Matrix Rigidity Depends on the Target Field

László Babai
University of Chicago, IL, USA

Bohdan Kivva
University of Chicago, IL, USA

Abstract

The *rigidity* of a matrix A for target rank r is the minimum number of entries of A that need to be changed in order to obtain a matrix of rank at most r (Valiant, 1977).

We study the dependence of rigidity on the target field. We consider especially two natural regimes: when one is allowed to make changes only from the field of definition of the matrix ("strict rigidity"), and when the changes are allowed to be in an arbitrary extension field ("absolute rigidity").

We demonstrate, apparently for the first time, a separation between these two concepts. We establish a *gap of a factor of* $3/2 - o(1)$ between strict and absolute rigidities.

The question seems especially timely because of recent results by Dvir and Liu (*Theory of Computing*, 2020) where important families of matrices, previously expected to be rigid, are shown not to be absolutely rigid, while their strict rigidity remains open. Our lower-bound method combines elementary arguments from algebraic geometry with "untouched minors" arguments.

Finally, we point out that more families of long-time rigidity candidates fall as a consequence of the results of Dvir and Liu. These include the incidence matrices of projective planes over finite fields, proposed by Valiant as candidates for rigidity over $\mathbb{F}_2$.

2012 ACM Subject Classification Theory of computation; Theory of computation → Complexity theory and logic

Keywords and phrases Matrix rigidity, field extension

Digital Object Identifier 10.4230/LIPIcs.CCC.2021.41

Funding The work of the authors has been partially supported by L. Babai's NSF Grant CCF 1718902. All statements made are solely due to the authors and have not been evaluated or endorsed by the NSF.

Acknowledgements The senior author thanks Zeev Dvir and Allen Liu for clarifications regarding their results. The authors thank an anomymous reviewer for pointing out the work of Samorodnitsky et al.

1 Introduction

1.1 Matrix rigidity. Dependence on the field

Matrix rigidity was introduced by Leslie Valiant in his seminal paper [16] as a tool to prove lower bounds on the complexity of linear arithmetic circuits (where each gate computes a linear combination of its inputs). Such circuits compute linear functions $x \mapsto Ax$ for some matrix A. Razborov [12] linked the rigidity concept to separating the polynomial hierarchy in communication complexity.

▶ **Definition 1** (Matrix rigidity). *Let $\mathbb{L}/\mathbb{K}$ be a field extension ($\mathbb{K}$ is a subfield of $\mathbb{L}$) and let $A \in \mathbb{K}^{n\times m}$. Denote by $R_{\mathbb{L}}(A, r)$ the minimum number of non-zero entries in a matrix $Z \in \mathbb{L}^{n\times m}$ for which $A + Z$ has rank at most r. The function $R_{\mathbb{L}}(A, \cdot)$ is called the* matrix rigidity function *of A over $\mathbb{L}$.*

The definition of rigidity depends on a pair of fields: $\mathbb{K}$, the field in which the matrix lives, and the extension field $\mathbb{L} \supseteq \mathbb{K}$, over which the changes to A are to be made. There are two natural regimes in which we especially propose to study matrix rigidity.

36th Computational Complexity Conference (CCC 2021).
Editor: Valentine Kabanets; Article No. 41; pp. 41:1–41:26
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

We say that $\mathbb{K}$ is the *field of definition* of a matrix $A \in \mathbb{F}^{n\times m}$ (where $\mathbb{F}$ is a field) if $\mathbb{K}$ is the smallest subfield of $\mathbb{F}$ containing all elements of A.

▶ **Definition 2** (Strict rigidity). *Let $\mathbb{K}$ denote the field of definition of the matrix A. We call the function $R_{\mathbb{K}}(A,\cdot)$ the* strict rigidity *function of A.*

▶ **Definition 3** (Absolute rigidity). *We define the* absolute rigidity *of A as*

$$R^*(A,r) = \min_{\mathbb{L}} R_{\mathbb{L}}(A,r),$$

where the minimum ranges over all extension fields $\mathbb{L}$ of the field of definition of A.

The main result of this paper shows, apparently for the first time, that the notions of strict and absolute rigidity are indeed different. We establish a *gap of a factor of* $3/2 - o(1)$ between these quantities.

The *degree* of a field extension $\mathbb{L}/\mathbb{K}$ is the dimension of $\mathbb{L}$ over $\mathbb{K}$. Extensions of degree 2 are called *quadratic extensions.*

▶ **Theorem 4.** *Let $\mathbb{K}$ be a field of characteristic zero and let $\mathbb{L}$ be a quadratic extension of $\mathbb{K}$. For every r there exists a $2r \times 2r$ matrix A_r over $\mathbb{K}$ such that $R_{\mathbb{L}}(A_r,r) \le 2r$ while $R_{\mathbb{K}}(A_r,r) \ge 3r-2$.*

Note that the second bound requires a lower-bound technique for rigidity.

We expect much larger gaps; indeed, larger gaps will be needed to show the depedence of Valiant-rigidity on the field (see below).

We also point out that for any matrix A over a field $\mathbb{K}$ we have $R^*(A,r) = R_{\overline{\mathbb{K}}}(A,r)$, where $\overline{\mathbb{K}}$ denotes the algebraic closure of $\mathbb{K}$ (Sec. 4). In other words, for every matrix A, absolute rigidity can be achieved over a finite extension of the field of definition of A (see Cor. 55). However, effective bounds on the degree of this extension remain an open question.

A similar result holds for linear arithmetic circuits (Prop. 56).

1.2 Valiant-rigidity, non-rigidity results

While the distinction between strict and absolute rigidity seems natural and we find it somewhat surprising that apparently it has not previously been addressed, unexpected recent non-rigidity results give particular timeliness to this question.

To discuss these results, we need some asymptotic terminology.

We say that the *order* of an $n\times n$ matrix is n. We use the term *"family of square matrices"* to mean a set of square matrices of unbounded order.

▶ **Definition 5** (Valiant-rigid). *Let $\mathcal{F}$ be a family of square matrices. For $A \in \mathcal{F}$, let $\mathbb{K}(A)$ denote the field of definition of A, and let $\mathbb{L}(A)$ be an extension field of $\mathbb{K}(A)$. We say that the family $\mathcal{F}$ is* Valiant-rigid over the extension fields $\mathbb{L}(A)$ *if there exists $\epsilon > 0$ such that for every function $r(n) = O(n/\log\log n)$, for all matrices A in the family, $R_{\mathbb{L}(A)}(A, r(n_A)) = \Omega(n_A^{1+\epsilon})$, where n_A denotes the order of A.*

It seems the term "Valiant-rigid" was introduced in [3] (but their definition did not consider the effect of the field).

