover more singular matrix spaces without shrunk subspaces, hopefully in a more systematic way. This is the main motivation of this present article.

Overview of our main results.

Noting that the linear space of skew-symmetric matrices is closed under the commutator bracket, we set out to study matrix Lie algebras. Our main results can be summarized as follows.

- First, we show that matrix Lie algebras over $\mathbb{C}$ gives rise to a family of singular matrix spaces without shrunk subspaces. This result, partly inspired by [9], vastly generalizes the linear spaces of skew-symmetric matrices.
- Second, we present a deterministic polynomial-time algorithm to solve SDIT for matrix Lie algebras over $\mathbb{C}$. This algorithm heavily relies on the structural theory of, and algorithms for, Lie algebras.
- Third, we examine when matrix Lie algebras are of the form in Example 1 (2) as above, giving representation-theoretic criteria for such matrix Lie algebras.

In the rest of this introduction, we detail our results.

1.2 Our results

Recall that $\mathcal{B} \leq \mathrm{M}(n, \mathbb{F})$ is a *matrix Lie algebra*, if $\mathcal{B}$ is closed under the commutator bracket, i.e. for any $A, B \in \mathcal{B}$, $[A, B] := AB - BA \in \mathcal{B}$.

We have striven to make this introduction as self-contained as possible. In an effort to make this article accessible to wider audience, we summarize notions and results on Lie algebras and representations relevant to this paper in Appendices A, B, and C.

Two results and a message.

We first study shrunk subspaces of matrix Lie algebras over $\mathbb{C}$. To state our results, we need the following notions.

Given a matrix space $\mathcal{B} \leq \mathrm{M}(n, \mathbb{F})$, $U \leq \mathbb{F}^n$ is an *invariant subspace* of $\mathcal{B}$, if for any $B \in \mathcal{B}$, $B(U) \subseteq U$. We say that $\mathcal{B}$ is *irreducible*, if the only invariant subspaces of $\mathcal{B}$ are 0 and $\mathbb{F}^n$. The above notions naturally apply to matrix Lie algebras. The matrix space $\mathcal{B} = 0 \leq \mathrm{M}(1, \mathbb{F})$ is called the *trivial irreducible* matrix Lie algebra.

In general, let $\mathcal{B} \leq \mathrm{M}(n, \mathbb{F})$ be a matrix Lie algebra. Then there exists $A \in \mathrm{GL}(n, \mathbb{F})$, such that $A^{-1}\mathcal{B}A$ is of block upper-triangular form, and each block on the diagonal defines an irreducible matrix Lie algebra, called a *composition factor* of $\mathcal{B}$. Such an A defines a chain of subspaces, called a *composition series* of the matrix Lie algebra $\mathcal{B}$. By the Jordan-Hölder theorem, the isomorphic types of the composition factors are the same for different composition series.

We then have the following criteria for the existence of shrunk subspaces of matrix Lie algebras over $\mathbb{C}$.

▶ **Theorem 2.** *Let $\mathcal{B} \leq \mathrm{M}(n, \mathbb{C})$ be a non-trivial irreducible matrix Lie algebra. Then $\mathcal{B}$ does not have a shrunk subspace.*

Let $\mathcal{B} \leq \mathrm{M}(n, \mathbb{C})$ be a matrix Lie algebra. Then $\mathcal{B}$ has a shrunk subspace, if and only if one of its composition factors is the trivial matrix Lie algebra.

The proof of Theorem 2 for the irreducible case makes use of the connection of Lie algebras and Lie groups as summarized in Appendix B. Going from the irreducible to the general case, we prove some basic properties of shrunk subspaces which may be of independent interest in Section 2.

After we proved Theorem 2, we learnt that Derksen and Makam independently proved it using a different approach via representation theory of Lie algebras [7].

We then present a deterministic polynomial-time algorithm to solve SDIT for matrix Lie algebras over $\mathbb{C}$. Our model of computation over $\mathbb{C}$ will be explained in Section 4.

▶ **Theorem 3.** *Let $\mathcal{B} \leq \mathrm{M}(n, \mathbb{C})$ be a matrix Lie algebra. Then there is a deterministic polynomial-time algorithm to solve the symbolic determinant identity testing problem for $\mathcal{B}$.*

We believe that the strategy for the algorithm in Theorem 3 is interesting. It rests on the key observation that the maximum rank of $\mathcal{B}$ is equal to the maximum rank of a Cartan subalgebra of $\mathcal{B}$. (We collect the notions and results on Cartan algebras relevant to this paper in Appendix C.) We then resort to the algorithm computing a Cartan subalgebra by de Graaf, Ivanyos and Rónyai [5] to get one. As Cartan subalgebras are upper-triangularisable, an SDIT algorithm can be devised easily.

Theorems 2 and 3 together bring out *the main message in this paper*: we identify non-trivial irreducible matrix Lie algebras over $\mathbb{C}$ as an interesting families of matrix spaces, as (1) they do not admit shrunk subspaces, and (2) SDIT for such spaces can be solved in deterministic polynomial time.

To see that matrix Lie algebras do form an interesting family for the maximum rank problem, we list some examples.

▶ **Example 4.** **1.** Note that $\Lambda(n, \mathbb{F})$ is closed under the commutator bracket. Indeed, $\Lambda(n, \mathbb{F})$ together with the commutator bracket is well-known as the orthogonal Lie algebra, and it is easy to see that it is irreducible.

2. Representations of abstract Lie algebras give rise to matrix Lie algebras. For example, let $\mathfrak{sl}(n, \mathbb{C})$ be the special linear Lie algebra, i.e, the Lie algebra of all $n \times n$ complex matrices with trace 0. Let $E_{i,j}$ be the elementary matrix with the only non-zero entry being 1 in the $(i, j)^{th}$ entry. A linear basis of $\mathfrak{sl}(n, \mathbb{C})$ consists of $E_{i,j}$, $i \neq j$. Consider for any fixed d, the vector space V spanned by all degree dn monomials in the variables $\{x_1, \cdots, x_n\}$. Then, the representation is defined as $\rho(E_{ij})(x_1^{e_1} \cdots x_n^{e_n}) = x_i \frac{\partial(x_1^{e_1} \cdots x_n^{e_n})}{\partial x_j}$. This gives rise to an irreducible matrix Lie algebra in $\mathrm{M}(\binom{dn+n-1}{n-1}, \mathbb{C})$.

One may wonder whether irreducible matrix Lie algebras encompass singular and non-singular matrix spaces. To see this, note that $\Lambda(n, \mathbb{F})$ (as defined in Example 4) can be singular (for odd n) or non-singular (for even n). In fact, there is a representation-theoretic explanation for the maximum rank of certain irreducible matrix Lie algebras via weight spaces (Fact 34) as already observed by Draisma [8], from which it is evident that irreducible matrix Lie algebras can be singular or non-singular.

Other singularity witnesses and matrix Lie algebras.

After Theorem 2 and 3, we study further properties of matrix Lie algebras related to singularity as follows. Let $\mathcal{B} = \langle B_1, \ldots, B_m \rangle \leq \mathrm{M}(n, \mathbb{F})$ be a matrix space. Let $x_1, \ldots, x_m$

be a set of commutative variables. Then $B = x_1B_1 + \cdots + x_mB_m$ is a matrix of linear forms in x_i's. When $\mathbb{F}$ is large enough, the singularity of $\mathcal{B}$ is equivalent to that of B over the function field. Viewing B as a matrix over the rational function field $\mathbb{F}(x_1, \ldots, x_n)$, its kernel is spanned by vectors whose entries are polynomials. Let $v \in \mathbb{F}[x_1, \ldots, x_m]^n$ be in $\ker(B)$. By splitting v according to degrees if necessary, we can assume that v is *homogeneous*, i.e. each component of v is homogeneous of degree d.

We are interested in those vectors in the kernel whose entries are linear forms. This is also partly motivated by understanding witnesses for singularity of matrix spaces, as by [18], putting SDIT in NP $\cap$ coNP already implies strong circuit lower bounds. Suppose B admits $v \in \ker(B)$ whose components are homogeneous degree-d polynomials. Then, ignoring bit complexities, v is a singularity witness of $\mathcal{B}$ of size $O(m^d \times n)$, and the existence of a certificate of degree d can be checked and found in time $O(m^d \times n)$, by writing a linear system in $O(m^d \times n)$ variables.

Let $v_1, \ldots, v_m \in \mathbb{F}^n$, and $v = x_1v_1 + \cdots + x_mv_m$ be a vector of linear forms. We say that v is a (left homogeneous) *linear kernel vector* of B, if each entry of v^tB is the zero polynomial. Similarly, v is a right homogeneous linear kernel vector, if each entry of Bv is the zero polynomial.

Clearly, whether such a nonzero v exists does not depend on the choice of bases. Indeed, we can give a basis-free definition of a linear kernel vector for a matrix space $\mathcal{B} \leq \mathrm{M}(n, \mathbb{F})$ as a non-zero linear map $\psi : \mathcal{B} \to \mathbb{F}^n$ such that for each A, $\psi(A)^tA = 0$.

Matrix spaces with linear kernel vectors have appeared in papers by Lovász [20] and Raz and Wigderson [22]. To see this, note that matrix spaces with linear kernel vectors can be constructed from alternating matrices as exhibited in Example 1 (2).

One approach for Lie algebras to yield matrix spaces with linear kernel vectors is through adjoint representations.

Recall that, given a Lie algebra $[-,-] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$, the adjoint representation of $\mathfrak{g}$ is $\mathrm{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$ defined as $\mathrm{ad}_x(y) = [x, y]$ for $x, y \in \mathfrak{g}$. The image of ad is a matrix space $\mathcal{A} \leq \mathrm{M}(d, \mathbb{F})$ where $d = \dim(\mathfrak{g})$. As the Lie bracket $[,]$ is alternating, $\mathcal{A}$ admits a linear kernel vector by the construction in Example 1 (2).

Our next theorem characterizes Lie algebra representations with linear kernel vectors. (We collect some basic notions of Lie algebra representations relevant to this paper in Appendix A.) Since we are concerned with matrix spaces which are images of Lie algebra representations, i.e. $\mathcal{B} = \rho(\mathfrak{g})$ where ρ is a representation of the Lie algebra $\mathfrak{g}$, we can assume without generality that ρ is faithful.

