Article:

Coscojuela, P., Katzman, M., Mahavadi, K. et al. (2027) On the complexity, tractability and group theoretic applications of the relative eigenvector problem. Journal of Symbolic Computation, 138. 102609. ISSN: 0747-7171

https://doi.org/10.1016/j.jsc.2026.102609

Journal of Symbolic Computation 138 (2027) 102609

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

On the complexity, tractability and group theoretic applications of the relative eigenvector problem ☆

Pilar Coscojuela [a], Mordechai Katzman [b], Krishna Mahavadi [c], Ludovic Perret [d,e], Alex Ryba [f], Simona Samardjiska [g]

[a] *Department of Mathematics, Universidad Complutense de Madrid, Av. Séneca, 2, Madrid, 28040, Madrid, Spain*
[b] *School of Mathematical and Physical Sciences, University of Sheffield, Hicks Building, Sheffield, S3 7RH, UK*
[c] *Department of Mathematics and Computer Science, Kingsborough Community College, CUNY, New York, USA*
[d] *EPITA, LRE, 14-16, rue Voltaire, Le Kremlin-Bicêtre, 94270, France*
[e] *Sorbonne Université, CNRS, LIP6, Paris, 75005, France*
[f] *Department of Computer Science, Queens College, CUNY, New York, USA*
[g] *Department of Digital Security, Radboud University, PO Box 9010, Nijmegen, 6500GL, Netherlands*

A R T I C L E   I N F O

Article history:
Received 29 January 2026
Received in revised form 16 July 2026
Accepted 23 July 2026
Available online 28 July 2026

MSC:
13P10
22E46
68Q17
68Q25

Keywords:
Relative eigenvector problem
MinRank problem
Gröbner bases
Determinantal ideals
NP-completeness
Embeddings into simple Lie groups

A B S T R A C T

The Relative Eigenvector Problem (REP) generalizes the classical eigenvector problem and arises naturally in computational group theory and representation theory. It plays a central role in methods for constructing finite simple subgroups of exceptional algebraic groups, as well as in algorithms for computing tensor decompositions and systems of imprimitivity of group representations.

In this paper, we investigate both the computational complexity and the practical tractability of REP. We show that a decision variant of REP is NP-complete, over fixed finite fields, via a direct reduction from CNF-SAT. We then relate REP to the MinRank problem with target rank 1 and use algebraic techniques involving determinantal ideals to derive complexity bounds and identify broad parameter regimes in which generic instances of REP can be solved efficiently.

We conclude with an application to the classification of embeddings of the alternating group A_6 into algebraic groups of type F_4. This example demonstrates how REP-based methods may admit spurious solutions and how additional polynomial constraints

☆ This research has been partially supported by the Dutch government through the NWO grant OCNW.M.21.193 (ALPaQCa).
E-mail address: picoscoj@ucm.es (P. Coscojuela).

https://doi.org/10.1016/j.jsc.2026.102609

can be used to refine REP instances to recover genuine embeddings.

1. Introduction

In this paper, we consider Relative Eigenvector Problems (REP) (see (Ryba, 2022, Problem 5)).

Problem 1 *(Relative Eigenvector Problem (*REP*)).* Given a set of matrices $\mathbf{A}_1, \ldots, \mathbf{A}_k \in \mathcal{M}_{m\times n}(\mathbb{K})$, compute one or all non-zero vectors $\mathbf{x} \in \overline{\mathbb{K}}^m$ for which there exist scalars $\lambda_1, \ldots, \lambda_k \in \overline{\mathbb{K}}$ and a vector $\mathbf{y} \in \overline{\mathbb{K}}^n$ such that

$$\mathbf{x}\mathbf{A}_1 = \lambda_1 \mathbf{y}, \ldots, \mathbf{x}\mathbf{A}_k = \lambda_k \mathbf{y}.$$

Here, $\overline{\mathbb{K}}$ is the algebraic closure of the field $\mathbb{K}$. We note that Problem 1 covers two closely related problems: to find one solution or to find all solutions. Both have applications in Computational Group Theory. In this paper, we consider the complexity and tractability of the problem of finding one solution, possibly of a restricted form. Observe that the input matrices for REP need not be square. The special case of REP where $m = n$ and $\mathbf{A}_1$ is the identity matrix is either a standard eigenvector problem, when $k = 2$, or a simultaneous eigenvector problem when $k > 2$. Both of these special cases have well-known polynomial time solutions.

The case of REP with $k = 2$ has also been called the *Generalized Eigenvalue Problem*. A reduction from the Generalized Eigenvalue Problem to the Eigenvalue Problem is given in (Wong, 1974). The hardness results that we establish show that, in general, REP cannot be reduced to an eigenvalue problem.

Over the real numbers, the Generalized Eigenvalue Problem has important applications in the study of differential equations and control systems (Christou et al., 2025). However, we consider instances of REP over finite fields. These instances have important applications in computational group theory. In particular REP has been used as the non-linear step in the construction of simple subgroups of exceptional groups of Lie type and in the construction of tensor decompositions, semilinear tensor decompositions and systems of imprimitivity for irreducible modular representations of finite groups.

The classification of finite simple subgroups of exceptional groups of Lie type has been studied extensively, see (Cohen and Griess, 1987), (Serre, 1996), (Serre, 2000). It requires the construction of many particular examples of embeddings. The most convenient computer construction of such embeddings requires all solutions to a relative eigenvector problem. This method was introduced in (Griess and Ryba, 2002), and has been applied more recently in (Ryba, 2007), (Frey and Ryba, 2018), (Craven, 2022).

In (Ryba, 2022), the computation of one solution of an instance of REP is the key step in an algorithm to find tensor decompositions and systems of imprimitivity for an absolutely irreducible representation of a finite group. This algorithm supplies the last of the recursive steps in the original strategy for the Matrix Group Recognition Project (Leedham-Green, 2001). A related algorithm (Mahavadi and Ryba, 2024) applies REP to compute semilinear tensor decompositions of a matrix representation.

In these applications, REP provides a necessary condition for the existence of the desired structure, but not a sufficient one. Specifically, instances of REP may admit solutions that do not correspond to genuine group embeddings or decompositions. Understanding and eliminating such spurious solutions is an essential practical issue, even in parameter regimes where REP itself is computationally tractable.

1.1. Main results and organization

Motivated by the variety of applications of REP, in this paper we investigate both its theoretical hardness and practical tractability.

In Section 2, we show that REP is a MinRank problem with target rank 1. In the general MinRank problem defined by (Buss et al., 1999; Courtois, 2001) the target rank r is a non-negative problem parameter. The general problem is known to be NP-complete (Buss et al., 1999). However, tractability of instances has been the topic of intense research in computer algebra, e.g. (Faugère et al., 2010, 2013; Spaenlehauer, 2012; Gopalakrishnan et al., 2024; Gopalakrishnan, 2024), with many applications in cryptography, e.g. (Kipnis and Shamir, 1999; Faugère et al., 2008; Bardet et al., 2020a,b; Bardet and Bertin, 2022; Faugère et al., 2015), or real algebraic geometry (Gopalakrishnan et al., 2024; Henrion et al., 2016).

The case of the MinRank problem where the target rank is 0 is computationally easy (it reduces to the computation of a null space). Since Problem 1 corresponds to the next possibility for the target rank, we expect it to be more tractable than the general MinRank problem. However, in Section 3 we show that over fixed finite fields, there is an NP-complete decision problem that is a special case of REP. Over arbitrary fixed fields, the same construction yields NP-hardness, subject to the usual assumptions on the representation of field elements. Nonetheless, in Section 4, we show that tractability results on the general MinRank problem give many ranges of the parameters k, m and n, for which we expect to be able to solve REP efficiently.

We achieve these concrete tractability results by reducing REP to MinRank instances of rank 1. The complexity of REP is then investigated by considering the determinantal ideal $\mathcal{I}_{\text{REP}} = \mathcal{I}_{\text{Minors}(2)} \subset \mathbb{K}[x_1, \ldots, x_m]$ generated by the rank 2 minors of a linear matrix derived from the input matrices of a REP instance. Extending classical results on the complexity of solving MinRank with determinantal ideals (Faugère et al., 2010, 2013), and under some genericity assumptions, we provide new bounds on the algorithmic hardness of REP:

- When $m > (k-1)(n-1)$, then the determinantal ideal $\mathcal{I}_{\text{REP}}$ corresponding to REP has positive dimension. Generically, the maximal degree in a reduced Gröbner basis of $\mathcal{I}_{\text{REP}}$ is n.
- The well-defined case occurs when $m = (k-1)(n-1)$. Generically, the problem has finitely many solutions, $\prod_{i=0}^{n-2} \frac{i!(k+i)!}{(n-1-i)!(k-1+i)!}$, assuming $n \le k$, and the degree of regularity of $\mathcal{I}_{\text{REP}}$ is n.
- Finally, $m < (k-1)(n-1)$ is called the over-determined case. Using a determinantal variant of Fröberg's Conjecture (see (Spaenlehauer, 2012), Conjecture 4.11), we provide an explicit formula for the Hilbert series, i.e.

$$\mathbf{HS}_{\mathbb{K}[x_1,\ldots,x_m]/\mathcal{I}_{\text{REP}}}(t) = \left[(1-t)^{(k-1)(n-1)} \frac{C^{k,n}(t)}{(1-t)^m} \right]_+ ,$$

with $C^{k,n}(t) = \sum_{\ell \in \mathbb{N}} \binom{k-i}{\ell}\binom{n-j}{\ell} t^{\ell}$.

We also provide concrete ranges of the parameters for which we can show that generic instances of REP can be solved in polynomial-time. In particular, Proposition 4 shows that REP can be solved in polynomial-time in several cases once they are slightly over-defined. Recently, (Gopalakrishnan et al., 2024; Gopalakrishnan, 2024) proposed improved complexity results for determinantal ideals generated by maximal minors. In some sense, we consider here the opposite situation by considering determinantal ideals generated by minimal rank minors.

In Subsection 4.1 we apply our results on four different instances arising from different problems in computational group theory. We show both theoretically and confirm experimentally that these instances can be efficiently solved, thus providing simpler, alternative methods for tackling these problems.

In the final section of the paper, we return to the role of REP in concrete embedding problems for finite groups into Lie groups of exceptional type. In such applications, every embedding corresponds to a solution of a relative eigenvector problem, but the converse need not hold: REP may admit *spurious* solutions that do not yield valid embeddings.

We show how algebraic information obtained from a spurious relative eigenvector can be used to construct additional polynomial constraints that refine the original REP instance. These constraints arise naturally from representation-theoretic conditions (such as submodule multiplicities) and can be expressed as explicit homogeneous polynomial equations. Augmenting the REP ideal with these equations leads to a strictly smaller solution variety that eliminates the spurious solutions while preserving all genuine ones.

This refined approach is illustrated in detail by a case study involving embeddings of the alternating group A_6 into a Lie group of type F_4. We demonstrate that, although the initially constructed relative eigenvector problem yields high-dimensional solution sets, the addition of representation-theoretically motivated constraints reduces the problem to a manageable collection of components that can be analyzed explicitly. This provides a practical computational framework for embedding problems where REP supplies necessary but not sufficient conditions.

2. Preliminaries

In this section, we explain the relationship between REP and the MinRank problem and introduce notation used throughout this paper.

$\mathbb{K}$ will denote a finite field, $\mathbb{K}[x_1, \dots, x_m]$ the polynomial ring in m variables, and $\mathcal{M}_{k\times n}(\mathbb{K})$ (resp. $\mathcal{M}_{k\times n}(\mathbb{K}[x_1, \dots, x_m])$) will refer to the set of $k \times n$ matrices with coefficients in $\mathbb{K}$ (resp. in $\mathbb{K}[x_1, \dots, x_m]$). Vectors and matrices will be denoted using bold letters.

The degree and degree of regularity of an ideal play a crucial role in estimating the complexity of computing a Gröbner basis for the ideal. In the case of a zero-dimensional homogeneous ideal, they can be computed directly from its Hilbert series. For precise definitions and statements, we refer the reader to Appendix A.

2.1. The MinRank problem and its relation to REP

The Relative Eigenvector Problem (REP) defined in Problem 1 is closely related to the MinRank problem (Buss et al., 1999; Courtois, 2001).