The terms "strictly" and "absolutely" Valiant-rigid should now be self-explanatory.

For one of the families, long believed to be rigid, the family of Walsh–Hadamard matrices, Alman and Williams [2] proved that it is in fact not strictly Valiant-rigid.

Recently, Dvir and Liu [4] proved that no family of Discrete Fourier Transform (DFT) matrices for abelian groups G and no family of G-circulant matrices (see Def. 57) is absolutely Valiant-rigid. However, strict Valiant-rigidity of these families remains an open problem.

Note that the Walsh–Hadamard matrices are the DFT matrices for elementary abelian 2-groups, yet the Dvir–Liu result does not fully reproduce the Alman–Williams result for these matrices precisely because of the target field: while Dvir and Liu prove that these matrices are not absolutely Valiant-rigid, Alman and Williams proved the stronger result that these matrices are not strictly rigid.

In Section 5 we point out that the following families of long-time rigidity candidates also fall as a consequence of the results of Dvir and Liu.

1. No family of Paley–Hadamard matrices is absolutely Valiant-rigid. (Note: The orders of these Hadamard matrices are exponentially denser than the orders of the Walsh–Hadamard matrices, shown not to be strictly Valiant-rigid by Alman and Williams [2].)
2. No family of point–hyperplane incidence matrices of Galois geometries (projective geometries over finite fields) is strictly Valiant-rigid over any fixed finite field. (Note: The incidence matrices of finite projective planes were proposed by Valiant [16] as candidates for rigidity over $\mathbb{F}_2$.)
3. No family of point–hyperplane incidence matrices of Galois geometries is absolutely Valiant-rigid in characteristic zero.
4. No family of Vandermonde matrices whose generators form a geometric progression is absolutely Valiant-rigid.

We should remind the reader that absolute rigidity is a stronger property than strict rigidity; and therefore the statement that a matrix is "not strictly rigid" is stronger than the statement that it is "not absolutely rigid."

We mention that Samorodnitsky *et al.* [13] proved rigidity lower bounds for the point-hyperplane incidence matrices of Galois geometries (projective spaces over finite fields), conditional on their conjecture that the set of normalized $\{0, 1\}$-vectors arising from an arbitrary low-dimensional subspace of $\mathbb{F}_2^n$ admits non-trivial approximation by a low-dimensional Euclidean space. They show that if their conjecture is true, then there exists $\delta > 0$, such that $R_{\mathbb{F}_2}(V_d, n^{(2/d)+\delta}) \geq n^{1-2/d}$, where V_d is the $n \times n$ point–hyperplane incidence matrix of the d-dimensional Galois geometry $PG(d, q)$. Our results do not refute their conjecture, as we prove upper bounds for the target rank of an order $n \cdot \exp(-(\log n)^c)$, while [13] aims at a much smaller target rank, $n^{(2/d)+\delta}$.

1.3 Implications to complexity theory

This line of work may lead to peculiar consequences in complexity theory. Gaps between strict and absolute rigidity raise the prospect that rational linear functions may be easier to compute by arithmetic circuits over larger fields than over $\mathbb{Q}$.

▶ **Problem 6.** Does there exist a family of square matrices A over $\mathbb{Q}$ such that the linear functions $x \mapsto Ax$ can be computed by logarithmic-depth, linear-size circuits over $\mathbb{C}$ but not over $\mathbb{Q}$?

While $\mathbb{C}$ can be replaced by a finite extension of $\mathbb{Q}$ without changing the topology of the circuit (Prop. 56), a field extension of bounded degree will not create a gap in circuit complexity. Indeed, if the degree of the extension $\mathbb{L}/\mathbb{K}$ is k then operations in $\mathbb{L}$ can be simulated by operations on vectors of length k over $\mathbb{K}$. So our belief that strong separation of rigidity may exist already for quadratic extensions (Conj. 9), if true, will not help.

1.4 Our construction

We make the following "standard assumption."

($*$) Let $\mathbb{K}$ be a field of characteristic zero and let $\mathbb{L}/\mathbb{K}$ be a quadratic extension.

We prove that under this assumption, the rigidity with respect to $\mathbb{K}$ in general does not equal the rigidity with respect to $\mathbb{L}$. In order to show this, for some $A \in \mathbb{K}^{n\times n}$ and $r, k \geq 1$ one needs to establish both an upper bound and a lower bound,

(UB) $R_{\mathbb{L}}(A, r) \leq k$ (LB) $R_{\mathbb{K}}(A, r) > k$.

It is clear that for all $A \in \mathbb{K}^{n\times n}$, the inequality $R_{\mathbb{K}}(A, r) \leq (n-r)^2$ is satisfied. In [16], Valiant showed that for an infinite field $\mathbb{K}$, almost all matrices $A \in \mathbb{K}^{n\times n}$ have maximal possible absolute rigidity $R^*(A, r) = (n-r)^2$. In particular, this means that we should not expect (UB) to hold, unless A is selected in some special way.

We take the following approach. In order to automatically satisfy (UB) we start with a matrix $M \in \mathbb{L}^{n\times n}$ of rank r that has at most k entries not in $\mathbb{K}$. Then every matrix A, obtained from M by replacing these entries with elements from $\mathbb{K}$, satisfies (UB). Hence, we only need to show that for a proper choice of M and for a proper choice of changes for elements not in $\mathbb{K}$, A satisfies (LB).

By our standard assumption ($*$), we can write $\mathbb{L} = \mathbb{K}[\omega]$ for some $\omega \in \mathbb{L}$ with $\omega^2 \in \mathbb{K}$. We focus on the following (algebraic) sets of matrices:

$$\mathcal{D}_r(\mathbb{K}, \omega) = \{M \in \mathbb{K}^{2r\times 2r} \mid \operatorname{rank}(M + \omega I) \leq r\}, \tag{1}$$

$$\mathcal{C}_r(\mathbb{K}, \omega) = \{M + D \in \mathbb{K}^{2r\times 2r} \mid M \in \mathcal{D}_r(\mathbb{K}, \omega),\ D \in \mathbb{K}^{2r\times 2r} \text{ is diagonal}\}. \tag{2}$$

By definition, for every $A \in \mathcal{C}_r(\mathbb{K}, \omega)$, $R_{\mathbb{L}}(A, r) \leq 2r$. Our main result is the following.

▶ **Theorem 7.** *Let $r \geq 3$. There exists a matrix $A \in \mathcal{C}_r(\mathbb{K}, \omega)$ with $R_{\mathbb{K}}(A, r) \geq 3r - 2$.*

As an immediate corollary, we establish the promised gap between the strict and the absolute rigidities.