▶ **Theorem 5.** *Let $\mathcal{B}$ be the image of a faithful irreducible representation ϕ of a semisimple Lie algebra $\mathfrak{g}$ over algebraically closed fields of characteristic not 2 or 3. Then $\mathcal{B}$ admits a linear kernel vector if and only if $\mathcal{B}$ is trivial, or $\mathfrak{g}$ is simple and ϕ is isomorphic to the adjoint representation.*

1.3 Open questions.

Several questions can be asked after this work. First, can we identify more families of singular matrix spaces without shrunk subspaces? Second, our algorithm for SDIT of matrix Lie algebras heavily relies on the structure theory of Lie algebras and works over $\mathbb{C}$. It will be interesting to devise an alternative algorithm that is of a different nature, and works for matrix Lie algebras over fields of positive characteristics. Third, characterize those representations of non-semisimple Lie algebras with linear kernel vectors.

The structure of the paper.

In Section 2 we prove some results on shrunk subspaces that will be useful to prove Theorem 2. In Section 3 we prove Theorem 2. In Section 4 we prove Theorem 3. In Section 5 we prove Theorem 5.

2 On shrunk subspaces of matrix spaces

In this section we present some basic results and properties regarding shrunk subspaces and non-commutative ranks of matrix spaces.

2.1 Canonical shrunk subspaces

Let $\mathcal{B} \leq \mathrm{M}(n, \mathbb{F})$. For a subspace U of $\mathbb{F}^n$ define $\mathrm{sd}_{\mathcal{B}}(U)$ as the difference $\dim(U) - \dim(\mathcal{B}(U))$. Thus $\mathrm{sd}_{\mathcal{B}}(U)$ is positive for a shrunk subspace U and negative if $\mathcal{B}$ expands U. We then have the following.

▶ **Lemma 6.** *The function* $\mathrm{sd}_{\mathcal{B}}$ *is supermodular. More specifically, if* U_1 *and* U_2 *are two subspaces of* $\mathbb{F}^n$*, then,*

$$\mathrm{sd}_{\mathcal{B}}(U_1 \cap U_2) + \mathrm{sd}_{\mathcal{B}}(\langle U_1 \cup U_2 \rangle) \geq \mathrm{sd}_{\mathcal{B}}(U_1) + \mathrm{sd}_{\mathcal{B}}(U_2). \tag{1}$$

Proof. By modularity of the dimension, we have

$$\dim(U_1 \cap U_2) + \dim(\langle U_1 \cup U_2 \rangle) = \dim(U_1) + \dim(U_2)$$

and

$$\dim(\mathcal{B}(U_1) \cap \mathcal{B}(U_2)) + \dim(\langle \mathcal{B}(U_1) \cup \mathcal{B}(U_2) \rangle) = \dim(\mathcal{B}(U_1)) + \dim(\mathcal{B}(U_2)).$$

The second equality, using also that $\mathcal{B}(\langle U_1 \cup U_2 \rangle) = \langle \mathcal{B}(U_1) \cup \mathcal{B}(U_2) \rangle$ and $\mathcal{B}(U_1 \cap U_2) \leq \mathcal{B}(U_1) \cap \mathcal{B}(U_2)$, gives,

$$\dim(\mathcal{B}(U_1 \cap U_2)) + \dim(\mathcal{B}(\langle U_1 \cup U_2 \rangle)) \leq \dim(\mathcal{B}(U_1)) + \dim(\mathcal{B}(U_2)).$$

Subtracting the last inequality from the first equality gives (1). ◀

▶ **Proposition 7.** *Let* $\mathcal{B} \leq \mathrm{M}(n, \mathbb{F})$*. Suppose* $\mathrm{ncrk}(\mathcal{B}) = n - c$ *for* $c > 0$*. Then there exists a unique subspace* $U \leq \mathbb{F}^n$ *of the smallest dimension satisfying* $\dim(U) - \dim(\mathcal{B}(U)) = c$*, and there exists a unique subspace* $U' \leq \mathbb{F}^n$ *of the largest dimension such that* $\dim(U') - \dim(\mathcal{B}(U')) = c$*.*

Proof. We use the supermodular function $\mathrm{sd}_{\mathcal{B}}$ defined in Lemma 6. Let U_1 and U_2 be subspaces with $\mathrm{sd}_{\mathcal{B}}(U_i) = c$. Then Lemma 6 gives $\mathrm{sd}_{\mathcal{B}}(U_1 \cap U_2) + \mathrm{sd}_{\mathcal{B}}(\langle U_1 \cup U_2 \rangle) \geq 2c$. On the other hand, by the definition of the noncommutative rank, $\mathrm{sd}_{\mathcal{B}}(U_1 \cap U_2) \leq c$ and $\mathrm{sd}_{\mathcal{B}}(\langle U_1 \cup U_2 \rangle) \leq c$. It follows that all the three inequalities are in fact equalities. Thus the intersection as well as the span of all the subspaces U with $\mathrm{sd}_{\mathcal{B}}(U) = c$ also have this property. ◀

By Proposition 7, in the case $\mathrm{ncrk}(\mathcal{B}) = n - c$ for $c > 0$, we shall refer to the subspace U of the smallest dimension satisfying $\dim(U) - \dim(\mathcal{B}(U)) = c$ as the (lower) *canonical shrunk subspace*. The algorithm from [15, 16] actually computes the canonical shrunk subspace.

A natural group action on matrix spaces is as follows. Let $G = \mathrm{GL}(n, \mathbb{F}) \times \mathrm{GL}(n, \mathbb{F})$. Then $(A, C) \in G$ sends $\mathcal{B} \leq \mathrm{M}(n, \mathbb{F})$ to $A\mathcal{B}C^{-1} = \{ABC^{-1} : B \in \mathcal{B}\}$. The stabilizer group of this action on $\mathcal{B}$ is denoted as $\mathrm{Stab}(\mathcal{B}) = \{(A, C) \in G : A\mathcal{B}C^{-1} = \mathcal{B}\}$. We then have the following proposition.

▶ **Proposition 8.** *Let $\mathcal{B} \leq \mathrm{M}(n, \mathbb{F})$. Suppose $\mathrm{ncrk}(\mathcal{B}) = n - c$[3] for $c > 0$. Then for $\forall (A, C) \in \mathrm{Stab}(\mathcal{B})$, the canonical shrunk subspace U is invariant under C, i.e., $C(U) = U$.*

Proof. From the definition of $\mathrm{Stab}(\mathcal{B})$, we have $A\mathcal{B}C^{-1} = \mathcal{B}$ and thus, $A\mathcal{B} = \mathcal{B}C$. Consider the subspace $A(U)$. Then, $\mathcal{B}(C(U)) = (\mathcal{B}C)(U) = (A\mathcal{B})(U) = A(\mathcal{B}(U))$. Since $A, C \in \mathrm{GL}(n, \mathbb{F})$, $\dim(C(U)) = \dim(U)$ and $\dim(A(\mathcal{B}(U))) = \dim(\mathcal{B}(U))$. It follows that $C(U)$ is also a c-shrunk subspace of the same dimension as U. We then conclude that $C(U) = U$ by Proposition 7. ◀

2.2 Shrunk subspaces of block upper-triangular matrix spaces

Consider the following situation. Suppose $\mathcal{B} \leq \mathrm{M}(n, \mathbb{F})$ satisfies that any $B \in \mathcal{B}$ is in the block upper-triangular form, i.e.

$$B = \begin{bmatrix} C_1 & D_{1,2} & \dots & D_{1,d} \\ 0 & C_2 & \dots & D_{2,d} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & C_d \end{bmatrix},$$

where C_i is of size $n_i \times n_i$. Let

$$\mathcal{C}_i = \langle C_i \in \mathrm{M}(n_i, \mathbb{F}) : C_i \text{ appears as the } i\text{th diagonal block of some } B \in \mathcal{B} \rangle.$$

▶ **Lemma 9.** *Let $\mathcal{B} \leq \mathrm{M}(n, \mathbb{F})$, and let $V \leq \mathbb{F}^n$ such that $\mathcal{B}(V) \leq V$. If there exists a shrunk subspace for $\mathcal{B}$, then there also exist one which is either included in V or contains V.*

Proof. Assume that V itself is not a shrunk subspace. Then $\mathcal{B}(V) = V$. Let U be a shrunk subspace of $\mathcal{B}$. By Lemma 6, we have $\mathrm{sd}_{\mathcal{B}}(V \cap U) + \mathrm{sd}_{\mathcal{B}}(\langle V \cup U \rangle) \geq \mathrm{sd}_{\mathcal{B}}(V) + \mathrm{sd}_{\mathcal{B}}(U) = 0 + \mathrm{sd}_{\mathcal{B}}(U) > 0$. Thus either $\mathrm{sd}_{\mathcal{B}}(V \cap U)$ or $\mathrm{sd}_{\mathcal{B}}(\langle V \cup U \rangle)$ must be positive. ◀

The following proposition characterizes the existence of shrunk subspaces in block upper-triangular matrix spaces.

▶ **Proposition 10.** *Let $\mathcal{B} \leq \mathrm{M}(n, \mathbb{F})$ and $\mathcal{C}_i \leq \mathrm{M}(n_i, \mathbb{F})$, $i \in [d]$, as above. Then $\mathcal{B}$ has a shrunk subspace if and only if there exists $i \in [d]$ such that $\mathcal{C}_i$ has a shrunk subspace.*

Proof. The if direction can be verified easily. For the only if direction, we induct on d. When $d = 1$, this is clear. Suppose this holds for $d < k$. Consider $d = k$, and suppose $\mathcal{B}$ admits a shrunk subspace. Let $V \leq \mathbb{F}^n$ be the subspace spanned by those standard basis vectors $e_{n_1+1}, e_{n_1+2}, \dots, e_n$. We then have two cases.

1. There exists a shrunk subspace $W \leq V$. In this case, by the induction hypothesis, there exists $i \in \{2, \dots, n\}$ such that $\mathcal{C}_i$ has a shrunk subspace.
2. There are no shrunk subspaces $W \leq V$. Then by Lemma 9, there exists a shrunk subspace W such that $W > V$. Then by considering W/V, we obtain a shrunk subspace for $\mathcal{C}_1$.

This concludes the proof of Proposition 10. ◀

[3] Recall that $\mathrm{ncrk}(\mathcal{B}) := \max\{\dim(U) - \dim(\mathcal{B}(U)) : U \leq \mathbb{F}^n\}$.

3 Shrunk subspaces of matrix Lie algebras over $\mathbb{C}$

In this section, we will give a characterization of those matrix Lie algebras over $\mathbb{C}$ with shrunk subspaces, proving Theorem 2. The main reason for working over $\mathbb{C}$ is to make use of the connections between Lie algebras and Lie groups as described in Appendix B.

We will first give such a characterization for irreducible matrix Lie algebras. The general case then follows by combining this with the results in Section 2.2.

The key to understanding the irreducible case lies in the following lemma; for notions such as matrix exponentiation and derivation, cf. Appendix B.