Problem 2 *(*MinRank *problem).* Given a set of m matrices $\mathbf{A}_1, \dots, \mathbf{A}_m \in \mathcal{M}_{k\times n}(\mathbb{K})$ and an integer $r < \min(k, n)$, find a nonzero vector $(\beta_1, \dots, \beta_m) \in \mathbb{K}^m$ such that

$$\operatorname{Rank}\left(\sum_{i=1}^{m} \beta_i \mathbf{A}_i\right) \le r.$$

For complexity-theoretic purposes, we also consider the associated *MinRank decision problem*, which asks whether there exists a nonzero vector $(\beta_1, \dots, \beta_m) \in \mathbb{K}^m$ satisfying the above rank condition.

Similarly, we define the $\mathbb{K}$-rational decision REP as the question of whether there exists a nonzero vector $x \in \mathbb{K}^m$ satisfying the defining condition of REP.

We fix the field $\mathbb{K}$ throughout and do not treat it as part of the input for either MinRank or REP. The following lemma shows that the $\mathbb{K}$-rational decision REP is equivalent to the MinRank decision problem with target rank 1.

Lemma 1. *Let $(\mathbf{A}_1, \dots, \mathbf{A}_k)$ be a k-tuple of matrices in $\mathcal{M}_{m\times n}(\mathbb{K})$. Define matrices $\mathbf{B}_1, \dots, \mathbf{B}_m$ in $\mathcal{M}_{k\times n}(\mathbb{K})$ by*

$$(\mathbf{B}_i)_{\ell,j} = (\mathbf{A}_\ell)_{i,j},$$

i.e., $\mathbf{B}_i$ consists of the i-th rows of the matrices $\mathbf{A}_1, \dots, \mathbf{A}_k$. Then $\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{K}^m$ is a relative eigenvector for $(\mathbf{A}_1, \dots, \mathbf{A}_k)$ if and only if $\mathbf{x} \neq 0$ and

$$\operatorname{Rank}\left(\sum_{i=1}^{m} x_i \mathbf{B}_i\right) \le 1,$$

i.e., if and only if $\mathbf{x}$ *is a solution to the MinRank problem for the matrices* $\mathbf{B}_1, \ldots, \mathbf{B}_m$ *with target rank* 1.

Proof. By definition, a nonzero vector $\mathbf{x} \in \mathbb{K}^m$ is a relative eigenvector for $(\mathbf{A}_1, \ldots, \mathbf{A}_k)$ if and only if the vectors $\mathbf{x}\mathbf{A}_1, \ldots, \mathbf{x}\mathbf{A}_k$ are all proportional, i.e., they span a subspace of $\mathbb{K}^n$ of dimension at most one. Thus, there exist scalars $\lambda_1, \ldots, \lambda_k \in \mathbb{K}$ and a vector $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{K}^n$ such that

$$\mathbf{x}\mathbf{A}_\ell = \lambda_\ell \mathbf{y} \quad \text{for all } \ell = 1, \ldots, k.$$

In coordinates, this means that for all $1 \le \ell \le k$ and $1 \le j \le n$,

$$\sum_{i=1}^m x_i (\mathbf{A}_\ell)_{i,j} = \lambda_\ell y_j.$$

Using the definition of $\mathbf{B}_i$, this becomes

$$\sum_{i=1}^m x_i (\mathbf{B}_i)_{\ell,j} = \lambda_\ell y_j.$$

Hence, the ℓ-th row of the matrix $\sum_{i=1}^m x_i \mathbf{B}_i$ is equal to $\lambda_\ell \mathbf{y}$, and every row is a scalar multiple of $\mathbf{y}$. Therefore,

$$\operatorname{Rank}\left(\sum_{i=1}^m x_i \mathbf{B}_i\right) \le 1.$$

Conversely, if $\operatorname{Rank}\left(\sum_{i=1}^m x_i \mathbf{B}_i\right) \le 1$, then all rows of this matrix are proportional to some vector $\mathbf{y} \in \mathbb{K}^n$. Thus there exist scalars $\lambda_\ell \in \mathbb{K}$ such that the ℓ-th row equals $\lambda_\ell \mathbf{y}$, which yields

$$\sum_{i=1}^m x_i (\mathbf{B}_i)_{\ell,j} = \lambda_\ell y_j$$

for all ℓ, j. Rewriting in terms of $\mathbf{A}_\ell$, we recover

$$\mathbf{x}\mathbf{A}_\ell = \lambda_\ell \mathbf{y},$$

showing that $\mathbf{x}$ is a relative eigenvector.

This construction yields a linear-time reduction from the $\mathbb{K}$-rational decision REP to the MinRank decision problem with target rank 1. $\square$

Remark 1. The construction in Lemma 1 is invertible: given matrices $\mathbf{B}_1, \ldots, \mathbf{B}_m \in \mathcal{M}_{k \times n}(\mathbb{K})$, one recovers $\mathbf{A}_1, \ldots, \mathbf{A}_k \in \mathcal{M}_{m \times n}(\mathbb{K})$ by setting $(\mathbf{A}_\ell)_{i,j} = (\mathbf{B}_i)_{\ell,j}$. Thus, the construction defines a bijection between instances of the $\mathbb{K}$-rational decision REP and instances of the MinRank decision problem with target rank 1, under which the sets of solutions coincide. In particular, this shows that the MinRank decision instances arising from this construction are not a restricted subclass.

Remark 1 shows that the $\mathbb{K}$-rational decision version of REP is equivalent to the MinRank decision problem with target rank 1. In particular, structural and complexity results for one problem translate directly to the other.

For example, (Wong, 1974) shows that REP can be solved in polynomial time when applied to $k = 2$ matrices whose entries lie in a finite field. This implies that MinRank with target rank 1 is polynomial-time solvable for instances whose input consists of matrices in $\mathcal{M}_{2 \times n}(\mathbb{K})$, where $\mathbb{K}$ is finite.

The formulation of REP is closely related to eigenvalue problems, for which it is standard to consider solutions over field extensions of $\mathbb{K}$. This naturally leads to the question of how MinRank behaves under field extensions. We may consider solutions to REP over a field L satisfying $\mathbb{K} \subseteq L \subseteq \overline{\mathbb{K}}$.

We refer to this as the L-rational form of REP, in which one asks for a nonzero vector $\mathbf{x} \in L^m$ satisfying the defining condition.

The proof of Lemma 1 applies verbatim over L, and shows that the L-rational form of REP is equivalent to a MinRank instance in which the matrices $\mathbf{B}_1, \dots, \mathbf{B}_m$, originally defined over $\mathbb{K}$, are regarded as elements of $\mathcal{M}_{k\times n}(L)$.

A field extension may introduce additional relative eigenvectors, and thus may change the feasibility of the corresponding MinRank instance. For example, the matrix

$$\mathbf{A}_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

has no eigenvectors over $\mathbb{R}$, but has eigenvectors over $\mathbb{C}$. Let

$$\mathbf{A}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then the pair $(\mathbf{A}_1, \mathbf{A}_2)$ admits no solution to REP that has entries in $\mathbb{R}$, but does admit a solution defined over $\mathbb{C}$.

Applying the construction of Lemma 1, we obtain matrices

$$\mathbf{B}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \mathbf{B}_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

for which the associated MinRank instance with target rank 1 is infeasible over $\mathbb{R}$, but feasible over $\mathbb{C}$. This shows that feasibility of MinRank is not invariant under extension of the base field.

2.2. Known methods for solving MinRank

Although the MinRank problem is NP-hard over finite fields (Buss et al., 1999), efficient methods have been proposed for solving many instances. The fastest known algorithms are algebraic: they reduce the problem to solving systems of polynomial equations. These methods fall into three main categories: Kipnis-Shamir modeling, Minors modeling, and Support-Minors modeling (Kipnis and Shamir, 1999; Faugère et al., 2008, 2010; Bardet et al., 2020b).

2.2.1. Kipnis-Shamir modeling

In (Kipnis and Shamir, 1999), it was proposed to model the MinRank problem as a bilinear system of equations of the form

$$\begin{pmatrix} 1 & & & x_{1,1} & \dots & x_{1,r} \\ & \ddots & & \vdots & & \vdots \\ & & 1 & x_{k-r,1} & \dots & x_{k-r,r} \end{pmatrix} \cdot \sum_{i=1}^{m} \beta_i \mathbf{A}_i = \mathbf{0}_{(k-r)\times n},$$

where the matrix on the left is an unknown basis of the left kernel of $\sum_{i=1}^{m} \beta_i \mathbf{A}_i$, of dimension $k-r$. This basis is given in systematic form to ensure independence of the found vectors and to reduce the number of variables and can be shown to exist with high probability. The original work of (Kipnis and Shamir, 1999) used linearization to solve this algebraic system. The approach was later improved (Faugère et al., 2008; Spaenlehauer, 2012) resulting in an upper bound of the complexity of $O\left(\binom{d_{\mathrm{reg}} + (k-r)r + m}{d_{\mathrm{reg}}}^{\omega}\right)$ where d_{reg} is bounded by $\min((k-r)r, m) + 1$.

In (Verbel et al., 2019), this bound was significantly improved in the so-called "superdetermined" case when $m < rn$. They show that the equations in the Kipnis-Shamir model contain additional structure by explicitly constructing syzygies that lead to degree falls and subsequently to improved complexity. For example, when $n = m = k$ their analysis provides quadratic speedup compared to previous results.

2.2.2. Minors modeling

Alternatively, MinRank is equivalent to finding a vector $(\beta_1, \ldots, \beta_m) \in \mathbb{K}^m$ such that all minors of size $r+1$ of the matrix $\sum_{i=1}^m \beta_i \mathbf{A}_i$ are zero. We then have to solve a multivariate polynomial system of $\binom{n}{r+1}^2$ equations in m variables as shown in (Faugère et al., 2008, 2010). Compared with the Kipnis-Shamir modeling, this formulation has more equations, fewer variables, and equations of higher degree.

In particular, the authors (Faugère et al., 2010, 2013) consider determinantal ideals, i.e. ideals generated by the minors of rank $(r+1)$ of a matrix $\mathbf{M}(x_1, \ldots, x_m) \in \mathcal{M}_{k\times n}(\mathbb{K}[x_1, \ldots, x_m])$. They give precise formulas for computing the degree and degree of regularity of determinantal ideals, by providing explicitly their Hilbert series.

2.2.3. Support-minors modeling

Inspired by techniques in coding theory, (Bardet et al., 2020b) proposed the following algebraic model.

Suppose $\mathbf{C}$ is an (unknown) $r \times n$ basis matrix of the row space of $\sum_{i=1}^m \beta_i \mathbf{A}_i$ (assuming the MinRank problem has a solution). Assume further that $\mathbf{C}_i$, where $i \in C(n,r)$ are all (unknown) minors of order r of $\mathbf{C}$.

Then the matrix $\mathbf{C}_i = \begin{pmatrix} \mathbf{a}_i \\ \mathbf{C} \end{pmatrix}$, for all $1 \leqslant i \leqslant k$, has rank r, and we can make equations by equating all $r+1$ minors of $\mathbf{C}_i$ to 0. Considering $\mathbf{C}_i$, $i \in C(n,r)$ and β_j, $1 \leqslant j \leqslant m$ as unknowns, we obtain $k\binom{n}{r+1}$ bilinear equations in the two sets of unknowns.

Observe that the number of monomials is $m\binom{n}{r}$, which is relatively small compared with the number of equations. This means that for a wide range of parameters, we can determine an upper bound on the complexity by posing conditions for direct linearization at a different degree. For example, if we expect a unique solution of the MinRank problem, we expect to be able to solve the Support-Minors modeling by direct linearization if $k\binom{n}{r+1} \geqslant m\binom{n}{r} - 1$.

3. A relative eigenvector decision problem is NP-complete

In this section we introduce RED, a restricted decision version of the relative eigenvector problem. We prove that RED is NP-hard. Throughout, the field $\mathbb{K}$ is considered fixed, and is not treated as part of the input.

Problem 3 *(Relative Eigenvector Decision (*RED*)).* Given k matrices of size $m \times n$ with entries in the field $\mathbb{K}$, does there exist a relative eigenvector whose first coordinate is 1 and whose other coordinates belong to $\{0, 1\}$?