▶ **Theorem 8.** *Let $\mathbb{K}$ and $\mathbb{L}$ satisfy the standard assumption ($*$). Then, for every $\varepsilon > 0$ and all sufficiently large r there exists a square matrix $M \in \mathbb{K}^{2r\times 2r}$ satisfying $R_{\mathbb{K}}(M, r) \geq (3/2 - \varepsilon)R_{\mathbb{L}}(M, r)$.*

We conjecture that much larger separation is possible.

▶ **Conjecture 9.** *Let $\mathbb{L} = \mathbb{Q}[\sqrt{2}]$. There exist $\varepsilon > 0$ and matrices M of arbitrarily large order $n = 2r$ such that $R_{\mathbb{Q}}(M, r) \geq n^{1+\varepsilon}$, while $R_{\mathbb{L}}(M, r) \leq O(n)$.*

In particular, we expect that such matrices M can be found in $\mathcal{C}_r(\mathbb{Q}, \sqrt{2})$.

We also ask whether the maximum possible rigidity can be achieved for matrices in $\mathcal{C}_r$.

▶ **Problem 10.** Is it true that for infinitely many r there exists a matrix $A \in \mathcal{C}_r(\mathbb{Q}, \sqrt{2})$ with $R_{\mathbb{Q}}(A, r) = r^2$?

1.5 Known lower bounds on rigidity: untouched minors

Despite decades of effort, progress on proving lower bounds on rigidity for explicit families of matrices has been limited. The best known general lower bound for a family of explicit $n \times n$ matrices A has the form $R^*(A,r) = \Omega((n^2/r)\log(n/r))$ [5, 14]. This lower bound is achieved through the "untouched minors argument": If all $(r+1) \times (r+1)$ minors of a matrix A are non-singular, then to reduce the rank of A to r, one needs to change at least one entry in every such minor. However, as discussed in [10], that is the best bound one can achieve through this argument.

For some semi-explicit families of matrices, stronger lower bounds are known. For $n \times n$ matrices whose entries are square roots of distinct prime numbers, Lokam [11] gives optimal, $\Omega(n^2)$ absolute rigidity for rank $r \leq n/17$. This result uses an algebraic dimension concept introduced by Shoup and Smolensky [15].

In the domain of reduced randomness, Goldreich and Tal [6] show that for random $n \times n$ Toepliz matrices A over $\mathbb{F}_2$ the bound $R_{\mathbb{F}_2}(A,r) = \Omega(n^3/(r^2 \log n))$ holds for $r \geq \sqrt{n}$.

1.6 Key steps of the proof of Theorem 7. Organization of the paper

First, observe that untouched minors arguments alone cannot answer our question; they do not distinguish between entries from $\mathbb{K}$ and $\mathbb{L}$. In order to prove the lower bound in Theorem 7 we use a combination of the untouched minors argument and arguments based on elements of algebraic geometry about the structure of $\mathcal{D}_r(\mathbb{K},\omega)$.

We begin by noticing that for almost all matrices $A \in \mathcal{C}_r(\mathbb{K},\omega)$, all $(r+1) \times (r+1)$ minors are non-singular (Lemma 32). So, an untouched minors argument can be used to show that if $R_{\mathbb{K}}(A,r) \leq 3r-3$, then the entries that are being changed have a "nice" layout inside $[2r] \times [2r]$. More precisely, we argue that then there are $(r+2)$ columns with at most 1 element changed in each of them (see Section 3.1).

Next, assume that for some $M \in \mathcal{D}_r(\mathbb{K},\omega)$ and every diagonal matrix D we have $R_{\mathbb{K}}(M+D,r) \leq 3r-3$. We can argue that since there are only finitely many choices for $3r-3$ entries in $[2r] \times [2r]$, there should be a fixed set π of $3r-3$ cells in $[2r] \times [2r]$, such that for a "large" set of diagonal matrices D, the rank of $M+D$ can be made $\leq r$ by only changing entries inside π (see Section 3.2).

Finally, we exploit the geometry of the set $\mathcal{D}_r = \mathcal{D}_r(\mathbb{K},\omega)$ to show that for almost all matrices $M \in \mathcal{D}_r$ no such fixed π exists. In order to do this, we show that among $2r^2$ entries in arbitrary r columns of $M \in \mathcal{D}_r$ there is no algebraic dependence imposed by $\mathcal{D}_r$ (see Section 2). Next, we consider a properly chosen set of $r+2$ columns with at most one entry from π in each of them, and exploit the fact that we have sufficiently many algebraic degrees of freedom for the entries in these columns so that changing entries in π typically is not sufficient to make the rank of these columns to be r (see Sections 3.3 - 3.5). This last step is the hardest part of the proof and requires us to consider several cases.

We present the parts of the proof in a slightly different order than described above. The geometry of the set $\mathcal{D}_r$ is studied in Section 2. Other parts of the proof are contained in Section 3. We combine these parts into a complete proof of Theorem 7 in Section 3.5.

In Section 4 we show that finite extensions suffice for absolute rigidity. In Section 5 we prove the refutation of rigidity candidates mentioned in Sec. 1.2.

We review some basic concepts from algebraic geometry over arbitrary fields in Appendix A. The proofs omitted in Section 3.4 are provided in Appendix B. The model-theoretic reduction to countable fields is outlined in Appendix C. In Appendix D we exhibit a concrete 5×5 matrix of strict rigidity 9 and absolute rigidity 8. Some open problems are raised in Sec. 1.7.

1.7 Open problems

The most intriguing question to come out of this work is Problem 6, the separation of the linear arithmetic complexity of linear functions by the extension field permitted in the circuit.

Strong separation between strict and absolute rigidities is suggested in Conjecture 9.

For a matrix over a field $\mathbb{K}$, absolute rigidity can be achieved over a finite extension of $\mathbb{K}$ (Prop. 49). However, that result is not effective.

▶ **Problem 11.** Is there a computable function f that maps rational matrices to positive integers, such that the absolute rigidity of any rational matrix A can be achieved over an extension of $\mathbb{Q}$ of degree $\leq f(A)$? Can such an f be made a function of the dimensions of the matrix A?

Recent non-rigidity results [2, 3, 4] inspire the following problems.

We remind the reader that by a *family* of square matrices we mean a set of square matrices of unbounded order.

In our submission to this conference (Feb. 15, 2021) we proposed the following conjecture.

▶ **Conjecture 12.** *Let $\mathcal{F}$ be a finite set of matrices over $\mathbb{C}$. Let $\mathcal{A}$ denote the set of all possible Kronecker products of these matrices (taking each member of $\mathcal{F}$ any number of times). Then no subfamily of $\mathcal{A}$ is Valiant-rigid over $\mathbb{C}$.*

We stated that this would generalize the result that the DFT matrices for abelian groups of bounded exponent are not absolutely Valiant rigid [2, 4].

