Electronic Colloquium on Computational Complexity, Report No. 42 (2019)

Determinant equivalence test over finite fields and over $\mathbb{Q}$

Ankit Garg
Microsoft Research India
garga@microsoft.com

Nikhil Gupta
Indian Institute of Science
nikhilg@iisc.ac.in

Neeraj Kayal
Microsoft Research India
neeraka@microsoft.com

Chandan Saha
Indian Institute of Science
chandan@iisc.ac.in

March 18, 2019

Abstract

The determinant polynomial $\mathsf{Det}_n(\mathbf{x})$ of degree n is the determinant of a $n \times n$ matrix of formal variables. A polynomial f is equivalent to $\mathsf{Det}_n(\mathbf{x})$ over a field $\mathbb{F}$ if there exists a $A \in \mathrm{GL}(n^2, \mathbb{F})$ such that $f = \mathsf{Det}_n(A \cdot \mathbf{x})$. *Determinant equivalence test over* $\mathbb{F}$ is the following algorithmic task: Given black-box access to a $f \in \mathbb{F}[\mathbf{x}]$, check if f is equivalent to $\mathsf{Det}_n(\mathbf{x})$ over $\mathbb{F}$, and if so then output a transformation matrix $A \in \mathrm{GL}(n^2, \mathbb{F})$. In [Kay12], a randomized polynomial time determinant equivalence test was given over $\mathbb{F} = \mathbb{C}$. But, to our knowledge, the complexity of the problem over finite fields and over $\mathbb{Q}$ was not well understood.

In this work, we give a randomized $\mathrm{poly}(n, \log |\mathbb{F}|)$ time determinant equivalence test over finite fields $\mathbb{F}$ (under mild restrictions on the characteristic and size of $\mathbb{F}$). Over $\mathbb{Q}$, we give an efficient randomized reduction from factoring square-free integers to determinant equivalence test for quadratic forms (i.e. the $n = 2$ case), assuming GRH. This shows that designing a polynomial-time determinant equivalence test over $\mathbb{Q}$ is a challenging task. Nevertheless, we show that determinant equivalence test over $\mathbb{Q}$ is decidable: For bounded n, there is a randomized polynomial-time determinant equivalence test over $\mathbb{Q}$ with access to an oracle for integer factoring. Moreover, for *any* n, there is a randomized polynomial-time algorithm that takes input black-box access to a $f \in \mathbb{Q}[\mathbf{x}]$ and if f is equivalent to Det_n over $\mathbb{Q}$ then it returns a $A \in \mathrm{GL}(n^2, \mathbb{L})$ such that $f = \mathsf{Det}_n(A \cdot \mathbf{x})$, where $\mathbb{L}$ is an extension field of $\mathbb{Q}$ and $[\mathbb{L} : \mathbb{Q}] \leq n$.

The above algorithms over finite fields and over $\mathbb{Q}$ are obtained by giving a polynomial-time randomized reduction from determinant equivalence test to another problem, namely the *full matrix algebra isomorphism* problem. We also show a reduction in the converse direction which is efficient if n is bounded. These reductions, which hold over any $\mathbb{F}$ (under mild restrictions on the characteristic and size of $\mathbb{F}$), establish a close connection between the complexity of the two problems. This then lead to our results via applications of known results on the full algebra isomorphism problem over finite fields [Rón87, Rón90] and over $\mathbb{Q}$ [IRS12, BR90].

ISSN 1433-8092

1 Introduction

Two m-variate polynomials $f(\mathbf{x})$ and $g(\mathbf{x})$ with coefficients from a field $\mathbb{F}$ are said to be *equivalent over* $\mathbb{F}$ if there exists a $A \in \mathrm{GL}(m, \mathbb{F})$ such that $f = g(A \cdot \mathbf{x})$. The algorithmic task of determining if f is equivalent to g, and if so then finding a linear transformation A such that $f = g(A \cdot \mathbf{x})$, is known as the polynomial *equivalence test* problem. It is a natural problem arising in algebraic complexity theory, becoming more important with the advent of Geometric Complexity Theory (GCT) [MS01] – which proposes the uses of deep tools and insights from group theory, representation theory and algebraic geometry towards the study of the VP vs VNP question.

A naïve approach for equivalence test is to reduce it to solving a system of polynomial equations over $\mathbb{F}$. But, unfortunately, the complexity of polynomial solvability over $\mathbb{F}$ is quite high[1]. Nevertheless, it does appear that the complexity of equivalence test is much lower than the complexity of solving polynomial systems. It is known that over finite fields, the polynomial equivalence problem is in $\mathsf{NP} \cap \mathsf{co}\text{-}\mathsf{AM}$ (when the polynomials are given as lists of coefficients) [Thi98,Sax06].

Can we hope to solve equivalence test over $\mathbb{C}$ and over finite fields [2] in (randomized) polynomial time? Finding such an algorithm is indeed quite demanding as it was shown in [AS05, AS06] that the graph isomorphism problem reduces in polynomial time to equivalence test for cubic forms (i.e. homogeneous degree three polynomials) over *any* field. Over $\mathbb{Q}$, it is not even known if cubic form equivalence is decidable. On the other hand, we have a fairly good understanding of the complexity of quadratic form equivalence test: Over $\mathbb{C}$ and finite fields, equivalence of two quadratic forms can be tested in polynomial time due to well-known results on classification of quadratic forms. Quadratic form equivalence over $\mathbb{Q}$ can be done in polynomial-time with access to an oracle for integer factoring (IntFact). Moreover, IntFact reduces in randomized polynomial time to quadratic form equivalence over $\mathbb{Q}$ (see [Wal13]). Given this state of affairs, designing efficient equivalence tests for even bounded degree polynomials seems like a difficult proposition. Indeed, there is a cryptographic authentication scheme based on the presumed average-case hardness of equivalence test for constant degree polynomials (see [Pat96]).

The work in [Kay11] initiated the study of a kind of equivalence test in which one polynomial f is given as input and the other polynomial g belongs to a well-defined polynomial family. Some of the polynomial families that are well-studied in algebraic complexity theory, particularly in the context of arithmetic circuit lower bounds, are those defined by the power symmetric polynomial, the elementary symmetric polynomial, the permanent, the determinant and the iterated matrix multiplication polynomial. In [Kay11], randomized polynomial time equivalence tests over $\mathbb{C}$ were given for the power symmetric polynomial and the elementary symmetric polynomial families. These equivalence tests, which also hold over finite fields and $\mathbb{Q}$, work even if f is given as a black-box[3]. Henceforth, let us assume that the input polynomial f is given as a black-box. Sub-

[1] Over $\mathbb{C}$ and finite fields, polynomial solvability has time complexity exponential in the input parameters. Over $\mathbb{Q}$, it is not known to be decidable.

[2] Typically, a computation model over $\mathbb{C}$ assumes that basic arithmetic operations with complex numbers and root finding of univariate polynomials over $\mathbb{C}$ can be done efficiently. Also, we will work with finite fields that have sufficiently large size and characteristic.

[3] An algorithm with black-box access to a m-variate polynomial f is only allowed to query the black-box for evaluations of f at points in $\mathbb{F}^m$.

sequently, in [Kay12], randomized polynomial time equivalence tests over $\mathbb{C}$ were given for the permanent and the determinant polynomial families. The test for the permanent holds over finite fields and $\mathbb{Q}$, but the same is *not true* for the determinant equivalence test in [Kay12]. In [KNST17], an equivalence test for the iterated matrix multiplication (IMM) was given which holds over $\mathbb{C}$, finite fields and $\mathbb{Q}$ (see also [Gro12]). The iterated matrix multiplication and the determinant families have very similar circuit complexity: Both the families are complete under p-projections for class of algebraic branching programs (ABP) (see [MV97a, MV97b]). But, it was unclear if determinant admits an efficient equivalence test over finite fields and $\mathbb{Q}$, just like the iterated matrix multiplication polynomial. In this paper, we fill in this gap in our understanding.

It is worth noting that determinant equivalence test is interesting in the context of the permanent versus determinant problem [Val79], which conjectures that the permanent is not an affine projection of a polynomial-size determinant. Geometric Complexity Theory [MS01], an approach to resolving this conjecture, suggests (among other things) to look for an algorithm to determine if the (padded) permanent is in the orbit closure of a polynomial-size determinant. In this language, determinant equivalence testing is the related problem of checking if a given polynomial is in the orbit of the determinant polynomial.

1.1 Our results

Let $n \in \mathbb{N}^\times$, $X = (x_{ij})_{i,j\in[n]}$ be a $n \times n$ matrix of formal variables, and $\mathbf{x} = (x_{11}\ x_{12}\ \ldots\ x_{n\,n-1}\ x_{nn})^T$ a column vector consisting of the variables in X arranged in a row-major fashion. The polynomial $\mathsf{Det}_n(\mathbf{x}) := \det(X)$; we will drop the subscript n whenever it is clear from the context. Hereafter, we will use the acronym DET for Determinant Equivalence Test.

Theorem 1 (DET over finite fields)**.** *Let $\mathbb{F}$ be a finite field such that $|\mathbb{F}| \geq 10n^4$ and $\mathrm{char}(\mathbb{F}) \nmid n(n-1)$. There is a randomized $\mathrm{poly}(n, \log|\mathbb{F}|)$ time algorithm that takes input black-box access to a $f \in \mathbb{F}[\mathbf{x}]$ of degree n and does the following with high probability: If f is equivalent to $\mathsf{Det}(\mathbf{x})$ over $\mathbb{F}$ then it outputs a $A \in \mathrm{GL}(n^2, \mathbb{F})$ such that $f = \mathsf{Det}(A \cdot \mathbf{x})$; otherwise, it outputs 'Fail'.*

In [KNS18], a DET over a finite field $\mathbb{F}_q$ was given that is similar to the equivalence test for the permanent in [Kay12], but the test outputs a $A \in \mathrm{GL}(n^2, \mathbb{F}_{q^n})$. Whereas, our algorithm (which is different and relatively more involved) outputs a $A \in \mathrm{GL}(n^2, \mathbb{F}_q)$. One consequence of this is that the average-case ABP reconstruction algorithm in [KNS18] holds over the base field $\mathbb{F}_q$.

Theorem 2 (DET over $\mathbb{Q}$)**.** *(a) There is a randomized algorithm, with oracle access to* $\mathsf{IntFact}$, *that takes input black-box access to a $f \in \mathbb{Q}[\mathbf{x}]$ of degree n and does the following with high probability: If f is equivalent to $\mathsf{Det}(\mathbf{x})$ over $\mathbb{Q}$ then it outputs a $A \in \mathrm{GL}(n^2, \mathbb{Q})$ such that $f = \mathsf{Det}(A \cdot \mathbf{x})$; otherwise, it outputs 'Fail'. If n is bounded then the algorithm runs in time polynomial in the bit length of the coefficients of f.*

(b) There is a randomized algorithm that takes input black-box access to a $f \in \mathbb{Q}[\mathbf{x}]$ of degree n and does the following with high probability: If f is equivalent to $\mathsf{Det}(\mathbf{x})$ over $\mathbb{Q}$ then it outputs a $A \in \mathrm{GL}(n^2, \mathbb{L})$ such that $f = \mathsf{Det}(A \cdot \mathbf{x})$, where $\mathbb{L}$ is an extension field of $\mathbb{Q}$ and $[\mathbb{L} : \mathbb{Q}] \leq n$. The algorithm runs in time polynomial in n and the bit length of the coefficients of f.

To our knowledge, it was not known if DET over $\mathbb{Q}$ is decidable prior to this work. It is natural to wonder if we can get rid of the $\mathsf{IntFact}$ oracle from part (a) of the above theorem. In this regard, we show the following.

Theorem 3 (IntFact reduces to DET for quadratic forms)**.** *Assuming GRH, we give a randomized polynomial-time reduction from factoring square-free integers to finding a $A \in M_2(\mathbb{Q})$ such that a given quadratic form $f \in \mathbb{Q}[\mathbf{x}]$ equals $\mathrm{Det}_2(A \cdot \mathbf{x})$, if f is equivalent to Det_2.*

In other words, the complexity of IntFact is the same as that of DET over $\mathbb{Q}$ for quadratic forms (modulo GRH and the use of randomization).

Theorem 1 and 2 are proved by reducing DET to the *full matrix algebra isomorphism* problem. A $\mathbb{F}$-algebra $\mathcal{A}$ has two binary operations $+$ and $\cdot$ defined on its elements such that $(\mathcal{A}, +)$ is a $\mathbb{F}$-vector space, $(\mathcal{A}, +, \cdot)$ is an associative ring, and for every $a, b \in \mathbb{F}$ and $B, C \in \mathcal{A}$ it holds that $(aB)C = B(aC) = a(BC)$. For example, the set $M_n(\mathbb{F})$ of all $n \times n$ matrices over $\mathbb{F}$ is a $\mathbb{F}$-algebra with respect to the usual matrix addition and multiplication operations; it is called the full matrix algebra. Two $\mathbb{F}$-algebra $\mathcal{A}_1$ and $\mathcal{A}_2$ are isomorphic, denoted by $\mathcal{A}_1 \cong \mathcal{A}_2$, if there is a bijection ϕ from $\mathcal{A}_1$ to $\mathcal{A}_2$ such that for every $a, b \in \mathbb{F}$ and $B, C \in \mathcal{A}$ it holds that $\phi(aB + bC) = a\phi(B) + b\phi(C)$ and $\phi(BC) = \phi(B)\phi(C)$. Any finite dimensional $\mathbb{F}$-algebra is isomorphic to a $\mathbb{F}$-algebra $\mathcal{A}' \subseteq M_m(\mathbb{F})$, where $m = \dim_{\mathbb{F}}(\mathcal{A})$. A $\mathbb{F}$-algebra $\mathcal{A} \subseteq M_m(\mathbb{F})$ can be specified by a $\mathbb{F}$-basis $B_1, \ldots, B_r \in M_m(\mathbb{F})$.

Definition 1.1. The full matrix algebra isomorphism (FMAI) problem over $\mathbb{F}$ is the following: Given a basis of a $\mathbb{F}$-algebra $\mathcal{A} \subseteq M_m(\mathbb{F})$, check if $\mathcal{A} \cong M_n(\mathbb{F})$, where $n^2 = \dim_{\mathbb{F}}(\mathcal{A})$. If $\mathcal{A} \cong M_n(\mathbb{F})$ then output an isomorphism from $\mathcal{A}$ to $M_n(\mathbb{F})$.

In [Rón87, Rón90], a $\mathrm{poly}(m, \log|\mathbb{F}|)$ time randomized algorithm was given to solve FMAI over a finite field $\mathbb{F}$. Over $\mathbb{Q}$, the FMAI problem is more difficult. In [IRS12, CFO+15], a randomized algorithm (with access to a IntFact oracle) was given to solve FMAI over $\mathbb{Q}$. The algorithm runs in polynomial-time if $\dim_{\mathbb{Q}}(\mathcal{A})$ is bounded. In [BR90, Ebe89], randomized polynomial time algorithms were given to compute an isomorphism from $\mathcal{A} \otimes_{\mathbb{Q}} \mathbb{L}$ to $M_n(\mathbb{L})$ for some extension field $\mathbb{L} \supseteq \mathbb{Q}$ satisfying $[\mathbb{L} : \mathbb{Q}] \leq n$, if $\mathcal{A} \cong M_n(\mathbb{Q})$ to begin with. We give a randomized polynomial-time reduction from DET to FMAI over any sufficiently large $\mathbb{F}$ in Sections 4, thereby proving Theorem 1 and 2. The reduction is obtained by giving an algorithm to decompose the Lie algebra of f into its two simple Lie subalgebras over any sufficiently large $\mathbb{F}$ (see Section 3). We also show a reduction from FMAI to DET (in Section 7) which is efficient if the dimension n is bounded.

The above results underscore the close connection between the DET and the FMAI problems. In order to get efficient DET over $\mathbb{Q}$ for even bounded degree polynomials, we *need to* solve FMAI efficiently for $\mathbb{Q}$-algebras of bounded dimensions. Currently, the best known algorithm for FMAI over $\mathbb{Q}$ uses an IntFact oracle [IRS12]. This situation of the determinant is somewhat surprising as it contrasts that of IMM (the close cousin of the determinant) – IMM equivalence test over $\mathbb{Q}$ can be solved efficiently for polynomials of degree greater than four [KNST17].