▶ **Lemma 11** ([12, Proposition 4.5 (1)]). *Let $\mathcal{B} \leq \mathrm{M}(n, \mathbb{C})$ be an irreducible matrix Lie algebra. Let $W \leq \mathbb{C}^n$ and $M \in \mathcal{B}$. If $e^{tM}(W) \leq W$ for all $t \in \mathbb{R}$, then $M(W) \leq W$.*

Proof. Take any $w \in W$. Note that $\frac{d(e^{tM})}{dt}(w) = (Me^{tM})(w) = M(e^{tM}(w))$, and $\frac{d(e^{tM})}{dt} = \lim_{h\to t} \frac{e^{hM}-e^{tM}}{h-t}$. So at $t = 0$, we have $M(w) = \lim_{h\to 0} \frac{e^{hM}(w)-w}{h}$. Since $e^{tM}(w) \in W$ for all $t \in \mathbb{R}$, $\frac{e^{hM}(w)-w}{h}$ lies in W for any h, and so does the limit which is $M(w)$. ◀

We will also need the following result.

▶ **Lemma 12.** *Given a matrix Lie algebra $\mathcal{B} \leq \mathrm{M}(n, \mathbb{C})$, we have that $\forall t \in \mathbb{R}$ and $M \in \mathcal{B}$, $e^{tM}\mathcal{B}e^{-tM} = \mathcal{B}$.*

Proof. By the connection between Lie groups and Lie algebras (cf. Theorem 25), there exists some Lie group G whose associated Lie algebra is $\mathcal{B}$. This implies that for any $M \in \mathcal{B}$, $e^{tM} \in G$. Then by the fact that the conjugation of $g \in G$ stabilizes $\mathcal{B}$ (cf. Theorem 26), we have $e^{tM}\mathcal{B}e^{-tM} = \mathcal{B}$. ◀

We are now ready to prove Theorem 2.

▶ **Theorem 2.** *Let $\mathcal{B} \leq \mathrm{M}(n, \mathbb{C})$ be a non-trivial irreducible matrix Lie algebra. Then $\mathcal{B}$ does not have a shrunk subspace.*

Let $\mathcal{B} \leq \mathrm{M}(n, \mathbb{C})$ be a matrix Lie algebra. Then $\mathcal{B}$ has a shrunk subspace, if and only if one of its composition factors is the trivial matrix Lie algebra.

Proof. We first handle the irreducible case.

For the sake of contradiction, suppose $\mathcal{B}$ has a shrunk subspace. Then let $V = \mathbb{C}^n$, and let $U \leq V$ be the canonical shrunk subspace of $\mathcal{B}$. By Lemma 12, for any $M \in \mathcal{B}$, we have that $(e^{tM}, e^{tM}) \in \mathrm{Stab}(\mathcal{B})$. By Proposition 8, U is invariant under e^{tM}. By Lemma 11, U is an invariant subspace of $\mathcal{B}$.

Since $\mathcal{B}$ is irreducible as a matrix Lie algebra, the only invariant subspaces are 0 and V. Since U is a shrunk subspace, it cannot be 0. If $U = V$, then $\mathcal{B}(V)$ is a proper subspace of V. If $\mathcal{B}(V)$ is non-zero, then $\mathcal{B}(\mathcal{B}(V)) \leq \mathcal{B}(V)$. This implies that $\mathcal{B}(V)$ is a proper and non-zero invariant subspace of $\mathcal{B}$, which is impossible as $\mathcal{B}$ is irreducible. It follows that $U = V$ and $\mathcal{B}(V) = 0$. In this case, V must be of dimension 1, as any non-zero proper subspace of V is an invariant subspace. It follows that $\mathcal{B}$ has to be the trivial matrix Lie algebra. We then arrive at the desired contradiction.

The general case follows from the irreducible case as shown above, and Proposition 10. ◀

4 SDIT for matrix Lie algebras over $\mathbb{C}$

In this section, we present a deterministic polynomial-time algorithm that solves SDIT for matrix Lie algebras over $\mathbb{C}$, proving Theorem 3.

The basic idea is to realize that $\mathcal{B}$ is singular if and only if every Cartan subalgebra of $\mathcal{B}$ is singular. Furthermore, a Cartan subalgebra is nilpotent, so in particular it is solvable. It follows, by Lie's theorem (Theorem 28), that a Cartan subalgebra of a matrix Lie algebra is upper-triangularisable by the conjugation action. A key task here is to compute a Cartan subalgebra of $\mathcal{B}$. This problem has been solved by de Graaf, Ivanyos, and Rónyai in [5].

Computation model over $\mathbb{C}$.

We adopt the following computation model over $\mathbb{C}$, in consistent with that in [5]. That is, we assume the input matrices are over a number field $\mathbb{E}$. Therefore $\mathbb{E}$ is a finite-dimensional algebra over $\mathbb{Q}$. If $\dim_{\mathbb{Q}}(\mathbb{E}) = d$, then $\mathbb{E}$ is the extension of $\mathbb{F}$ by a single generating element α, so $\mathbb{E}$ can be represented by the minimal polynomial of α over $\mathbb{F}$, together with an isolating rectangle for α in the case of $\mathbb{C}$.

4.1 Cartan subalgebras.

We collect notions and results on Cartan subalgebras useful to us in Appendix C. Here, we recall the following. Let $\mathfrak{g}$ be a Lie algebra. A subalgebra $\mathfrak{h} \subseteq \mathfrak{g}$ is a *Cartan subalgebra*, if it is nilpotent and self-normalizing.

In [5], de Graaf, Ivanyos, and Rónyai studied the problem of computing Cartan subalgebras. We state the following version of their main result in our context as follows. For a more precise statement, see Theorem 30.

▶ **Theorem 13** ([5, Theorem 5.8]). *Let $\mathcal{B} \leq \mathrm{M}(n, \mathbb{C})$ be a matrix Lie algebra. Then there exists a deterministic polynomial-time algorithm that computes a linear basis of a Cartan subalgebra $\mathcal{A}$ of $\mathcal{B}$.*

4.1.1 Maximum ranks of Cartan subalgebras.

The key lemma that supports our algorithm is the following.

▶ **Lemma 14.** *Let $\mathcal{B} \leq \mathrm{M}(n, \mathbb{C})$ be a matrix Lie algebra. Let $\mathcal{A} \leq \mathcal{B}$ be a Cartan subalgebra. Then,* $\mathrm{mrk}(\mathcal{B}) = \mathrm{mrk}(\mathcal{A})$.

Proof. We shall utilise two results about Cartan subalgebras; for details see Appendix C.

First, let $\mathfrak{g}$ be a Lie algebra over a large enough field. Then there exists a set of generic[4] elements $R \subseteq \mathfrak{g}$, such that for any $x \in R$, the Fitting null component of ad_x, $\mathrm{F}_0(\mathrm{ad}_x) = \{y \in \mathfrak{g} : \exists m > 0, \mathrm{ad}_x^m(y) = 0\}$, is a Cartan subalgebra. For a precise statement, see Theorem 29.

Second, let $\mathcal{B}$ be a matrix Lie algebra over $\mathbb{C}$. Then for any two Cartan subalgebras $\mathcal{A}$, $\mathcal{A}'$ of $\mathcal{B}$, they are conjugate, namely there exists $T \in \mathrm{GL}(n, \mathbb{C})$ such that $T\mathcal{A}T^{-1} = \mathcal{A}'$. For a precise statement, see Theorem 27.

By the first result, in particular by the fact that elements in R are generic, there exists a matrix $C \in \mathcal{B}$ of rank $\mathrm{mrk}(\mathcal{B})$, such that $\mathcal{C} := \mathrm{F}_0(\mathrm{ad}_C)$ is a Cartan subalgebra. Noting that

[4] This means that after identifying $\mathfrak{g}$ with $\mathbb{F}^{\dim(\mathfrak{g})}$, these elements form a Zariski open set.

$C \in \mathcal{C}$, $\mathrm{mrk}(\mathcal{C}) = \mathrm{mrk}(\mathcal{B})$. By the second result, for any Cartan subalgebra $\mathcal{A}$ of $\mathcal{B}$, $\mathcal{A}$ and $\mathcal{C}$ are conjugate, which implies that $\mathrm{mrk}(\mathcal{A}) = \mathrm{mrk}(\mathcal{C}) = \mathrm{mrk}(\mathcal{B})$. ◀

4.2 Upper-triangularisable matrix spaces.

Let $\mathcal{B} \leq \mathrm{M}(n, \mathbb{F})$. We say that $\mathcal{B}$ is upper-triangularisable, if there exists $S, T \in \mathrm{GL}(n, \mathbb{F})$, such that for any $B \in \mathcal{B}$, $S\mathcal{B}T$ is upper-triangular. Upper-triangularisable matrix spaces are of interest to us, because solvable matrix Lie algebras can be made simultaneously upper-triangular via conjugation by Lie's theorem (Theorem 28).

If a matrix space is upper-triangularisable, then we can decide if $\mathcal{B}$ is singular in a black-box fashion, as its singularity is completely determined by the diagonals of the resulting upper-triangular matrix space. The following lemma is well-known and we include a proof for completeness.

▶ **Lemma 15.** *Let $n, k \in \mathbb{N}$. Let $\mathbb{F}$ be a field such that $|\mathbb{F}| > (k-1)n$. There exists a deterministic algorithm that outputs in time* $\mathrm{poly}(n, k)$ *a set $\mathcal{H} \subseteq \mathbb{F}^k$, such that any non-zero k-variate degree-n polynomial, which is a product of linear forms, evaluates to a non-zero value on at least one point in $\mathcal{H}$.*

Proof. Let $\ell_1, \ldots, \ell_n$ be n non-zero linear forms in k variables. We can also identify them as vectors in $\mathbb{F}^k$ by taking their coefficients. Fix a subset $S \subseteq \mathbb{F}$ of size $(k-1)n+1$. Let $\mathcal{H} = \{(1, \alpha, \cdots, \alpha^{k-1}) \mid \alpha \in S\}$. This is clearly a set of size $(k-1)n+1$.

We claim that any non-zero linear form ℓ_i vanishes on at most $k-1$ points in $\mathcal{H}$. This is because if it vanishes on k points, we have $A\ell_i = 0$ where A is the Vandermonde matrix corresponding to those k points. This is impossible because the Vandermonde matrix is invertible and ℓ_i is non-zero.

It follows that there is at least one point in $\mathcal{H}$ such that every ℓ_i has a non-zero evaluation at this point. This concludes the proof.

◀

4.3 The algorithm.

Given the above preparation, we present the following algorithm for computing the commutative rank of a matrix Lie algebra.