On Feb. 24, 2021, a paper by Josh Alman appeared on arXiv [1] that raises the same question and answers it in the positive in the case that all matrices in the family $\mathcal{F}$ have the same order. This restriction was subsequently removed by one of us, confirming Conjecture 12 [8]. That paper also exponentially improves Alman's non-rigidity exponent. Like Alman's, our result establishes strict non-rigidity. We state the main result of [8].

▶ **Theorem 13** (Kivva [8]). *Given $d \geq 2$ and $\varepsilon > 0$, there exists $\gamma > 0$ such that the following holds for any sequence of matrices $M_1, \ldots, M_n$ of respective orders $d_i \leq d$ over the field $\mathbb{F}$. Let $M = \otimes_{i=1}^{n} M_i$ and $N = \prod_{i=1}^{n} d_i$. If $N \geq d^{1/\gamma}$ then $R_{\mathbb{F}}(M, N^{1-\gamma}) \leq N^{1+\epsilon}$. Here γ can be chosen to be $\gamma = \Omega\left(\frac{1}{d^{3/2}\log^3(d)} \cdot \frac{\varepsilon^2}{\log^2(1/\varepsilon)}\right)$.*

The following problem remains open.

▶ **Problem 14.** Does there exist a strictly Valiant-rigid family of rational circulant matrices?

No such family is absolutely rigid by Dvir and Liu [4].

2 Basic properties of $\mathcal{D}_r$

We continue to make our standard assumption $(*)$. Let $\mathbb{L} = \mathbb{K}[\omega]$ be a quadratic extension, where $\omega^2 \in \mathbb{K}$. $\mathbb{F}$ denotes an arbitrary infinite field (not necessarily of characteristic zero).

Additionally, we assume that $\mathbb{L}$ is a subfield of $\mathbb{C}$. This assumption can be made without loss of generality. Indeed, a simple model-theoretic argument shows that we can assume that $\mathbb{K}$ is countable (Prop. 91). The proof of Prop. 91 can also be adapted to reducing Theorem 7 to countable fields.

Since $\mathbb{K}$ and ω are fixed, we use the notation $\mathcal{D}_r = \mathcal{D}_r(\mathbb{K}, \omega)$ and $\mathcal{C}_r = \mathcal{C}_r(\mathbb{K}, \omega)$. Recall that these are algebraic sets in $\mathbb{K}^{2r} \times \mathbb{K}^{2r}$.

2.1 Matrices over $\mathbb{L}$ of low rank and with few entries outside $\mathbb{K}$

We start by giving a short motivation for the family $\mathcal{D}_r$. Recall the following elementary fact from linear algebra.

▶ **Fact 15.** Let $M \in \mathbb{F}^{n\times n}$ be a matrix of rank r. Let $L \in \mathbb{F}^{n\times r}$ be a matrix consisting of r linearly independent columns of M. Then there exists $R \in \mathbb{F}^{r\times n}$ such that $M = LR$.

Let $L \in \mathbb{K}[\omega]^{n\times r}$ and $R \in \mathbb{K}[\omega]^{r\times n}$. Denote the i-th row of L by $a_i + b_i\omega$ and j-th column by $x_j + y_j\omega$, where $a_i, b_i, x_j, y_j \in \mathbb{K}^r$.

▶ **Definition 16.** *For $x, y \in \mathbb{K}^n$ define $\langle x, y\rangle = \sum_{i=1}^{n} x_i \cdot y_i$.*

▶ **Observation 17.** *$(LR)_{ij} \in \mathbb{K}$ if and only if $\langle x_j, b_i\rangle + \langle y_j, a_i\rangle = 0$.*

▶ Remark 18. For a field extension of degree k, a similar criterion consists of $k-1$ linear equations to be satisfied by components of R.

▶ **Corollary 19.** *Take $n = 2r$. Then for every choice of $2r$ linearly independent vectors $(a_i, b_i) \in \mathbb{K}^{2r}$ there exists a unique choice of $2r$ vectors (x_i, y_i) such that LR is in $\mathcal{D}_r + \omega I$.*

Note that if $n \geq 2r$, and L is a generic $n \times r$ matrix, we should expect at least $n(n-2r+1)$ entries of LR to be from $\mathbb{L} \setminus \mathbb{K}$. At the same time, $R_{\mathbb{K}}(LR, r) \leq (n-r)^2$. We prefer the quotient of these numbers to be as small as possible, which is achieved for $n = 2r$ (if $n \geq 2r$).

2.2 Geometry of $\mathcal{D}_r$

In this section we study the geometry of the set $\mathcal{D}_r$. See Appendix A for some basic definitions and facts from algebraic geometry that are used in this paper.

▶ **Definition 20** (proj_S). *For a matrix $A \in \mathbb{F}^{n\times n}$ and $S \subseteq [n]$ define $\mathrm{proj}_S(A)$ to be the matrix consisting of columns of A with indices in S.*

▶ **Definition 21** (Small set). *We say that a set $A \subseteq \mathbb{K}^n$ is* small *(in $\mathbb{K}^n$) if it is contained in a proper algebraic subset in $\mathbb{K}^n$.*

▶ **Definition 22** (${}^\sigma M^\tau$). *For permutations $\sigma \in S_n$, $\tau \in S_m$ and an $n \times m$ matrix M, define ${}^\sigma M^\tau$ to be the matrix obtained from M by permuting rows by σ and columns by τ.*

Our first goal is to show that for $S \subseteq [2r]$ with $|S| = r$ only a small set of matrices from $\mathbb{K}^{2r\times r}$ is not in the image of $\mathrm{proj}_S : \mathcal{D}_r \to \mathbb{K}^{2r\times r}$. Note that for every permutation $\sigma \in S_{2r}$ and $M \in \mathcal{D}_r$ we have ${}^\sigma M^\sigma \in \mathcal{D}_r$. Thus, it is sufficient to study $\mathrm{proj}_{[r]}$.

▶ **Lemma 23.** *Let $A_1, A_2 \in \mathbb{K}^{r\times r}$. Assume that A_2 is invertible. Then*

$$\begin{pmatrix} A_1 & -A_1^2A_2^{-1} + \omega^2 A_2^{-1} \\ A_2 & -A_2A_1A_2^{-1} \end{pmatrix} \in \mathcal{D}_r. \tag{3}$$

Proof. Observe that

$$\begin{pmatrix} A_1 + I\omega & -A_1^2A_2^{-1} + \omega^2 A_2^{-1} \\ A_2 & -A_2A_1A_2^{-1} + I\omega \end{pmatrix} = \begin{pmatrix} A_1 + I\omega \\ A_2 \end{pmatrix} \cdot \left(I, \quad -A_1A_2^{-1} + A_2^{-1}\omega\right). \qquad ◀$$

Next, we observe that a simple condition on $M \in \mathcal{D}_r$ guarantees that $\mathrm{proj}_{[r]}$ is injective.