2 Preliminaries

2.1 Notations

The set of trace zero or traceless matrices in $M_n(\mathbb{F})$ is denoted by $\mathcal{Z}_n(\mathbb{F})$; we will drop $\mathbb{F}$ from $M_n(\mathbb{F})$ and $\mathcal{Z}_n(\mathbb{F})$ when it is clear from the context. Let I_n be the $n \times n$ identity matrix. Define,

$$\mathcal{M}_{\text{col}} := I_n \otimes M_n, \;\; \mathcal{M}_{\text{row}} := M_n \otimes I_n \quad \text{and} \quad \mathscr{L}_{\text{col}} := I_n \otimes \mathcal{Z}_n, \;\; \mathscr{L}_{\text{row}} := \mathcal{Z}_n \otimes I_n.$$

Observe that $\mathcal{M}_{\text{col}}, \mathcal{M}_{\text{row}} \subseteq M_{n^2}$ are $\mathbb{F}$-algebras isomorphic to M_n, and $\mathscr{L}_{\text{col}}, \mathscr{L}_{\text{row}}$ are subspaces of $\mathcal{M}_{\text{col}}, \mathcal{M}_{\text{row}}$, respectively, of dimension $n^2 - 1$ each. Henceforth, we set $m = n^2$ and $r = n^2 - 1$.

2.2 Definitions

Definition 2.1. (Lie bracket): For $A, B \in M_n$, the Lie bracket operation $[A, B] := AB - BA$.

Definition 2.2. (Lie algebra of a polynomial): The Lie algebra $\mathfrak{g}_f$ of a m-variate polynomial $f \in \mathbb{F}[\mathbf{x}]$ is the set of matrices $B = (b_{i,j})_{i,j \in [m]}$ satisfying,

$$\sum_{i,j \in [m]} b_{i,j} \cdot x_j \cdot \frac{\partial f}{\partial x_i} = 0.$$

It is easy to verify that $[\cdot, \cdot]$ is a $\mathbb{F}$-bilinear map on M_n, and $\mathfrak{g}_f$ is an $\mathbb{F}$-vector space.[4]

Definition 2.3. (Invariant subspace): Let $\mathcal{V}$ be a $\mathbb{F}$-vector space and $\mathcal{T} \subseteq \text{End}_{\mathbb{F}}(\mathcal{V})$, where $\text{End}_{\mathbb{F}}(\mathcal{V}) := \{\varphi : \varphi \text{ is a } \mathbb{F}\text{-linear map from } \mathcal{V} \text{ to } \mathcal{V}\}$. A subspace $\mathcal{U}$ of $\mathcal{V}$ is called a $\mathcal{T}$-invariant subspace of $\mathcal{V}$ if for every $\varphi \in \mathcal{T}$, $\varphi(\mathcal{U}) \subseteq \mathcal{U}$.

If $\mathcal{T} \subseteq M_{2r}$ then the terminology 'invariant subspace of $\mathcal{T}$' means $\mathcal{T}$-invariant subspace of $\mathbb{F}^{2r}$.

Definition 2.4. (Irreducible invariant subspace): Let $\mathcal{V}$ be a $\mathbb{F}$-vector space and $\mathcal{T} \subseteq \text{End}_{\mathbb{F}}(\mathcal{V})$. Then, a $\mathcal{T}$-invariant subspace $\mathcal{U}$ of $\mathcal{V}$ is irreducible if there do not exist proper $\mathcal{T}$-invariant subspaces $\mathcal{U}_1, \mathcal{U}_2$ of $\mathcal{U}$, such that $\mathcal{U} = \mathcal{U}_1 \oplus \mathcal{U}_2$.

Definition 2.5. (Closure of a vector): Let $\mathcal{V}$ be a $\mathbb{F}$-vector space, $\mathbf{w} \in \mathcal{V}$ and $\mathcal{T} \subseteq \text{End}_{\mathbb{F}}(\mathcal{V})$. Then, the closure of $\mathbf{w}$ with respect to $\mathcal{T}$, denoted $\text{closure}_{\mathcal{T}}(\mathbf{w})$, is the smallest $\mathcal{T}$-invariant subspace of $\mathcal{V}$ containing $\mathbf{w}$.

2.3 Some basic results

Observation 2.1. *For $i, j \in [n], i \neq j$, let $E_{ij} \in M_n$ be such that the (i, j)-th entry is 1 and other entries are 0, and for $\ell \in [2, n]$, let $E_\ell \in M_n$ be a diagonal matrix with the $(1, 1)$-th and (ℓ, ℓ)-th entries as 1 and -1 respectively and other entries as 0. Then,*

1. *$\{I_n \otimes E_{ij},\ I_n \otimes E_\ell \ :\ i, j \in [n], i \neq j, \text{ and } \ell \in [2, n]\}$ is a basis of $\mathscr{L}_{col}$. Denote the elements of this standard basis as $S_1, \ldots, S_r$.*
2. *$\{E_{ij} \otimes I_n,\ E_\ell \otimes I_n \ :\ i, j \in [n], i \neq j, \text{ and } \ell \in [2, n]\}$ is a basis of $\mathscr{L}_{row}$. Denote the elements of this standard basis as $S_{r+1}, \ldots, S_{2r}$.*

Observation 2.2. *For every $F \in \mathcal{M}_{row}$ and $L \in \mathcal{M}_{col}$, $[F, L] = FL - LF = 0$.*

Observation 2.3. *For every $L_1, L_2 \in \mathscr{L}_{col}$ (similarly, $\mathscr{L}_{row}$), $[L_1, L_2] \in \mathscr{L}_{col}$ (respectively. $\mathscr{L}_{row}$).*

A proof of the following standard fact is given in Section A.1 of the Appendix.

[4]Over $\mathbb{C}$, $\mathfrak{g}_f$ also turns out to be a Lie algebra i.e. closed under the Lie bracket operation. However, over finite fields, it is not clear if it is closed under the bracket operation. We still stick with the terminology Lie algebra of a polynomial since in many cases, it does turn out to be closed under the bracket operation.

Fact 1. *Let $B \in M_n$. Then, the dimension of the space of matrices in M_n that commute with B is at least n, and the dimension of the space of matrices in $\mathcal{Z}_n$ that commute with B is at least $n-1$.*

We would also need the following facts (see [Kay12, KNST17] for their proofs).

Fact 2. *If $g \in \mathbb{F}[\mathbf{x}]$ is m-variate and $f(\mathbf{x}) = g(A \cdot \mathbf{x})$ for some $A \in \mathrm{GL}(m, \mathbb{F})$ then $\mathfrak{g}_f = A^{-1} \cdot \mathfrak{g}_g \cdot A$.*

Fact 3. *Suppose we have black box access to a m-variate polynomial $f \in \mathbb{F}[\mathbf{x}]$, where $|\mathbb{F}| \geq 2n^3$. Then, a basis of $\mathfrak{g}_f$ can be computed in randomized polynomial time.*

Fact 4. *Let $\mathcal{T} \subseteq M_{2r}$ be a $\mathbb{F}$-vector space. Given a basis $\{T_1, \ldots, T_s\}$ of $\mathcal{T}$ and a $\mathbf{w} \in \mathbb{F}^{2r}$, a basis of $\mathrm{closure}_{\mathcal{T}}(\mathbf{w})$ can be computed in time polynomial in r and the bit length of the entries in $\mathbf{w}$ and $T_1, \ldots, T_s$.*

The following theorem on the Lie algebra of Det is well-known over $\mathbb{C}$. We give a proof over any field (with a mild condition on the characteristic) in Section A.2 of the Appendix.

Theorem 4 (Lie algebra of Det)**.** *Let $n \geq 2$ and $\mathbb{F}$ be a field such that $\mathrm{char}(\mathbb{F}) \nmid n$. Then, the Lie algebra of Det_n equals the direct sum of the spaces $\mathscr{L}_{row}$ and $\mathscr{L}_{col}$, i.e., $\mathfrak{g}_{\mathsf{Det}} = \mathscr{L}_{row} \oplus \mathscr{L}_{col}$.*

The theorem implies that the set $\{S_1, \ldots, S_{2r}\}$, in Observation 2.1, forms a basis of $\mathfrak{g}_{\mathsf{Det}}$. The rows and columns of every element in $\mathfrak{g}_{\mathsf{Det}}$ are indexed by the $\mathbf{x}$ variables, in order. Let $f = \mathsf{Det}(A \cdot \mathbf{x})$ for some $A \in \mathrm{GL}(m, \mathbb{F})$. Then, Theorem 4 and Fact 2 imply that $\mathfrak{g}_f = A^{-1} \cdot \mathscr{L}_{\mathrm{row}} \cdot A \,\oplus\, A^{-1} \cdot \mathscr{L}_{\mathrm{col}} \cdot A$. We denote $A^{-1} \cdot \mathscr{L}_{\mathrm{row}} \cdot A$ and $A^{-1} \cdot \mathscr{L}_{\mathrm{col}} \cdot A$ by $\mathcal{F}_{\mathrm{row}}$ and $\mathcal{F}_{\mathrm{col}}$ respectively, and refer to $\mathcal{F}_{\mathrm{row}}$ and $\mathcal{F}_{\mathrm{col}}$ (similarly, $\mathscr{L}_{\mathrm{row}}$ and $\mathscr{L}_{\mathrm{col}}$) as the Lie subalgebras of $\mathfrak{g}_f$ (respectively, $\mathfrak{g}_{\mathsf{Det}}$) [5]. From Theorem 4, Observation 2.2 and 2.3, we get the following.

Observation 2.4. *For every $E, F \in \mathfrak{g}_f$, $[E, F] \in \mathfrak{g}_f$.*

It is also easy to prove the following observation.

Observation 2.5. *Let $\mathcal{A} \subseteq M_m$ be the $\mathbb{F}$-algebra generated by a basis of $\mathcal{F}_{col}$. Then,*

$$\mathcal{A} = A^{-1} \cdot (I_n \otimes M_n) \cdot A.$$

Finally, we record a special case of the Skolem-Noether theorem which will be used in Section 4. The general statement of the theorem can be found in [Lor08] (Theorem 20 on page 173).

Theorem 5 (Skolem-Noether)**.** *Let $n, s \in \mathbb{N}^{\times}$ such that $n \mid s$, and $\mathcal{A} \subseteq M_s$ be a $\mathbb{F}$-algebra (containing I_s) that is isomorphic to M_n via a map $\phi : M_n \to \mathcal{A}$. Then, there exists a $K \in \mathrm{GL}(s, \mathbb{F})$ such that,*

$$\phi(C) = K^{-1} \cdot (I_{s/n} \otimes C) \cdot K, \quad \textit{for every } C \in M_n.$$

3 Decomposition of $\mathfrak{g}_f$ into its Lie subalgebras

We show how to compute bases of $\mathcal{F}_{\mathrm{row}}$ and $\mathcal{F}_{\mathrm{col}}$ from black box access to $f = \mathsf{Det}(A \cdot \mathbf{x})$.

Theorem 6 (Decomposition of $\mathfrak{g}_f$)**.** *Let $n \geq 2$, $|\mathbb{F}| \geq 10n^4$ and $\mathrm{char}(\mathbb{F}) \nmid n(n-1)$. There is a randomized algorithm, which takes input black box access to f and outputs bases of $\mathcal{F}_{row}$ and $\mathcal{F}_{col}$ with high probability. The running time is $\mathrm{poly}(n, \gamma)$, where γ is the bit length of the coefficients of f.*

We first present the proof idea, and then the algorithm and its proof of correctness. The missing proofs of all the observations, claims and lemmas are given in Sections B, C and D of the Appendix.

[5] Observation 2.3 implies that $\mathcal{F}_{\mathrm{row}}$ and $\mathcal{F}_{\mathrm{col}}$ are closed under the Lie bracket operation and hence they are matrix Lie algebras.

3.1 Proof of Theorem 6: The idea

The algorithm relies on finding the irreducible invariant subspaces of a set of $\mathbb{F}$-linear maps on $\mathfrak{g}_f$. These linear maps (a.k.a adjoint homomorphisms of $\mathfrak{g}_f$) are defined as follows: For every $F \in \mathfrak{g}_f$,

$$\begin{aligned} \rho_F : \mathfrak{g}_f &\to \mathfrak{g}_f \\ E &\mapsto [E, F]. \end{aligned}$$

It is easy to see that ρ_F is a $\mathbb{F}$-linear map. Let $\{B_1, \ldots, B_{2r}\}$ be a basis of $\mathfrak{g}_f$ which can be computed in randomized polynomial time (by Fact 3). As ρ_F is $\mathbb{F}$-linear, we can associate a matrix $P_F \in M_{2r}$ with ρ_F, after fixing an ordering of the basis $(B_1, \ldots, B_{2r})$. Let $\mathcal{P} := \{P_F : F \in \mathfrak{g}_\mathrm{f}\}$.

Claim 3.1. *$\mathfrak{g}_f$ and $\mathcal{P}$ are isomorphic as $\mathbb{F}$-vector spaces via the map $F \mapsto P_F$ for every $F \in \mathfrak{g}_f$.*

Its proof is given in Section B.1 of the Appendix. This implies the following.

Observation 3.1. *The matrices $\{P_{B_1}, \ldots, P_{B_{2r}}\}$ is a basis of $\mathcal{P}$, which can be efficiently computed from $\{B_1, \ldots, B_{2r}\}$ (by considering the elements $[B_i, B_j]$, for $i, j \in [2r]$).*

We intend to study the irreducible invariant subspaces of $\mathcal{P}$ in order to compute bases of $\mathcal{F}_{\text{row}}$ and $\mathcal{F}_{\text{col}}$. The following Claim 3.2 would be useful in this regard.

It follows from Fact 2 that $J_i := A \cdot B_i \cdot A^{-1}$, for $i \in [2r]$, is a basis of $\mathfrak{g}_{\mathsf{Det}}$. Like ρ_F, we can associate a $\mathbb{F}$-linear map (i.e. adjoint homomorphism) χ_L with every $L \in \mathfrak{g}_{\mathsf{Det}}$ as follows:

$$\begin{aligned} \chi_L : \mathfrak{g}_{\mathsf{Det}} &\to \mathfrak{g}_{\mathsf{Det}} \\ K &\mapsto [K, L]. \end{aligned}$$

Let $Q_L \in M_{2r}$ be the matrix corresponding to the linear map χ_L, with respect to the (ordered) basis $(J_1, \ldots, J_{2r})$. The following claim implies that $\mathcal{P}$ does not depend on the transformation matrix A. Thus, it is sufficient to focus on $\mathfrak{g}_{\mathsf{Det}}$ to study the invariant subspaces of $\mathcal{P}$. The proof of the claim is given in Section B.2 of the Appendix.

Claim 3.2. *For every $i \in [2r]$, $Q_{J_i} = P_{B_i}$ and so the space $\mathcal{P} = \{Q_L : L \in \mathfrak{g}_{\mathsf{Det}}\}$.*

Like Claim 3.1, $\mathfrak{g}_{\mathsf{Det}}$ and $\mathcal{P}$ are isomorphic as $\mathbb{F}$-vector spaces via the map $L \mapsto Q_L$, for $L \in \mathfrak{g}_{\mathsf{Det}}$. The algorithm computes two invariant subspaces $\mathcal{V}_1$ and $\mathcal{V}_2$ of $\mathcal{P}$ that are defined as follows.

$$\begin{aligned} \mathcal{V}_1 &= \left\{ \mathbf{v} = (a_1, \ldots, a_{2r})^T \in \mathbb{F}^{2r} : \sum_{i \in [2r]} a_i \cdot J_i \in \mathscr{L}_{\text{col}} \right\}, \\ \mathcal{V}_2 &= \left\{ \mathbf{v} = (b_1, \ldots, b_{2r})^T \in \mathbb{F}^{2r} : \sum_{i \in [2r]} b_i \cdot J_i \in \mathscr{L}_{\text{row}} \right\}. \end{aligned} \tag{1}$$

Clearly, $\dim(\mathcal{V}_1) = \dim(\mathcal{V}_2) = r$. As $B_i = A^{-1} \cdot J_i \cdot A$, for $i \in [2r]$, we get

$$\begin{aligned} \mathcal{V}_1 &= \left\{ \mathbf{v} = (a_1, \ldots, a_{2r})^T \in \mathbb{F}^{2r} : \sum_{i \in [2r]} a_i \cdot B_i \in \mathcal{F}_{\text{col}} \right\}, \\ \mathcal{V}_2 &= \left\{ \mathbf{v} = (b, \ldots, b_{2r})^T \in \mathbb{F}^{2r} : \sum_{i \in [2r]} b_i \cdot B_i \in \mathcal{F}_{\text{row}} \right\}. \end{aligned} \tag{2}$$

From bases of $\mathcal{V}_1$ and $\mathcal{V}_2$, and $(B_1, \ldots, B_{2r})$, we get bases of $\mathcal{F}_{\text{col}}$ and $\mathcal{F}_{\text{row}}$ readily. The aspects of the space $\mathcal{P}$ that help in computing $\mathcal{V}_1$ and $\mathcal{V}_2$ are the facts that these are the only two irreducible invariant subspaces of $\mathcal{P}$ and bases of these can be computed from a random element of $\mathcal{P}$. These facts are proved and elaborated upon in the proof of correctness of Algorithm 1.