Input: $\mathcal{B} = \langle B_1, \ldots, B_m \rangle \leq \mathrm{M}(n, \mathbb{C})$, such that $\mathcal{B}$ is a matrix Lie algebra.
Output: "Singular" if $\mathcal{B}$ is singular, and "Non-singular" otherwise.
Algorithm:
1. Use Theorem 13 to obtain $\mathcal{C} = \langle C_1, \ldots, C_k \rangle \leq \mathcal{B}$, such that $\mathcal{C}$ is a Cartan subalgebra of $\mathcal{B}$.
2. Use Lemma 15 to obtain $H \subseteq \mathbb{C}^k$, $|H| = (k-1)n+1$.
3. For any $(\alpha_1, \ldots, \alpha_k) \in H$, if $\sum_{i \in [k]} \alpha_i C_i$ is non-singular, return "Non-singular".
4. Return "Singular".

The above algorithm clearly runs in polynomial time. The correctness of the above algorithm follows from Lemmas Lemmas 14 and 15, as well as Lie's theorem on solvable Lie algebras (Theorem 28). This concludes the proof of Theorem 3.

▶ Remark 16. We do not solve the maximum rank problem for matrix Lie algebras in general. While the maximum rank problem for matrix Lie algebras reduces to the maximum rank problem for upper-triangularisable matrix spaces through Cartan subalgebras, to compute the maximum rank for the latter deterministically seems difficult. This is because the maximum

rank problem for upper-triangularisable matrix spaces is as difficult as the general SDIT problem, an observation already in [14].

There is one case where we do solve the maximum rank problem, that is, when the matrix Lie algebra over $\mathbb{C}$ is semisimple. In this case, Cartan subalgebras are diagonalizable [13, Theorem in Chapter 6.4]. Therefore, in the above algorithm we can output the maximum rank over $\sum_{i\in[k]} \alpha_i C_i$ where $(\alpha_1, \ldots, \alpha_k) \in H$ as the maximum rank of $\mathcal{B}$.

5 Linear kernel vectors of matrix Lie algebras

The goal of this section is to study existence of linear kernel vectors for matrix spaces arising from representations of Lie algebras.

Let $\mathfrak{g}$ be a Lie algebra and (ρ, V) be a representation of $\mathfrak{g}$, where $V \cong \mathbb{F}^n$. Let $\mathcal{B} = \rho(\mathfrak{g}) \leq \mathrm{M}(n, \mathbb{F})$.

First, note that $\mathcal{B}$ admits a common kernel vector[5] if and only if (ρ, V) has a trivial subrepresentation. We view this as a degenerate case, so in the following we shall mainly consider representations without trivial subrepresentations.

By the basis-free definition of linear kernel vectors in Section 1.2, $\mathcal{B} = \rho(\mathfrak{g})$ has a linear kernel vector if we have a linear map $\beta : \rho(\mathfrak{g}) \to V$ such that $\rho(x)\beta(\rho(x)) = 0$. For our purposes, it will be more convenient to work with a map from $\mathfrak{g}$ itself to V. This leads us to define that for a representation (ρ, V), the linear map $\psi : \mathfrak{g} \to V$ is a *linear kernel vector* if

$$\rho(x)\psi(x) = 0 \tag{2}$$

for every $x \in \mathfrak{g}$. We further assume that ψ is not identically zero.

▶ Remark 17. The definition of linear kernel vectors above is a generalization that allows for possibly more linear kernel vectors. This is because a linear kernel vector β yields a generalized one by taking $\psi = \beta \circ \rho$. However, when ρ is not injective, we can have many more generalized maps. For example, for a trivial representation $(0, V)$, β has to be 0 but any linear map from $\mathfrak{g}$ to V is a generalized linear kernel vector.

Applying Equation (2) to x, y and $x + y$ one obtains for every $x, y \in \mathfrak{g}$,

$$\rho(x)\psi(y) + \rho(y)\psi(x) = 0 \tag{3}$$

Since $[x, x] = 0$ for the adjoint representation, the identity map of $\mathfrak{g}$ and its scalar multiples are generalized linear kernel vectors.

Assume that $\psi : \mathfrak{g} \to V$ is a linear kernel vector for (ρ, V). Let (ρ', V') be another representation of $\mathfrak{g}$. Then, if $\phi : V \to V'$ is a non-zero linear map such that $\phi \circ \rho = \rho' \circ \phi$ (that is, ϕ is a homomorphism between the two representations) then $\phi \circ \psi$ is a linear kernel vector for (ρ', V'). Indeed, $\rho'(x)\phi(\psi(x)) = \phi(\rho(x)(\psi(x)) = \phi(0) = 0$.

Our aim is to show that for many of Lie algebras $\mathfrak{g}$, unless the representation (ρ, V) includes a trivial subrepresentation, every linear kernel vector $\psi : \mathfrak{g} \to V$ can be obtained as the composition of the adjoint representation and a homomorphism.

▶ **Theorem 18.** *Let $\mathfrak{g}$ be a semisimple Lie algebra $\mathfrak{g}$ over an algebraically closed field $\mathbb{F}$ of characteristic not 2 or 3. Assume that that the trivial representation is not a subrepresentation of the representation (ρ, V) of $\mathfrak{g}$. Then any linear kernel vector ψ defines a homomorphism $\psi : (ad, \mathfrak{g}) \to (\rho, V)$ i.e., for every $x, y \in \mathfrak{g}$,*

$$\psi([x, y]) - \rho(x)\psi(y) = 0. \tag{4}$$

[5] That is $v \in \mathbb{F}^n$ such that for any $B \in \mathcal{B}$, $Bv = 0$.

We defer the proof of Theorem 18 in Section 5.1. We now derive a corollary of Theorem 18 and use it to prove Theorem 5.

▶ **Corollary 19.** *Let $\mathfrak{g}, (\rho, V)$ satisfy the condition in Theorem 18. Then, $(\rho, V) \cong \oplus_i (\mathrm{ad}, \mathfrak{g}_i) \oplus (\rho', V')$ where $\mathfrak{g}_i$ are not necessarily disjoint or distinct quotient algebras of $\mathfrak{g}$, and (ρ', V') has no linear kernel vectors.*

Proof. Let ψ be a linear kernel vector (ρ, V). Let $V_1 = \mathrm{im}(\psi) \cong \mathfrak{g}/\ker\psi =: \mathfrak{g}_1$. Then V_1 is invariant under ρ as for any $x \in \mathfrak{g}, \psi(y) \in V_1$, $\rho(x)\psi(y) = \psi([x, y]) \in V_1$. Therefore, $(\rho, V) \cong (\mathrm{ad}, \mathfrak{g}_1) \oplus (\rho', V')$ by the semisimplicity of $\mathfrak{g}$. We can then repeat till we no longer have linear kernel vectors. ◀

▶ **Theorem 5.** *Let $\mathcal{B}$ be the image of a faithful irreducible representation ϕ of a semisimple Lie algebra $\mathfrak{g}$ over algebraically closed fields of characteristic not 2 or 3. Then $\mathcal{B}$ admits a linear kernel vector if and only if $\mathcal{B}$ is trivial, or $\mathfrak{g}$ is simple and ϕ is isomorphic to the adjoint representation.*

Proof. When $\mathcal{B}$ is trivial it clearly has a linear vector kernel. So assume it is not. Applying Corollary 19 in the case of ρ being irreducible, we get $(\rho, V) \cong (\mathrm{ad}, \mathfrak{g}')$ for some quotient algebra $\mathfrak{g}'$ of $\mathfrak{g}$. Since ρ is faithful, we must have $\mathfrak{g} = \mathfrak{g}_i$. By definition, subrepresentations of the adjoint representation are the same as ideals. Thus irreducibility of the adjoint representation implies that $\mathfrak{g}$ is simple. ◀

▶ Remark 20.
1. Theorem 18 and Theorem 5 also hold over sufficiently large perfect fields as a semisimple Lie algebra over a perfect field remains semisimple over the algebraic closure of such fields. However, passing over to the closure need not preserve semisimplicity in general and thus, the current proof of Theorem 24 does not work for any sufficiently large field.
2. Initially we proved a fact equivalent to (Equation (4)) for irreducible representations of classical Lie algebras using Chevalley bases. In an attempt to simplify the proof by reducing to certain subalgebras and taking trivial subrepresentations into account, we discovered relevance of equalities (5) and (6) below. We include the previous proof in Appendix E, as some ideas and techniques there may be useful for future references.

5.1 Proof of Theorem 18

To prove Theorem 18, we need the following preparations.

▶ **Proposition 21.** *Let $\psi : \mathfrak{g} \to V$ be a linear kernel vector for the representation (ρ, V) of a Lie algebra $\mathfrak{g}$. Then,*

$$\rho(x)\big(\psi([x, y]) - \rho(x)\psi(y)\big) = 0 \tag{5}$$

and

$$\rho(y)\big(\psi([x, y]) - \rho(x)\psi(y)\big) = 0 \tag{6}$$

Consequently, the difference $\psi([x, y]) - \rho(x)\psi(y)$ is annihilated by $\rho(z)$ for every element z of the Lie subalgebra of $\mathfrak{g}$ generated by x and y.

Proof.

$$\begin{aligned}
\rho(x)\psi([x,y]) &= -\rho([x,y])\psi(x) && \text{Applying (3) to } [x,y],x\\
&= -\rho(x)\rho(y)\psi(x) + \rho(y)\rho(x)\psi(x) && (\rho,V) \text{ is a representation}\\
&= -\rho(x)\rho(y)\psi(x) && \text{Applying (2) to } x\\
&= \rho(x)\rho(x)\psi(y) && \text{Applying (3) to } x,y
\end{aligned}$$

Similarly (Equation (6)) follows because

$$\rho(y)\psi([x,y]) = -\rho([x,y])\psi(y) = -\rho(x)\rho(y)\psi(y) + \rho(y)\rho(x)\psi(y) = \rho(y)\rho(x)\psi(y). \quad \blacktriangleleft$$

The following statement follows from standard density arguments but we provide a proof in Appendix D.

▶ **Proposition 22** (Proposition 31). *Let $\mathfrak{g}$ be an m-dimensional Lie algebra over a large enough field $\mathbb{F}$, such that there exist two elements $x_0, y_0 \in \mathbb{F}$ that generate $\mathfrak{g}$. Then there are elements $x_i, y_i \in \mathfrak{g}$, $(i = 1, \ldots, m^2)$ such that x_i and y_i generate $\mathfrak{g}$ for every i and that $x_i \otimes y_i$ span $\mathfrak{g} \otimes \mathfrak{g}$.*

The following lemma is a major step to prove Theorem 18.