▶ **Lemma 24.** *Let $A_1, A_2 \in \mathbb{K}^{r\times r}$ and $M \in \mathcal{D}_r$. Assume that* $\mathrm{proj}_{[r]}(M+\omega I) = \begin{pmatrix} A_1+\omega I \\ A_2 \end{pmatrix}$ *has rank r (over $\mathbb{L}$). Then, A_2 is invertible, and M is uniquely determined by* $\mathrm{proj}_{[r]}(M)$*, and we have*

$$M = \phi_{[r]}\begin{pmatrix} A_1 \\ A_2 \end{pmatrix} := \begin{pmatrix} A_1 & -A_1^2 A_2^{-1} + \omega^2 A_2^{-1} \\ A_2 & -A_2 A_1 A_2^{-1} \end{pmatrix}.$$

Proof. Denote $L = \mathrm{proj}_{[r]}(M+\omega I)$. Since $\mathrm{rank}(L) = r$, $M+\omega I = LR$ for some $R \in \mathbb{L}^{r\times 2r}$. Let $R = (X_1 + Y_1\omega, X_2 + Y_2\omega)$ for $X_1, Y_1, X_2, Y_2 \in \mathbb{K}^{r\times r}$. The inclusion $M \in \mathcal{D}_r$ imposes the following constraints.

$$A_1Y_1 + X_1 = I, \qquad A_1Y_2 + X_2 = 0, \qquad A_2Y_1 = 0 \quad \text{and} \quad A_2Y_2 = I. \tag{4}$$

The last equality implies that A_2 is invertible. Therefore $Y_1 = 0$, $Y_2 = A_2^{-1}$, $X_1 = I$ and $X_2 = -A_1A_2^{-1}$. ◀

Define $U_{[r]}$ to be the set of $X \in \mathbb{K}^{2r\times r}$ such that the matrix formed by the last r rows of X is non-singular. Note that $\phi_{[r]} : U_{[r]} \to \mathbb{K}^{2r\times r}$ defined in the lemma above is a regular map according to Def. 82 (see Lemma 83).

Due to Lemma 24, it will be convenient to work with the following subset of $\mathcal{D}_r$.

$$\mathcal{D}'_r = \{M \in \mathcal{D}_r \mid \forall S \subset [2r],\ |S| = r :\ \mathrm{rank}(\mathrm{proj}_S(M+\omega I)) = r\}. \tag{5}$$

Let $I_{2r,r} \in \mathbb{K}^{2r\times r}$ be the identity matrix padded with r zero rows. Define

$$\mathcal{L} = \{L \in \mathbb{K}^{2r\times r} \mid \text{all } r\times r \text{ minors of } L + \omega I_{2r,r} \text{ are non-singular}\}. \tag{6}$$

▶ **Observation 25.** *$\mathcal{L}$ is an irreducible Zariski-open subset of $\mathbb{K}^{2r\times r}$.*

Proof. The set of L for which $L + \omega I_{2r,r}$ has a singular $r \times r$ minor is a finite union of proper Zariski-closed subsets of $\mathbb{K}^{2r\times r}$. Since, $\mathbb{K}^{2r\times r}$ is irreducible, this union is a proper Zariski-closed subset. Hence $\mathcal{L}$ is Zariski-open and it is irreducible, as a Zariski-open subset of an irreducible set. ◀

Then, by Lemmas 23 – 24, for every $L \in \mathcal{L}$ there exists a unique matrix $M \in \mathcal{D}_r$ with $\mathrm{proj}_{[r]}(M) = L$. For $\phi_{[r]}$ as in Lemma 24, define

$$\mathcal{D}^*_r = \{\phi_{[r]}(L)^T \mid L \in \mathcal{L}\}. \tag{7}$$

▶ **Lemma 26.** *The set $\mathcal{D}^*_r$ is an irreducible quasi-affine variety. Moreover, $\mathcal{D}^*_r \subseteq \mathcal{D}'_r$, and for every $S \subseteq [2r]$ with $|S| = r$ only a small set of matrices in $\mathbb{K}^{2r\times r}$ is not in $\mathrm{proj}_S(\mathcal{D}^*_r) \subseteq \mathbb{K}^{2r\times r}$.*

Proof. Observe, that for $L \in \mathcal{L}$ and $M = \phi_{[r]}(L)$, any r distinct rows of $M + \omega I$ are linearly independent. Therefore, $M^T \in \mathcal{D}'_r$, and so $\mathcal{D}^*_r \subseteq \mathcal{D}'_r$. The set $\mathcal{L} \subseteq \mathbb{K}^{2r\times r}$ is a non-empty Zariski-open irreducible set. Recall that $\mathcal{D}_r$ is an affine algebraic set. By Lemma 24, the set $\mathcal{D}^*_r$ is equal to $\psi^{-1}_{[r]}(\mathcal{L}) \cap \mathcal{D}_r$, where $\psi_{[r]} : \mathbb{K}^{2r\times 2r} \to \mathbb{K}^{2r\times r}$ is defined by $M \mapsto \mathrm{proj}_{[r]}(M^T)$. Since $\psi_{[r]}$ is regular, $\mathcal{D}^*_r$ is a quasi-affine algebraic set. The map $(\phi_{[r]})^T : \mathcal{L} \to \mathbb{K}^{2r\times 2r}$ is regular, so $\mathcal{D}^*_r$ is irreducible (see Obs. 76).

For every $S \subseteq [2r]$ with $|S| = r$, let $\phi_S : U_S \to \mathbb{K}^{2r\times 2r}$ (defined similarly as in Lemma 24) be an inverse function to proj_S, where U_S is a Zariski-open subset of $\mathbb{K}^{2r\times r}$ where ϕ_S is well-defined. The map ϕ_S is regular and injective. Therefore, by Lemma 24, $\mathrm{proj}_S(\mathcal{D}^*_r) = (\phi_S \circ \psi_{[r]})^{-1}(\mathcal{L})$, and so it is a Zariski-open subset of $\mathbb{K}^{2r\times r}$. Hence, only a small set of matrices in $\mathbb{K}^{2r\times r}$ is not in $\mathrm{proj}_S(\mathcal{D}^*_r) \subseteq \mathbb{K}^{2r\times r}$. ◀

Def. 78 defines the notion of "almost all elements" of an irreducible quasi-variety. Since we have not proved that $\mathcal{D}_r$ is irreducible, we need a special definition to formalize our references to "almost all elements of $\mathcal{D}_r$."