3.2 The decomposition algorithm

Algorithm 1 Computation of bases of $\mathcal{F}_{row}$ and $\mathcal{F}_{col}$

Input: Black box access to f.
Output: Bases of spaces $\mathcal{V}_1$ and $\mathcal{V}_2$ (as in Equation (2)).

1. Compute a basis $\{B_1, \ldots, B_{2r}\}$ of $\mathfrak{g}_f$ (see Fact 3), and form the basis $\{P_{B_1}, \ldots, P_{B_{2r}}\}$ of $\mathcal{P}$.
2. Pick a random element $Q = r_1 P_{B_1} + \cdots + r_{2r} P_{B_{2r}}$ from $\mathcal{P}$, where every r_i is chosen uniformly and independently at random from a fixed subset of $\mathbb{F}$ of size $10n^4$.
3. Compute the characteristic polynomial $h(z)$ of Q.
4. Factor $h(z)$ into irreducible factors over $\mathbb{F}$. Let $h(z) = z^{2(n-1)} \cdot h_1(z) \cdots h_k(z)$, where $z, h_1, \ldots, h_k$ are mutually coprime and irreducible. If h does not split as above, output 'Fail'.
5. For every $i \in [k]$, compute a basis of the null space $\mathcal{N}_i$ of $h_i(Q)$, pick a vector $\mathbf{v}$ from the basis of $\mathcal{N}_i$ and compute a basis of $\mathcal{C}_i := \text{closure}_{\mathcal{P}}(\mathbf{v})$ (using Fact 4).
6. Remove repetitive spaces from the set $\{\mathcal{C}_1, \ldots, \mathcal{C}_k\}$. After this, if we are *not* left with exactly two spaces $\mathcal{U}_1$ and $\mathcal{U}_2$ then output 'Fail'. Else, output bases of $\mathcal{U}_1$ and $\mathcal{U}_2$.

3.3 Analysis of the algorithm

Let us view the space $\mathcal{P}$ through the lens of a convenient basis of $\mathfrak{g}_{\mathsf{Det}}$, namely the standard basis $\{S_1, \ldots, S_{2r}\}$ (given in Observation 2.1). For $K \in \mathfrak{g}_{\mathsf{Det}}$, let $\mathbf{w}_K, \mathbf{v}_K \in \mathbb{F}^{2r}$ be the coordinate vectors of K with respect to the ordered bases $(S_1, \ldots, S_{2r})$ and $(J_1, \ldots, J_{2r})$ respectively. There is a basis change matrix $H \in \text{GL}(2r, \mathbb{F})$, such that for every $K \in \mathfrak{g}_{\mathsf{Det}}$,

$$\mathbf{v}_K = H \cdot \mathbf{w}_K. \tag{3}$$

Recall Q_L from Claim 3.2. Let $R_L := H^{-1} \cdot Q_L \cdot H$, for every $L \in \mathfrak{g}_{\mathsf{Det}}$, and

$$\mathcal{R} := \{R_L \ : \ L \in \mathfrak{g}_{\mathsf{Det}}\} = H^{-1} \cdot \mathcal{P} \cdot H. \tag{4}$$

Observe that $\{R_{S_1}, \ldots, R_{S_{2r}}\}$ is a basis of $\mathcal{R}$. Also,

$$R_L \cdot \mathbf{w}_K = \mathbf{w}_{[K,L]}, \tag{5}$$

for every $L, K \in \mathfrak{g}_{\mathsf{Det}}$. Let us note a few properties of $\mathcal{R}$.

Observation 3.2. *Every $R \in \mathcal{R} \subseteq M_{2r}$ is a block diagonal matrix having two blocks of size $r \times r$ each, i.e, the non-zero entries of R are confined to the entries $\{(S_i, S_j) \ : \ i, j \in [r]\}$ and $\{(S_i, S_j) \ : \ i, j \in [r+1, 2r]\}$.*

The proof of Observation 3.2 is given in Section C.1 of the Appendix. We refer to the two blocks of R as $R^{(1)}$ and $R^{(2)}$, corresponding to $\{S_1, \ldots, S_r\}$ and $\{S_{r+1}, \ldots, S_{2r}\}$, respectively. A snapshot of R is given in Figure 1. The next observation follows directly from the definition of $\mathcal{R}$.

Observation 3.3. *$\mathcal{W}$ is an invariant subspace of $\mathcal{R}$ if and only if $H \cdot \mathcal{W}$ is an invariant subspace of $\mathcal{P}$.*

It allows us to switch from $\mathcal{P}$ to $\mathcal{R}$ while studying the invariant subspaces of $\mathcal{P}$. The following lemmas on the invariant subspaces of $\mathcal{R}$ are crucial in arguing the correctness of Algorithm 1. Their proofs are given in Sections C.2 and C.3 of the Appendix.

Lemma 3.1 (Irreducible invariant subspaces)**.** *Let $\mathbf{w}_K \in \mathbb{F}^{2r}$ for a nonzero K in $\mathscr{L}_{col}$ or in $\mathscr{L}_{row}$. Then,*

$$\begin{aligned} \text{closure}_{\mathcal{R}}(\mathbf{w}_K) &= \{\mathbf{w}_L \;:\; L \in \mathscr{L}_{col}\} =: \mathcal{W}_1, \quad \text{if } K \in \mathscr{L}_{\text{col}}, \\ \text{closure}_{\mathcal{R}}(\mathbf{w}_K) &= \{\mathbf{w}_L \;:\; L \in \mathscr{L}_{row}\} =: \mathcal{W}_2, \quad \text{if } K \in \mathscr{L}_{\text{row}}. \end{aligned}$$

Moreover, $\mathcal{W}_1$ and $\mathcal{W}_2$ are the only two irreducible invariant subspaces of $\mathcal{R}$, and $\mathbb{F}^{2r} = \mathcal{W}_1 \oplus \mathcal{W}_2$.

Lemma 3.2 (Characteristic polynomial)**.** *Let $R = \sum_{i \in [2r]} \ell_i(r_1, \ldots, r_{2r}) \cdot R_{S_i}$, where $\ell_1, \ldots, \ell_{2r}$ are $\mathbb{F}$-linearly independent linear forms and $r_1, \ldots, r_{2r}$ are picked uniformly and independently at random from a fixed subset of $\mathbb{F}$ of size $10n^4$. Then, with high probability, the characteristic polynomial $h_R(z)$ of R factors as $z^{2(n-1)} \cdot h_1(z) \cdots h_k(z)$, where $z, h_1(z), \ldots, h_k(z)$ are mutually coprime irreducible polynomials over $\mathbb{F}$.*

3.3.1 Proof of correctness of Algorithm 1

In Step 2, we choose a random Q from $\mathcal{P}$. By Equation (4), there is a $R \in \mathcal{R}$, such that,

$$R = H^{-1} \cdot Q \cdot H \;=\; r_1 R_{J_1} + \cdots + r_{2r} R_{J_{2r}} \;=\; \ell_1(r_1, \ldots, r_{2r}) \cdot R_{S_1} + \cdots + \ell_{2r}(r_1, \ldots, r_{2r}) \cdot R_{S_{2r}},$$

where $\ell_1, \ldots, \ell_{2r}$ are $\mathbb{F}$-linearly independent linear forms in $r_1, \ldots, r_{2r}$. By Lemma 3.2, Step 4 holds with high probability. From Observation 3.2, R is a block diagonal matrix with blocks $R^{(1)}$ and $R^{(2)}$. Let $h(z) = g_1(z) \cdot g_2(z)$, where $g_1(z)$ and $g_2(z)$ are the characteristic polynomials of $R^{(1)}$ and $R^{(2)}$, respectively. There are a couple of factors of h, say h_1 and h_2, that divide g_1 and g_2, respectively. In Step 5, we compute the null spaces $\mathcal{N}_1$ and $\mathcal{N}_2$ of $h_1(Q)$ and $h_2(Q)$ respectively. As $h_1(R) = H^{-1} \cdot h_1(Q) \cdot H$ and $h_2(R) = H^{-1} \cdot h_2(Q) \cdot H$, the null spaces of $h_1(R)$ and $h_2(R)$, denoted by $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively, satisfy the following (due to Equation (3)):

$$\mathcal{O}_1 = H^{-1} \cdot \mathcal{N}_1 \quad \text{and} \quad \mathcal{O}_2 = H^{-1} \cdot \mathcal{N}_2.$$

Claim 3.3. *If $\mathbf{w}_K \in \mathcal{O}_1$ (similarly, $\mathbf{w}_K \in \mathcal{O}_2$) then $K \in \mathscr{L}_{col}$ (respectively, $K \in \mathscr{L}_{row}$).*

The proof of the claim is given in Section D.1 of the Appendix. In Step 5, we also pick a vector $\mathbf{v}$ from a null space, say $\mathcal{N}_1$, and compute $\text{closure}_{\mathcal{P}}(\mathbf{v})$. Clearly, $\mathbf{v} = \mathbf{v}_K$ for some $K \in \mathfrak{g}_{\text{Det}}$. So, $\mathbf{v}_K \in \mathcal{N}_1$ if and only if $\mathbf{w}_K = H^{-1} \cdot \mathbf{v}_K \in \mathcal{O}_1$. As $\mathcal{R} = H^{-1} \cdot \mathcal{P} \cdot H$, Observation 3.3 implies that

$$\begin{aligned} \text{closure}_{\mathcal{P}}(\mathbf{v}_K) &= H \cdot \text{closure}_{\mathcal{R}}(\mathbf{w}_K) \\ &= H \cdot \mathcal{W}_1 \quad (\text{ by Claim 3.3 and Lemma 3.1}) \\ &= \mathcal{V}_1 \qquad (\text{ by Equations (1) and (3), as } \mathcal{V}_1 = \{\mathbf{v}_L \;:\; L \in \mathscr{L}_{\text{col}}\}). \end{aligned}$$

Similarly, if we pick a $\mathbf{v} \in \mathcal{N}_2$ then $\text{closure}_{\mathcal{P}}(\mathbf{v}) = \mathcal{V}_2$. Thus, in Step 6, one of $\mathcal{U}_1$ and $\mathcal{U}_2$ is $\mathcal{V}_1$ and the other is $\mathcal{V}_2$. Finally, we can take $\mathcal{U}_1 = \mathcal{V}_1$ and $\mathcal{U}_2 = \mathcal{V}_2$ without loss of generality: Let $P \in M_m$ be the permutation matrix corresponding to the transposition map, i.e., P maps x_{ij} to x_{ji} when multiplied to $\mathbf{x}$. Clearly, $P^{-1} = P$. The following equation holds because P is a symmetry of Det.

$$\mathsf{Det}(\mathbf{x}) = \mathsf{Det}(P \cdot \mathbf{x}) \quad \text{and hence} \quad f(\mathbf{x}) = \mathsf{Det}(A \cdot \mathbf{x}) = \mathsf{Det}(PA \cdot \mathbf{x}).$$

Observe that $\mathscr{L}_{\text{col}} = P^{-1} \cdot \mathscr{L}_{\text{row}} \cdot P$. Hence,

$$\mathcal{F}_{\text{col}} = A^{-1}P^{-1} \cdot \mathscr{L}_{\text{row}} \cdot PA \quad \text{and} \quad \mathcal{F}_{\text{row}} = A^{-1}P^{-1} \cdot \mathscr{L}_{\text{col}} \cdot PA.$$

As the transformation matrix is unknown to the algorithm, we can take it to be either A or PA.

A comparison with [dG97b] and [CIK97]: In [dG97b, dG97a], a polynomial time algorithm was given to decompose a semisimple Lie algebra over $\mathbb{Q}$ (more generally, a characteristic 0 field) into a direct sum of simple Lie subalgebras. The Lie algebra $\mathfrak{g}_{\text{Det}}$ is semisimple and $\mathscr{L}_{\text{col}}$ and $\mathscr{L}_{\text{row}}$ are its two simple Lie subalgebras. So, our decomposition problem is a special case of the problem studied in [dG97b]. However, our algorithm works over any sufficiently large field $\mathbb{F}$ (in particular, finite fields), if $\text{char}(F) \nmid n(n-1)$. It is not quite clear to us if the algorithm in [dG97b] (which is somewhat different from our algorithm) can be easily adapted to achieve the same result in this special case. Lemma 3.1 shows that the decomposition of $\mathbb{F}^{2r}$ into irreducible invariant subspaces of $\mathcal{R}$ is unique. Using this information, it is possible to use the module decomposition algorithm in [CIK97] to compute bases of $\mathcal{F}_{\text{col}}$ and $\mathcal{F}_{\text{row}}$ in randomized polynomial time over finite fields. However, the module decomposition algorithm in [CIK97] does not work in general over $\mathbb{Q}$ without moving to an extension field.

4 Reduction of DET to FMAI

We give a randomized polynomial time reduction from DET to the FMAI problem. Recall the FMAI problem from Definition 1.1: An algorithm for FMAI takes input an ordered basis $(L_1, \ldots, L_m)$ of a $\mathbb{F}$-algebra $\mathcal{A} \subseteq M_s$ such that $\mathcal{A} \cong M_n$, and outputs a $\mathbb{F}$-algebra isomorphism $\phi : \mathcal{A} \to M_n$ in the form of an ordered basis $(C_1, \ldots, C_m)$ of M_n, where $C_i = \phi(L_i)$ for $i \in [m]$.

Lemma 4.1 (Reduction of DET to FMAI)**.** *Let $n \geq 2$, $|\mathbb{F}| > 10n^4$ and $\text{char}(\mathbb{F}) \nmid n(n-1)$. Then, there exists a randomized algorithm, with oracle access to FMAI, that takes input black-box access to a $f \in \mathbb{F}[\mathbf{x}]$ of degree n and solves DET for f over $\mathbb{F}$ with high probability. The running time of the algorithm is polynomial in n and the bit length of the coefficients of f.*

The proof of this lemma follows from the proof of correctness of the following algorithm.

4.1 The algorithm

Algorithm 2 Reduction of DET to FMAI

Input: Black-box access to a $f \in \mathbb{F}[\mathbf{x}]$ of degree n, and oracle access to an algorithm for FMAI.
Output: A matrix $B \in \text{GL}(m, \mathbb{F})$ such that $f = \text{Det}(B \cdot \mathbf{x})$, if such a B exists. Else, output 'Fail'.

1. Invoke Algorithm 1. Let $\{U_1, \ldots, U_r\}$ be the basis of the space $\mathcal{U}_1$ returned by Algorithm 1.
2. Generate a basis $\{L_1, \ldots, L_k\}$ of the algebra $\mathcal{A} := \mathbb{F}[U_1, \ldots, U_r]$. If $k \neq m$, output 'Fail'.
3. Invoke the FMAI oracle on $(L_1, \ldots, L_m)$ which returns a basis $(C_1, \ldots, C_m)$ of M_n.
4. Pick a *random* $M \in M_m$ satisfying $L_i \cdot M = M \cdot (I_n \otimes C_i)$ for every $i \in [m]$.
5. Let b be the evaluation of $f(M \cdot \mathbf{x})$ at $x_{11} = \ldots = x_{nn} = 1$ and remaining x_{ij} set to 0.
6. If $M \notin \text{GL}(m, \mathbb{F})$ or $b = 0$, output 'Fail'. Else, set $D = \text{diag}(b, 1, \ldots, 1) \in M_n$. Output $(I_n \otimes D) \cdot M^{-1}$.