▶ **Lemma 23.** *Let $\psi : \mathfrak{g} \to V$ be a linear kernel vector for the representation (ρ, V) of a Lie algebra $\mathfrak{g}$ over a large enough field $\mathbb{F}$. Suppose $\mathfrak{g}$ can be generated by two elements, and the trivial representation is not a subrepresentation of the representation (ρ, V) of $\mathfrak{g}$. Then for every $x, y \in \mathfrak{g}$,*

$$\psi([x,y]) - \rho(x)\psi(y) = 0.$$

Proof. By standard arguments, it is sufficient to prove the theorem for the special case when $\mathbb{F}$ is algebraically closed. We assume that. By Proposition 22, we have $\{(x_i, y_i)\}$ that each generate $\mathfrak{g}$ as a Lie algebra and collectively linearly span $\mathfrak{g} \otimes \mathfrak{g}$. For each i, by Proposition 21, $\rho(z)\big(\psi([x_i,y_i]) - \rho(x_i)\psi(y_i)\big) = 0$ for every $z \in \mathfrak{g}$. This equality is trilinear and therefore it holds for every $z \otimes x \otimes y$ for $(z,x,y) \in \mathfrak{g} \times (\mathrm{span}_i\{(x_i \otimes y_i)\})$. By Proposition 22, $\mathrm{span}_i\{(x_i \otimes y_i)\} = \mathfrak{g} \otimes \mathfrak{g}$ and thus, $\rho(z)\big(\psi([x,y]) - \rho(x)\psi(y)\big)$ is identically zero on $\mathfrak{g}^{\otimes 3}$. Now for every fixed (x,y) the vector $\psi([x,y]) - \rho(x)\psi(y)$ is annihilated by all of $\rho(\mathfrak{g})$. It follows that the vector must be zero, as otherwise it would span a trivial subrepresentation. ◀

To deduce Theorem 18 from Lemma 23, we need a result for the number of generators of certain Lie algebras. We recall some classical results on this topic. First, Kuranishi gave a simple proof that over characteristic 0, there exists two elements that generate any semisimple Lie algebra [19, Thm. 6]. The proof of the statement works directly in positive characteristic (> 3) for sum of *classical simple* lie algebras, i.e. those obtained from a Chevalley basis. This was extended in [2] to other kinds of simple Lie algebras over positive characteristic (> 3). This can be extended to the semisimple case based on a density argument which is standard. However, we couldn't find a reference for this, so we include a proof in Appendix D (see Lemma 32).

▶ **Theorem 24** ([19, 2]+ Lemma 32). *Let $\mathfrak{g}$ be a semisimple Lie algebra $\mathfrak{g}$ over an algebraically closed field $\mathbb{F}$ of characteristic not 2 or 3. Then $\mathfrak{g}$ can be generated by two elements.*

Theorem 18 follows from Lemma 23 and Theorem 24. ◀

A Basic notions for Lie algebras and its representations

A *Lie algebra* is vector space $\mathfrak{g}$ with an alternating bilinear map, called a Lie bracket, $[-,-]: \mathfrak{g}\times\mathfrak{g}\to\mathfrak{g}$ that satisfies the Jacobi identity $\forall x,y,z\in\mathfrak{g}, [x,[y,z]]+[z,[x,y]]+[y,[z,x]]=0$. A subalgebra of a Lie algebra $\mathfrak{g}$ is a vector subspace which is closed under the Lie bracket.

Given two Lie algebras $\mathfrak{g}$ and $\mathfrak{h}$, a *Lie algebra homomorphism* is a linear map respecting the Lie bracket, i.e., a linear map $\phi:\mathfrak{g}\to\mathfrak{h}$ such that $\phi([a,b])=[\phi(a),\phi(b)]$.

Given a vector space V, we use $\mathfrak{gl}(V)$ to denote the Lie algebra, which consists of linear endomorphisms of V with the Lie bracket $[A,B]=AB-BA$ for $A,B\in\mathfrak{gl}(V)$.

A *representation of a Lie algebra* $\mathfrak{g}$ is a Lie algebra homomorphism $\phi:\mathfrak{g}\to\mathfrak{gl}(V)$ for some vector space V. A subspace $U\leq V$ is *invariant* under ϕ, if for any $a\in\mathfrak{g}$, $\phi(a)(U)=U$. We say that ϕ is *irreducible*, if the only invariant subspaces under ϕ are the zero space and the full space. We say that ϕ is *completely reducible*, if there exists a proper direct sum decomposition of $V=V_1\oplus\cdots\oplus V_c$, such that each V_i is invariant under ϕ.

A representation $\phi:\mathfrak{g}\to\mathfrak{gl}(V)$ is trivial, if $\phi(x)=0\in\mathfrak{gl}(V)$ for any $x\in\mathfrak{g}$. In this case, when V is of dimension 1, ϕ is the *trivial irreducible representation*. The adjoint representation of $\mathfrak{g}$, $\mathrm{ad}:\mathfrak{g}\to\mathfrak{gl}(\mathfrak{g})$ is defined as $\mathrm{ad}_x(y)=[x,y]$ for $x,y\in\mathfrak{g}$.

Suppose V is of dimension n over a field $\mathbb{F}$. After fixing a basis of V, $\mathfrak{gl}(V)$ can be identified as $\mathrm{M}(n,\mathbb{F})$. Then the image of a Lie algebra representation ϕ is a matrix subspace $\mathcal{B}\leq\mathrm{M}(n,\mathbb{F})$ that is closed under the natural Lie bracket $[A,B]=AB-BA$ for $A,B\in\mathcal{B}$.

B Correspondences between Lie algebras and Lie groups

Lie algebras are closely related to Lie groups. In the case of finite dimensional complex and real Lie algebras, there is a tight correspondence. Since matrix Lie algebras are the main object of study in this article, we only need results for matrix Lie algebras and matrix Lie groups, and not the most general definitions. In the following, we present some basic facts about the correspondence between Lie algebras and Lie groups in the matrix setting.

We follow [12] for the definitions and some basic results about matrix Lie groups and Lie algebras over $\mathbb{C}$ that we will use later.

A *matrix Lie group* is a subgroup G of $\mathrm{GL}(n,\mathbb{C})$ with the property that if $(A_m)_{m\in\mathbb{N}}$ is any sequence of matrices in G, and A_m converges to some matrix A, then either A is in G or A is non-invertible.

For $X\in\mathrm{M}(n,\mathbb{C})$, define the exponential by the usual power series, that is, $e^X=\sum_{i=0}^{\infty}\frac{X^i}{i!}$. By [12, Proposition 2.1], this power series converges absolutely for any $X\in\mathrm{M}(n,\mathbb{C})$, and e^X is a continuous function of X. A straightforward consequence of the absolute convergence is that we can differentiate term by term, which implies that $\frac{d}{dt}e^{tX}=Xe^{tX}=e^{tX}X$.

Given a matrix Lie group G, the associated Lie algebra $\mathrm{Lie}(G)$ is defined as $\mathrm{Lie}(G)=\{X\in\mathrm{M}(n,\mathbb{C})\mid\forall t\in\mathbb{R}, e^{tX}\in G\}$. Let $\mathfrak{g}$ denote $\mathrm{Lie}(G)$; this notation is consistent with our previous notation. Clearly, for any $M\in\mathfrak{g}$, the one-parameter group $\{e^{tM}\mid t\in\mathbb{R}\}$ is a subgroup of G.

We need the following two classical results relating matrix Lie groups and matrix Lie algebras in Section 3.

▶ **Theorem 25** ([12, Theorem 5.20]). *Let G be a matrix Lie group with Lie algebra $\mathfrak{g}$ and let $\mathfrak{h}$ be a Lie subalgebra of $\mathfrak{g}$. Then there exists a unique connected Lie subgroup H of G with Lie algebra $\mathfrak{h}$. In particular, every matrix Lie algebra $\mathfrak{g}$ is the Lie algebra of a Lie group.*

▶ **Theorem 26** ([12, Theorem 3.20 (1)]). *Let G be a matrix Lie group, and let $\mathfrak{g}=\mathrm{Lie}(G)$. Then for any $X\in\mathfrak{g}$ and $g\in G$, we have $gXg^{-1}\in\mathfrak{g}$.*

C Some results about Cartan subalgebras

Cartan subalgebras.

Let $\mathfrak{g}$ be a Lie algebra. A *subalgebra* $\mathfrak{h} \subseteq \mathfrak{g}$ is a vector subspace that is closed under the Lie bracket (inherited from $\mathfrak{g}$). In other words, $[\mathfrak{h}, \mathfrak{h}] \subseteq \mathfrak{h}$. An *ideal* $\mathfrak{i} \subseteq \mathfrak{g}$ is a subalgebra such that $[\mathfrak{g}, \mathfrak{i}] \subseteq \mathfrak{i}$. Let $\mathfrak{g}_1$ and $\mathfrak{g}_2$ be ideals of $\mathfrak{g}$. Define $[\mathfrak{g}_1, \mathfrak{g}_2] = \text{span}\left([x, y] \mid x \in \mathfrak{g}_1, y \in \mathfrak{g}_2\right)$. Let $\mathfrak{g}^1 = \mathfrak{g}$ and inductively define $\mathfrak{g}^i = [\mathfrak{g}^{i-1}, \mathfrak{g}]$. An algebra $\mathfrak{g}$ is called *nilpotent* if there is an n such that $\mathfrak{g}^n = 0$. Similarly, define $\mathfrak{g}^{(1)} = \mathfrak{g}$ and $\mathfrak{g}^{(i)} = [\mathfrak{g}^{(i-1)}, \mathfrak{g}^{(i-1)}]$. An algebra $\mathfrak{g}$ is called *solvable* if there is an n such that $\mathfrak{g}^{(n)} = 0$. The *normalizer* of a subspace $\mathfrak{a}$ of $\mathfrak{g}$ is defined as $\mathfrak{n}_\mathfrak{g}(\mathfrak{a}) = \{x \in \mathfrak{g} \mid [x, \mathfrak{a}] \subseteq \mathfrak{a}\}$. A subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ is a *Cartan subalgebra* if it is nilpotent and $\mathfrak{n}_\mathfrak{g}(\mathfrak{h}) = \mathfrak{h}$.

We shall need the following classical result on Cartan subalgebras. For $x \in \mathfrak{g}$, recall that $\text{ad}_x : \mathfrak{g} \to \mathfrak{g}$ is the linear map defined by $\text{ad}_x(y) = [x, y]$ for $y \in \mathfrak{g}$. In particular, the exponentiation e^{ad_x} is a linear map from $\mathfrak{g}$ to $\mathfrak{g}$, and it is a Lie algebra automorphism if ad_x is nilpotent, called an inner automorphism. The group generated by inner automorphisms is denoted by $\text{Int}(\mathfrak{g})$.