RED is more strictly constrained than $\mathbb{K}$-rational decision REP. When $\mathbb{K} = GF(2)$, the $\{0, 1\}$ constraint is automatic, but the condition that $x_1 = 1$ in a relative eigenvector $\mathbf{x}$ remains an additional requirement. In particular, even in the case $\mathbb{K} = GF(2)$, the restriction is nontrivial, since it requires the existence of a solution whose first coordinate is equal to 1. We emphasize that our proof of NP-hardness of RED does not establish a similar result for $\mathbb{K}$-rational decision REP, whose complexity remains open.

If elements of the field $\mathbb{K}$ are represented so that field operations (addition, multiplication, and testing for equality) can be performed in time polynomial in the input size, then RED lies in NP. Indeed, a certificate is given by a vector $\mathbf{x} \in \{0, 1\}^m$, and verification can be carried out in polynomial time by checking that $\mathbf{x}$ satisfies the requirements of a relative eigenvector together with the imposed constraints. The number of field operations needed is bounded by a polynomial in the dimensions of the input matrices, so the size of all intermediate values remains polynomially bounded. The assumption on complexity of field operations holds, for example, for finite fields with standard representations.

We give a full proof that RED is NP-complete when $\mathbb{K} = GF(2)$. We also give a complete example that illustrates the reduction used in our proof. After the proof we indicate how the argument can be adjusted to show that if we fix any field $\mathbb{K}$, Problem RED is NP-hard.

When $\mathbb{K} = GF(2)$, input for an instance of RED is a set of boolean matrices, $\mathbf{A}_1, \mathbf{A}_2, \ldots \mathbf{A}_k$. (As usual, we identify the binary digits 1 and 0 with the respective boolean values *true* and *false*.) The problem asks whether there exist $1 \times m$ and $1 \times n$ boolean vectors, which we write as $\mathbf{x}$ and $\mathbf{y}$, such that for each index i, the vector $\mathbf{x}\mathbf{A}_i$ is either $\mathbf{y}$ or $\mathbf{0}$.

Theorem 1. *Over the field $\mathbb{K} = GF(2)$, Problem* RED *belongs to the class NPC.*

To prove the theorem we exhibit a polynomial reduction from the NPC problem CNF SAT to the problem RED.

Problem 4 *(CNF SAT).* Is there a truth assignment that satisfies a boolean formula given in conjunctive normal form (CNF)?

A formula in CNF is a conjunction of c clauses, each of which is a disjunction of terms. The formula contains b terms that are selected from a set of a variables and their negations. The following is an example with $c = 2$ clauses, $a = 4$ variables, and $b = 5$ terms:

$$(X_1 \vee \overline{X_2} \vee X_3) \wedge (\overline{X_1} \vee X_4). \tag{1}$$

Given a truth assignment $X_1 = s_1, X_2 = s_2, \ldots X_a = s_a$, for a CNF formula, we shall associate an *assignment vector* in $GF(2)^{2a+1}$. The entries of the assignment vector are

$$(1, s_1, \overline{s_1}, s_2, \overline{s_2}, \ldots, s_a, \overline{s_a}).$$

If the truth assignment satisfies the CNF formula, we call its assignment vector a *satisfying vector*. For example, from the satisfying assignment $X_1 = X_2 = X_3 = X_4 = true$ for formula (1), we obtain a satisfying vector $(1, 1, 0, 1, 0, 1, 0, 1, 0)$.

We shall refer to the *partial clauses* $Z_1, Z_2, \ldots, Z_b$ of a CNF formula. A partial clause is an initial segment of one of the clauses in the formula. For example, the 5 partial clauses in formula (1) are:

$$X_1,\ (X_1 \vee \overline{X_2}),\ (X_1 \vee \overline{X_2} \vee X_3),\ \overline{X_1},\ (\overline{X_1} \vee X_4).$$

Clearly, there are b partial clauses in a CNF formula that has b terms, because there is a bijection that maps each partial clause to its last term.

From an instance of CNF SAT that is given by a formula that uses a variables, b terms, and c clauses we construct a corresponding instance of RED, which uses $k = 1 + a + b + c$ boolean matrices with $m = (b+1)(2a+1)$ rows and $n = 2a+2$ columns. We show that the instance of CNF SAT has a solution if and only if the corresponding instance of RED has one.

The matrices $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_k$ that we use are tall and thin. Each has $2a+2$ columns. It is convenient to imagine these columns as divided into two *slices* with widths $2a+1$ and 1. It is also helpful to imagine that the $(b+1)(2a+1)$ rows of the matrix are divided into $1+b$ *blocks* of size $2a+1$. In this way each block of the left slice of a matrix $\mathbf{A}_i$ is a square submatrix of size $(2a+1) \times (2a+1)$. We index the blocks of our matrices with the sequence $0, 1, 2, \ldots, b$. Within each block, we label the rows as $0, 1, 1', 2, 2', \ldots, a, a'$.

We write $\mathbf{x}$ for a putative relative eigenvector of $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_k$ that has a first entry of 1. The row vector $\mathbf{x}$ has size $1 \times (b+1)(2a+1)$. We partition it into blocks $(\mathbf{x_0}, \mathbf{x_1}, \ldots, \mathbf{x_b})$, where each block $\mathbf{x_i}$ is a $1 \times (2a+1)$ vector. We write the entries of the block $\mathbf{x_0}$ as $x_{0,0} = 1, x_{0,1}, x_{0,1'}, x_{0,2}, x_{0,2'}, \ldots x_{0,a'}$ with the indices chosen to match those of the rows of the first block of a $(b+1)(2a+1) \times (2a+2)$ matrix, such as $\mathbf{A}_1$.

We shall choose the matrices $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_k$ to force the blocks of $\mathbf{x}$ to have the form:

$$(\mathbf{x_0}, z_1\mathbf{x_0}, z_2\mathbf{x_0}, \ldots, z_b\mathbf{x_0})$$

where $\mathbf{x_0}$ is the satisfying vector determined by a solution of the CNF formula under consideration, and $z_1, z_2, \ldots z_b$ are scalars that give the values of the partial clauses of the CNF formula when evaluated at that solution. Moreover, all of the matrices that we define map such a vector to an image proportional to a vector $\mathbf{y}$ that has slices $(\mathbf{x_0} \mid 0)$.

Each matrix $\mathbf{A}_i$ has a single copy of the identity $\mathbf{I}_{2a+1}$ in its left slice. This occupies the full width of the slice. Its vertical position aligns with one of the blocks of rows. The right slice has a few isolated entries of 1 and the other entries are all zero. We define each of the matrices by giving a picture in which zero entries are normally omitted. Our pictures have arrows at the right to give the positions of any non-zero entries in the right slice. We use arrows at the left to indicate the block occupied by the copy of the identity matrix in the left slice. Each matrix $\mathbf{A}_i$ has many rows that contain only 0 entries — these rows are omitted from our pictures. This means that our pictures are compact.

As a small example to illustrate how to read our pictures, we suppose that a is 2 and b is 1. Here, a $(b+1)(2a+1) \times (2a+2)$ matrix such as A_i has size 10×6. For example, one of these matrices might be:

$$
\begin{array}{ccccc|c}
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
\hline
1 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0
\end{array}
$$

we may specify this matrix with the following compact picture.

$$
\begin{array}{rcccc|cl}
 & & & & & 1 & \leftarrow (0,1') \\
\text{block } 1 \rightarrow & 1 & & & & 1 & \leftarrow (1,0) \\
\rightarrow & & 1 & & & & \\
\rightarrow & & & & & 1 & \leftarrow (1,2) \\
\rightarrow & & & & 1 & &
\end{array}
$$

The picture specifies a 10×6 matrix that divides into 2 vertical slices, each of which is subdivided into $b+1=2$ blocks (we omit the horizontal line). An identity matrix appears as the second block of the left slice (as indicated by the zero-based indexing label at the left of our picture). The right slice is a column vector with only three non-zero entries. These correspond to the three arrows at the right of the picture. For example, the arrow marked $(1,2)$ shows that in the second block (indexed by 1), the entry in the fourth row (indexed by 2) is 1. (Recall that when $a=2$, the rows of each block are indexed as $0, 1, 1', 2, 2'$.)

We now construct the required matrices $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_k$. The first matrix $\mathbf{A}_1$ has the following picture. (We have included some 0 entries to indicate that there is a right slice. In later pictures we omit all entries that are 0.)

$$
\begin{array}{rcccc|c}
\text{block } 0 \rightarrow & 1 & & & & 0 \\
\rightarrow & & 1 & & & 0 \\
\rightarrow & & & \cdots & & \\
\rightarrow & & & & 1 & 0 \\
 & & & \cdots & &
\end{array}
$$

Observe that the image $\mathbf{x}\mathbf{A}_1$ is the non-zero vector $\mathbf{y} = (\mathbf{x_0} \mid 0)$. Since all nonzero images must equal $\mathbf{y}$, whose last coordinate is 0, it follows that every image $\mathbf{x}\mathbf{A}_i$ has last coordinate 0.

Our next a matrices are chosen to force $\mathbf{x_0}$ to be an assignment vector for the instance of CNF SAT under consideration. The j^{th} of these matrices has the following picture.

$$
\begin{array}{r ccccc | r l}
\text{block } 0 \rightarrow & 1 & & & & & -1 & \leftarrow (0,0) \\
\rightarrow & & 1 & & & & & \\
\rightarrow & & \dots & & & & & \\
\rightarrow & & & 1 & & & 1 & \leftarrow (0,j) \\
\rightarrow & & & & 1 & & 1 & \leftarrow (0,j') \\
\rightarrow & & & & & & & \\
\rightarrow & & & & & 1 & & \\
 & & \dots & & & & &
\end{array}
$$

The entry written -1 that appears in the first row of the matrix is read as 1 since it belongs to $GF(2)$. Later, when we generalize to other fields, the value -1 is used. Since the image of $\mathbf{x}$ under this matrix ends with a 0 coordinate, we have $x_{0,j} + x_{0,j'} = 1$. It follows that the adjacent entries $x_{0,j}$ and $x_{0,j'}$ of the block $\mathbf{x_0}$ are boolean complements. In other words, $\mathbf{x_0}$ is the assignment vector for the truth assignment $X_1 = x_{0,1}, X_2 = x_{0,2}, \dots X_a = x_{0,a}$.

Our next b matrices correspond to partial clauses. A partial clause Z_i is either a disjunction $Z_i = Z_{i-1} \vee T_i$, where T_i is a term and Z_{i-1} is the previous partial clause, or it is a single term T_i. In both cases, T_i is either a variable X_j, or the negation of a variable $\overline{X_j}$. Let $h = j$ if $T_i = X_j$, and $h = j'$ if $T_i = \overline{X_j}$. The matrix that corresponds to the partial clause Z_i has the following picture. (We omit the entries of the second slice with indices $(i-1, 0)$ and $(i-1, h)$ for any partial clause with only a single term T_i.)

$$
\begin{array}{r ccc | r l}
 & & & & -1 & \leftarrow (0,h) \\
 & & & & -1 & \leftarrow (i-1,0) \\
 & & & & 1 & \leftarrow (i-1,h) \\
\text{block } i \rightarrow & 1 & & & 1 & \leftarrow (i,0) \\
\rightarrow & & 1 & & & \\
\rightarrow & & & & & \\
\rightarrow & & & 1 & &
\end{array}
$$

Since the left slice of the image of $\mathbf{x}$ under this matrix is a scalar multiple of $\mathbf{x_0}$, we find that $\mathbf{x_i} = z_i \mathbf{x_0}$, for some scalar z_i. Moreover, since the right slice of the image is 0, we have $z_i = z_{i-1} + x_{0,h} - z_{i-1}x_{0,h}$. It follows that $z_i = z_{i-1} \vee x_{0,h}$. Now, $x_{0,h}$ is the value of T_i when $X_1, X_2, \dots X_a$ are given the values $x_{0,1}, x_{0,2}, \dots x_{0,a}$. An obvious induction shows that z_i is the value of the partial clause Z_i, when $X_1, X_2, \dots, X_a$ are given these values.