4.2 Proof of correctness of Algorithm 2

If f is not equivalent to Det then it can be detected with high probability by checking if $f(\mathbf{a}) = b \cdot \mathsf{Det}(M^{-1}\mathbf{a})$ at a random point $\mathbf{a} \in_r S^m$, where $S \subseteq \mathbb{F}$ is sufficiently large. So, assume that $f = \mathsf{Det}(A \cdot \mathbf{x})$ for some $A \in \mathrm{GL}(m, \mathbb{F})$. The correctness of Algorithm 1 ensure that $\mathcal{U}_1 = \mathcal{F}_{\text{col}}$ without loss of generality. Step 2 can be executed efficiently by checking if $U_i U_j \in \operatorname{span}_{\mathbb{F}}\{U_1, \ldots, U_r\}$ for $i, j \in [r]$. Observation 2.5 implies that $\mathcal{A} \cong M_n$, i.e., $L_i = A^{-1} \cdot (I_n \otimes B_i) \cdot A$ for every $i \in [m]$, where $\{B_1, \ldots, B_m\}$ is a basis of M_n. In Step 3, the FMAI oracle returns a $\mathbb{F}$-algebra isomorphism $\phi : \mathcal{A} \to M_n$ such that $\{C_i = \phi(L_i) : i \in [m]\}$ is a basis of M_n. The following claim ensures the existence of a matrix M, computed in Step 4. Its proof is given in Section E.1 of the Appendix.

Claim 4.1. *There exists a $S \in \mathrm{GL}(n, \mathbb{F})$ such that $B_i = S^{-1} \cdot C_i \cdot S$ for every $i \in [m]$.*

Consider the linear system defined by the equation $L_i \cdot M = M \cdot (I_n \otimes C_i)$, where the entries of M are taken as variables. Step 4 is executed by picking the free variables of the solution space of the system from a sufficiently large subset of $\mathbb{F}$. Finally, the correctness of Step 6 is argued in the proof of the following claim which is given in Section E.2 of the Appendix.

Claim 4.2. *Suppose $f = \mathsf{Det}(A \cdot \mathbf{x})$, where $A \in \mathrm{GL}(m, \mathbb{F})$. Then, $f = \mathsf{Det}((I_n \otimes D) \cdot M^{-1} \cdot \mathbf{x})$ with high probability.*

5 DET over finite fields and over $\mathbb{Q}$

The proofs of Theorem 1 and 2 are completed by replacing the FMAI oracle in Step 3 of Algorithm 2 by known algorithms for FMAI over finite fields and $\mathbb{Q}$. These known results are stated below.

Theorem 7. [Theorem 5.1 of [Rón90]] *Let $\mathbb{F}$ be a finite field. Given a basis of a $\mathbb{F}$-algebra $\mathcal{A} \subseteq M_m$ such that $\mathcal{A} \cong M_n$, an isomorphism $\phi : \mathcal{A} \to M_n$ can be constructed in randomized* $\mathrm{poly}(m, \log |\mathbb{F}|)$ *time.*

Theorem 8. [Theorem 1 of [IRS12]] *There is a randomized algorithm with oracle access to* $\mathsf{IntFact}$ *that takes input a basis of a $\mathbb{Q}$-algebra $\mathcal{A} \subseteq M_m$ such that $\mathcal{A} \cong M_n$, and outputs an isomorphism $\phi : \mathcal{A} \to M_n$ with high probability. The algorithm runs in time polynomial in the bit length of the input, if n is bounded.*

Theorem 9. [Lemma 2.5 of [BR90]] *There is a randomized algorithm that takes input a basis of a $\mathbb{Q}$-algebra $\mathcal{A} \subseteq M_m$ such that $\mathcal{A} \cong M_n$, and outputs an isomorphism $\phi : \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{L} \to M_n(\mathbb{L})$ with high probability, where $\mathbb{L}$ is an extension field of $\mathbb{Q}$ satisfying $[\mathbb{L} : \mathbb{Q}] \leq n$. The algorithm runs in time polynomial in the bit length of the input.*

6 Factoring hardness of DET over $\mathbb{Q}$

This section is devoted to proving Theorem 3. We show that DET in the 2×2 setting over $\mathbb{Q}$ is at least as hard as factoring square-free integers. We will need the following theorem from [Rón87].

Theorem 10 ([Rón87]). *Assuming GRH, there is a randomized polynomial time reduction from the problem of factoring square-free integers to the following problem: Given non-zero $a, b \in \mathbb{Q}$, find rational numbers x, y, z (not all zero) such that $x^2 - ay^2 - bz^2 = 0$, if there exists such a solution.*

We will also need the following proposition, cited in [Rón87], to prove the next theorem. We give a proof from [Con16] in Section F.1, for completeness.

Proposition 6.1. *Let $a, b \in \mathbb{Q}$ be non-zero. Then the equation $x^2 - ay^2 - bz^2 = 0$ has a non-zero rational solution if and only if the equation $x^2 - ay^2 - bz^2 + abw^2 = 0$ has a non-zero rational solution.*

We are now ready to prove integer factoring hardness of DET in the next theorem. The proof is given in Section F.2.

Theorem 11. *Consider the polynomial $f_{a,b}(\mathbf{x}) = x_{1,1}^2 - ax_{1,2}^2 - bx_{2,1}^2 + abx_{2,2}^2$, where $a, b \in \mathbb{Q}$ are non-zero. Then $f_{a,b}(\mathbf{x}) = \mathsf{Det}_2(A \cdot \mathbf{x})$ for some $A \in \mathrm{GL}(4, \mathbb{Q})$ if and only if the equation $x^2 - ay^2 - bz^2 = 0$ has a non-zero rational solution (moreover, such a rational solution can be efficiently computed from A).*

Combining Theorems 10 and 11, we obtain Theorem 3.

Remark 1. *We want to explain how we got to the above reduction. Ronyai [Rón87] proved that the FMAI problem over $\mathbb{Q}$ is factoring hard even for $n = 2$ via quaternion algebras. If one takes a specific quaternion algebra and tries to constructs a polynomial f whose Lie algebra is the traceless part of the quaternion algebra, then it turns out the polynomial $f_{a,b}(\mathbf{x})$ is the unique homogeneous degree 2 polynomial that comes out. But in any case, in hindsight, the polynomial $f_{a,b}(\mathbf{x})$ seems like a natural candidate to use.*

7 Characterization of the determinant by its Lie algebra

In this section, we reduce the FMAI problem to DET under mild restrictions on $\mathbb{F}$. We start with the following claim that the Lie algebra of the determinant characterizes the determinant. This is well known over $\mathbb{C}$, but we give a proof in Section G.1 that works under mild restrictions on $\mathbb{F}$.

Lemma 7.1. *Let $f \in \mathbb{F}[\mathbf{x}]$ be any homogeneous polynomial of degree n such that $\mathscr{L}_{col} \subseteq \mathfrak{g}_f$ (see Section 2 for definition of $\mathscr{L}_{col}$). Also suppose $\mathrm{char}(\mathbb{F}) \nmid n$. Then $f(\mathbf{x}) = \alpha \cdot \mathsf{Det}_n(\mathbf{x})$ for some $\alpha \in \mathbb{F}$.*

Remark 2. *Note that without the $\mathrm{char}(\mathbb{F}) \nmid n$ condition, Lemma 7.1 is not true. For example, the polynomial $f(\mathbf{x}) = x_{1,1}^n + \mathsf{Det}_n(\mathbf{x})$ will have the same Lie algebra as $\mathsf{Det}_n(\mathbf{x})$ if $\mathrm{char}(\mathbb{F})$ divides n.*

We get the following corollary of Lemma 7.1.

Corollary 7.1. *Let $f \in \mathbb{F}[\mathbf{x}]$ be any homogeneous polynomial of degree n. Suppose that $A^{-1} \cdot \mathscr{L}_{col} \cdot A \subseteq \mathfrak{g}_f$ for some $A \in \mathrm{GL}(n^2, \mathbb{F})$ and $\mathrm{char}(\mathbb{F}) \nmid n$. Then $f(\mathbf{x}) = \alpha \cdot \mathsf{Det}_n(A \cdot \mathbf{x})$ for some $\alpha \in \mathbb{F}$.*

Proof. Consider $f'(\mathbf{x}) = f(A^{-1} \cdot \mathbf{x})$. By Fact 2, $\mathfrak{g}_{f'} = A \cdot \mathfrak{g}_f \cdot A^{-1}$ and so $\mathscr{L}_{\mathrm{col}} \subseteq \mathfrak{g}_{f'}$. By Lemma 7.1, we get that $f'(\mathbf{x}) = \alpha \cdot \mathsf{Det}_n(\mathbf{x})$ for some $\alpha \in \mathbb{F}$ and hence $f(\mathbf{x}) = \alpha \cdot \mathsf{Det}_n(A \cdot \mathbf{x})$. ☐

Corollary 7.1 allows us to reduce the FMAI problem to DET when n is constant (see Algorithm 3).

7.1 Proof of correctness of Algorithm 3 when $\mathrm{char}(\mathbb{F}) \nmid n$

The proof of correctness will follow from the following proposition, proved in Section G.2. The matrices $B_{i,j}$ and $L_{i,j}$ are as defined in Step 2 of the algorithm.

Proposition 7.1. *Suppose the algebra $\mathcal{A}$ spanned by $B_{1,1}, \ldots, B_{n,n}$ is isomorphic to M_n. Then there exist $K \in \mathrm{GL}(n^2, \mathbb{F})$ and matrices $C_{1,1}, \ldots, C_{n,n} \in M_n$ such that $L_{i,j} = K^{-1} \cdot (I_n \otimes C_{i,j}) \cdot K$ for all $i, j \in [n]$.*

Algorithm 3 Reduction of FMAI to DET

Input: Basis $\{B_1, \ldots, B_r\}$ of a $\mathbb{F}$-algebra $\mathcal{A} \subseteq M_m$, and access to an algorithm for DET.
Output: 1 if $\mathcal{A} \cong M_n$ for some $n \in \mathbb{N}$, 0 otherwise. If $\mathcal{A} \cong M_n$ then output an isomorphism.

1. If $r = \dim_{\mathbb{F}} \mathcal{A} \neq n^2$ for any $n \in \mathbb{N}$, output 0 and halt.
2. Index the basis elements by $[n] \times [n]$, i.e., rename them as $B_{1,1}, \ldots, B_{n,n}$. Compute $n^2 \times n^2$ matrices $L_{1,1}, \ldots, L_{n,n}$ as follows: $L_{i,j}$ is the matrix corresponding to the left-multiplication action of $B_{i,j}$ on $B_{1,1}, \ldots, B_{n,n}$. That is $B_{i,j} \cdot B_{i_2,j_2} = \sum_{i_1,j_1} L_{i,j}\left((i_1, j_1), (i_2, j_2)\right) \cdot B_{i_1,j_1}$.
3. Compute a basis for the traceless parts of the matrices $L_{i,j}$. That is, compute a basis $\tilde{L}_1, \ldots, \tilde{L}_s$ of the space spanned by $L_{1,1} - \frac{\operatorname{tr}(L_{1,1})}{n^2} I_{n^2}, \ldots, L_{n,n} - \frac{\operatorname{tr}(L_{n,n})}{n^2} I_{n^2}$. If $s \neq n^2 - 1$, output 0 and halt.
4. Find a non-zero homogeneous polynomial of degree n, $f(\mathbf{x})$, satisfying the equations
$$\sum_{i_1,j_1,i_2,j_2} M((i_1, j_1), (i_2, j_2)) \cdot x_{i_2,j_2} \cdot \frac{\partial f}{\partial x_{i_1,j_1}} = 0$$
for every $M \in \{\tilde{L}_1, \ldots, \tilde{L}_{n^2-1}\}$ (these give linear equations in the coefficients of f). If no such non-zero polynomial exists then output 0 and halt.
5. Run DET on f. If the output is 'Fail' then output 0 and halt. If $f(\mathbf{x}) = \operatorname{Det}_n(A \cdot \mathbf{x})$ then check if there exist matrices $F_{1,1}, \ldots, F_{n,n} \in M_n$ such $A \cdot L_{i,j} \cdot A^{-1} = I_n \otimes F_{i,j}$ for all i, j. If yes, output 1 and the isomorphism $\phi(B_{i,j}) = F_{i,j}$ (extended linearly to whole of $\mathcal{A}$). If no, check if there exist matrices $F_{1,1}, \ldots, F_{n,n} \in M_n$ such that $A \cdot L_{i,j} \cdot A^{-1} = F_{i,j} \otimes I_n$ for all i, j. If yes, output 1 and the isomorphism $\phi(B_{i,j}) = F_{i,j}$ (extended linearly to whole of $\mathcal{A}$). If no, output 0.

Now let us proceed to the proof of correctness of Algorithm 3. First of all, it is easy to ensure that whenever the algorithm outputs an isomorphism, it is actually an isomorphism. So what we need to prove is the converse. Suppose the algebra $\mathcal{A}$ is isomorphic to M_n. Then by Proposition 7.1, the space spanned by $\tilde{L}_1, \ldots, \tilde{L}_{n^2-1}$ is $K^{-1} \cdot \mathscr{L}_{\text{col}} \cdot K$. Then by Corollary 7.1, there is a unique solution to the equations in Step 4 given by $f(\mathbf{x}) = \alpha \cdot \operatorname{Det}_n(K \cdot \mathbf{x})$, for some $\alpha \in \mathbb{F}$, and so f is equivalent to the determinant. Hence, in Step 5, we will get an $A \in \mathrm{GL}(n^2, \mathbb{F})$ s.t. $f(\mathbf{x}) = \operatorname{Det}_n(A \cdot \mathbf{x})$. Since $\tilde{L}_1, \ldots, \tilde{L}_{n^2-1}$ span a Lie algebra of dimension $n^2 - 1$ and since they lie inside the Lie algebra of $\operatorname{Det}_n(A \cdot \mathbf{x})$, we must have that $\tilde{L}_1, \ldots, \tilde{L}_{n^2-1}$ span either $A^{-1} \cdot \mathscr{L}_{\text{col}} \cdot A$ or $A^{-1} \cdot \mathscr{L}_{\text{row}} \cdot A$. From this, we get that one of the following conditions should be true:

- There exist matrices $F_{1,1}, \ldots, F_{n,n} \in M_n$ such that $A \cdot L_{i,j} \cdot A^{-1} = I_n \otimes F_{i,j}$ for all $i, j \in [n]$.
- There exist matrices $F_{1,1}, \ldots, F_{n,n} \in M_n$ such that $A \cdot L_{i,j} \cdot A^{-1} = F_{i,j} \otimes I_n$ for all $i, j \in [n]$.

The implies that the algorithm will output 1 and an isomorphism into M_n. The complexity of the reduction is dominated by Step 4 which takes $n^{O(n)}$ field operations.

Acknowledgments

We would like to thank Youming Qiao for pointing us to the module decomposition algorithm in [CIK97]. NG would like to thank Vineet Nair for discussions on the structure of the Lie algebra of Det. We thank him for sharing his proof of Theorem 4.

References

[AS05] Manindra Agrawal and Nitin Saxena. Automorphisms of Finite Rings and Applications to Complexity of Problems. In *STACS 2005, 22nd Annual Symposium on Theoretical Aspects of Computer Science, Stuttgart, Germany, February 24-26, 2005, Proceedings*, pages 1–17, 2005.

[AS06] Manindra Agrawal and Nitin Saxena. Equivalence of f-algebras and cubic forms. In *STACS 2006, 23rd Annual Symposium on Theoretical Aspects of Computer Science, Marseille, France, February 23-25, 2006, Proceedings*, pages 115–126, 2006.

[BR90] László Babai and Lajos Rónyai. Computing irreducible representations of finite groups. *Mathematics of Computation*, 55(192):705–722, 1990.

[CFO$^+$15] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll. Explicit n-descent on elliptic curves III. Algorithms. *Math. Comput.*, 84(292):895–922, 2015.