▶ **Theorem 27** (See e.g. [4, Chapter 3.5]). *Let $\mathfrak{g}$ be a Lie algebra over an algebraically closed field $\mathbb{F}$ of characteristic zero. For any two Cartan subalgebras $\mathfrak{h}_1$ and $\mathfrak{h}_2$, there exists $g \in \text{Int}(\mathfrak{g})$ such that $\mathfrak{h}_1 = g(\mathfrak{h}_2)$.*

To recover the statement in Lemma 14, note that for a matrix Lie algebra $\mathcal{B} \leq \text{M}(n, \mathbb{C})$, an inner automorphism takes the form as a conjugation by an invertible matrix. This is because $\text{Ad}(e^x) = e^{\text{ad}_x}$, where Ad is the conjugation by matrices. This can be seen, e.g., by taking the derivative of $\text{Ad}(e^x)Y = e^{tx}Ye^{-tx}$ at $t = 0$.

▶ **Theorem 28** (Lie's theorem on solvable Lie algebras). *Let $\mathbb{F}$ be an algebraically closed field of characteristic zero. Let $\mathcal{B} \leq \text{M}(n, \mathbb{F})$ be a solvable matrix Lie algebra over $\mathbb{F}$. Then there exists $T \in \text{GL}(n, \mathbb{F})$, such that for any $B \in \mathcal{B}$, TBT^{-1} is upper triangular.*

Regular elements of Lie algebras.

Let λ be a formal variable, and let $\sum_i c_{i,x}\lambda^i$ be the characteristic polynomial of ad_x. The smallest r such that $c_{r,x}$ is not identically zero over all $x \in \mathfrak{g}$ is called the *rank* of $\mathfrak{g}$. The open set of points $\{x \in \mathfrak{g} \mid c_r(x) \neq 0\}$ is the set of *regular points*. A simple observation is that the set of regular elements is Zariski open and thus it is dense.

For $x \in \mathfrak{g}$, the Fitting null component of ad_x is $\text{F}_0(\text{ad}_x) = \{y \in \mathfrak{g} : \exists m > 0, \text{ad}_x^m(y) = 0\}$.

Regular elements and Cartan subalgebras are closely related as the following theorem shows.

▶ **Theorem 29** ([4, Corollary 3.2.8]). *Let $\mathfrak{g}$ be a Lie algebra over a field of order larger than $\dim(\mathfrak{g})$. For a regular $x \in \mathfrak{g}$, $\text{F}_0(\text{ad}_x)$ is a Cartan subalgebra.*

Computing Cartan subalgebras.

We shall need the following result of de Graaf, Ivanyos, and Rónyai [5] regarding computing Cartan subalgebras. In algorithms, Lie algebras are often given by structure constants. That is, let $\mathfrak{g}$ be a Lie algebra of dimension n over a field $\mathbb{F}$, and let $a_1, \ldots, a_n$ be a linear basis of $\mathfrak{g}$. The *structure constants* α_{ijk} $(i, j, k \in \{1, \ldots, n\})$ are field elements such that $[a_i, a_j] = \sum_{k=1}^n \alpha_{ijk}a_k$.

▶ **Theorem 30** ([5, Theorem 5.8]). *Let $\mathfrak{g}$ be a Lie algebra of dimension n over a field $\mathbb{F}$ with $|\mathbb{F}| > n$. Suppose $\mathfrak{g}$ is given by its structure constants with respect to a basis $a_1, \ldots, a_n$, and fix $\Omega \subseteq \mathbb{F}$ such that $|\Omega| = n + 1$. Then there is a deterministic polynomial-time algorithm which computes a regular element $x = \sum \alpha_i a_i$, $\alpha_i \in \Omega$, such that $\mathrm{F}_0(\mathrm{ad}_x)$ is a Cartan subalgebra of $\mathfrak{g}$.*

Note that to obtain Theorem 13, we start with a matrix Lie algebra $\mathcal{B} = \langle B_1, \ldots, B_m \rangle \leq \mathrm{M}(n, \mathbb{F})$, compute structure constants by expanding $[B_i, B_j] = \sum_{k \in [m]} \alpha_{i,j,k} B_k$, apply Theorem 30, and use its output to obtain a subspace of $\mathcal{B}$ which is a Cartan subalgebra.

D Density arguments and the generation of Lie algebras

In this part we prove some facts based on standard density arguments.

Let U be an m-dimensional vector space over an infinite field $\mathbb{F}$. By choosing a basis we identify U with $\mathbb{F}^m$. We say that a nonempty subset D of U is *huge* if there exists a nonzero polynomial $f(t_1, \ldots, t_m) \in \mathbb{F}[t_1, \ldots, t_m]$ such that if $u = (u_1, \ldots, u_m)^T \notin D$ then $f(u_1, \ldots, u_m) = 0$. (Thus, huge subsets are those that contain Zariski open subsets.) It is easy to see that hugeness is independent of the choice of the basis and that the intersection of finitely many huge subsets is huge as well. As a hyperplane of U consists of the zeros of a linear function on U, we have that any huge subset of U spans U.

Let $\mathfrak{g}$ be an m-dimensional Lie algebra over $\mathbb{F}$. Let $u_1, \ldots, u_m$ be a basis for $\mathfrak{g}$. Recall that the structure constants α_{ijk} $(i, j, k \in \{1, \ldots, m\})$ are field elements such that such that $[u_i, u_j] = \sum_{k=1}^m \alpha_{ijk} u_k$. A *Lie expression* or Lie polynomial $E(z_1, \ldots, z_\ell)$ in ℓ variables $z_1, \ldots, z_\ell$ is an expression that can be recursively built using linear combinations and the bracket symbol. Let $x_i = \sum_{j=1}^m x_{ij} u_j$ $(i = 1, \ldots, \ell)$. Then the structure constants can be used to expand $E(x_1, \ldots, x_\ell)$ as a vector whose coordinates are polynomials in x_{ij}. If we assign $m - 1$ elements of $\mathfrak{g}$ to the variables $z_2, \ldots, z_\ell$ then E expands to an a vector whose coordinates are polynomials in $x_{11}, \ldots, x_{1\ell}$ that may include nonzero constant terms. Therefore it will be convenient to also consider Lie expressions *over* $\mathfrak{g}$: these are expressions which may include constant elements from $\mathfrak{g}$. From the definition of density it follows that if E is an expression in a single variable z that is not identically zero on $\mathfrak{g}$ then the elements x of $\mathfrak{g}$ on which E evaluates to a nonzero element of $\mathfrak{g}$ is huge. Furthermore, if there are m expressions $E_1(z), \ldots, E_m(z)$ such that there exists an element $x \in \mathfrak{g}$ such that $E_1(x), \ldots, E_m(x)$ are linearly independent then such elements are a huge subset of $\mathfrak{g}$. To see this, just consider the determinant expressing that $E_1(x) \ldots, E_m(x)$ are linearly dependent.

▶ **Proposition 31.** *Let $\mathfrak{g}$ be an m-dimensional Lie algebra over a large enough field $\mathbb{F}$ such that there exist two elements $x_0, y_0 \in \mathbb{F}$ that generate $\mathfrak{g}$. Then there are elements $x_i, y_i \in \mathfrak{g}$, $(i = 1, \ldots, m^2)$ such that x_i and y_i generate $\mathfrak{g}$ for every i and that $x_i \otimes y_i$ span $\mathfrak{g} \otimes \mathfrak{g}$.*

Proof. Pick expressions $E_i(z, w)$ $(i = 1, \ldots, m)$ such that $E_i(x_0, y_0)$ are linearly independent. Then the set of elements x such that $E_i(x, y_0)$ are linearly independent is huge and hence contains a basis $x_1, \ldots, x_m$ of $\mathfrak{g}$. For each j, the subset consisting of those y for which $E_i(x_j, y)$ are linearly independent is a huge set $D_j \subset \mathfrak{g}$ whence there exist elements $y_{jk} \in D_j$ $(k = 1, \ldots, m)$ that are a basis for $\mathfrak{g}$. Each of the m^2 pairs x_j, y_{jk} generate $\mathfrak{g}$. To see that they span $\mathfrak{g} \otimes \mathfrak{g}$, write an element $z \in \mathfrak{g} \otimes \mathfrak{g}$ in the form $z = \sum x_j \otimes y'_j$ and express y'_j as $y'_j = \sum_k \alpha_{jk} y_{jk}$. Then $z = \sum_{j,k} \alpha_{jk} x_j \otimes y_{jk}$. ◀

▶ **Lemma 32.** *Let $\mathfrak{g}_1, \ldots, \mathfrak{g}_m$ be finite dimensional simple Lie algebras over a large enough field $\mathbb{F}$, each generated by 2 elements. Then $\mathfrak{g}_1 \oplus \ldots \oplus \mathfrak{g}_m$ is also generated by two elements.*

Proof. Assume that x_i and y_i generate $\mathfrak{g}_i$ $(i = 1, \ldots, m)$. We claim that we may further assume that $\mathrm{ad}(x)^{d_i} y_i \neq 0$ where $d_i = \dim_{\mathbb{F}}(\mathfrak{g}_i)$. Indeed, if $\mathrm{ad}(x)^{d_i} y_i = 0$ then, by Engel's theorem, there exists a pair $(w_i, z_i) \in \mathfrak{g} \times \mathfrak{g}$ such that $\mathrm{ad}(w_i)^{d_i} z_i \neq 0$. If we fix z_i from such a pair then the elements w_i such that $\mathrm{ad}(w_i)^{d_i} z_i \neq 0$ is a huge set. There exist d_i Lie expressions $E_1, \ldots, E_{d_i}$ in in two variables such that $E_1(x_i, y_i), \ldots, E_{d_i}(x_i, y_i)$ are linearly independent elements of $\mathfrak{g}_i$. The elements w_i such that $E_1(w_i, y_i), \ldots, E_{d_i}(x_i, y_i)$ are linearly independent form a huge set. The intersection of these two huge sets is still huge and hence non-empty. We replace x_i with an element from the intersection. Now the set of w_i such that $\mathrm{ad}(x_i)_i^d w_i \neq 0$ is huge as well as these set of those for which $E_j(x_i, w_i)$ are linearly independent. We can replace y_i with an element from the intersection.

Let $f_i = f_i(t)$ be the monic polynomial of smallest degree such that $f_i(\mathrm{ad}(x_i))y_i = 0$. Note that f_i has degree at most d_i and the assumption on x_i and y_i implies that f_i is not a divisor of t^{d_i}. Therefore each f_i has a nonzero root (in the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$). Let R_i be the set of nonzero roots of f_i in $\overline{\mathbb{F}}$. There exist field elements $\alpha_1, \ldots, \alpha_m \in \mathbb{F}$ such that the sets $\alpha_i R_i$ are pairwise disjoint. Replacing x_i with $\alpha_i x_i$ we arrange that the sets R_i become pairwise disjoint. Then for each i, put $h_i = \prod_{j \neq i} f_j$. We have that $h_i(\mathrm{ad}(x_j))y_j = 0$ for every $j \neq i$, while $h_i(\mathrm{ad}(x_j))y_i \neq 0$ as h_i is not divisible by f_i.