Our last c matrices correspond to the (complete) clauses. If the i^{th} clause arises as the j^{th} partial clause Z_j, then the corresponding matrix is:

$$
\begin{array}{r cccc | r l}
\text{block } 0 \rightarrow & 1 & & & & -1 & \leftarrow (0,0) \\
\rightarrow & & 1 & & & & \\
\rightarrow & & & \dots & & & \\
\rightarrow & & & & 1 & & \\
 & & & \dots & & & \\
 & & & & & 1 & \leftarrow (j,0) \\
 & & & \dots & & &
\end{array}
$$

The last column of this matrix shows that if $\mathbf{x}$ is a relative eigenvector for our matrices, then $z_j = 1$. However, z_j is the value obtained when Z_j, which is the i^{th} clause, is computed using the values $X_1 = x_{0,1}, X_2 = x_{0,2}, \dots X_a = x_{0,a}$. In other words, this assignment makes the i^{th} clause true. Since this is the case for all clauses, $\mathbf{x_0}$ is a satisfying vector for the CNF formula under consideration.

We have now shown that the map from an instance of CNF SAT to the instance of RED given by the set of $k = 1+a+b+c$ matrices defined above is a reduction. We finish by observing that the reduction can be computed in polynomial time. The computation requires only the inspection of the input formula and then the output of matrices. The output uses $(1+a+b+c) \times (b+1)(2a+1) \times (2a+2)$ bits to write the matrices. This is bounded by a polynomial in the length b of the CNF formula since both a and c are bounded by b. $\square$

We remark that the boolean values true and false correspond to the entries 1 and 0 of any field. The boolean expressions $x \wedge y$ and $x \vee y$ are represented by arithmetic expressions xy and $x + y - xy$. Accordingly, if we modify the proof of Theorem 1 to view the entries of the $k = 1 + a + b + c$ matrices $\mathbf{A}_1, \mathbf{A}_2, \dots \mathbf{A}_k$ as the elements $\{0, 1, -1\}$ of a field $\mathbb{K}$ of arbitrary characteristic, we obtain a proof that over $\mathbb{K}$, RED belongs to the class NPH.

We now illustrate the reduction concretely on a small instance. We consider the CNF SAT formula

$$(X_1 \vee \overline{X_2}) \wedge X_2, \tag{2}$$

that has $c = 2$ clauses, $a = 2$ variables, and $b = 3$ terms. The corresponding instance of RED has $8 = 1 + a + b + c$ matrices, $\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_8$ as input. Each matrix has size $(b+1)(2a+1) \times (2a+2) = 20 \times 6$. The matrices are partitioned into $b + 1 = 4$ blocks of rows and 2 slices of columns. In this way, each matrix is formed from submatrices with the following dimensions:

$$\left[\begin{array}{c|c} 5\times 5 & 5\times 1 \\ \hline 5\times 5 & 5\times 1 \\ \hline 5\times 5 & 5\times 1 \\ \hline 5\times 5 & 5\times 1 \end{array}\right]$$

Every 5×5 submatrix in a left slice is either the identity $\mathbf{1}$ or the zero matrix $\mathbf{0}$. The 5×1 submatrices that are used to define the right slices are combinations of: $0 = (0, 0, 0, 0, 0)^T$, $\gamma = (1, 0, 0, 0, 0)^T$, $\alpha_2 = (0, 1, 1, 0, 0)^T$, $\alpha_3 = (0, 0, 0, 1, 1)^T$, $\beta_1 = (0, 1, 0, 0, 0)^T$, $\beta_2 = (0, 0, 0, 0, 1)^T$, and $\beta_3 = (0, 0, 0, 1, 0)^T$. (The positions of the non-zero coordinates in $\beta_1, \beta_2, \beta_3$ correspond to the positions of the three terms X_1, $\overline{X_2}$, and X_2 in the sequence $1, X_1, \overline{X_1}, X_2, \overline{X_2}$.)

The matrices we consider are:

$$\mathbf{A}_1 = \left[\begin{array}{c|c} \mathbf{1} & 0 \\ \hline \mathbf{0} & 0 \\ \hline \mathbf{0} & 0 \\ \hline \mathbf{0} & 0 \end{array}\right] \quad \mathbf{A}_2 = \left[\begin{array}{c|c} \mathbf{1} & \alpha_2 - \gamma \\ \hline \mathbf{0} & 0 \\ \hline \mathbf{0} & 0 \\ \hline \mathbf{0} & 0 \end{array}\right] \quad \mathbf{A}_3 = \left[\begin{array}{c|c} \mathbf{1} & \alpha_3 - \gamma \\ \hline \mathbf{0} & 0 \\ \hline \mathbf{0} & 0 \\ \hline \mathbf{0} & 0 \end{array}\right]$$

$$\mathbf{A}_4 = \left[\begin{array}{c|c} \mathbf{0} & -\beta_1 \\ \hline \mathbf{1} & \gamma \\ \hline \mathbf{0} & 0 \\ \hline \mathbf{0} & 0 \end{array}\right] \quad \mathbf{A}_5 = \left[\begin{array}{c|c} \mathbf{0} & -\beta_2 \\ \hline \mathbf{0} & -\gamma + \beta_2 \\ \hline \mathbf{1} & \gamma \\ \hline \mathbf{0} & 0 \end{array}\right] \quad \mathbf{A}_6 = \left[\begin{array}{c|c} \mathbf{0} & -\beta_3 \\ \hline \mathbf{0} & 0 \\ \hline \mathbf{0} & 0 \\ \hline \mathbf{1} & \gamma \end{array}\right]$$

$$\mathbf{A}_7 = \left[\begin{array}{c|c} \mathbf{1} & -\gamma \\ \hline \mathbf{0} & 0 \\ \hline \mathbf{0} & \gamma \\ \hline \mathbf{0} & 0 \end{array}\right] \quad \mathbf{A}_8 = \left[\begin{array}{c|c} \mathbf{1} & -\gamma \\ \hline \mathbf{0} & 0 \\ \hline \mathbf{0} & 0 \\ \hline \mathbf{0} & \gamma \end{array}\right]$$

Any relative eigenvector $\mathbf{x}$ for the matrices $\mathbf{A}_1, \dots, \mathbf{A}_8$ is a 1×20 vector, which we divide into $b + 1 = 4$ blocks, $\mathbf{x} = (\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3)$. Here $\mathbf{x}_i$ is a 1×5 vector, for $0 \le i \le 3$. We shall divide the coordinates of any image $\mathbf{x}\mathbf{A}_i$ into two slices with sizes 1×5 and 1×1. These correspond to the two slices of $\mathbf{A}_i$. Thus, for example, we write $(\mathbf{x}_0 \mid 0)$ for the image $\mathbf{x}A_1$.

If $\mathbf{x}$ is a solution to RED, then $\mathbf{x}_0$ is non-zero since its first coordinate is 1. It follows that $\mathbf{x}\mathbf{A}_1 = (\mathbf{x}_0 \mid 0) \neq 0$. Therefore, for $1 \le i \le 8$, the image $\mathbf{x}\mathbf{A}_i$ is a scalar multiple of $(\mathbf{x}_0 \mid 0)$. In particular, in each such image the second slice is 0.

For $2 \le i \le 3$, we have $\mathbf{x}\mathbf{A}_i = (\mathbf{x}_0 \mid \mathbf{x}_0\alpha_i - 1)$. We deduce that $\mathbf{x}_0\alpha_2 = \mathbf{x}_0\alpha_3 = 1$. This means that $\mathbf{x}_0$ has the form $(1, x, \overline{x}, y, \overline{y})$ where x and y are boolean values.

Next, observe that $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ are the first slices of $\mathbf{x}A_4, \mathbf{x}A_5, \mathbf{x}A_6$. Hence, these vectors are scalar multiples of $\mathbf{x}_0$. We write $\mathbf{x}_1 = z_1\mathbf{x}_0, \mathbf{x}_2 = z_2\mathbf{x}_0, \mathbf{x}_3 = z_3\mathbf{x}_0$, where the scalars z_1, z_2, z_3 belong to the set $\{0, 1\}$.

The second slice of $\mathbf{x}A_4$ is $z_1\mathbf{x}_0\gamma - \mathbf{x}_0\beta_1 = z_1 - x$. Hence, $z_1 = x$. Similarly, the second slice of $\mathbf{x}A_5$ is $z_1\mathbf{x}_0(\beta_2 - \gamma) - \mathbf{x}_0\beta_2 + z_2\mathbf{x}_0\gamma = z_2 - z_1 - \overline{y} + z_1\overline{y}$. Hence $z_2 = z_1 \vee \overline{y} = x \vee \overline{y}$. And, the second slice of $\mathbf{x}A_6$ is $z_3\mathbf{x}_0\gamma - \mathbf{x}_0\beta_3 = z_3 - y$. Hence $z_3 = y$.

Finally, the second slices of $\mathbf{x}A_7$ and $\mathbf{x}A_8$ are $(z_2-1)\mathbf{x}_0\gamma = z_2 - 1$ and $(z_3-1)\mathbf{x}_0\gamma = z_3 - 1$. Hence, $z_2 = z_3 = 1$. In other words $(x \vee \overline{y}) \wedge y = 1$. Which shows that $X_1 = x$, $X_2 = y$ solves the CNF SAT instance given by formula (2).

4. Algorithmic hardness of the relative eigenvector problem

In this section, we study the algorithmic and practical tractability of REP (Problem 1). We conclude the section with experimental results on instances of REP that occur in some practical applications using this new connection (Section 4.1).

The reduction of REP to a MinRank problem leads to a homogeneous ideal. However, some of the experimental results provided in Section 4.1 require fixing some variables, resulting in affine polynomials. Therefore, it will be more convenient to consider the following generalization of the MinRank problem (Section 2.1):

Problem 5 *(MinRank problem, affine form).* Given a matrix $\mathbf{M}(x_1,\ldots,x_m) \in \mathcal{M}_{k\times n}(\mathbb{K}[x_1,\ldots,x_m])$ whose entries are polynomials of degree one and an integer $r < \min(k,n)$, the MinRank problem asks to find a nonzero vector $(x_1,\ldots,x_m) \in \mathbb{K}^m$ such that:

$$\operatorname{Rank}\left(\mathbf{M}(x_1,\ldots,x_m)\right) \le r. \tag{3}$$

This problem was studied in (Faugère et al., 2010) for a square matrix ($k=n$) and then extended in (Faugère et al., 2013), in particular, for rectangular matrices. Our algebraic model for REP considers the determinantal ideal $\mathcal{I}_{\text{REP}} = \mathcal{I}_{\text{Minors}(2)} \subset \mathbb{K}[x_1,\ldots,x_m]$ generated by the rank 2 minors of the matrix $\mathbf{M}_{\text{REP}}(x_1,\ldots,x_m)$ whose rows are $\mathbf{x}\mathbf{A}_1, \mathbf{x}\mathbf{A}_2, \ldots, \mathbf{x}\mathbf{A}_k$, where $\mathbf{x} = (x_1,\ldots,x_m)$. Note that if some variables x_i, $1 \le i \le m$ are fixed, the entries of $\mathbf{M}_{\text{REP}}(x_1,\ldots,x_m)$ become affine. We show that for certain values of the parameters k, m, n, a solution to a generic instance of REP can be computed in polynomial time.

Definition 1. An instance is said to be generic if there exists a multivariate polynomial h, defined on the coefficients of the polynomials of the entries of the matrix $\mathbf{M}_{\text{REP}}(x_1,\ldots,x_m)$, such that the complexity results hold for those instances for which $h \neq 0$. By the Schwartz-Zippel lemma, the probability that a randomly chosen instance over a large finite field $\mathbb{K}$ satisfies $h \neq 0$ is high, provided the degree of h is small compared to $|\mathbb{K}|$.

We identify the following parameter regimes where a solution of REP can be found in polynomial-time:

- Regime 1: If $n = m = k \ge 6$.
- Regime 2: The dimension of the ideal of minors of order 2 of $\mathbf{M}_{\text{REP}}(x_1,\ldots,x_m)$ is at least $m+2$, and the following inequality holds:
$$\binom{m+1}{2} + \binom{k-1}{2}\binom{n-1}{2} < \binom{(k-1)(n-1)}{2}.$$
- Regime 3: The dimension of the ideal of minors of size 2 of $\mathbf{M}_{\text{REP}}(x_1,\ldots,x_m)$ is one less than the number of variables and the following inequality holds:
$$n\binom{m+1}{2} - 1 \leqslant \binom{n}{2}mk - \binom{n}{3}\binom{k+1}{2}$$

The proof for Regime 3 follows the approach from (Bardet et al., 2020b):

Proposition 1. *Assuming a generic instance of REP, and a one-dimensional solution space, if*

$$n\binom{m+1}{2} - 1 \leqslant \binom{n}{2}mk - \binom{n}{3}\binom{k+1}{2}$$

REP *can be solved in time* $O\left(\left(n\binom{m+1}{2}\right)^{\omega}\right)$.