▶ **Definition 27** (Almost all elements of $\mathcal{D}_r$). *We shall say that some property holds for* almost all *matrices in $\mathcal{D}_r$ if it holds for almost all elements of $\mathcal{D}_r^*$.*

We believe that, in fact, $\mathcal{D}_r$ is irreducible. If that is the case, Def. 27 remains consistent with Def. 78.

By Obs. 79, if each of a finite number of properties holds for almost all elements of $\mathcal{D}_r$, then they all hold simultaneously for almost all elements of $\mathcal{D}_r$.

▶ Remark 28. If $\mathcal{A} \subseteq \mathcal{D}_r^*$ is such that for some $S \subseteq [2r]$ with $|S| = r$ the set $\mathrm{proj}_S(\mathcal{A})$ is small in $\mathbb{K}^{2r\times r}$, then by Lemma 26, almost all matrices in $\mathcal{D}_r$ are not in $\mathcal{A}$.

▶ **Definition 29** ($\mathcal{D}_r^\#$). *Let $\mathcal{D}_r^\#$ denote the set of matrices $M \in \mathcal{D}_r^*$ such that for all $k \le r$ every $k \times k$ minor of M is non-singular.*

▶ **Corollary 30.** *$\mathcal{D}_r^\#$ is a non-empty Zariski-open subset of $\mathcal{D}_r^*$.*

Proof. Let X be the Zariski-open subset of $\mathbb{K}^{2r\times r}$ consisting of matrices with all $k \times k$ minors being non-singular for all $k \le r$. Then, $\mathcal{D}_r^\# = \bigcap_{S\subseteq[2r],\ |S|=r} \left(\mathcal{D}_r^* \cap \mathrm{proj}_S^{-1}(X)\right)$. ◀

▶ **Definition 31** ($\mathrm{Diag}(\mathbb{F}^{n\times m})$). *Define $\mathrm{Diag}(\mathbb{F}^{n\times m})$ to be the set of matrices in $\mathbb{F}^{n\times m}$ that have non-zero entries only in the cells with indices $\{(i,i) \mid 1 \le i \le \min(n,m)\}$.*

▶ **Lemma 32.** *For every $M \in \mathcal{D}_r^\#$ let $\mathcal{L}_M$ be the set of $D \in \mathrm{Diag}(\mathbb{K}^{2r\times 2r}) \cong \mathbb{K}^{2r}$ such that some $(r+1)\times(r+1)$ minor of $M + D$ is singular. Then $\mathcal{L}_M$ is a proper Zariski-closed subset of $\mathrm{Diag}(\mathbb{K}^{2r\times 2r})$.*

Proof. Let X be an $(r+1)\times(r+1)$ minor of $M + D$ that involves k diagonal entries of D: $x_1, x_2, \dots, x_k$. Then $k > 0$. Moreover, $\det(X)$ is a polynomial over $\mathbb{K}$ in variables $\{x_i \mid i \in [k]\}$ and the coefficient in front of $x_1x_2\dots x_k$ is the determinant of a minor formed by rows and columns of X that have no diagonal entries of D. Since $M \in \mathcal{D}_r^\#$, this coefficient is non-zero. Hence, the set of D for which $\det(X) = 0$ is a proper Zariski-closed set in $\mathrm{Diag}(\mathbb{K}^{2r\times 2r})$. Since $\mathrm{Diag}(\mathbb{K}^{2r\times 2r}) \cong \mathbb{K}^{2r}$ is irreducible, the finite union (over all $(r+1)\times(r+1)$ minors) of proper Zariski-closed subsets is a proper Zariski-closed subset. ◀

3 A lower bound on the strict rigidity for a matrix in $\mathcal{C}_r$

In this section we prove the following stronger version of Theorem 7.

▶ **Theorem 33.** *Let $r \ge 3$. For almost all matrices $M \in \mathcal{D}_r$ there exists a diagonal matrix $D \in \mathrm{Diag}(\mathbb{K}^{2r\times 2r})$ such that $R_{\mathbb{K}}(M + D, r) \ge 3r - 2$.*

▶ **Definition 34** ($\mathbb{F}^{(\pi)}$). *For $\pi \subseteq [n] \times [m]$ denote by $\mathbb{F}^{(\pi)}$ the subset of matrices in $\mathbb{F}^{n\times m}$ with zero entries in every cell outside of π (we assume that n and m are clear from the context).*

Assume $R_{\mathbb{K}}(M + D, r) \le 3r - 3$ for all diagonal matrices D. Intuitively, since there are only finitely many subsets $\pi \subset [2r] \times [2r]$ of size $3r - 3$, there should exist π such that for a "large set" of diagonal matrices D there exists a corresponding $Z \in \mathbb{K}^{(\pi)}$ with $\mathrm{rank}(M + D + Z) \le r$. In Section 3.2, we are going to make this intuitive argument precise.

Then, in order to prove Theorem 33 it is sufficient to show that for an arbitrary fixed π of size $3r - 3$ for almost all matrices $M \in \mathcal{D}_r$ there is no "large set" of diagonal matrices D such that $\mathrm{rank}(M + D + Z) \le r$ for all D is this set and all $Z \in \mathbb{K}^{(\pi)}$.

3.1 Structure of the subsets of $[2r] \times [2r]$ with at most $3r - 3$ elements

We start the discussion towards the proof of Theorem 33 with the study of the structure of the subsets of $[2r] \times [2r]$ with at most $3r - 3$ elements.

▶ **Definition 35** (Well-distributed). *Let $m \geq r + 1$. We say that $\pi \subseteq [2r] \times [m]$ is* well-distributed, *if every $(r+1) \times (r+1)$ minor contains at least one element of π.*

Note that if π is not well-distributed and all $(r+1) \times (r+1)$ minors of $A \in \mathbb{C}^{2r \times 2r}$ are non-singular, then for every $Z \in \mathbb{C}^{(\pi)}$ we have $\operatorname{rank}(A + Z) \geq r + 1$. By Lemma 32, for all $M \in \mathcal{D}_r^{\#}$, for a Zariski-open (so, "large") set of diagonal matrices D all $(r+1) \times (r+1)$ minors of $M + D$ are non-singular.

Hence, we mainly need to concentrate on well-distributed sets π.