[CIK97] Alexander L. Chistov, Gábor Ivanyos, and Marek Karpinski. Polynomial time algorithms for modules over finite dimensional algebras. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation, ISSAC '97, Maui, Hawaii, USA, July 21-23, 1997*, pages 68–74, 1997.

[Con16] Keith Conrad. Quaternion algebras, 2016.

[dG97a] W.A. de Graaf. *Algorithms for Finite-Dimensional Lie Algebras*. PhD thesis, Technical University of Eindhoven, 1997.

[dG97b] W.A. de Graaf. Calculating the structure of a semisimple Lie algebra. *Journal of Pure and Applied Algebra*, 117-118:319–329, 1997.

[Ebe89] W.M. Eberly. *Computations for algebras and group representations*. PhD thesis, Department of Computer Science, University of Toronto, 1989.

[Gro12] Joshua Abraham Grochow. *Symmetry and equivalence relations in classical and geometric complexity theory*. PhD thesis, Department of Computer Science, The University of Chicago, Chicago, Illinois, 2012.

[IRS12] Gábor Ivanyos, Lajos Rónyai, and Josef Schicho. Splitting full matrix algebras over algebraic number fields. *Journal of Algebra*, 354:211–223, 2012.

[Kay11] Neeraj Kayal. Efficient algorithms for some special cases of the polynomial equivalence problem. In *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2011, San Francisco, California, USA, January 23-25, 2011*, pages 1409–1421, 2011.

[Kay12] Neeraj Kayal. Affine projections of polynomials: extended abstract. In *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 643–662, 2012.

[KNS18] Neeraj Kayal, Vineet Nair, and Chandan Saha. Average-case linear matrix factorization and reconstruction of low width algebraic branching programs. *Electronic Colloquium on Computational Complexity (ECCC)*, 25:29, 2018.

[KNST17] Neeraj Kayal, Vineet Nair, Chandan Saha, and Sébastien Tavenas. Reconstruction of Full Rank Algebraic Branching Programs. In *32nd Computational Complexity Conference, CCC 2017, July 6-9, 2017, Riga, Latvia*, pages 21:1–21:61, 2017.

[Lor08] Falko Lorenz. *Algebra Volumne 2: Fields with structures, Algebras and advanced topics*. Springer, 2008.

[MS01] Ketan Mulmuley and Milind A. Sohoni. Geometric complexity theory I: an approach to the P vs. NP and related problems. *SIAM J. Comput.*, 31(2):496–526, 2001.

[MV97a] Meena Mahajan and V. Vinay. A Combinatorial Algorithm for the Determinant. In *Proceedings of the Eighth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), 5-7 January 1997, New Orleans, Louisiana, USA.*, pages 730–738, 1997.

[MV97b] Meena Mahajan and V. Vinay. Determinant: Combinatorics, Algorithms, and Complexity. *Chicago J. Theor. Comput. Sci.*, 1997, 1997.

[Pat96] Jacques Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*, pages 33–48, 1996.

[Rón87] Lajos Rónyai. Simple Algebras Are Difficult. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC), 1987, New York, New York, USA*, pages 398–408, 1987.

[Rón90] Lajos Rónyai. Computing the Structure of Finite Algebras. *J. Symb. Comput.*, 9(3):355–373, 1990.

[Sax06] Nitin Saxena. *Morphisms of rings and applications to complexity*. PhD thesis, Indian Institute of Technology Kanpur, 2006.

[Thi98] Thomas Thierauf. The Isomorphism Problem for Read-Once Branching Programs and Arithmetic Circuits. *Chicago J. Theor. Comput. Sci.*, 1998, 1998.

[Val79] Leslie G. Valiant. Completeness classes in algebra. In *Proceedings of the 11h Annual ACM Symposium on Theory of Computing, April 30 - May 2, 1979, Atlanta, Georgia, USA*, pages 249–261, 1979.

[Wal13] Lars Ambrosius Wallenborn. Computing the Hilbert symbol, quadratic form equivalence and integer factoring. Diploma thesis, University of Bonn, 2013.

A Proofs from Section 2

A.1 Proof of Fact 1

Fact 1 (restated): *Let $B \in M_n$. Then, the dimension of the space of matrices in M_n that commute with B is at least n, and the dimension of the space of matrices in $\mathcal{Z}_n$ that commute with B is at least $n-1$.*

Proof. Let $\overline{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}$ and $\tilde{B}$ be the Jordan Normal form of B over $\overline{\mathbb{F}}$. Then there exists a $G \in \mathrm{GL}(n, \overline{\mathbb{F}})$, such that

$$\tilde{B} = G \cdot B \cdot G^{-1}.$$

It is easy to see that if $\mathcal{S}, \tilde{\mathcal{S}}$ are the spaces of $n \times n$ matrices that commute with $B, \tilde{B}$ over $\mathbb{F}$ and $\overline{\mathbb{F}}$ respectively, then

$$\tilde{\mathcal{S}} = G \cdot \mathcal{S} \cdot G^{-1}.$$

Thus, it is sufficient to show that the dimension $\tilde{S}$ is at least n. As $\tilde{B}$ is the Jordan normal form of B, it is a block diagonal matrix, i.e. $\tilde{B} = \mathrm{diag}(G_1, \ldots, G_t)$, where G_i is an $n_i \times n_i$ size Jordan block for $i \in [t]$, such that $\sum_{i \in [t]} n_i = n$. For a fixed $i \in [t]$, the Jordan block $G_i \in M_{n_i}(\overline{\mathbb{F}})$ looks like

$$G_i = \begin{bmatrix} \lambda_i & 1 & 0 & \ldots & 0 & 0 \\ 0 & \lambda_i & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & 0 & \ldots & \lambda_i & 1 \\ 0 & 0 & 0 & \ldots & 0 & \lambda_i \end{bmatrix},$$

where $\lambda_i \in \overline{\mathbb{F}}$. Clearly, we can write

$$G_i = \lambda_i \cdot I_{n_i} + N_i,$$

where N_i (mentioned below) is a nilpotent matrix.

$$N_i = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 0 \end{bmatrix}.$$

It is easy to see that $I_{n_i}, N_i, \ldots, N_i^{n_i-1}$ are $\overline{\mathbb{F}}$-linearly independent and they commute with G_i. Since $\tilde{B}$ is a block diagonal matrix, the dimension of the space of matrices commuting with $\tilde{B}$ over $\overline{F}$ is at least $\sum_{i \in [t]} n_i = n$. This proves that the dimension of the space of matrices in M_n that commutes with B is at least n.

Let $B_1, \ldots, B_s$ be a basis of the space of matrices commuting with B. We are interested in the space of traceless matrices that commute with B. Let $\mathcal{C}$ be that space, defined as follows

$$\mathcal{C} := \left\{ a_1 B_1 + \cdots + a_s B_s \ : \ a_1, \ldots, a_s \in \mathbb{F} \quad \text{and} \quad \mathrm{tr}(\sum_{i \in [s]} a_i B_i) = 0 \right\}.$$

Observe that the dimension of $\mathcal{C}$ is $s-1$, which is at least $n-1$ as $s \geq n$.

□

A.2 Proof of Theorem 4

Theorem 4 (restated): *Let $n \geq 2$ and $\mathbb{F}$ be a field such that $\mathrm{char}(\mathbb{F}) \nmid n$. Then, the Lie algebra of Det_n equals the direct sum of the spaces $\mathscr{L}_{row}$ and $\mathscr{L}_{col}$, i.e., $\mathfrak{g}_{\mathsf{Det}} = \mathscr{L}_{row} \oplus \mathscr{L}_{col}$.*

Proof. Since $\mathscr{L}_{\text{row}} \cap \mathscr{L}_{\text{col}} = \{0\}$, it is sufficient to show $\mathfrak{g}_{\mathsf{Det}} = \mathscr{L}_{\text{row}} + \mathscr{L}_{\text{col}}$. Recall from Definition 2.2 that $B \in \mathfrak{g}_{\mathsf{Det}}$ satisfies

$$\sum_{i_1, j_1, i_2, j_2 \in [n]} b_{(i_1,j_1),(i_2,j_2)} \cdot x_{i_2,j_2} \cdot \partial_{i_1,j_1} \mathsf{Det} = 0 \ , \tag{6}$$

where $\partial_{i_1,j_1}\mathsf{Det} = \frac{\partial \mathsf{Det}}{\partial x_{i_1,j_1}}$ and $b_{(i_1,j_1),(i_2,j_2)}$ is the entry of B whose row and column are indexed by x_{i_1,j_1} and x_{i_2,j_2} respectively. For convenience, if $i_1 = i_2$ and $j_1 = j_2$ then we denote $b_{(i_1,j_1),(i_1,j_1)}$ as b_{i_1,j_1}. The following claims and observation imply that $\mathfrak{g}_{\mathsf{Det}} = \mathscr{L}_{\text{row}} \oplus \mathscr{L}_{\text{col}}$.

Claim A.1. *A matrix $B \in \mathfrak{g}_{\mathsf{Det}}$ if and only if the following equations are satisfied for $i_1, i_2, j_1, j_2 \in [n]$.*

$$b_{(i_1,j_1),(i_2,j_2)} = 0 \qquad \text{for } i_1 \neq i_2 \text{ and } j_1 \neq j_2 \ , \tag{7a}$$

$$\sum_{i \in [n]} b_{i,\sigma(i)} = 0 \qquad \text{for all permutations } \sigma \text{ of } [n], \tag{7b}$$

$$b_{(i_1,j_1),(i_1,j_2)} = b_{(i_2,j_1),(i_2,j_2)} \qquad \text{for } j_1 \neq j_2 \ , \tag{7c}$$

$$b_{(i_1,j_1),(i_2,j_1)} = b_{(i_1,j_2),(i_2,j_2)} \qquad \text{for } i_1 \neq i_2 \ . \tag{7d}$$

The proof of Claim A.1 is given in Section A.2.1.

Observation A.1. *Every matrix in $\mathscr{L}_{row} \oplus \mathscr{L}_{col}$ satisfies all the equations mentioned in Claim A.1.*

The proof of this observation can be verified easily. This implies that $\mathscr{L}_{\text{row}} \oplus \mathscr{L}_{\text{col}} \subseteq \mathfrak{g}_{\mathsf{Det}}$.

Claim A.2. *Suppose $B \in M_m$ satisfies all the equations given in Claim A.1. Then, there exist $M, N \in \mathscr{Z}_n$, such that*

$$B = M \otimes I_n + I_n \otimes N.$$

Claim A.2 implies that $\mathfrak{g}_{\mathsf{Det}} \subseteq \mathscr{L}_{\text{row}} \oplus \mathscr{L}_{\text{col}}$. Its proof is given in Section A.2.2. This completes the proof of Theorem 4. ☐

Now we give the proofs of Claims A.1 and A.2.

A.2.1 Proof of Claim A.1

It is easy to verify that if B satisfies the given equations then $B \in \mathfrak{g}_{\mathsf{Det}}$. Suppose $B \in \mathfrak{g}_{\mathsf{Det}}$. We prove the claim by understanding the types of monomials on the L.H.S of Equation (6). The following observation implies that Equation (7a) holds for every $i_1 \neq i_2$ and $j_1 \neq j_2$.

Observation A.2. *In Equation (6), if $i_1 \neq i_2$ and $j_1 \neq j_2$ then $b_{(i_1,j_1),(i_2,j_2)} = 0$.*

The proof of Observation A.2 follows from the fact that there is a monomial containing $x^2_{i_2,j_2}$ in the term $x_{i_2,j_2} \cdot \partial_{i_1,j_1}\mathsf{Det}$, that appears exactly once in Equation (6). This observation allows us to categorize the monomials occurring more than once in Equation (6) as follows:

1. We derive and multiply Det by same variable, i.e. $x_{i,j} \cdot \partial_{i,j}\mathsf{Det}$ for $i, j \in [n]$.

2. We derive and multiply Det with the variables having same 1st indices but different 2nd indices, i.e. $x_{i_1,j_2} \cdot \partial_{i_1,j_1}\text{Det}$ for $i_1, j_1, j_2 \in [n], j_1 \neq j_2$.

3. We derive and multiply Det with the variables having same 2nd indices but different 1st indices, i.e. $x_{i_2,j_1} \cdot \partial_{i_1,j_1}\text{Det}$ for $i_1, i_2, j_1 \in [n], i_1 \neq i_2$.

Observe that these three categories are pairwise monomial disjoint. This implies that Equation (6) can be decomposed into the following equations:

$$\sum_{i,j\in[n]} b_{i,j} \cdot x_{i,j} \cdot \partial_{i,j}\text{Det} = 0, \tag{8a}$$

$$\sum_{\substack{i_1,j_1,j_2\in[n]\\ j_1\neq j_2}} b_{(i_1,j_1),(i_1,j_2)} \cdot x_{i_1,j_2} \cdot \partial_{i_1,j_1}\text{Det} = 0, \tag{8b}$$

$$\sum_{\substack{i_1,i_2,j_1\in[n]\\ i_1\neq i_2}} b_{(i_1,j_1),(i_2,j_1)} \cdot x_{i_2,j_1} \cdot \partial_{i_1,j_1}\text{Det} = 0. \tag{8c}$$

Now we show that the analysis of Equations (8a), (8b) and (8c) imply Equations (7b), (7c) and (7d) respectively.

Analysis of Equation (8a): Observe that the L.H.S of Equation (8a) only contains the monomials of Det. As every monomial of Det is associated with a permutation on $[n]$, Equation (8a) implies that Equation (7b) holds, i.e. for every permutation σ on $[n]$,

$$\sum_{i\in[n]} b_{i,\sigma(i)} = 0.$$

Analysis of Equation (8b): We show here that every monomial in the term $x_{i_1,j_2} \cdot \partial_{i_1,j_1}\text{Det}$ occurs exactly twice in Equation (8b). The following subclaim would be helpful in this regard.

Subclaim A.1. *Let μ be a monomial of the term $x_{i_1,j_2} \cdot \partial_{i_1,j_1}\text{Det}$ in Equation (8b) such that μ contains the variables x_{i_1,j_2} and x_{i_2,j_2} for some $i_2 \in [n]$, $i_2 \neq i_1$. Then μ is a monomial of the term $x_{p_1,q_2} \cdot \partial_{p_1,q_1}\text{Det}$, where $q_1 \neq q_2$ in Equation (8b) if and only if $p_1 = i_1$ or $p_1 = i_2$, and $q_2 = j_2$ and $q_1 = j_1$. Further, the coefficient of μ in $x_{i_1,j_2} \cdot \partial_{i_1,j_1}\text{Det}$ and $x_{i_2,j_2} \cdot \partial_{i_2,j_1}\text{Det}$ are either 1 and -1, or -1 and 1 respectively.*

Proof. Observe that the monomial μ in $x_{i_1,j_2} \cdot \partial_{i_1,j_1}\text{Det}$ has no variable with the second index j_1 and has two variables with second index j_2. Since $q_1 \neq q_2$ in Equation (8b), it must be that $q_1 = j_1$ and $q_2 = j_2$. Further, as x_{p_1,j_2} is part of every monomial in $x_{p_1,j_2} \cdot \partial_{p_1,j_1}\text{Det}$, we have $p_1 = i_1$ or $p_1 = i_2$.