Proof. We perform linearization at degree three by multiplying the equations in the Support-Minors modeling by linear monomials in the linear variables β_j. We obtain a system of equations that is quadratic in the β_j variables and linear in the $\mathbf{C}_i$ variables. Then the condition above is exactly the condition for full linearization of the system. $\square$

To prove the Regime 1 and 2, we show that the degree of regularity is constant in those settings (see Propositions 3 and 4 below). As a consequence, computing the DRL Gröbner basis requires only polynomial time. To this end, we first provide estimates for the degree of regularity of the ideal $\mathcal{I}_{\text{REP}}$. Following (Faugère et al., 2008, 2010, 2013; Spaenlehauer, 2012), we have to distinguish three cases:

- Case $m > (k-1)(n-1)$. This is the positive dimension case. Under a genericity assumption on the entries of the matrix $\mathbf{M}_{\text{REP}}(x_1 \dots, x_m)$, the dimension of the set of solutions of REP is positive and expected to be $m-(k-1)(n-1)$.
- Case $m = (k-1)(n-1)$. This is the well-defined case where REP has finitely many solutions under a genericity assumption.
- Case $m < (k-1)(n-1)$. This is the over-determined case where we get explicit formulas for the Hilbert series but assuming a determinantal variant of Fröberg's Conjecture (see (Spaenlehauer, 2012), Conjecture 4.11).

First, we consider the complexity of REP in the zero-dimensional case, i.e. $(k-1)(n-1) \geq m$. The result below follows from (Faugère et al., 2013) by specializing the results for rank 1.

Theorem 2 *((Faugère et al., 2013), Theorem 3). Let* $m \leq (k-1)(n-1)$. *If the entries of the matrix* $\mathbf{M}_{\text{REP}}(x_1, \dots, x_m) \in \mathcal{M}_{k\times n}(\mathbb{K}[x_1, \dots, x_m])$ *are generic homogeneous linear polynomials, then the arithmetic complexity of computing a Lexicographic* (LEX) *Gröbner basis of* $\mathcal{I}_{\text{REP}}$ *is bounded by:*

$$O\left(\binom{k}{2}\binom{n}{2}\binom{d_{\text{reg}}(\mathcal{I}_{\text{REP}})+m}{m}^{\omega} + m(\text{DEG}(\mathcal{I}_{\text{REP}}))^3\right),$$

where $2 \leq \omega \leq 3$ *is a feasible exponent for the matrix multiplication. Also:*

- *If* $m = (k-1)(n-1)$, *and assuming* $n \leq k$, *then*
  - $d_{\text{reg}}(\mathcal{I}_{\text{REP}}) = deg\left(\mathbf{HS}_{\mathbb{K}[x_1,\dots,x_m]/\mathcal{I}_{\text{REP}}}(t)\right) + 1 = n$
  - $\text{DEG}(\mathcal{I}_{\text{REP}}) = \mathbf{HS}_{\mathbb{K}[x_1,\dots,x_m]/\mathcal{I}_{\text{REP}}}(1) = \prod_{i=0}^{n-2} \frac{i!(k+i)!}{(n-1-i)!(k-1+i)!}$

  with

  $$\mathbf{HS}_{\mathbb{K}[x_1,\dots,x_m]/\mathcal{I}_{\text{REP}}}(t) = C^{k,n}(t).$$
- *If* $m < (k-1)(n-1)$, *and assuming a determinantal variant of Fröberg's Conjecture (see (Spaenlehauer, 2012), Conjecture 4.11), then:*
  - $d_{\text{reg}}(\mathcal{I}_{\text{REP}}) = deg\left(\mathbf{HS}_{\mathbb{K}[x_1,\dots,x_m]/\mathcal{I}_{\text{REP}}}(t)\right) + 1$
  - $\text{DEG}(\mathcal{I}_{\text{REP}}) = \mathbf{HS}_{\mathbb{K}[x_1,\dots,x_m]/\mathcal{I}_{\text{REP}}}(1)$

  with

  $$\mathbf{HS}_{\mathbb{K}[x_1,\dots,x_m]/\mathcal{I}_{\text{REP}}}(t) = \left[(1-t)^{(k-1)(n-1)}\frac{C^{k,n}(t)}{(1-t)^m}\right]_+$$

where $C^{k,n}(t) = \sum_{\ell\in\mathbb{N}} \binom{k-i}{\ell}\binom{n-j}{\ell} t^{\ell}$ *and* $[.]_+$ *denotes the truncation of the series at its first non-positive coefficient.*

In positive dimension, the degree of regularity is not a bound of the maximal degree of polynomials in a reduced Gröbner basis of the ideal. However, it coincides with the degree of regularity obtained for the well-defined case in Theorem 2.

Lemma 2 *((Spaenlehauer, 2012), Theorem 4.18). Let $m > (k-1)(n-1)$ and assume that the entries of the matrix $\mathbf{M}_{\text{REP}}(x_1, \dots, x_m) \in \mathcal{M}_{k\times n}(\mathbb{K}[x_1, \dots, x_m])$ are generic homogeneous linear polynomials. Then, the maximal degree in a reduced Gröbner basis of $\mathcal{I}_{\text{REP}}$ is n. Also:*

$$\mathbf{HS}_{\mathbb{K}[x_1,\dots,x_m]/\mathcal{I}_{\text{REP}}}(t) = (1-t)^{(k-1)(n-1)} \frac{C^{k,n}(t)}{(1-t)^m},$$

with $C^{k,n}(t) = \sum_{\ell\in\mathbb{N}} \binom{k-i}{\ell}\binom{n-j}{\ell} t^{\ell}$.

From this result, the following complexity bound can be deduced in the case of positive dimension.

Theorem 3 *((Spaenlehauer, 2012), Theorem 4.20). Let the notations be as in Lemma 2. The arithmetic complexity of computing a Degree Reverse Lexicographic (DRL) Gröbner basis of $\mathcal{I}_{\text{REP}}$ is bounded by*

$$O\left(\binom{k}{2}\binom{n}{2}\binom{n+m}{m}^{\omega}\right), \tag{4}$$

where $2 \le \omega \le 3$ is a feasible exponent for the matrix multiplication.

Complexity when entries of $\mathbf{M}_{\text{REP}}$ are affine polynomials can be derived from the homogeneous case (Faugère et al., 2013).

Proposition 2. *Let $\mathbf{M}_{\text{REP}}(x_1, \dots, x_m) \in \mathcal{M}_{k\times n}(\mathbb{K}[x_1, \dots, x_m])$ be generic affine linear polynomials and $\mathcal{I}_{\text{REP}} = \mathcal{I}_{\text{Minors}(2)} \subset \mathbb{K}[x_1, \dots, x_m]$ be the corresponding determinantal ideal generated by the rank 2 minors.*

- *If $m = (k-1)(n-1)$, then $d_{reg}(\mathcal{I}_{\text{REP}}) \le n$.*
- *If $m < (k-1)(n-1)$, then*

  $$d_{reg}(\mathcal{I}_{\text{REP}}) \le deg(\mathbf{HS}_{\mathbb{K}[x_1,\dots,x_m]/\mathcal{I}^{(h)}_{\text{REP}}}(t)) + 1,$$

  where $\mathcal{I}^{(h)}_{\text{REP}}$ is the ideal generated by the homogenous components of highest degree in $\mathcal{I}_{\text{REP}}$.

At this point we can give a detailed proof of the existence of a polynomial-time algorithm for Regimes 1 and 2:

Proposition 3. *Let $\mathbf{M}_{\text{REP}}(x_1, \dots, x_m) \in \mathcal{M}_{k\times n}(\mathbb{K}[x_1, \dots, x_m])$ be generic linear polynomials of degree one and $\mathcal{I}_{\text{REP}} = \mathcal{I}_{\text{Minors}(2)} \subset \mathbb{K}[x_1, \dots, x_m]$ be the corresponding determinantal ideal. When $n = m = k \ge 6$, then $d_{\text{reg}}(\mathcal{I}_{\text{REP}}) = 2$ as soon as a determinantal variant of Fröberg's conjecture holds. Under these conditions,* REP *can be solved in polynomial-time.*

Proof. The proof follows from (Bettale et al., 2013) who demonstrated that the degree of regularity of $\mathcal{I}_{\text{REP}}$ is exactly 2 when $n \ge 6$. This implies that a DRL Gröbner basis of $\mathcal{I}_{\text{REP}}$ can be computed in polynomial-time (Theorem 2). $\square$

Proposition 4. *Let the notations be as in Proposition 3. Assume that $k, n \ge 3$, $(k-1)(n-1) - m \ge 2$ and:*

$$\binom{m+1}{2} + \binom{k-1}{2}\binom{n-1}{2} < \binom{(k-1)(n-1)}{2}$$

then $d_{\text{reg}}(\mathcal{I}_{\text{REP}}) = 2$ as soon as a determinantal variant of Fröberg's conjecture holds. Under these conditions, REP *can be solved in polynomial-time.*

Proof. In the over-determined case, we know from Theorem 2 that d_{reg} can be computed as $\deg(\mathbf{HS}_{\mathbb{K}[x_1,\ldots,x_m]/\mathcal{I}_{\text{REP}}})+1$ where

$$\mathbf{HS}_{\mathbb{K}[x_1,\ldots,x_m]/\mathcal{I}_{\text{REP}}} = [(1-t)^{(k-1)(n-1)-m}\, C^{k,n}(t)]_{+}.$$

Therefore, the degree of regularity is 2 if and only if the coefficient of t^2 is the first non-positive coefficient.

Since $k-1 \geq 2, n-1 \geq 2$ and $(k-1)(n-1)-m \geq 2$, we have

$$(1-t)^{(k-1)(n-1)-m}\, C^{k,n}(t) = \big[1 - \big((k-1)(n-1)-m\big)t + \binom{(k-1)(n-1)-m}{2}t^2 + o(t^3)\big] \cdot \big[1+(k-1)(n-1)t + \frac{1}{4}(k-1)(k-2)(n-1)(n-2)t^2 + o(t^3)\big]$$

Consequently, the coefficient of t is

$$(k-1)(n-1) - \big((k-1)(n-1)-m\big) > 0.$$

The coefficient of t^2 is

$$\frac{1}{4}(k-1)(k-2)(n-1)(n-2) + \frac{1}{2}\big((k-1)(n-1)-m\big)\cdot\big((k-1)(n-1)-(m+1)\big) - (k-1)(n-1)\big((k-1)(n-1)-m\big) = (k-1)(n-1) \left[\frac{1}{4}(k-2)(n-2) + \frac{1}{2}\big((k-1)(n-1)-2m-1\big) - \big((k-1)(n-1)-m\big)\right] + \frac{1}{2}m(m+1) = (k-1)(n-1) \cdot \left[\frac{1}{4}(k-2)(n-2) - \frac{1}{2}(k-1)(n-1) - \frac{1}{2}\right] + \frac{1}{2}m(m+1).$$

Note that $\frac{1}{4}(k-2)(n-2) - \frac{1}{2}(k-1)(n-1) - \frac{1}{2} < 0$ for all $k, n \geq 2$. Then the coefficient of t^2 is non-positive if and only if

$$m(m+1) < (k-1)(n-1)\big[-\frac{1}{2}(k-2)(n-2) + (k-1)(n-1) + 1\big]. \quad \square$$

4.1. *Concrete examples of* REP *and experimental results*

In this part, we present experimental results about the complexity of solving REP using the method of computing a Gröbner basis of the determinantal ideal $\mathcal{I}_{\text{REP}}$, as previously described.

We considered random instances of REP, and four different examples of this problem coming from applications in algebra. These examples are available upon request.