▶ **Observation 36.** *Let $\pi \subseteq [2r] \times [m]$ be well-distributed. Then for any set of $r+1$ columns, π contains elements in at least r distinct rows.*

Proof. If not, we immediately find an $(r+1) \times (r+1)$ minor with no elements from π. ◀

▶ **Lemma 37.** *Let $\pi \subseteq [2r] \times [2r]$ be well-distributed. For each $i \in [2r]$, let t_i be the number of elements of π in the i-th column. Let $t_{(j)}$ be the j-th smallest number among $\{t_i \mid i \in [2r]\}$.*

1. *Then, either $t_{(r+2)} = 1$, or $|\pi| \geq 3r - 2$.*
2. *If $t_{(1)} = 1$, then either $t_{(r+3)} = 1$, or $|\pi| \geq 3r - 2$.*

Proof. Assume $t_{(r+2)} \geq 2$. By Observation 36, $r + 1$ columns that contain the least number of elements from π have at least r elements from π. The other $r - 1$ columns contain at least $2(r-1)$ elements from π. Thus, in this case, $|\pi| \geq 3r - 2$.

Finally, if $t_{(1)} = t_{(r+2)} = 1$, but $t_{(r+3)} \geq 2$, then $|\pi| \geq 2(r-2) + r + 2 = 3r - 2$. ◀

▶ **Definition 38** (Matching). *We say that $\pi \subseteq [n] \times [m]$ is a* matching *if the projections of π on each of its two coordinates are injective.*

▶ **Lemma 39.** *Let $r \geq 3$. Assume that $\pi \subseteq [2r] \times [r+3]$ has precisely one element in every column and is well-distributed, then π contains a matching of size $r + 2$.*

Proof. Note that $|\pi| = r + 3$ and Observation 36 implies that π has elements in at least r rows. Since $3r > r + 3$ for $r \geq 3$ there is at least one row with ≤ 2 elements. Considering $r + 1$ columns that do not contain these elements, by Observation 36, we get that π has elements in at least $r + 1$ distinct rows. Since $2r + 1 > r + 3$ for $r \geq 3$ there are at least two rows with precisely one element in each. We match each of these rows to the unique available column. Consider the set of the other $r + 1$ columns. By Observation 36, there are at least r rows that have elements in these columns. Since every column has precisely 1 element, by picking one element in each row we will get a matching of size $r + 2$. ◀

3.2 Reduction to a fixed well-distributed π

▶ **Definition 40** (Unbounded). *For a subfield $\mathbb{F} \subseteq \mathbb{C}$ we say that a set of points $\{x_i\}_{i \in I} \subseteq \mathbb{F}$ is unbounded, if it is unbounded as a set in $\mathbb{C}$.*

▶ **Definition 41** ($\mathcal{C}_{r,\pi}$, $\mathcal{C}'_{r,\pi}$). *For $\pi \subseteq [2r] \times [2r]$ define*

$$\begin{aligned} \mathcal{C}_{r,\pi} &= \{A \in \mathcal{C}_r \mid \exists Z \in \mathbb{C}^{(\pi)} : \operatorname{rank}(A + Z) \leq r\}, \text{ and} \\ \mathcal{C}'_{r,\pi} &= \{A \in \mathcal{C}_r \mid \exists Z \in \mathbb{K}^{(\pi)} : \operatorname{rank}(A + Z) \leq r\}. \end{aligned} \tag{8}$$

▶ **Lemma 42.** *Let $M \in \mathcal{D}_r$ and P be a finite collection of subsets of $[2r] \times [2r]$. Let Ω_M be a non-empty Zariski-open set in $\mathrm{Diag}(\mathbb{K}^{2r\times 2r})$. Assume that for every diagonal matrix $D \in \Omega_M$ we have $M + D \in \bigcup_{\pi\in P} \mathcal{C}_{r,\pi}$. Then there exist unbounded sets $E_1, E_2, \dots E_{2r} \subseteq \mathbb{K}$ and $\pi \in P$ such that for all diagonal D with $D_{ii} \in E_i$ for all $i \in [2r]$ we have $M + D \in \mathcal{C}_{r,\pi}$.*

Proof. For $\pi \in P$, consider the algebraic set

$$W_M(\pi) = \{(D, Z) \mid D \in \mathrm{Diag}(\mathbb{C}^{2r\times 2r}), Z \in \mathbb{C}^{(\pi)},\ \mathrm{rank}(M + D + Z) \le r\}.$$

Since $\mathrm{Diag}(\mathbb{C}^{2r\times 2r}) \cong \mathbb{C}^{2r}$, we can treat $W_M(\pi)$ as a subvariety of $\mathbb{C}^{2r} \times \mathbb{C}^{|\pi|}$. The projection on the first coordinate $p : (D, Z) \mapsto D$ is regular, so by Chevalley's Theorem (Theorem 87) the image $p(W_M(\pi))$ under this projection is a constructible set for every π. Since a constructible set is an intersection of a closed and an open set, for every π, either $p(W_M(\pi))$ is Zariski-open, or there exists a non-trivial polynomial f_π that completely vanishes on $p(W_M(\pi))$. If neither of $p(W_M(\pi))$ is Zariski-open, then there exists a nontrivial polynomial (e.g., $\prod_{\pi\in P} f_\pi$) that vanishes on $\bigcup_{\pi\in P} p(W_M(\pi))$, and so vanishes on Ω_M. This is a contradiction, as $\mathrm{Diag}(\mathbb{K}^{2r\times 2r}) \cong \mathbb{K}^{2r}$ is irreducible and Ω_M is non-empty Zariski-open.

Hence, there exists $\pi \in P$, such that $p(W_M(\pi))$ is Zariski-open in $\mathrm{Diag}(\mathbb{C}^{2r\times 2r})$, and so $\Omega'_M = \Omega_M \cap p(W_M(\pi))$ is Zariski-open in $\mathrm{Diag}(\mathbb{K}^{2r\times 2r})$. Hence, the claim of the lemma follows from Lemma 85. ◀

Note that in the definition of $\mathcal{C}_{r,\pi}$ we allow the entries of Z to be from $\mathbb{C}$ instead of $\mathbb{K}$. So if P contains a superset of $\{(i, i) \mid i \in [2r]\}$ the lemma above gives a trivial statement. Thus we shall consider two different regimes, when π is "close to containing the diagonal" and when it is not.

More precisely, as we saw in Lemma 37, there exists a subset $S' \subset [2r]$ of size $r + 2$ such that every column with index in S' has at most one element of π. We will discuss how to pick S' in Section 3.5, if for π this choice is not unique. We distinguish two cases: (a) when π restricted to columns in S' is a subset of the diagonal and (b) when it is not.

In the case (a) we will show that for almost all $M \in D_r^{\#}$ for all diagonal $D \in \mathrm{Diag}(\mathbb{K}^{2r\times 2r})$ we have $A = M + D \notin \mathcal{C}'_{r,\pi}$.