Put $x = \sum_{i=1}^m x_i$ and $y = \sum_{i=1}^m y_i$. Then $h_i(x)y$ is a nonzero element of $\mathfrak{g}_i$. Let M be the subalgebra of $\mathfrak{g}$ generated by x and y. We see that M has a nonzero element, say z_i contained in $\mathfrak{g}_i$. The projection of M on the ith component is clearly $\mathfrak{g}_i$ and x_i and y_i generate $\mathfrak{g}_i$. As $\mathfrak{g}_i$ is simple we have that the ideal of M generated by z_i is $\mathfrak{g}_i$. This holds for all $i = 1, \ldots, m$, showing that $M = \mathfrak{g}$. ◀

E Linear kernel vectors of matrix Lie algebras

In this section, we will give an alternative proof of Lemma 23, which doesn't use density arguments, but instead uses weight decomposition of representations of semi-simple Lie algebras over $\mathbb{C}$.

E.1 Weight decomposition of Lie algebra representations

Fix a Cartan subalgebra $\mathfrak{h}$ of a semisimple Lie algebra $\mathfrak{g}$ over $\mathbb{C}$. By definition $\mathfrak{h}$ is nilpotent. If $\mathfrak{g}$ is semisimple, $\mathfrak{h}$ is abelian [24, Thm3, Ch.3]. Similar to the notion of eigenvalues and eigenspaces is the concept of a weight and its weight space. Intuitively, it can be thought of as a linear function that captures the eigenvalues of a set of matrices simultaneously. Formally, a *weight* is an element of $\mathfrak{h}^*$. If $w \in \mathfrak{h}^*$, then the w-weight space of V is defined as $V_w = \{v \in V \mid \forall\, h \in \mathfrak{h}, \rho(h) \cdot v = w(h)v\ \}$.

▶ **Theorem 33.** *If $\mathfrak{g}$ is a complex semi-simple Lie algebra, then every representation (ρ, V) can be decomposed into weight spaces $V = \oplus_w V_w$.*

Using this decomposition we have a basis such that for any $h \in \mathfrak{h}$, $\rho(h)$ is a diagonal matrix with $w(h)$ as diagonal elements where w runs over all weights of V.

▶ **Fact 34.** *The matrix space defined by the image $\rho(\mathfrak{g})$ of the representation (ρ, V) is singular iff 0 is a weight of the representation, i.e. V_0 occurs with multiplicity at least one.*

Proof. This follows easily from the observation about $\rho(h_i)$ which implies that $\rho(\mathfrak{h})$ is singular if 0 is a weight. From Section 4, we know that the entire algebra is singular if any of its Cartan subalgebra is. If 0 is not a weight, then it is easy to construct a element $h \in \mathfrak{h}$ such that $w(h) \neq 0$ for every weight. Thus, $\rho(h)$ has full rank. ◀

If we decompose the adjoint representation, the weights we obtain are called *roots* usually denoted by Φ. It is also a fact that if $\alpha \in \Phi$, then $-\alpha \in \Phi$. We thus can write $\mathfrak{g} = \mathfrak{h} \oplus_{\alpha \in \Phi} \mathfrak{g}_\alpha$. Moreover, each of the spaces $\mathfrak{g}_\alpha$ is one-dimensional. We denote an element of $\mathfrak{g}_\alpha$ by g_α which is unique upto a scalar. Such a decomposition of the Lie algebra is very useful as we can understand the action under any representation of these subspaces g_α as follows .

▶ **Proposition 35.** *[24, Prop.1, Chapter 7] For any representation (ρ, V) of $\mathfrak{g}$, $\rho(g_\alpha)V_w \subset V_{w+\alpha}$ for every weight w and every root α.*

E.2 Notation

Fix a complex semi-simple Lie algebra $\mathfrak{g}$ and a Cartan subalgebra $\mathfrak{h}$. Let Φ be its set of roots. We choose a Cartan-Weyl basis[6] for $\mathfrak{g}$ (cf. e.g. [24, pp. 48]). This means that we have a set of simple roots[7] $S = \{\alpha_1, \cdots \alpha_n\}$ and a basis of $\mathfrak{h}$, $\{h_1, \cdots h_n\}$ such that the following hold,

$$
\begin{aligned}
[h_i, g_{\alpha_j}] &= \alpha_j(h_i) g_{\alpha_j} && \forall i, j \in [n] \\
[g_\alpha, g_\beta] &= c_{\alpha\beta} g_{\alpha+\beta} \ \ (c_{\alpha\beta} \neq 0) && \alpha + \beta \in \Phi \\
[g_\alpha, g_\beta] &= 0 && \text{if } \alpha + \beta \notin \Phi \\
[g_{\alpha_i}, g_{-\alpha_i}] &= h_i && \forall i \in [n]
\end{aligned}
$$

Choose a basis of $V \cong \mathbb{F}^N$, such that $\rho(\mathfrak{h})$ is diagonal. Let W be the set of weights of V and thus $V = \oplus_{w \in W} V_w$ such that V_w is the w weight space of $\mathfrak{h}$. Note that we are assuming that $0 \in W$ as non-singular spaces anyway cannot have a linear kernel.

E.3 Main proof

We recall that given a Lie algebra $\mathfrak{g}$ and a representation (ρ, V) a linear kernel vector $\phi : \mathfrak{g} \to V$ is a linear map such that $\rho(x)\psi(x) = 0$ for every $x \in \mathfrak{g}$. We state the main lemma we need and will prove it later.

▶ **Lemma 36.** *Assume that trivial representation is not a subrepresentation of the representation (ρ, V) of $\mathfrak{g}$. Let $\psi : \mathfrak{g} \to V$ be a linear kernel vector. Then for any $\alpha, \beta \in \Phi$ such that $\alpha + \beta \neq 0$ and $h \in \mathfrak{h}$ we have*

$$
\begin{aligned}
&\psi(h) \in V_0, \psi(g_\alpha) \in V_\alpha \text{ and} \\
&\psi([g_\alpha, g_\beta]) = \rho(g_\alpha)\psi(g_\beta) \\
&\psi([h, g_\alpha]) = \rho(h)\psi(g_\alpha)
\end{aligned}
$$

▶ **Theorem 37.** *Assume that trivial representation is not a subrepresentation of the representation (ρ, V) of $\mathfrak{g}$. Then for every $x, y \in \mathfrak{g}$,*

$$\psi([x, y]) - \rho(x)\psi(y) = 0$$

Proof. By linearity, it suffices to show this for the basis vectors h_i, g_α. Lemma 36 shows it in every except when we have $(x, y) = (g_\alpha, g_{-\alpha})$. Fix any root α. By Lemma 36 and Proposition 35, the vector $\psi([g_\alpha, g_{-\alpha}]) - \rho(g_\alpha)\psi(g_{-\alpha}) \in V_0$ and thus is annihilated by $\rho(\mathfrak{h})$.

---

[6] Cartan-Weyl basis and the Chevally basis differ only by a normalization. We do not need properties of the coefficients $c_{\alpha,\beta}$ and thus either basis works well.

[7] Simple roots are just a basis of $\mathfrak{h}^*$ while the set of all roots can be linearly dependent.

We now wish to show that it is annihilated by $\rho(g_\beta)$ for any root β. The assumption that there are no trivial subrepresentations then implies that this vector must be zero.

Proposition 21 already shows it if $\beta \in \{\alpha, -\alpha\}$ and so we assume that's not the case.

$$\begin{aligned}
\rho(g_\beta)\rho(g_\alpha)\psi(g_{-\alpha}) &= \rho([g_\beta, g_\alpha])\psi(g_{-\alpha}) + \rho(g_\alpha)\rho(g_\beta)\psi(g_{-\alpha}) && \rho \text{ is a representation} \\
&= \rho([g_\beta, g_\alpha])\psi(g_{-\alpha}) + \rho(g_\alpha)\psi([g_\beta, g_{-\alpha}]) && \text{Lemma 36 for } (\beta, -\alpha) \\
&= \psi([[g_\beta, g_\alpha], g_{-\alpha}]) + \psi([g_\alpha, [g_\beta, g_{-\alpha}]]) && 36 \text{ for } (\alpha+\beta, -\alpha), (\alpha, \beta-\alpha) \\
&= \psi\left([g_\beta, g_\alpha], g_{-\alpha}] + [g_\alpha, [g_\beta, g_{-\alpha}]]\right) && \text{By linearity} \\
&= \psi\left([g_\beta, [g_\alpha, g_{-\alpha}]]\right) && \text{By Jacobi identity} \\
&= \rho(g_\beta)\psi\left([g_\alpha, g_{-\alpha}]\right) && 36 \text{ for } (\beta, h),\ h = [g_\alpha, g_{-\alpha}] \in \mathfrak{h}
\end{aligned}$$

Here, we have used Lemma 36 formally even if one of them is not a root to prevent dividing into cases. For example, if $\beta - \alpha$ is not a root then that term is anyway 0 and we can represent 0 as $\psi(0) = \psi([g_\beta, g_{-\alpha}])$. ◀

E.4 Proof of Lemma 36

For ease of notation, we label $H_i = \rho(h_i)$ for $1 \le i \le n$ and $X_\alpha = \rho(g_\alpha)$, $\alpha \in \Phi$. Similarly, we will have $v_i := \psi(h_i)$, $v_\alpha := \psi(g_\alpha)$. We restate Equation (3) in more verbose terms,

$$H_i v_i = 0 \qquad \forall i \in [n] \tag{7}$$

$$X_\alpha v_\alpha = 0 \qquad \forall \alpha \in \Phi \tag{8}$$

$$H_i v_j + H_j v_i = 0 \qquad \forall i, j \in [n], i \neq j \tag{9}$$

$$H_i v_\alpha + X_\alpha v_i = 0 \qquad \forall i \in [n], \alpha \in \Phi \tag{10}$$

$$X_\beta v_\alpha + X_\alpha v_\beta = 0 \qquad \forall \alpha, \beta \in \Phi \tag{11}$$

▶ **Lemma 38** (Structure). *For every $i \in [n]$, $v_i \in V_0$, and for every root α, $v_\alpha \in V_\alpha$ if α is a weight and is 0 otherwise.*

Proof. i) Let $v_j = \sum_{w \in W} u_w$ where $u_w \in V_w$. Since $0 = H_j v_j = \sum_{w \in W} w(h_j) u_w$, we have that $w(h_j)u_w = 0$. For any $w \neq 0$ such that $u_w \neq 0$ we have $w(h_j) = 0$. Pick $k \in [n]$ such that $w(h_k) \neq 0$. Then, $H_k v_j + H_j v_k = 0$. Looking at the V_w component $w(h_k)u_w + w(h_j)v_k = 0$. Since, $w(h_j) = 0$, we get that $w(h_k)u_w = 0$. But k is chosen such that $w(h_k) \neq 0$ and thus, $u_w = 0$.

ii) Fix an α. We just proved that $\forall i$, $v_i \in V_0$ and using Proposition 35 we get $X_\alpha v_i \in V_\alpha$. Suppose $v_\alpha = \sum_{w \in W} u_w$, where $u_w \in V_w$. For any non-zero $w \neq \alpha$, pick i such that $w(h_i) \neq 0$. Then, $H_i v_\alpha + X_\alpha v_i = 0$. But we already know that $X_\alpha v_i \in V_\alpha$ and thus $H_i v_\alpha \in V_\alpha$. Suppose $H_i v_\alpha = \sum_{w \in W} w(h_i) u_w \in V_\alpha$.