Examples 1 and 2 are used in the computation of semilinear tensor decompositions of a 30-dimensional irreducible $GF(5)$-module for the triple cover of S_6 (see 6.4 of (Mahavadi and Ryba, 2024)). Examples 3 and 4 are used to construct embeddings of the alternating group A_6 into the Lie groups F_4 and E_6.

In Table 1, we compare the theoretical estimates with the observed behavior (using Magma (Bosma et al., 1997)), to see how accurate they are for real examples.

Table 1
Comparison of theoretical vs experimental degree of regularity for random instances and Examples 1–4. The columns $d_{\mathrm{reg}}(\mathcal{I}_{\mathrm{REP}})$ and the upper bound of $d_{\mathrm{reg}}(\tilde{\mathcal{I}}_{\mathrm{REP}})$ are computed using Theorem 3 and Proposition 2, respectively. The columns experimental degree ("exp. degree") of $\mathcal{I}_{\mathrm{REP}}$ and experimental degree of $\tilde{\mathcal{I}}_{\mathrm{REP}}$ report the highest degree reached during the DRL Gröbner basis computation in Magma. Examples 1′, 2′, and 3′ refer to randomly generated instances.

Examples	$\mathbb{K}$	k	m	n	$d_{\mathrm{reg}}(\mathcal{I}_{\mathrm{REP}})$	exp. deg. $\mathcal{I}_{\mathrm{REP}}$	$\dim(\mathcal{I}_{\mathrm{REP}})$	upper bound $d_{\mathrm{reg}}(\tilde{\mathcal{I}}_{\mathrm{REP}})$	exp. deg. $\tilde{\mathcal{I}}_{\mathrm{REP}}$
1	GF(5)	5	5	6	2	2	1	2	2
2	GF(5)	6	9	6	2	3	1	2	2
3	GF(121)	7	40	8	4	6	6	2	2
4	GF(11)	16	251	17	17	–	11	2	2
Random Examples	$\mathbb{K}$	k	m	n	$d_{\mathrm{reg}}(\mathcal{I}_{\mathrm{REP}})$	exp. deg. $\mathcal{I}_{\mathrm{REP}}$	$\dim(\mathcal{I}_{\mathrm{REP}})$		
1′	GF(5)	5	5	6	2	2	0		
2′	GF(5)	6	9	6	2	2	0		
3′	GF(121)	7	40	8	4	4	0		

For random instances, the theory matches with experimental results. For the examples coming from applications, the situation is different, the experimentally observed $d_{\mathrm{reg}}(\mathcal{I}_{\mathrm{REP}})$ does not always match the theoretical degree. This discrepancy can be explained by the fact that the theoretical bounds are derived under some generic conditions. We also observe that the practical dimension is also distinct from the dimension expected. Whilst $m < (k-1)(n-1)$ for Examples 1, 2 and 3, they have a positive dimension.

It is then natural to randomly fix some of the variables. We then get a new ideal $\tilde{\mathcal{I}}_{\mathrm{REP}}$ that is zero-dimensional. From Proposition 2, we have an upper bound for $d_{\mathrm{reg}}(\tilde{\mathcal{I}}_{\mathrm{REP}})$ which is included in Table 1 under the column *upper bound of* $d_{reg}(\tilde{\mathcal{I}}_{\mathrm{REP}})$. Note that this new ideal $\tilde{\mathcal{I}}_{\mathrm{REP}}$ has dimension zero which is consistent with $\tilde{m} = m - d < (k-1)(n-1)$ and the experimental degree of $\tilde{\mathcal{I}}_{\mathrm{REP}}$ is now bounded by the upper bound of the degree of regularity of $\tilde{\mathcal{I}}_{\mathrm{REP}}$. This suggests that the derived affine zero-dimensional instances, $\tilde{\mathcal{I}}_{\mathrm{REP}}$, for Examples 1, 2 and 3 behave more as generic instances than their original homogeneous instances, $\mathcal{I}_{\mathrm{REP}}$. This is to be expected, as specializing variables typically removes the algebraic structure present in the original system.

Remark 2. The degree of regularity for positive dimension is not defined, so in Table 1 the value $d_{\mathrm{reg}}(\mathcal{I}_{\mathrm{REP}})$ for Example 4 should be interpreted as a bound for the maximal degree of a polynomial in a Gröbner basis (see Lemma 2). Additionally, the experimental degree of $\mathcal{I}_{\mathrm{REP}}$ for this example does not appear in 1 because the complete Gröbner basis computation was not completed.

5. Embeddings of A_6 in $F_4(\mathbb{C})$

In this section, we consider a concrete problem in computational group theory: the classification of certain embeddings of the alternating group A_6 into algebraic groups of type F_4. Our computational approach to this problem provides an example of a Relative Eigenvector Problem, and highlights both the power and the limitations of REP-based methods.

In (Griess and Ryba, 2002), embeddings of the group $SL(2,27)$ into the Lie group $2E_7(\mathbb{C})$ are constructed by transforming the task into a relative eigenvector problem. This approach has since been applied successfully to other classifications of embeddings of finite subgroups into exceptional Lie groups (Ryba, 2007; Frey and Ryba, 2018; Craven, 2022). In each case, every embedding corresponds to a solution of a relative eigenvector problem. However, there may also exist solutions, which we call *spurious* relative eigenvectors, that do not correspond to actual embeddings. (In other words, the relative eigenvector problem gives a necessary, but does not always give a sufficient, condition for an embedding.)

The existence of spurious relative eigenvectors has made the method of (Griess and Ryba, 2002) ineffective for some embedding problems. In this section, we introduce a new method that adds additional necessary polynomial conditions to the relative eigenvector problem. These additional conditions are constructed from a spurious relative eigenvector by investigating what algebraic conditions prevent it from yielding an embedding. The observation of Section 4.1 that particular solutions to a relative eigenvector problem are readily available is a key consideration that makes this approach practical.

The following embedding problem remained unsolved by a direct application of the method of (Griess and Ryba, 2002):

Problem 6. Classify the conjugacy classes of embeddings of the alternating group A_6 into the Lie group $F_4(\mathbb{C})$ for which the 26- and 52-dimensional representations of $F_4(\mathbb{C})$ restrict to representations of A_6 with characters

$$8a + 9^2 \quad \text{and} \quad 8a + 8b^3 + 10^2$$

(using ATLAS notation (Conway et al., 1985)).

We shall refer to any embedding of A_6 into a group of type F_4 (in any characteristic that does not divide the order of A_6) as *admissible* if it satisfies the character conditions specified in Problem 6. An action of A_6 on a Lie algebra of type F_4 is called *admissible* if the embedding of A_6 in the automorphism group of the Lie algebra is admissible. Problem 6 first arose in (Cohen and Wales, 1997). Cohen and Wales successfully classified all embedding classes of A_6 in $F_4(\mathbb{C})$ except for the admissible classes or their images under an outer automorphism of A_6. They also observed that there are admissible embeddings of A_6 into $F_4(\mathbb{C})$ that factor through an intermediate subgroup $A_2(\mathbb{C}) \circ A_2(\mathbb{C})$. However, they were unable to determine if any admissible embeddings exist *without* such an intermediate subgroup. Problem 6 remained open in (Frey, 2016) and (Frey and Ryba, 2018), but was eventually settled without computation in (Craven, 2023). We now adapt the method of (Griess and Ryba, 2002) to provide a computational solution to Problem 6.

5.1. Construction of the relative eigenvector problem

Let G be the alternating group A_6, let $\mathbb{Z}_{11}$ be the finite field of size 11, and let k be the algebraic closure of $\mathbb{Z}_{11}$. Larsen's Theorem (Griess and Ryba, 1998, Appendix 1) shows that the conjugacy classes of embeddings of G into $F_4(k)$ are in bijection with embeddings into $F_4(\mathbb{C})$. In particular, our later computation demonstrating that every admissible embedding of G into $F_4(k)$ factors through a subgroup $A_2(k) \circ A_2(k)$ proves that every admissible embedding of G into $F_4(\mathbb{C})$ factors through $A_2(\mathbb{C}) \circ A_2(\mathbb{C})$. Since 11 does not divide $|G|$, the irreducible kG-modules correspond to the irreducible ordinary characters of G. Following (Conway et al., 1985), we label these characters 1, $5a$, $5b$, $8a$, $8b$, 9, and 10. Note that the alphabetic suffixes for degrees 5 and 8 may be chosen arbitrarily and independently, as G possesses outer automorphisms that switch these pairs independently. We use the name of an irreducible character to denote its corresponding irreducible kG-module. Let V be a 26-dimensional kG-module with character $8a + 9^2$, and let $(\cdot,\cdot)$ be a G-invariant symmetric bilinear form on V. Note that V and $(\cdot,\cdot)$ are essentially unique: V is unique up to kG-module isomorphism, and the G-invariant symmetric bilinear forms on V form a single orbit under the action of the centralizer of G in $\mathrm{GL}(V)$. Let $\mathrm{O}(V)$ denote the orthogonal group of $(V, (\cdot,\cdot))$, consisting of elements of $\mathrm{GL}(V)$ that fix the bilinear form. The group $C_{\mathrm{O}(V)}(G)$ is a direct product $\mathrm{O}_1(k) \times \mathrm{O}_2(k)$, where the factors act on the complementary submodules of V with structures $8a$ and 9^2. Let $C \cong k^\times$ be the torus of rank 1 in the second factor; this group has index 4 in $C_{\mathrm{O}(V)}(G)$.

The Lie algebra L of $\mathrm{GO}(V)$ is isomorphic to $\Lambda^2 V$ as a kG-module. Hence, as a kG-module, L has character $1 + 5a^3 + 5b^3 + 8a^7 + 8b^8 + 9^6 + 10^{12}$. Let L_F be the kG-submodule of L with character $8a^7 + 8b^8 + 10^{12}$. If a kG-submodule $M \le L$ is contained in an admissible G-invariant Lie subalgebra of type F_4, we shall say that M is admissible. If M is admissible, then the Lie subalgebra of L generated by M is contained in L_F. For $n \ge 1$, let M^n be the kG-submodule of L spanned by Lie products of n elements of M, so that $M^1 = M$ and $M^n = [M^{n-1}, M]$. We define $M^n_F = M^n/(M^n \cap L_F)$. We aim to identify all submodules $M \le L$, with $M \cong 8a$, for which $M^n_F = 0$, as these are the only ones that could be admissible. In (Frey and Ryba, 2018), it is shown that a condition such as $M^n_F = 0$ yields computable polynomial equations that can be viewed as a relative eigenvector problem.

5.2. Computational setup

Let V_{8a} be an irreducible kG-module with character $8a$. Let $H = \mathrm{Hom}_{kG}(V_{8a}, L)$. Then H is a 7-dimensional vector space over k, and $C_{O(V)}(G)$ acts on H. The 1-dimensional subspaces of H classify kG-submodules $M \leq L$ with $M \cong V_{8a}$. To compute in H, we first choose a matrix representation of G on V where all matrix entries lie in $\mathbb{Z}_{11}$. We select a basis $\{v_1, \ldots, v_{26}\}$ of V such that the bilinear form is the identity matrix, meaning G acts by orthogonal matrices. We identify the Lie algebra L with $\Lambda^2 V$. The Lie product on $\Lambda^2 V$ is the bilinear product for which

$$[w \wedge v, x \wedge y] = (v, x) w \wedge y + (w, y) v \wedge x - (w, x) v \wedge y - (v, y) w \wedge x.$$

We compute a basis of H using the C-Meat-axe (Parker, 1984; Ringe). The vectors of this basis lie in the $\mathbb{Z}_{11}$-span of the standard basis vectors $v_i \wedge v_j$ of $\Lambda^2 V$. We only need to consider orbits of $C_{O(V)}(G)$ on H because if $c \in C_{O(V)}(G)$ and $h \in H$, then $(V_{8a})(hc)$ is admissible if and only if $(V_{8a})h$ is admissible. To make the action of C on H transparent, we work in a quadratic extension of $\mathbb{Z}_{11}$ and compute a basis of H that consists of eigenvectors $h_1, \ldots, h_7$ of an element of C with order 120. The first three eigenvectors are fixed by C, while the others span 1-dimensional C-modules with characters ψ, ψ^{-1}, ψ^2, ψ^{-2}, where ψ is a particular faithful character of C. Any element of H has the form $h(x) = \sum_i x_i h_i$ for $x \in k^7$. The corresponding $8a$-submodule $M(x) \leq L$ is the image $(V_{8a})h(x)$. If $M(x)$ is admissible, then $M(x)_F^3 = 0$. As shown in (Frey and Ryba, 2018), this gives homogeneous cubic conditions on x that define an ideal I_F in $k[x_1, \ldots, x_7]$. A Gröbner basis computation shows that the variety X_F determined by I_F has seven irreducible components: one of these has dimension 4, four have dimension 3, and two have dimension 2. A straightforward application of the method of (Griess and Ryba, 2002) fails because these dimensions are too large to allow us to search through the orbits of C on points of X_F and investigate the Lie algebras generated by the corresponding images of V_{8a} in L.