We now prove that the signs of the coefficients of μ in the two terms $x_{i_1,j_2} \cdot \partial_{i_1,j_1}\text{Det}$ and $x_{i_2,j_2} \cdot \partial_{i_2,j_1}\text{Det}$ are opposite. Let

$$\mu_1 = \frac{\mu \cdot x_{i_1,j_1}}{x_{i_1,j_2}} \quad \text{and} \quad \mu_2 = \frac{\mu \cdot x_{i_2,j_1}}{x_{i_2,j_2}}.$$

Then, observe that the monomials μ_1, and μ_2 are actually the monomials of Det, and the coefficient of μ in $x_{i_1,j_2} \cdot \partial_{i_1,j_1}\text{Det}$ and $x_{i_2,j_2} \cdot \partial_{i_2,j_1}\text{Det}$ are the coefficients of μ_1 and μ_2 respectively in Det. Since μ_1, and μ_2 are monomials of Det, there are two permutations σ, τ on $[n]$, such that

$$\mu_1 = \prod_{k=1}^{n} x_{k,\sigma(k)} \quad \text{and} \quad \mu_2 = \prod_{k=1}^{n} x_{k,\tau(k)}$$

and the coefficient of μ_1, μ_2 in Det are the signs of the permutation σ, τ respectively. From the definition of μ_1 and μ_2, for all $k \in [n]$, $k \neq i_1$ and $k \neq i_2$, $\sigma(k) = \tau(k)$. Observe that $\sigma(i_1) = j_1$, $\sigma(i_2) = j_2$, $\tau(i_1) = j_2$, and $\tau(i_2) = j_1$. Hence

$$\tau = (j_1, j_2) \cdot \sigma,$$

where (j_1, j_2) denotes the transposition that swaps j_1 and j_2. This implies the signs of σ and τ are opposite of each other. $\square$

The above subclaim immediately implies that Equation (7c) holds, i.e. for $i_1, i_2, j_1, j_2 \in [n], j_1 \neq j_2$,

$$b_{(i_1,j_1),(i_1,j_2)} = b_{(i_2,j_1),(i_2,j_2)}.$$

The analysis of Equation (8c) is similar to that of Equation (8b) and this implies that Equation (7d) holds, i.e. for $i_1, i_2, i_1, i_2 \in [n], i_1 \neq i_2$,

$$b_{(i_1,j_1),(i_2,j_1)} = b_{(i_1,j_2),(i_2,j_2)}.$$

This completes the proof of the claim.

A.2.2 Proof of Claim A.2

Let $B = (b_{(i_1,j_1),(i_2,j_2)})_{i_1,j_1,i_2,j_2 \in [n]}$. We define the matrices $M = (m_{i,j})_{i,j \in [n]}, N = (n_{i,j})_{i,j \in [n]}$ as follows:

1. For $i, j \in [n]$ and $i \neq j$
$$m_{i,j} := b_{(i,1),(j,1)} \quad \text{and} \quad n_{i,j} := b_{(1,i),(1,j)}.$$
2. For $i \in [n]$,
$$m_{i,i} := a_i \quad \text{and} \quad n_{i,i} := b'_{1,i} \quad ,$$
where $a_i := \frac{\sum_{j \in [n]} b_{i,j}}{n}$ (assuming $\mathrm{char}(\mathbb{F}) \nmid n$), and for $i, j \in [n]$, $b'_{i,j} := b_{i,j} - a_i$.

Now we argue that $B = M \otimes I_n + I_n \otimes N$, and $M, N \in \mathcal{Z}_n$. Since $B \in \mathfrak{g}_{\mathsf{Det}}$, the non-diagonal entries of B satisfy Equations (7a), (7c) and (7d). Hence, the non-diagonal entries of B are equal to the non-diagonal entries of $I_n \otimes M + N \otimes I_n$. Note that $\sum_{i \in [n]} b'_{1,i} = 0$, which implies $N \in \mathcal{Z}_n$. Let $t = \sum_{i \in [n]} a_i$. Consider the following equations we get from Equation (7b) corresponding to different permutations on $[n]$.

1. Equation with respect to the identity permutation on $[n]$:
$$b_{j,j} + \sum_{\substack{q \in [n] \\ q \neq j}} b_{q,q} \;=\; b'_{j,j} + (\sum_{\substack{q \in [n] \\ q \neq j}} b'_{q,q}) + t = 0. \tag{9}$$
2. Equation corresponding to the transposition (i, j) for $i, j \in [n]$:
$$b_{j,i} + b_{i,j} + \sum_{\substack{q \in [n] \\ q \neq i, q \neq j}} b_{q,q} \;=\; b'_{j,i} + b'_{i,j} + (\sum_{\substack{q \in [n] \\ q \neq i, q \neq j}} b'_{q,q}) + t = 0. \tag{10}$$

3. Equations corresponding to the transposition (p,i) for distinct $i,j,p \in [n]$:

$$b_{j,j} + b_{p,i} + b_{i,p} + \sum_{q \in [n] \setminus \{i,j,p\}} b_{q,q} \;=\; b'_{j,j} + b'_{p,i} + b'_{i,p} + (\sum_{q \in [n] \setminus \{i,j,p\}} b'_{q,q}) + t = 0. \tag{11}$$

4. Equations corresponding to the cycle (p,i,j) for distinct $i,j,p \in [n]$:

$$b_{p,i} + b_{i,j} + b_{j,p} + \sum_{q \in [n] \setminus \{i,j,p\}} b_{q,q} \;=\; b'_{p,i} + b'_{i,j} + b'_{j,p} + (\sum_{q \in [n] \setminus \{i,j,p\}} b'_{q,q}) + t = 0. \tag{12}$$

On subtracting Equation (10) from Equation (9), we have

$$b'_{j,j} - b'_{j,i} = b'_{i,j} - b'_{i,i} \,. \tag{13}$$

Similarly on subtracting Equation (12) from Equation (11), for all $p \in [n]$, and $p \neq i$, $p \neq j$ we have

$$b'_{j,j} - b'_{j,p} = b'_{i,j} - b'_{i,p} \,. \tag{14}$$

Adding Equation (13), and Equation (14) for all $p \in [n] \setminus \{i,j\}$, we have

$$(n-1)b'_{j,j} - \sum_{p \in [n], p \neq j} b'_{j,p} = (n-1)b'_{i,j} - \sum_{p \in [n], p \neq j} b'_{i,p} \quad .$$

This implies,

$$n \cdot b'_{j,j} - \sum_{p \in [n]} b'_{j,p} = n \cdot b'_{i,j} - \sum_{p \in [n]} b'_{i,p} \quad .$$

Since $\sum_{p \in [n]} b'_{j,p} = 0$ and $\sum_{p \in [n]} b'_{i,p} = 0$ (by definition of $b'_{i,j}$), and $\mathrm{char}(\mathbb{F}) \nmid n$, it follows that $b'_{j,j} = b'_{i,j}$. Since $b'_{j,j} = b'_{i,j}$ for all $i,j \in [n]$, from Equation (9) we have $t = \sum_{i \in [n]} a_i = 0$ (once again by using the fact that $\sum_{q \in [n]} b'_{i,q} = 0$), and hence $M \in \mathscr{Z}_n$. This completes the proof.

B Proofs from Section 3.1

B.1 Proof of Claim 3.1

Claim 3.1 (restated) *$\mathfrak{g}_f$ and $\mathcal{P}$ are isomorphic as $\mathbb{F}$-vector spaces via the map $F \mapsto P_F$ for every $F \in \mathfrak{g}_f$.*

Proof. It is easy to see that $\mathcal{P}$ is a $\mathbb{F}$-vector space. Consider the map $\tau(F) = P_F$. Observe that τ is $\mathbb{F}$-linear and onto. Let $F \in \mathrm{Ker}(\tau)$. Then $P_F = 0$, i.e., $[E,F] = 0$ for every $E \in \mathfrak{g}_f$, and hence $L := A \cdot F \cdot A^{-1} \in \mathfrak{g}_{\mathrm{Det}}$ commutes with every element of $\mathfrak{g}_{\mathrm{Det}}$. This implies $L \in \mathscr{L}_{\mathrm{col}} \cap \mathscr{L}_{\mathrm{row}}$, and so $L = \alpha \cdot I_{n^2}$ for some $\alpha \in \mathbb{F}$. As $\mathrm{tr}(L) = 0$ and $\mathrm{char}(\mathbb{F}) \nmid n$, we have $L = 0$. Hence, τ is injective. ☐

B.2 Proof of Claim 3.2

Claim 3.2 (restated): *For every $i \in [2r]$, $Q_{J_i} = P_{B_i}$ and so the space $\mathcal{P} = \{Q_L \,:\, L \in \mathfrak{g}_{\mathrm{Det}}\}$.*

Proof. Let $E \in \mathfrak{g}_{\mathrm{f}}, K \in \mathfrak{g}_{\mathrm{Det}}$ and $E = A \cdot K \cdot A^{-1}$. Observe that $\mathbf{u}_E = \mathbf{v}_K$, where $\mathbf{u}_E, \mathbf{v}_K$ are the coordinate vectors of E, K with respect to the bases $(B_1, \ldots, B_{2r})$ and $(J_1, \ldots, J_{2r})$ respectively. Hence, $Q_{J_i} \cdot \mathbf{v}_K = \mathbf{v}_{[K,J_i]} = \mathbf{u}_{[E,B_i]} = P_{B_i} \cdot \mathbf{u}_E = P_{B_i} \cdot \mathbf{v}_K$, implying $Q_{J_i} = P_{B_i}$. ☐

C Proofs from Section 3.3

C.1 Proof of Observation 3.2

Observation 3.2 (restated): *Every $R \in \mathcal{R} \subseteq M_{2r}$ is a block diagonal matrix having two blocks of size $r \times r$ each, i.e, the non-zero entries of R are confined to $\{(S_i, S_j) \;:\; i, j \in [r]\}$ and $\{(S_i, S_j) \;:\; i, j \in [r+1, 2r]\}$.*

Proof. Let $L = L_1 + L_2 \in \mathfrak{g}_{\mathrm{Det}}$, where $L_1 \in \mathscr{L}_{\mathrm{col}}, L_2 \in \mathscr{L}_{\mathrm{row}}$. From Equation (5), $R_L \cdot \mathbf{w}_{S_i} = \mathbf{w}_{[S_i, L]} = \mathbf{w}_{[Si, L_1] + [S_i, L_2]}$. Thus, $R_L \cdot \mathbf{w}_{S_i}$ is either $\mathbf{w}_{[S_i, L_1]}$ if $i \in [r]$, or $\mathbf{w}_{[S_i, L_2]}$ if $i \in [r+1, 2r]$. By Observation 2.3, $[S_i, L_1] \in \mathscr{L}_{\mathrm{col}}$ for $i \in [r]$ and $[S_i, L_2] \in \mathscr{L}_{\mathrm{row}}$ for $i \in [r+1, 2r]$. Hence R_L is block diagonal. $\square$

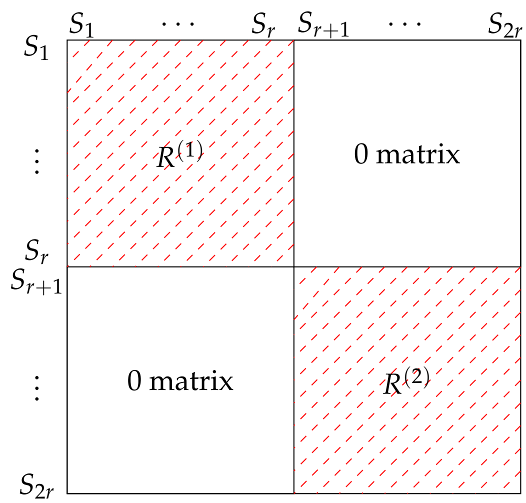

Figure 1: Structure of a matrix $R \in \mathcal{R}$

C.2 Proof of Lemma 3.1

Lemma 3.1 (restated) *Let $\mathbf{w}_K \in \mathbb{F}^{2r}$ for a nonzero $K \in \mathscr{L}_{col}$ or $K \in \mathscr{L}_{row}$. Then,*

$$\begin{aligned} \mathrm{closure}_{\mathcal{R}}(\mathbf{w}_K) &= \{\mathbf{w}_L \;:\; L \in \mathscr{L}_{\mathrm{col}}\} =: \mathcal{W}_1, \quad \text{if } K \in \mathscr{L}_{\mathrm{col}}, \\ \mathrm{closure}_{\mathcal{R}}(\mathbf{w}_K) &= \{\mathbf{w}_L \;:\; L \in \mathscr{L}_{\mathrm{row}}\} =: \mathcal{W}_2, \quad \text{if } K \in \mathscr{L}_{\mathrm{row}}. \end{aligned}$$

Moreover, $\mathcal{W}_1$ and $\mathcal{W}_2$ are the only two irreducible invariant subspaces of $\mathcal{R}$, and $\mathbb{F}^{2r} = \mathcal{W}_1 \oplus \mathcal{W}_2$.

Proof. We use the following three claims to prove the lemma. Their proofs are given in Sections C.2.1, C.2.2 and C.2.3 respectively. We prove these claims for $\mathscr{L}_{\mathrm{col}}$, similar proofs hold for $\mathscr{L}_{\mathrm{row}}$.

Claim C.1. *Let $\mathbf{w}_K$ be such that the entry indexed by $I_n \otimes E_{ij}$ (similarly, $E_{ij} \otimes I_n$) is nonzero for some $i, j \in [n], i \neq j$. Then $\mathrm{closure}_{\mathcal{R}}(\mathbf{w}_K)$ contains the unit vector $\mathbf{w}_{I_n \otimes E_{ij}}$ (respectively, $\mathbf{w}_{E_{ij} \otimes I_n}$).*

The next claim complements the previous one.

Claim C.2. *Let $p, q \in [n]$ and $p \neq q$. Then*

$$\mathrm{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{pq}}) = \{\mathbf{w}_L \;:\; L \in \mathscr{L}_{col}\} = \mathcal{W}_1.$$

Similarly, $\mathrm{closure}_{\mathcal{R}}(\mathbf{w}_{E_{pq} \otimes I_n}) = \{\mathbf{w}_L \;:\; L \in \mathscr{L}_{row}\} = \mathcal{W}_2$.

Claim C.3. *Suppose $\mathbf{w}_K \in \mathbb{F}^{2r}$ is such that the entry indexed by $I_n \otimes E_\ell$ (similarly, $E_\ell \otimes I_n$) for $\ell \in [2, n]$ is nonzero, and the entries indexed by $I_n \otimes E_{ij}$ (similarly, $E_{ij} \otimes I_n$) are zero for every $i, j \in [n], i \neq j$. Then, for some $i \neq \ell$,*

$$\mathbf{w}_{I_n \otimes E_{i\ell}} \in \text{closure}_{\mathcal{R}}(\mathbf{w}_K) \quad (\text{respectively, } \mathbf{w}_{E_{i\ell} \otimes I_n} \in \text{closure}_{\mathcal{R}}(\mathbf{w}_K)).$$

Claims C.1, C.2 and C.3 imply that for a nonzero $K \in \mathscr{L}_{\text{col}}$, $\text{closure}_{\mathcal{R}}(\mathbf{w}_K) = \mathcal{W}_1$ (similarly, for a nonzero $K \in \mathscr{L}_{\text{row}}$, $\text{closure}_{\mathcal{R}}(\mathbf{w}_K) = \mathcal{W}_2$). This completes the proof of the lemma. $\square$

C.2.1 Proof of Claim C.1

Consider the following subclaim whose proof is given in Section C.2.4.

Subclaim C.1. *There is a diagonal matrix $R \in \mathcal{R}$ such that $R(I_n \otimes E_\ell, I_n \otimes E_\ell) = R(E_\ell \otimes I_n, E_\ell \otimes I_n) = 0$ for every $\ell \in [2, n]$, and the remaining $2n^2 - 2n$ diagonal entries are distinct nonzero field elements.*

Let $R \in \mathcal{R}$ be the diagonal matrix mentioned above. Consider the following equation in the variables $a_1, \ldots, a_{2n^2-2n}$,

$$\mathbf{w}_{I_n \otimes E_{ij}} = \sum_{i=1}^{2n^2-2n} a_i \cdot R^i \cdot \mathbf{w}_K.$$

As the resulting system is a Vandermonde system, there is a solution over $\mathbb{F}$. Thus, $\mathbf{w}_{I_n \otimes E_{ij}} \in \text{closure}_{\mathcal{R}}(\mathbf{w}_K)$.

C.2.2 Proof of Claim C.2

We would show that the vectors $\mathbf{w}_{S_1}, \ldots, \mathbf{w}_{S_r}$ are in $\text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{pq}})$. The three observations below follow from the structure of matrices in $\mathcal{R}$ mentioned in Fact 7.