Then, the V_w component should be zero but $w(h_i) \neq 0 \implies u_w = 0$. It follows that $v_\alpha \in V_\alpha \oplus V_0$ for every root α. Fix α and now for every $\beta \neq \alpha$, we have $X_\alpha v_\beta + X_\beta v_\alpha = 0$. Comparing the V_β component we get that $X_\beta u_0 = 0$. This is true for every β and since $u_0 \in V_0$, it is also true for $\rho(h)$ for every $h \in \mathfrak{h}$. Thus, for every $x \in \mathfrak{g}$, $\rho(x)u_w$ and since there are no trivial submodules, $u_0 = 0$. Thus, $v_\alpha \in V_\alpha$ ◀

▶ **Lemma 39.** *For all pairs of roots α, β such that $0 \neq \beta + \alpha \in \Phi$, $X_\beta v_\alpha = c_{\alpha\beta} v_{\alpha+\beta}$.*

Proof. We have that $H_i v_{\alpha+\beta} + X_{\alpha+\beta} v_i = 0$. Similarly, $X_\alpha v_i = -H_i v_\alpha = -\alpha(h_i)v_\alpha$ and $X_\beta v_i = -H_i v_\beta = -\beta(h_i)v_\beta$. Moreover, $X_\beta v_\alpha + X_\alpha v_\beta = 0$.

Now, $X_{\alpha+\beta} = \rho(g_{\alpha+\beta}) = c\rho([g_\alpha, g_\beta]) = c(X_\alpha X_\beta - X_\beta X_\alpha)$ where $c = \frac{1}{c_{\alpha\beta}}$. Thus,

$$\begin{aligned}
-(\alpha+\beta)(h_i)v_{\alpha+\beta} &= X_{\alpha+\beta}v_i \\
&= c(X_\alpha X_\beta - X_\beta X_\alpha)v_i \\
&= c(X_\alpha(X_\beta v_i) - X_\beta(X_\alpha v_i)) \\
&= c(X_\alpha(-\beta(h_i)v_\beta) - X_\beta(-\alpha(h_i)v_\alpha) \\
&= -c\,(\beta(h_i)X_\alpha v_\beta - \alpha(h_i)X_\beta v_\alpha) \\
&= -c\,(-\beta(h_i)X_\beta v_\alpha - \alpha(h_i)X_\beta v_\alpha) \\
&= c\cdot(\alpha+\beta)(h_i)\cdot X_\beta v_\alpha.
\end{aligned}$$

Thus, picking h_i such that $(\alpha+\beta)(h_i) \neq 0$, we get that $X_\beta v_\alpha = \frac{1}{c}v_{\alpha+\beta}$. ◀

▶ **Lemma 40.** *Let α, β be roots such that $\beta \neq -\alpha, \alpha+\beta \notin \Phi$ Then. we have that $X_\alpha v_\beta = 0$.*

Proof. Since, $\alpha+\beta \notin \Phi$, $[g_\alpha, g_\beta] = 0$ which implies that $\rho([g_\alpha, g_\beta]) = 0$ and thus, $X_\alpha X_\beta = X_\beta X_\alpha$. Moreover, $\exists h_i$ such that $\alpha(h_i) \neq -\beta(h_i)$ because the h_i form a basis for $\mathfrak{h}$. We fix our i to be one such. Now, from Equation (11), we get that $X_\alpha v_\beta + X_\beta v_\alpha = 0$. From Equation (10), we get that $H_i v_\alpha + X_\alpha v_i = 0$ and multiplying it by X_β we obtain, $\alpha(h_i)X_\beta v_\alpha + X_\beta X_\alpha v_i = 0$. Repeating it with β and α switched, we get, $\beta(h_i)X_\alpha v_\beta + X_\alpha X_\beta v_i = 0$. Subtracting these 2 equations, we get $\alpha(h_i)X_\beta v_\alpha - \beta(h_i)X_\alpha v_\beta = 0$. We already have another equation i.e. $X_\alpha v_\beta + X_\beta v_\alpha = 0$. Since $\beta(h_i) \neq -\alpha(h_i)$, these two homogeneous equations are independent and thus, the only solution is that $X_\alpha v_\beta = X_\beta v_\alpha = 0$. ◀

The structure lemma establishes Lemma 36 when $y \in \mathfrak{h}$ i.e. for any $x \in \mathfrak{g}, h \in \mathfrak{h}$ we have $\rho(h)\psi(x) = \psi([h,x])$. To see this notice that $\rho(h)\psi(g_\alpha) = \alpha(h)\psi(g_\alpha) = \psi(\alpha(h)g_\alpha)) = \psi([h, g_\alpha])$ where the first equality uses that $\psi(g_\alpha) \in V_\alpha$ and the last by the property of the basis. And the other two lemmas extend it to α, β as $c_{\alpha\beta}v_{\alpha+\beta} = c_{\alpha\beta}\psi(g_{\alpha+\beta}) = \psi([g_\alpha, g_\beta])$.

References

1. M. D. Atkinson and R. Westwick. Spaces of linear transformations of equal rank. *Linear and Multilinear Algebra*, 13(3):231–239, 1983. doi:10.1080/03081088308817522.
2. Jean-Marie Bois. Generators of simple Lie algebras in arbitrary characteristics. *Mathematische Zeitschrift*, 262(4):715–741, 2009. doi:10.1007/s00209-008-0397-3.
3. 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. doi:10.1006/jcss.1998.1608.
4. W.A. de Graaf. *Lie Algebras: Theory and Algorithms*, volume 56 of *North-Holland Mathematical Library*. Elsevier Science, 2000. URL: https://www.sciencedirect.com/bookseries/north-holland-mathematical-library/vol/56/.
5. Willem De Graaf, Gábor Ivanyos, and Lajos Rónyai. Computing cartan subalgebras of lie algebras. *Applicable Algebra in Engineering, Communication and Computing*, 7(5):339–349, Sep 1996. doi:10.1007/BF01293593.
6. H. Derksen and V. Makam. Polynomial degree bounds for matrix semi-invariants. *Advances in Mathematics*, 310:44–63, 2017. doi:10.1016/j.aim.2017.01.018.
7. Harm Derksen and Visu Makam. Private communication, 2020.
8. Jan Draisma. Counting components of the null-cone on tuples. *Transformation Groups*, 11:609–624, 2006. doi:10.1007/s00031-005-1120-7.
9. Jan Draisma. Small maximal spaces of non-invertible matrices. *Bulletin of the London Mathematical Society*, 38(5):764–776, 2006. doi:10.1112/S0024609306018741.

10 David Eisenbud and Joe Harris. Vector spaces of matrices of low rank. *Advances in Mathematics*, 70(2):135 – 155, 1988. doi:10.1016/0001-8708(88)90054-0.

11 Ankit Garg, Leonid Gurvits, Rafael Mendes de Oliveira, and Avi Wigderson. Operator scaling: Theory and applications. *Found. Comput. Math.*, 20(2):223–290, 2020. doi:10.1007/s10208-019-09417-z.

12 Brian C. Hall. *Lie Groups, Lie Algebras, and Representations*. Springer International Publishing, 2015. doi:10.1007/978-3-319-13467-3.

13 James E Humphreys. *Introduction to Lie algebras and representation theory*, volume 9 of *Graduate Texts in Mathematics*. Springer Science & Business Media, 2012. doi:10.1007/978-1-4612-6398-2.

14 Gábor Ivanyos, Marek Karpinski, Youming Qiao, and Miklos Santha. Generalized Wong sequences and their applications to Edmonds' problems. *Journal of Computer and System Science*, 81(7):1373–1386, 2015. doi:10.1016/j.jcss.2015.04.006.

15 Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Non-commutative edmonds' problem and matrix semi-invariants. *Computational Complexity*, 26(3):717–763, Sep 2017. doi:10.1007/s00037-016-0143-x.

16 Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Constructive non-commutative rank computation is in deterministic polynomial time. *Computational Complexity*, 27(4):561–593, Dec 2018. doi:10.1007/s00037-018-0165-7.

17 Gábor Ivanyos, Tushant Mittal, and Youming Qiao. Symbolic determinant identity testing and non-commutative ranks of matrix Lie algebras, 2021. arXiv:2109.06403.

18 V. Kabanets and R. Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1/2):1–46, 2004. doi:10.1007/s00037-004-0182-6.

19 Masatake Kuranishi. On everywhere dense imbedding of free groups in Lie groups. *Nagoya Math. J.*, 2:63–71, 1951. URL: http://projecteuclid.org/euclid.nmj/1118764740.

20 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. doi:10.1007/BF02585470.

21 Visu Makam and Avi Wigderson. Singular tuples of matrices is not a null cone (and the symmetries of algebraic varieties). *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2021(780):79–131, 2021. arXiv:1909.00857, doi:10.1515/crelle-2021-0044.

22 Orit E. Raz and Avi Wigderson. *Subspace Arrangements, Graph Rigidity and Derandomization Through Submodular Optimization*, pages 377–415. Springer Berlin Heidelberg, Berlin, Heidelberg, 2019. doi:10.1007/978-3-662-59204-5_12.

23 Jacob T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980. doi:10.1145/322217.322225.

24 Jean-Pierre Serre. *Complex Semisimple Lie Algebras*. Springer Berlin Heidelberg, 2001. doi:10.1007/978-3-642-56884-8.

25 Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Symbolic and Algebraic Computation*, volume 72 of *Lecture Notes in Computer Science*, pages 216–226. Springer-Verlag, 1979. doi:10.1007/3-540-09519-5_73.