5.3. Extra constraints for the relative eigenvector problem

To proceed, we select a randomly chosen point $\hat{x}$ in the 4-dimensional component of X_F. We compute that $M(\hat{x})$ generates an 80-dimensional Lie subalgebra $L(\hat{x})$ with composition factors $8a^3 + 8b^2 + 10^4$. The multiplicity of $8a$ exceeds 1, which confirms that $\hat{x}$ is a spurious solution.

To create a polynomial condition that encodes the spurious nature of $\hat{x}$, we make use of the kG-module homomorphism π_{8a} from L onto its summand with character $8a^7$. We check that $[M(\hat{x}), M(\hat{x})]\pi_{8a}$ is not contained in $M(\hat{x})$. However, $[M(x), M(x)]\pi_{8a} \leq M(x)$ must hold whenever $M(x)$ is admissible. The following lemma shows that this condition may be written as a computable set of polynomial conditions on x. If we augment the ideal I_F by adding these polynomials, its ideal will be a proper subvariety of X_F that omits the point $\hat{x}$.

Lemma 3.

(i) *Let $\beta_1, \ldots, \beta_8$ be a basis of the kG-module V_{8a}. Let γ and δ be elements of V_{8a}. Suppose that $[\gamma h_i, \delta h_j]\pi_{8a} = \sum_{k,m} c^m_{i,j,k}(\beta_m h_k)$. Then $[M(x), M(x)]\pi_{8a}$ contains the vector*

$$\sum_{m,k} \left(\sum_{i,j} x_i x_j c^m_{i,j,k} \right) (\beta_m h_k).$$

(ii) *If $[M(x), M(x)]\pi_{8a} \leq M(x)$, then there exists a constant c such that for $1 \leq k \leq 7$:*

$$\sum_{i,j} c^1_{i,j,k} x_i x_j = c x_k.$$

Proof. Part (i) follows immediately from bilinearity of the Lie product, which shows that the specified vector is $[\gamma h(x), \delta h(x)]\pi_{8a}$. Since $\gamma h(x)$ and $\delta h(x)$ belong to $M(x)$, this projected vector belongs to the space $[M(x), M(x)]\pi_{8a}$. To prove part (ii), let π be a linear transformation from $L\pi_{8a}$ to $L\pi_{8a}$ defined by $\beta_1 h_k \pi = \beta_1 h_k$ for all k and $\beta_j h_k \pi = 0$ for $j > 1$. Then $M(x)\pi$ is a 1-dimensional subspace spanned by $\beta_1 h(x)$. Given that $[M(x), M(x)]\pi_{8a} \leq M(x)$, the image of the vector from part (i) under π must be a scalar multiple of $\beta_1 h(x)$, say $c\beta_1 h(x)$. Hence:

$$\sum_k \left(\sum_{i,j} c^1_{i,j,k} x_i x_j \right) \beta_1 h_k = c \sum_k x_k \beta_1 h_k.$$

Comparing the coefficients of the basis elements $\beta_1 h_k$ for $1 \leq k \leq 7$ yields the desired equations. $\square$

Lemma 3 provides a set of 7 quadratic conditions in the variables $x_1, \dots, x_7$ and c. By eliminating c, we obtain 49 homogeneous cubic constraints on $x_1, \dots, x_7$. Further experiments reveal another spurious solution: one for which the condition $[M(x), M(x)]\pi_{8a} \leq M(x)$ is satisfied, but $M(x)^3\pi_{8a}$ is not contained in $M(x)$. To exclude this case, we construct an analogous set of 49 homogeneous quartics in $x_1, \dots, x_7$. When these cubics and quartics are adjoined to the initial ideal I_F, the resulting variety is simple enough to investigate. Specifically, the variety of the augmented ideal consists of 7 irreducible components: one of dimension 2, and six of dimension 1.

These six 1-dimensional components are linear, and their points are fixed under the action of the torus C. The larger group $C_{\mathrm{O}(V)}(G)$ fixes two of these components, X_1 and X_2, and permutes the remaining four in two orbits of size two, represented by X_3 and X_4. Because each component is a single line, it defines a unique G-submodule of L isomorphic to $8a$. We label these submodules M_1, M_2, M_3, and M_4. These modules generate Lie subalgebras of L with dimensions 36, 8, 8, and 8, which are isomorphic to $B_4(k)$, $A_2(k)$, $A_2(k)$, and $A_2(k)$, respectively. The 2-dimensional component of the variety is defined by the equations $x_1^2 = x_4 x_5$ and $x_i = 0$ for $i \notin \{1, 4, 5\}$. The action of the torus C fixes the coordinate x_1 while scaling x_4 and x_5 by the characters ψ^2 and ψ^{-2}. This action results in three distinct orbits of lines within the component. Representatives of these orbits are spanned by the points:

1. $(x_1, x_4, x_5) = (1, 1, 1)$
2. $(x_1, x_4, x_5) = (0, 0, 1)$
3. $(x_1, x_4, x_5) = (0, 1, 0)$

The last two orbits are interchanged by elements of the centralizer $C_{\mathrm{O}(V)}(G)$. Consequently, these orbits contribute two additional classes of G-submodules of L isomorphic to V_{8a}, which we label as M_5 and M_6. Computation confirms that M_5 generates a 36-dimensional Lie subalgebra isomorphic to $B_4(k)$, whereas M_6 is an abelian subalgebra. We have now established:

Theorem 4. *If $M \cong 8a$ is an admissible kG-submodule of L, then M is a $C_{\mathrm{O}(V)}(G)$-image of one of the spaces M_i, with $1 \leq i \leq 6$. Moreover, if $i \leq 4$, then all points of M_i are fixed by the subgroup $C \leq C_{\mathrm{O}(V)}(G)$.*

5.4. Analysis of cases

We now show that of the six spaces in Theorem 4, only M_3 provides admissible embeddings. Our method is to consider admissible $8b$-submodules that could accompany the spaces of Theorem 4. For each of the spaces M_i with $1 \leq i \leq 6$, we compute candidates for submodules $N \leq L$, with $N \cong 8b$ such that $M_i + N$ is admissible. Such a module must satisfy $N^3 \leq L_i$, where L_i is generated by M_i and the submodule of L with character $8b^8 + 10^{12}$. This condition leads to an instance of REP that gives equations in 8-variables, $y_1, y_2, \dots, y_8$ (because $\mathrm{Hom}_{kG}(8b, L)$ is 8-dimensional). We write Y_i for the variety defined by these equations.

Notation. If Y_ℓ is a linear subvariety of Y_i, we write $N(Y_\ell)$ for the $8b$-pure submodule of L defined by points of Y_ℓ. We shall say that Y_ℓ is admissible if $N(Y_\ell) + M_i$ is admissible.

If $i \neq 3$, we compute that Y_i has 6 irreducible components, $Y_{i,1}, Y_{i,2}, \ldots, Y_{i,6}$, each of which is a 3-dimensional linear space. Now, if M_i is admissible, it is contained in an admissible module with character $8a + 8b^3$, which must have the form $M_i + N(Y_{i,j})$ with $1 \leq j \leq 6$. We compute the Lie subalgebras of L generated by these spaces when $i \neq 3$. In each of the thirty cases, we obtain a subalgebra of L with a dimension greater than or equal to 52, and in those cases where the dimension is 52, the subalgebra is not simple. Hence if $i \neq 3$, M_i is not admissible.

In the case of M_3, the variety Y_3 has 5 irreducible components. Four of these are 3-dimensional linear spaces. The method of the last paragraph shows those are all inadmissible. The last component, $Y_{3,5}$, is 4-dimensional. It is a subvariety of a 5-dimensional linear space $L_{3,5}$. We may choose coordinates so that $L_{3,5}$ is the space with $y_6 = y_7 = y_8 = 0$, and C acts with the characters $1, \psi, \psi^2, \psi^{-1}$, and ψ^{-2} on the coordinates y_1, y_2, y_3, y_4, and y_5, respectively. We may scale the coordinates so that $Y_{3,5}$ is the subvariety of $L_{3,5}$ that satisfies $y_2 y_4 = y_3 y_5$.

Notation. Write $\alpha_{i,j,\ldots,k}$ for the point of $L_{3,5}$ with $y_i = y_j = \cdots = y_k = 1$ and whose other coordinates are 0.

If M_3 is admissible, then there exists an admissible 3-dimensional linear subvariety $Y_{\ell,3,5}$ of $Y_{3,5}$. We remark that because M_3 is fixed by the action of C, the images of $Y_{\ell,3,5}$ under C are also admissible 3-dimensional linear subvarieties of $Y_{3,5}$. We observe that an admissible space $Y_{\ell,3,5}$ cannot contain α_3. If it did, then it has no point β with a non-zero y_4 or y_5 coordinate (because we compute that $[N(\alpha_3), N(\beta)]$ is not contained in L_3). Therefore, $Y_{\ell,3,5}$ must be spanned by $\alpha_1, \alpha_2, \alpha_3$. We now compute that the Lie algebra generated by M_3 and $N(Y_{\ell,3,5})$ is 52-dimensional, but not simple. Hence $Y_{\ell,3,5}$ is not admissible, a contradiction.

A similar argument shows that an admissible space $Y_{\ell,3,5}$ cannot contain α_5. We further observe that $Y_{\ell,3,5}$ cannot contain α_2 or $\alpha_{2,3}$ (because we compute that the Lie closures of $N(\alpha_2)$ and $N(\alpha_{2,3})$ contain $N(\alpha_3)$). Now every 3-dimensional subspace of $L_{3,5}$ contains a point in the C-orbit of one of $\alpha_2, \alpha_3, \alpha_5, \alpha_{2,3}$, or $\alpha_{2,5}$. It follows that if there is an admissible space $Y_{\ell,3,5}$, it is the image under C of a space that contains $\alpha_{2,5}$. We now compute the subalgebra of L that is generated by M_3 and $N(\alpha_{2,5})$: it is 52-dimensional, simple, and has type F_4. Moreover, it contains $N(\alpha_1)$, which is a copy of the Lie algebra A_2 that centralizes M_3. We have now proved the following theorem, which shows that an admissible embedding of G in $F_4(k)$ factors through a subgroup of type $A_2 \circ A_2$. This settles Problem 6.

Theorem 5. *There is one $C_{O(V)}(G)$-orbit of G-invariant admissible F_4 subalgebras of L. Moreover, each algebra in this orbit contains a G-invariant subalgebra with type $A_2 + A_2$.*

CRediT authorship contribution statement

Pilar Coscojuela: Software, Resources. **Mordechai Katzman:** Software, Investigation. **Krishna Mahavadi:** Validation, Software. **Ludovic Perret:** Methodology, Investigation. **Alex Ryba:** Methodology, Investigation. **Simona Samardjiska:** Methodology, Investigation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Ideals and Gröbner basis

In this appendix, we recall the notions of Hilbert function, Hilbert series, and Hilbert polynomial for a homogeneous ideal. In the case of zero-dimensional homogeneous ideals, we state the relationship between their Hilbert series and their degree and degree of regularity. Moreover, we recall a well-known upper bound on the complexity of computing a Gröbner basis for a homogeneous zero-dimensional ideal. Finally, we extend the definition of degree of regularity to the zero-dimensional affine case.