1. If $S = I_n \otimes E_{qj}$, where $j \neq p$ then $R_S \cdot \mathbf{w}_{I_n \otimes E_{pq}} = \mathbf{w}_{I_n \otimes E_{pj}}$. (From Fact 7 item 2(a))
2. If $S = I_n \otimes E_{ip}$, where $i \neq q$ then $R_S \cdot \mathbf{w}_{I_n \otimes E_{pq}} = -\mathbf{w}_{I_n \otimes E_{iq}}$. (From Fact 7 item 2(b))
3. If $q \neq 1, p = 1$ then for $S = I_n \otimes E_{q1}$, $R_S \cdot \mathbf{w}_{I_n \otimes E_{pq}} = \mathbf{w}_{I_n \otimes E_q}$. Similarly, if $p \neq 1, q = 1$ then for $S = I_n \otimes E_{1p}$, $R_S \cdot \mathbf{w}_{I_n \otimes E_{pq}} = -\mathbf{w}_{I_n \otimes E_p}$. (From Fact 7 item 2(d))

These properties immediately imply that

$$\begin{aligned}
\mathbf{w}_{I_n \otimes E_{pj}} &\in \text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{pq}}) \quad \text{for } j \in [n], j \neq p, \\
\mathbf{w}_{I_n \otimes E_{iq}} &\in \text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{pq}}) \quad \text{for } i \in [n], i \neq q, \\
\mathbf{w}_{I_n \otimes E_q} &\in \text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{pq}}) \quad \text{for } q \neq 1, p = 1, \\
\mathbf{w}_{I_n \otimes E_p} &\in \text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{pq}}) \quad \text{for } p \neq 1, q = 1.
\end{aligned} \tag{15}$$

Now we show that for $S = I_n \otimes E_{st}, \mathbf{w}_S \in \text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{pq}})$ for any $s, t \in [n]$, $s \neq t$. If $(s, t) = (p, q)$, there is nothing to prove. Suppose $(s, t) \neq (p, q)$.

Case 1: Suppose $t \neq p$, then from Equation (15), $\mathbf{w}_{I_n \otimes E_{pt}} \in \text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{pq}})$. Further, applying Equation (15) on $\mathbf{w}_{I_n \otimes E_{pt}}$, we get $\mathbf{w}_{I_n \otimes E_{st}} \in \text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{pt}})$ as $s \neq t$.

Case 2: Suppose $s \neq q$ then from Equation (15), $\mathbf{w}_{I_n \otimes E_{sq}} \in \text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{pq}})$. Further, applying Equation (15) on $\mathbf{w}_{I_n \otimes E_{sq}}$, we get $\mathbf{w}_{I_n \otimes E_{st}} \in \text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{sq}})$ as $s \neq t$.

Case 3: Let $(s,t) = (q,p)$. If $n \geq 3$ then pick a $j \in [n] \backslash \{p,q\}$. By applying Equation (15) repeatedly, we have $\mathbf{w}_{I_n \otimes E_{pj}} \in \text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{pq}})$, $\mathbf{w}_{I_n \otimes E_{qj}} \in \text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{pj}})$ and $\mathbf{w}_{I_n \otimes E_{qp}} \in \text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{qj}})$. If $n = 2$ then either p or q is 1. Suppose $p = 1$ and $s = q \neq 1$, then $\mathbf{w}_{I_n \otimes E_q} \in \text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{pq}})$ (from Equation (15)). On applying Fact 7 item 3(d), $\mathbf{w}_{I_n \otimes E_{qp}} \in \text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_q})$ (note that $\text{char}(\mathbb{F}) \neq 2$ as $\text{char}(\mathbb{F}) \nmid n(n-1)$).

To complete the proof of the claim, we would like to show that $\mathbf{w}_{I_n \otimes E_\ell} \in \text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{pq}})$ for every $\ell \in [2,n]$. It follows from what we have shown so far that $\mathbf{w}_{I_n \otimes E_{1\ell}} \in \text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{pq}})$. We conclude from Equation (15) that $\mathbf{w}_{I_n \otimes E_\ell} \in \text{closure}_{\mathcal{R}}(\mathbf{w}_{I_n \otimes E_{1\ell}})$.

C.2.3 Proof of Claim C.3

Let $K \in \mathscr{L}_{\text{col}}$ and $\mathbf{w}_K = \sum_{p \in [2,n]} a_p \cdot \mathbf{w}_{I_n \otimes E_p}$, where $a_p \in \mathbb{F}$ and $a_\ell \neq 0$. Then, for $i \notin \{1, \ell\}$,

$$R_{I_n \otimes E_{i\ell}} \cdot \mathbf{w}_K = \sum_{p \in [2,n]} a_p \cdot R_{I_n \otimes E_{i\ell}} \cdot \mathbf{w}_{I_n \otimes E_p} = (a_\ell - a_i) \cdot \mathbf{w}_{I_n \otimes E_{i\ell}}, \text{ from Fact 7 items 3(a) and 3(b), and}$$
$$R_{I_n \otimes E_{1\ell}} \cdot \mathbf{w}_K = \sum_{p \in [2,n]} a_p \cdot R_{I_n \otimes E_{1\ell}} \cdot \mathbf{w}_{I_n \otimes E_p} = (a_2 + \cdots + 2a_\ell + \cdots + a_n) \cdot \mathbf{w}_{I_n \otimes E_{1\ell}}, \text{ from Fact 7 item 3(c).}$$

If $R_{I_n \otimes E_{i\ell}} \cdot \mathbf{w}_K = 0$ for all $i \in [n] \setminus \{1, \ell\}$ then $a_i = a_\ell$ for all $i \in [n] \setminus \{1, \ell\}$, implying $R_{I_n \otimes E_{1\ell}} \cdot \mathbf{w}_K = n \cdot a_\ell \cdot \mathbf{w}_{I_n \otimes E_{1\ell}}$, which is non-zero as $\text{char}(\mathbb{F}) \nmid n$.

C.2.4 Proof of Subclaim C.1

The proof of the subclaim depends on the following facts, their proofs are given at the end of this section. We state these facts for $\mathscr{L}_{\text{col}}$, similar statements hold for $\mathscr{L}_{\text{row}}$.

Fact 5. *Let $S = I_n \otimes E_\ell$ for $\ell \in [2,n]$. Then $R_S \in \mathcal{R}$ is a diagonal matrix satisfying the following:*

1. *$R_S^{(2)}$ is an all zero matrix.*
2. *If $S_t = I_n \otimes E_{\ell'}, \ell' \in [2,n]$, then the (S_t, S_t)-th entry of R_S is 0.*
3. *If $S_t = I_n \otimes E_{ij}, i,j \in [n]$ and $i \neq j$, then the (S_t, S_t)-th entry of R_S is*
   (a) -1 *if $i = 1$ and $j \notin \{1, \ell\}$, or $j = \ell$ and $i \notin \{1, \ell\}$,*
   (b) 1 *if $i = \ell$ and $j \notin \{1, \ell\}$, or $j = 1$ and $i \notin \{1, \ell\}$,*
   (c) -2 *if $(i,j) = (1, \ell)$,*
   (d) 2 *if $(i,j) = (\ell, 1)$,*
   (e) 0 *otherwise.*

The next claim follows immediately from Fact 5.

Fact 6. *Let $R_1 = \sum_{\ell \in [2,n]} a_\ell \cdot R_{I_n \otimes E_\ell}$, where $a_2, \ldots, a_n \in \mathbb{F}$. Then R_1 is a diagonal matrix satisfying the following properties:*

1. $R_1^{(2)}$ *is a zero block.*

2. *If* $S_t = I_n \otimes E_{\ell'}, \ell' \in [2, n]$*, then the* (S_t, S_t)*-th entry of* R_1 *is 0.*

3. *If* $S_t = I_n \otimes E_{ij}, i, j \in [n], i \neq j$*, then the* (S_t, S_t)*-th entry of* R_1 *is*
   (a) $a_i - a_j$*, if* $i, j \in [2, n]$*,*
   (b) $-(\sum_{k=2}^{n} a_k + a_j)$ *if* $i = 1$*,*
   (c) $(\sum_{k=2}^{n} a_k + a_i)$ *if* $j = 1$*.*

Fact 7. *Let* $S = I_n \otimes E_{ij}$ *for* $i, j \in [n], i \neq j$*. Then,* R_S *satisfies the following properties:*

1. $R_S^{(2)}$ *is an all zero matrix.*

2. *A column indexed by* $I_n \otimes E_{pq}, p, q \in [n], p \neq q$ *has the following structure:*
   (a) *If* $p \neq j$ *and* $q = i$ *then the column contains exactly one nonzero entry, namely a* 1 *at the row indexed by* $I_n \otimes E_{pj}$*.*
   (b) *If* $q \neq i$ *and* $p = j$ *then the column contains exactly one nonzero entry, namely a* -1 *at the row indexed by* $I_n \otimes E_{iq}$ *.*
   (c) *If* $(p, q) = (j, i)$ *and* $i, j \neq 1$ *then the column has exactly two nonzero entries, namely a* 1 *and a* -1 *at the rows indexed by* $I_n \otimes E_i$ *and* $I_n \otimes E_j$ *respectively.*
   (d) *If* $(p, q) = (j, i)$ *and* $j = 1$ *(similarly,* $(p, q) = (j, i)$ *and* $i = 1$*) then the column has exactly one nonzero entry, a* 1 *(respectively, a* -1*) at the row indexed by* $I_n \otimes E_i$ *(respectively,* $I_n \otimes E_j$*).*
   (e) *Otherwise the entire column is zero.*

3. *A column indexed by* $I_n \otimes E_\ell, \ell \in [2, n]$ *has the following structure:*
   (a) *If* $i, j \neq 1$*, and* $\ell = i$ *then the column has exactly one nonzero entry, namely a* -1 *at the row indexed by* $I_n \otimes E_{ij}$*.*
   (b) *If* $i, j \neq 1$*, and* $\ell = j$ *then the column has exactly one nonzero entry, namely a* 1 *at the row indexed by* $I_n \otimes E_{ij}$*.*
   (c) *If* $i = 1$ *and* $\ell = j$ *then the column has exactly one nonzero entry, namely a* 2 *at the row indexed by* $I_n \otimes E_{ij}$*. If* $i = 1$ *and* $\ell \neq j$*, then the column exactly one nonzero entry, a* 1 *at the row indexed by* $I_n \otimes E_{ij}$*.*
   (d) *If* $j = 1$ *and* $\ell = i$*, then it has exactly one nonzero entry, a* -2 *at the row indexed by* $I_n \otimes E_{ij}$*. If* $j = 1$ *and* $\ell \neq i$*, then the column contains exactly one nonzero entry, a* -1 *at the row indexed by* $I_n \otimes E_{ij}$*.*
   (e) *Otherwise the column has all zero entries.*

Now we are ready to prove Subclaim C.1. We wish to show that $\mathcal{R}$ contains a diagonal matrix R such that $R(I_n \otimes E_\ell, I_n \otimes E_\ell) = R(E_\ell \otimes I_n, E_\ell \otimes I_n) = 0$ for every $\ell \in [2, n]$, and the remaining $2n^2 - 2n$ entries of R are distinct nonzero field elements. Let

$$R = \sum_{\ell \in [2,n]} (a_\ell \cdot R_{I_n \otimes E_\ell} + b_\ell \cdot R_{E_\ell \otimes I_n}),$$

where $a_\ell, b_\ell \in \mathbb{F}$. From Fact 6 (for both $\mathscr{L}_{\text{col}}$ and $\mathscr{L}_{\text{row}}$), R is a diagonal matrix with exactly $2(n-1)$ zero diagonal entries and the remaining diagonal entries are distinct nonzero linear forms in $a_2, \ldots, a_n$ and $b_2, \ldots, b_n$ (as $\text{char}(\mathbb{F}) \neq 2$). As $|\mathbb{F}| > \binom{2n^2-2n}{2}$, the Schwartz-Zippel lemma implies that if we substitute $a_2, \ldots, a_n$ and $b_2, \ldots, b_n$ randomly from a fixed subset of $\mathbb{F}$ of size $10n^4$, then R has the desired property.

The following is an immediate implication of the proof of Observation 3.2.

Observation C.1. *For all $i \in [r]$, $R^{(2)}_{S_i} = 0$. Similarly, for all $i \in [r+1, 2r]$, $R^{(1)}_{S_i} = 0$.*

Proof of Fact 5. Recall that $S = I_n \otimes E_\ell$ for $\ell \in [2, n]$. It follows from Observation C.1 that $R^{(2)}_S = 0$. To prove other parts of the fact, let us consider a generic element $T = I_n \otimes Z$ in $\mathscr{L}_{\text{col}}$, such that $Z = (a_{ij})_{i,j \in [n]}$. Clearly, $[T, S] = I_n \otimes [Z, E_\ell]$.

$$[Z, E_\ell] = \begin{bmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{\ell 1} & \ldots & a_{\ell n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{bmatrix} \cdot \begin{bmatrix} 1 & \ldots & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \ldots & -1 & \ldots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & \ldots & 0 \end{bmatrix} - \begin{bmatrix} 1 & \ldots & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \ldots & -1 & \ldots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & \ldots & 0 \end{bmatrix} \cdot \begin{bmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{\ell 1} & \ldots & a_{\ell n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{bmatrix}$$

From this, we get

$$[Z, E_\ell] = \begin{bmatrix} a_{11} & 0 & \ldots & -a_{i\ell} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{\ell 1} & 0 & \ldots & -a_{\ell\ell} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & 0 & \ldots & -a_{n\ell} & \vdots & 0 \end{bmatrix} - \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{i\ell} & \ldots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ -a_{\ell 1} & -a_{\ell 2} & \ldots & -a_{\ell\ell} & \ldots & -a_{\ell n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & \ldots & 0 \end{bmatrix}$$

This implies

$$[Z, E_\ell] = \begin{bmatrix} 0 & -a_{12} & \ldots & -2a_{i\ell} & \ldots & -a_{1n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 2a_{\ell 1} & a_{\ell 2} & \ldots & 0 & \ldots & a_{\ell n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & 0 & \ldots & -a_{n\ell} & \ldots & 0 \end{bmatrix}$$

Restricting Z to $E_{\ell'}$ and E_{ij} for different settings of i, j, ℓ' imply the result.

Proof of Fact 7. Part 1 follows from Observation C.1. Let us consider a generic element $T = I_n \otimes Z$ in $\mathscr{L}_{\text{col}}$, such that $Z = (a_{ij})_{i,j \in [n]}$. Clearly, $[T, S] = I_n \otimes [Z, E_{ij}]$. A derivation similar to that in the proof of Fact 5, implies the following.

$$[Z, E_{ij}] = \begin{bmatrix} 0 & 0 & \ldots & a_{1i} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ -a_{ji} & -a_{j2} & \ldots & a_{ii} - a_{jj} & \ldots & -a_{jn} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a_{ni} & \ldots & 0 \end{bmatrix},$$

where the rows and columns other than the i-th row and the j-th column are 0. Restricting Z to E_{pq} and E_ℓ for various settings of p, q, ℓ imply the result.

C.3 Proof of Lemma 3.2

Lemma 3.2 (restated). *Let $R = \sum_{i\in[2r]} \ell_i(r_1, \ldots, r_{2r}) \cdot R_{S_i}$, where $\ell_1, \ldots, \ell_{2r}$ are $\mathbb{F}$-linearly independent linear forms in $r_1, \ldots, r_{2r}$ that are picked uniformly and independently at random from a fixed subset of $\mathbb{F}$ of size $10n^4$. Then, with high probability, the characteristic polynomial $h_R(z)$ of R factors as $z^{2(n-1)} \cdot h_1(z) \cdots h_k(z)$, where $z, h_1(z), \ldots, h_k(z)$ are mutually coprime irreducible polynomials over $\mathbb{F}$.*

Proof. Let $R = R_L$ for some $L \in \mathfrak{g}_{\mathsf{Det}}$ and e be the maximum power of z dividing $h_R(z)$. Clearly, e is greater than equal to the dimension of the null space of R_L. Let us now lower bound the dimension of this null space. Suppose $\mathbf{w}_K$ is in the null space of R_L, where $K \in \mathfrak{g}_{\mathsf{Det}}$. Then,

$$R_L \cdot \mathbf{w}_K = 0,$$

which along with Equation (5) implies $\mathbf{w}_{[K,L]} = 0$. This means $[K, L] = 0$, i.e., K commutes with L. Thus, the dimension of the null space of R_L is exactly equal to the dimension of the subspace of $\mathfrak{g}_{\mathsf{Det}}$, that commute with L. We know that $L = L_1 + L_2$ and $K = K_1 + K_2$, where $L_1, K_1 \in \mathscr{L}_{\mathrm{col}}$ and $L_2, K_2 \in \mathscr{L}_{\mathrm{row}}$. Observation 2.2 implies that $[K, L] = 0$ if and only if $[K_1, L_1] = [K_2, L_2] = 0$. It follows from Fact 1 that $e \geq 2(n-1)$.