Definition 2. Let $I \subset \mathbb{K}[x_1, \ldots, x_m]$ be a homogeneous ideal. Then the Hilbert function of I, $\mathbf{HF}_{\mathbb{K}[x_1,\ldots,x_m]/I}$, is defined as

$$\mathbf{HF}_{\mathbb{K}[x_1,\ldots,x_m]/I} : \mathbb{N} \to \mathbb{N},$$
$$\mathbf{HF}_{\mathbb{K}[x_1,\ldots,x_m]/I}(d) = \dim(\mathbb{K}[x_1, \ldots, x_m]_d / I_d).$$

The Hilbert series of I, $\mathbf{HS}_{\mathbb{K}[x_1,\ldots,x_m]/I}$, is the formal series given by:

$$\mathbf{HS}_{\mathbb{K}[x_1,\ldots,x_m]/I}(t) = \sum_{d=0}^{\infty} \mathbf{HF}_{\mathbb{K}[x_1,\ldots,x_m]/I}(d) t^d.$$

Definition-Proposition 1. Let $I \subset \mathbb{K}[x_1, \ldots, x_m]$ be a proper homogeneous ideal. There exist a polynomial,

$$\mathbf{HP}_{\mathbb{K}[x_1,\ldots,x_m]/I}(t) \in \mathbb{Z}[t]$$

of degree $\dim(I) - 1$ and $d_0 \in \mathbb{N}$, such that

$$\mathbf{HF}_{\mathbb{K}[x_1,\ldots,x_m]/I}(d) = \mathbf{HP}_{\mathbb{K}[x_1,\ldots,x_m]/I}(d) \text{ for all } d \geq d_0.$$

The number d_0 is called the degree of regularity of I, $d_{\mathrm{reg}}(I)$. Moreover, there exists a polynomial $Q(t) \in \mathbb{Z}[t]$, with $Q(1) \neq 0$, such that

$$\mathbf{HS}_{\mathbb{K}[x_1,\ldots,x_m]/I}(t) = \frac{Q(t)}{(1-t)^a}.$$

Then $\dim(I) = a$.

Proposition 5. *If $I \subset \mathbb{K}[x_1, \ldots, x_m]$ is a zero dimensional homogeneous ideal, the Hilbert series of I is a polynomial and the degree of I, $DEG(I)$, can be computed as:*

$$DEG(I) = \mathbf{HS}_{\mathbb{K}[x_1,\ldots,x_m]/I}(1).$$

Proposition 6. *If $I \subset \mathbb{K}[x_1, \ldots, x_m]$ is a zero dimensional homogeneous ideal, then*

$$d_{reg}(I) = \deg(\mathbf{HS}_{\mathbb{K}[x_1,\ldots,x_m]/I}(t)) + 1.$$

In addition, for any monomial ordering, $d_{reg}(I)$ bounds the degree of all polynomials in a reduced homogeneous Gröbner basis of I.

Proposition 7. *Let $I = \langle f_1, \ldots, f_k \rangle \subset \mathbb{K}[x_1, \ldots, x_m]$ be a zero dimensional homogeneous ideal. The complexity of computing a Degree Reverse Lexicographical ordering (*DRL*) Gröbner basis is bounded by:*

$$O\left(k\binom{d_{reg}(I) + m}{m}^{\omega}\right).$$

*The DRL Gröbner basis can be turned into a Lexicographic (*LEX*) Gröbner basis with the FGLM algorithm, which has complexity*

$$O\left(m(DEG(I))^3\right).$$

The next definition extends the notion of degree of regularity to affine ideals:

Definition 3. Let $I = \langle f_1, \dots, f_k \rangle \subset \mathbb{K}[x_1, \dots, x_m]$ be a proper ideal and $I^{(h)} = \langle f_1^{(h)}, \dots, f_k^{(h)} \rangle$ where $f_i^{(h)}$ is the homogeneous component of f_i of largest degree, $1 \le i \le k$. If $\dim(I^{(h)}) = 0$, then $\dim(I) = 0$ and the degree of regularity of I is defined by

$$d_{\mathrm{reg}}(I) = d_{\mathrm{reg}}(I^{(h)}).$$

Data availability

Data will be made available on request.

References

Bardet, M., Bertin, M., 2022. Improvement of algebraic attacks for solving superdetermined minrank instances. In: International Conference on Post-Quantum Cryptography. Springer, pp. 107–123.

Bardet, M., Bros, M., Cabarcas, D., Gaborit, P., Perlner, R., Smith-Tone, D., Tillich, J.P., Verbel, J., 2020a. Algebraic attacks for solving the rank decoding and minrank problems without Gröbner basis. arXiv preprint arXiv:2002.08322.

Bardet, M., Bros, M., Cabarcas, D., Gaborit, P., Perlner, R.A., Smith-Tone, D., Tillich, J., Verbel, J.A., 2020b. Improvements of algebraic attacks for solving the rank decoding and minrank problems. In: Moriai, S., Wang, H. (Eds.), Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings, Part I. Daejeon, South Korea, December 7–11, 2020. Springer, pp. 507–536.

Bettale, L., Faugère, J., Perret, L., 2013. Cryptanalysis of hfe, multi-hfe and variants for odd and even characteristic. Des. Codes Cryptogr. 69, 1–52. https://doi.org/10.1007/s10623-012-9617-2.

Bosma, W., Cannon, J.J., Playoust, C., 1997. The Magma algebra system I: the user language. J. Symb. Comput. 24, 235–265.

Buss, J.F., Frandsen, G.S., Shallit, J.O., 1999. The computational complexity of some problems of linear algebra. J. Comput. Syst. Sci. 58, 572–596.

Christou, D., Mitrouli, M., Triantafyllou, D., 2025. A rank-updating technique for the Kronecker canonical form of singular pencils. Appl. Numer. Math. 208, 135–145. https://doi.org/10.1016/j.apnum.2024.01.015.

Cohen, A.M., Griess Jr., R.L., 1987. On finite simple subgroups of the complex Lie group of type E_8. In: The Arcata Conference on Representations of Finite Groups. Arcata, Calif., 1986. In: Proc. Sympos. Pure Math., vol. 2. Amer. Math. Soc., Providence, RI, pp. 367–405.

Cohen, A.M., Wales, D.B., 1997. Finite subgroups of $F_4(\mathbf{C})$ and $E_6(\mathbf{C})$. Proc. Lond. Math. Soc. (3) 74, 105–150. https://doi.org/10.1112/S0024611597000051.

Conway, J.H., Curtis, R.T., Norton, S.P., Parker, R.A., Wilson, R.A., 1985. $\mathbb{ATLAS}$ of finite groups. In: Maximal Subgroups and Ordinary Characters for Simple Groups. Oxford University Press, Eynsham. With computational assistance from J.G. Thackray.

Courtois, N.T., 2001. Efficient zero-knowledge authentication based on a linear algebra problem minrank. In: Boyd, C. (Ed.), Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings. Gold Coast, Australia, December 9–13, 2001. Springer, pp. 402–421.

Craven, D.A., 2022. On the maximal subgroups of $e_7(q)$ and related almost simple groups. arXiv URL: https://arxiv.org/pdf/2201.07081.

Craven, D.A., 2023. The maximal subgroups of the exceptional groups $F_4(q)$, $E_6(q)$ and ${}^2E_6(q)$ and related almost simple groups. Invent. Math. 234, 637–719. https://doi.org/10.1007/s00222-023-01208-2.

Faugère, J., Din, M.S.E., Spaenlehauer, P., 2010. Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology. In: Koepf, W. (Ed.), Symbolic and Algebraic Computation, International Symposium, Proceedings. ISSAC 2010, Munich, Germany, July 25–28, 2010. ACM, pp. 257–264.

Faugère, J., Din, M.S.E., Spaenlehauer, P., 2013. On the complexity of the generalized minrank problem. J. Symb. Comput. 55, 30–58. https://doi.org/10.1016/j.jsc.2013.03.004.

Faugère, J., Gligoroski, D., Perret, L., Samardjiska, S., Thomae, E., 2015. A polynomial-time key-recovery attack on MQQ cryptosystems. In: Katz, J. (Ed.), Public-Key Cryptography - PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography. Gaithersburg, MD, USA, March 30 – April 1, 2015. Springer, pp. 150–174.

Faugère, J., Levy-dit-Vehel, F., Perret, L., 2008. Cryptanalysis of minrank. In: Wagner, D.A. (Ed.), Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Proceedings. Santa Barbara, CA, USA, August 17–21, 2008. Springer, pp. 280–296.

Frey, D., Ryba, A., 2018. Conjugacy of embeddings of alternating groups in exceptional Lie groups. Bull. Inst. Math. Acad. Sin. (N.S.) 13, 463–480.

Frey, D.D., 2016. Embeddings of Alt_n and its perfect covers for $n \ge 6$ in exceptional complex Lie groups. J. Algebra 451, 1–45. https://doi.org/10.1016/j.jalgebra.2015.11.014.

Gopalakrishnan, S., 2024. On the arithmetic complexity of computing Gröbner bases of comaximal determinantal ideals. CoRR arXiv:2403.02160. https://doi.org/10.48550/arXiv.2403.02160.

Gopalakrishnan, S., Neiger, V., Din, M.S.E., 2024. Optimized Gröbner basis algorithms for maximal determinantal ideals and critical point computations. In: Hauenstein, J.D., Lee, W., Chen, S. (Eds.), Proceedings of the 2024 International Symposium on Symbolic and Algebraic Computation. ISSAC 2024, Raleigh, NC, USA, July 16–19, 2024. ACM, pp. 400–409.

Griess Jr., R.L., Ryba, A.J.E., 1998. Embeddings of $\mathrm{PGL}_2(31)$ and $\mathrm{SL}_2(32)$ in $E_8(\mathbf{C})$. Duke Math. J. 94, 181–211. https://doi.org/10.1215/S0012-7094-98-09409-1. With appendices by Michael Larsen and J.-P. Serre.
Griess Jr., R.L., Ryba, A.J.E., 2002. Embeddings of $\mathrm{SL}(2,27)$ in complex exceptional algebraic groups. Mich. Math. J. 50, 89–99.
Henrion, D., Naldi, S., Din, M.S.E., 2016. Real root finding for determinants of linear matrices. J. Symb. Comput. 74, 205–238. https://doi.org/10.1016/j.jsc.2015.06.010.
Kipnis, A., Shamir, A., 1999. Cryptanalysis of the HFE public key cryptosystem by relinearization. In: CRYPTO. Springer, pp. 19–30.
Leedham-Green, C.R., 2001. The computational matrix group project. In: Groups and Computation, III. Columbus, OH, 1999. In: Ohio State Univ. Math. Res. Inst. Publ., vol. 8. de Gruyter, Berlin, pp. 229–247.
Mahavadi, K.K., Ryba, A.J.E., 2024. Semilinear tensor decompositions. J. Comput. Algebra 9. https://doi.org/10.1016/j.jaca.2024.100013.
Parker, R., 1984. The computer calculation of modular characters (the meat-axe). In: Computational Group Theory. Durham, 1982, pp. 267–274.
Ringe, M. The C-meataxe. Available at http://www.math.rwth-aachen.de/~MTX.
Ryba, A., 2022. Recognition of absolutely irreducible matrix groups that are tensor decomposable or induced. J. Algebra 610, 911–934.
Ryba, A.J.E., 2007. Construction of some irreducible subgroups of E_8 and E_6. LMS J. Comput. Math. 10, 329–340.
Serre, J.P., 1996. Exemples de plongements des groupes $\mathrm{PSL}_2(\mathbf{F}_p)$ dans des groupes de Lie simples. Invent. Math. 124, 525–562.
Serre, J.P., 2000. Sous-groupes finis des groupes de Lie. In: Séminaire Bourbaki, vol. 1998/99. Astérisque, No. 864 5.
Spaenlehauer, P.J., 2012. Solving multi-homogeneous and determinantal systems: algorithms, complexity, applications. Ph.D. thesis. Université Pierre et Marie Curie (Univ. Paris 6).
Verbel, J., Baena, J., Cabarcas, D., Perlner, R., Smith-Tone, D., 2019. On the complexity of "superdetermined" minrank instances. In: Ding, J., Steinwandt, R. (Eds.), Post-Quantum Cryptography. Springer International Publishing, Cham, pp. 167–186.
Wong, K.T., 1974. The eigenvalue problem $\lambda Tx + Sx$. J. Differ. Equ. 16, 270–280. https://doi.org/10.1016/0022-0396(74)90014-X.