We know

$$R = \sum_{i\in[2r]} \ell_i(r_1, \ldots, r_{2r}) \cdot R_{S_i}.$$

Treat $r_1, \ldots, r_{2r}$ as formal variables. Then, from the above discussion, we get

$$h_R(z) = z^{2(n-1)} \cdot g(z),$$

where the coefficients of $g(z)$, which is a monic polynomial of degree $2n(n-1)$, are polynomials in $r_1, \ldots, r_{2r}$ of degree at most $2r$. As the linear forms $\ell_i(r_1, \ldots, r_{2r}), i \in [2r]$, are $\mathbb{F}$-linearly independent, Subclaim C.1 implies that there is a way to set the $\mathbf{r}$ variables to field constants, such that $g(z)$ is square-free and is not divisible by z. This means that the determinant of the Sylvester matrix of $g(z)$ and $\frac{\partial g(z)}{\partial z}$ is a nonzero polynomial in $\mathbf{r}$ variables of degree at most $8n^4$. As g is monic and $\mathrm{char}(\mathbb{F}) \nmid n(n-1)$, the dimension of the Sylvester matrix does not change with various settings of the $\mathbf{r}$ variables to field constants. Hence, from the Schwartz-Zippel lemma, if we plug $r_1, \ldots, r_{2r}$ with random values from a subset of $\mathbb{F}$ of size $10n^4$, then with high probability the characteristic polynomial $h_R(z)$ factors as

$$h_R(z) = z^{2(n-1)} \cdot h_1(z) \cdots h_k(z),$$

where $z, h_1, \ldots, h_k$ are mutually coprime irreducible polynomials over $\mathbb{F}$. □

D Proof from Section 3.3.1

D.1 Proof of Claim 3.3

Claim 3.3 (restated): *If $\mathbf{w}_k \in \mathcal{O}_1$ (similarly, $\mathbf{w}_k \in \mathcal{O}_2$) then $K \in \mathscr{L}_{col}$ (respectively, $K \in \mathscr{L}_{row}$).*

Proof. We give the proof for $\mathcal{O}_1$, a similar proof holds for $\mathcal{O}_2$. Recall that $\mathbf{w}_K$ is the coordinate vector of K with respect to the ordered basis $(S_1, \ldots, S_{2r})$ of $\mathfrak{g}_{\mathsf{Det}}$. Let $\mathbf{w}_K^{(1)}, \mathbf{w}_K^{(2)} \in \mathbb{F}^r$ be the sub vectors obtained from $\mathbf{w}_K$ by restricting it to the indices $S_1, \ldots, S_r$ and $S_{r+1}, \ldots, S_{2r}$ respectively. It is sufficient to show $\mathbf{w}_K^{(2)} = 0$ to prove $K \in \mathscr{L}_{\text{col}}$. Let $R \in \mathcal{R}$. Then, R is a block diagonal matrix with $R^{(1)}, R^{(2)}$ as the blocks. By definition, $h_1(R) \cdot \mathbf{w}_K = 0$, which implies

$$h_1(R^{(1)}) \cdot \mathbf{w}_K^{(1)} = h_1(R^{(2)}) \cdot \mathbf{w}_K^{(2)} = 0.$$

As $g_2(z)$ is the characteristic polynomial of $R^{(2)}$, from Cayley-Hamilton theorem $g_2(R^{(2)}) = 0$, which implies

$$g_2(R^{(2)}) \cdot \mathbf{w}_K^{(2)} = 0.$$

Since $h_1(z)$ and $g_2(z)$ are coprime polynomials, there exist $p_1, p_2 \in \mathbb{F}[z]$, such that

$$h_1(z) \cdot p_1(z) + g_2(z) \cdot p_2(z) = 1.$$

This implies

$$h_1(R^{(2)}) \cdot p_1(R^{(2)}) + g_2(R^{(2)}) \cdot p_2(R^{(2)}) = I_r.$$

On multiplying the above equation with $\mathbf{w}_K^{(2)}$, we get $\mathbf{w}_K^{(2)} = 0$ showing $K \in \mathscr{L}_{\text{col}}$. □

E Proofs from Section 4

E.1 Proof of Claim 4.1

Claim 4.1 (restated): *There exists a $S \in \mathrm{GL}(n, \mathbb{F})$ such that $B_i = S^{-1} \cdot C_i \cdot S$ for every $i \in [m]$.*

Proof. Recall that $L_i = A^{-1} \cdot (I_n \otimes B_i) \cdot A$, for $i \in [m]$, where $\{L_1, \ldots, L_m\}$ and $\{B_1, \ldots, B_m\}$ are bases of $\mathcal{A}$ and M_n respectively. Consider the following $\mathbb{F}$-algebra isomorphism from M_n to $\mathcal{A}$

$$\begin{aligned} \tau : M_n &\to \mathcal{A} \\ B &\mapsto A^{-1} \cdot (I_n \otimes B) \cdot A. \end{aligned}$$

Let $\Gamma = \phi \circ \tau$, where $\phi : \mathcal{A} \to M_n$ is the $\mathbb{F}$-algebra isomorphism constructed in Step 3 of Algorithm 2. Clearly, Γ is an $\mathbb{F}$-algebra isomorphism from M_n to M_n. On applying the Skolem-Noether theorem (Theorem 5) on Γ, we get a $S \in \mathrm{GL}(n, \mathbb{F})$ such that for every $i \in [m]$,

$$B_i = S^{-1} \cdot C_i \cdot S, \tag{16}$$

where $\Gamma(B_i) = \phi(L_i) = C_i$. □

E.2 Proof of Claim 4.2

Claim 4.2 (restated): *Suppose $f = \mathsf{Det}(A \cdot \mathbf{x})$, where $A \in \mathrm{GL}(m, \mathbb{F})$. Then, with high probability*

$$f = \mathsf{Det}((I_n \otimes D) \cdot M^{-1} \cdot \mathbf{x}).$$

Proof. Recall that $L_i = A^{-1} \cdot (I_n \otimes B_i) \cdot A$, where $L_1, \ldots, L_m$ and $B_1, \ldots, B_m$ are bases of the $\mathbb{F}$-algebras $\mathcal{A}$ and M_n respectively, and M satisfies the following equation for every $i \in [m]$,

$$L_i \cdot M = M \cdot (I_n \otimes C_i).$$

This implies, for all $i \in [m]$,

$$(I_n \otimes B_i) \cdot AM = AM \cdot (I_n \otimes C_i). \tag{17}$$

We view the matrix AM as a block matrix of block size $n \times n$. Let $M_{\ell k} \in M_n$ be the (ℓ, k)-th block of AM. Then, from Equation (17), we get the following equation for every $\ell, k \in [n]$ and $i \in [m]$:

$$B_i \cdot M_{\ell k} = M_{\ell k} \cdot C_i \tag{18}$$

Observation E.1. *The block $M_{11} \in M_n$ is an invertible matrix with high probability.*

Claim 4.1 implies that $A^{-1} \cdot (I_n \otimes S^{-1})$ is a candidate for M, and for this choice of M, $M_{11} = S^{-1}$. The Schwartz-Zippel lemma then implies the above observation.

From Observation E.1 and Equation (18), we get the next equation for every $\ell, k \in [n]$ and $i \in [m]$,

$$B_i \cdot M_{\ell k} \cdot M_{11}^{-1} = M_{\ell k} \cdot M_{11}^{-1} \cdot B_i.$$

As $B_1, \ldots, B_m$ is a basis of the M_n, the above equation implies that $M_{\ell k} \cdot M_{11}^{-1}$ commutes with every matrix in M_n. Thus, according to the following observation, $M_{\ell k} \cdot M_{11}^{-1} = b_{\ell k} \cdot I_n$, for some $b_{\ell k} \in \mathbb{F}$.

Observation E.2. *If $C \in M_n$ commutes with every $B \in M_n$ then $C = c \cdot I_n$ for some $c \in \mathbb{F}$.*

Observation E.2 can be easily proved by considering the basis $\{E_{ij} : i, j \in [n]\}$ of M_n, where E_{ij} is the matrix having (i, j)-th entry 1 and other entries 0. Thus, we get the following

$$A \cdot M = G \otimes M_{11} = (G \otimes I_n) \cdot (I_n \otimes M_{11}),$$

where $G = (b_{\ell k})_{\ell, k \in [n]}$. As $f = \mathsf{Det}(A \cdot \mathbf{x})$, we get

$$\begin{aligned} f(M \cdot \mathbf{x}) &= \mathsf{Det}(A \cdot M \cdot \mathbf{x}) \\ &= \mathsf{Det}((G \otimes I_n) \cdot (I_n \otimes M_{11}) \cdot \mathbf{x}) \\ &= \det(G \cdot X \cdot M_{11}^T) \\ &= b \cdot \det(X) \\ &= b \cdot \mathsf{Det}(\mathbf{x}) \\ &= \mathsf{Det}((I_n \otimes D) \cdot \mathbf{x}), \end{aligned}$$

where $D = \mathrm{diag}(b, 1, \ldots, 1) \in M_n$. This implies

$$f(\mathbf{x}) = \mathsf{Det}((I_n \otimes D) \cdot M^{-1} \cdot \mathbf{x}).$$

$\square$

F Proofs from Section 6

F.1 Proof of Proposition 6.1

One direction is trivial. For the other direction, we can assume a, b are not perfect squares. Otherwise, the equation $x^2 - ay^2 - bz^2 = 0$ has a non-zero rational solution and we are done. Suppose (x, y, z, w) is a non-zero rational solution to the equation $x^2 - ay^2 - bz^2 + abw^2 = 0$. We have

$$x^2 - ay^2 = b(z^2 - aw^2).$$

Now suppose that $z^2 - aw^2 = 0$. Then since a is not a perfect square, we get that $y = w = 0$. But then $x^2 = bz^2$. Since b is not a perfect square, $x = z = 0$ which contradicts the fact that (x, y, z, w) is non-zero. Hence $z^2 - aw^2$ is non-zero. We get that,

$$\begin{aligned} b = \frac{x^2 - ay^2}{z^2 - aw^2} = \frac{(x^2 - ay^2)(z^2 - aw^2)}{(z^2 - aw^2)^2} &= \frac{(xz + ayw)^2 - a(xw + yz)^2}{(z^2 - aw^2)^2} \\ &= \left(\frac{xz + ayw}{z^2 - aw^2}\right)^2 - a\left(\frac{xw + yz}{z^2 - aw^2}\right)^2. \end{aligned}$$

Hence we have a non-zero rational solution to the equation $x'^2 - ay'^2 - bz'^2 = 0$.

F.2 Proof of Theorem 11

First consider the case when $f_{a,b}(\mathbf{x}) = \mathsf{Det}_2(A \cdot \mathbf{x})$ for some $A \in \mathrm{GL}(4, \mathbb{Q})$. Then the equation $x^2 - ay^2 - bz^2 + abw^2 = 0$ has a non-zero rational solution given by

$$\begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} = A^{-1} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Then by Proposition 11, the equation $x^2 - ay^2 - bz^2 = 0$ also has a non-zero rational solution.
In the other direction, suppose that the equation $x^2 - ay^2 - bz^2 = 0$ also has a non-zero rational solution. Then at least one of the two equations, $u^2 - av^2 = b$ or $u^2 - bv^2 = a$ has a rational solution. Without loss of generality, assume it is the former. Then one can verify that

$$f_{a,b}(\mathbf{x}) = \mathsf{Det}_2 \begin{bmatrix} x_{1,1} + ux_{2,1} - avx_{2,2} & x_{1,2} + vx_{2,1} - ux_{2,2} \\ ax_{1,2} - avx_{2,1} + aux_{2,2} & x_{1,1} - ux_{2,1} + avx_{2,2} \end{bmatrix}.$$

To prove that the resulting transformation is invertible, denote

$$\begin{bmatrix} y_{1,1} \\ y_{1,2} \\ y_{2,1} \\ y_{2,2} \end{bmatrix} = \begin{bmatrix} x_{1,1} + ux_{2,1} - avx_{2,2} \\ x_{1,2} + vx_{2,1} - ux_{2,2} \\ ax_{1,2} - avx_{2,1} + aux_{2,2} \\ x_{1,1} - ux_{2,1} + avx_{2,2} \end{bmatrix}.$$

Then a tedious calculation reveals that

$$\begin{bmatrix} x_{1,1} \\ x_{1,2} \\ x_{2,1} \\ x_{2,2} \end{bmatrix} = \begin{bmatrix} (y_{1,1} + y_{2,2})/2 \\ (y_{1,2} + a^{-1}y_{2,1})/2 \\ (uy_{1,1} - avy_{1,2} + vy_{2,1} - uy_{2,2})/2b \\ (vy_{1,1} - uy_{1,2} + a^{-1}uy_{2,1} - vy_{2,2})/2b \end{bmatrix}.$$

G Proofs of Section 7

G.1 Proof of Lemma 7.1

We have that

$$\sum_{i,j,k,\ell} M_{(i,j),(k,\ell)} \cdot x_{k,\ell} \cdot \frac{\partial f}{\partial x_{i,j}} = 0, \tag{19}$$

for all $M \in \mathscr{L}_{\text{col}}$. Plugging in $M = I_n \otimes E_{j\ell}$ for $j \neq \ell$ (recall $E_{j\ell}$ is the elementary matrix with an 1 at position (j, ℓ), 0 everywhere else) into (19) gives that

$$\sum_i x_{i,\ell} \cdot \frac{\partial f}{\partial x_{i,j}} = 0, \ \forall j \neq \ell. \tag{20}$$

Plugging in $M = I_n \otimes \left(E_{jj} - n^{-1} I_n\right)$ ($\text{char}(\mathbb{F}) \nmid n$ and hence n^{-1} exists) into (19) gives that

$$\sum_i x_{i,j} \cdot \frac{\partial f}{\partial x_{i,j}} = n^{-1} \cdot \sum_{i',j'} x_{i',j'} \cdot \frac{\partial f}{\partial x_{i',j'}} = f(\mathbf{x}), \ \forall j, \tag{21}$$

where the second equality follows from Euler's identity (and the fact that $\text{char}(\mathbb{F}) \nmid n$). Let us denote by L, the matrix of polynomials, whose (j,i)-th entry is $\frac{\partial f}{\partial x_{i,j}}$. Then equations (20) and (21) tell us that[6]

$$LX = f(\mathbf{x}) \cdot I_n.$$

Hence

$$L = \frac{f(\mathbf{x})}{\text{Det}_n(\mathbf{x})} \cdot X_{\text{adj}},$$

where X_{adj} is the adjoint of the matrix X. Now entries of L and X_{adj} are homogeneous degree $n-1$ polynomials. Since $\text{Det}_n(\mathbf{x})$ is an irreducible polynomial, we get that $\text{Det}_n(\mathbf{x})$ divides $f(\mathbf{x})$. Since both are homogeneous of degree n, we get that $f(\mathbf{x}) = \alpha \cdot \text{Det}_n(\mathbf{x})$ for some $\alpha \in \mathbb{F}$.

G.2 Proof of Proposition 7.1

Let $\mathcal{L}$ be the algebra generated by the matrices $L_{1,1}, \ldots, L_{n,n}$. As $\mathcal{L}$ is isomorphic to $\mathcal{A}$ and $\mathcal{A} \cong M_n$, we have $\mathcal{L} \cong M_n$. Moreover, $\mathcal{L}$ contains the identity matrix I_{n^2}. Hence, by applying the Skolem-Noether theorem (Theorem 5), we get that there exist $K \in \text{GL}(n^2, \mathbb{F})$ and matrices $C_{1,1}, \ldots, C_{n,n} \in M_n$ such that $L_{i,j} = K^{-1} \cdot \left(I_n \otimes C_{i,j}\right) \cdot K$ for all $i, j \in [n]$.

[6] Recall the notation: X is a matrix whose (i,j)-th entry is the variable $x_{i,j}$ and $\mathbf{x}$ is the vectorized version with entries arranged in a row major fashion.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il