By applying Lemma 42 to the collection of all π from the case (b), we get that there exists a π from case (b) and a "large" set of diagonal matrices D such that $A = M + D \in \mathcal{C}_{r,\pi}$. We will argue that this does not happen for almost all $M \in D_r^{\#}$.

Both in case (a) and in case (b) we only study the matrix $B = \mathrm{proj}_{S'}(A)$ and show that for almost all M there is no change of entries inside π that allows to get a matrix of rank $\le r$ from B.

3.3 Case when π in columns S' coincides with the diagonal

In the next lemma we show that for almost all $M \in \mathcal{D}_r$ there is no $Z' \in \mathrm{Diag}(\mathbb{K}^{2r\times(r+2)})$ such that $\mathrm{rank}(\mathrm{proj}_{[r+2]}(M) + Z') \le r$.

In this and next section we use e_i to denote the vector in $\mathbb{K}^r$ with entry 1 in coordinate i and 0 in all other coordinates.

▶ **Lemma 43.** *Let $r \ge 3$. Consider $A_1 \in \mathbb{K}^{r\times r}$ and an invertible matrix $A_2 \in \mathbb{K}^{r\times r}$. Define*

$$v_i = -A_1^2 A_2^{-1} e_i + \omega^2 A_2^{-1} e_i \quad \text{and} \quad w_i = -A_2 A_1 A_2^{-1} e_i.$$

For a diagonal matrix $Z \in \mathbb{K}^{r\times r}$ and $z_1, z_2 \in \mathbb{K}$ consider

$$T(Z, z_1, z_2) = \begin{pmatrix} A_1 + Z & v_1 & v_2 \\ A_2 & w_1 + z_1 e_1 & w_2 + z_2 e_2 \end{pmatrix}.$$

The set of matrices $(A_1, A_2) \in \mathbb{K}^{2r^2}$ *for which there exist* $Z \in \mathrm{Diag}(\mathbb{K}^{r\times r})$*,* $z_1, z_2 \in \mathbb{K}$ *s.t.* $\mathrm{rank}(T(Z, z_1, z_2)) \le r$ *is small in* $\mathbb{K}^{2r^2}$*.*

Proof. Assume $\mathrm{rank}(T(Z, z_1, z_2)) \le r$. Since A_2 is invertible, the last two columns of $T(Z, z_1, z_2)$ can be expressed as a linear combination of the first r columns. Let $y_i \in \mathbb{K}^r$ satisfy

$$\begin{pmatrix} A_1 + Z \\ A_2 \end{pmatrix} y_i = \begin{pmatrix} v_i \\ w_i + z_i e_i \end{pmatrix}.$$

Then

$$y_i = A_2^{-1}(w_i + z_i e_i) \quad \Rightarrow \quad (A_1 + Z)A_2^{-1}(w_i + z_i e_i) = v_i,$$
$$-A_1^2 A_2^{-1} e_i + z_i A_1 A_2^{-1} e_i + Z(-A_1 A_2^{-1} e_i + z_i A_2^{-1} e_i) = -A_1^2 A_2^{-1} e_i + \omega^2 A_2^{-1} e_i.$$

Let $\alpha_i = A_1 A_2^{-1} e_i$ and $\beta_i = A_2^{-1} e_i$. Then for all $k \in [r]$ we have

$$Z_{kk} = \frac{\omega^2 \beta_{ik} - z_i \alpha_{ik}}{-\alpha_{ik} + z_i \beta_{ik}}.$$

Hence, for all $k \in [r]$,

$$\frac{\omega^2 \beta_{1k} - z_1 \alpha_{1k}}{-\alpha_{1k} + z_1 \beta_{1k}} = \frac{\omega^2 \beta_{2k} - z_2 \alpha_{2k}}{-\alpha_{2k} + z_2 \beta_{2k}}. \tag{9}$$

This can be rewritten as

$$\alpha_{2k} \left(\frac{\omega^2 \beta_{1k} - z_1 \alpha_{1k}}{-\alpha_{1k} + z_1 \beta_{1k}} - z_2 \right) = z_2 \beta_{2k} \left(\frac{\omega^2 \beta_{1k} - z_1 \alpha_{1k}}{-\alpha_{1k} + z_1 \beta_{1k}} \right) - \omega^2 \beta_{2k}. \tag{10}$$

The coefficient in front of α_{2k} is 0 if and only if

$$\omega^2 \beta_{1k} - z_1 \alpha_{1k} = -z_2 \alpha_{1k} + z_2 z_1 \beta_{1k} \quad \Leftrightarrow \quad \beta_{1k} = \frac{z_1 - z_2}{\omega^2 - z_1 z_2} \alpha_{1k}.$$

Unless $z_1 = z_2 = \pm\omega$, such equation can hold for at most one index k, or the set $(A_1, A_2) \in \mathbb{K}^{2r^2}$ is small. If the coefficient in front of α_{2k} is non-zero for some k, then α_{2k} can be expressed as a rational function of α_{1k}, β_{1k}, β_{2k} and z_1, z_2. Hence, for every k either α_{2k} is a function of α_{1k}, β_{1k}, β_{2k} and two parameters z_1, z_2, or β_{1k} is a function of α_{1k} and z_1, z_2. In any case, for $r \ge 3$ we see that the set $(A_1, A_2) \in \mathbb{K}^{2r^2}$ that satisfy Eq. (9) is small. ◀

3.4 Case when π in columns S' does not coincide with the diagonal

In the lemmas below we think of T as of a matrix obtained by permuting rows and columns of $\mathrm{proj}_{S'}(M + D + Z')$ for $M \in \mathcal{D}_r^{\#}$, $D \in \mathrm{Diag}(\mathbb{K}^{2r\times 2r})$ and $Z' \in \mathbb{C}^{\pi}$. The variables x_i correspond to selected diagonal entries of D and the variables Z, z_i correspond to entries of Z'.

Let $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ be the Riemann sphere, i. e., the one-point compactification of $\mathbb{C}$ with respect to the usual complex norm.

▶ **Observation 44.** *Let* $f : \widehat{\mathbb{C}} \to \widehat{\mathbb{C}}$ *be defined as* $f(x) = \dfrac{ax + b}{cx + d}$ *for* $a, b, c, d \in \mathbb{C}$*. If* $\{f(x_k)\}_{k=1}^{\infty}$ *converges to* y *in* $\widehat{\mathbb{C}}$*, then there exists* $x \in \widehat{\mathbb{C}}$ *such that* $f(x) = y$*.*

Proof. If $ad - bc \ne 0$, take x to be the limit of $\{x_k\}_{k=1}^{\infty}$ in $\widehat{\mathbb{C}}$. Else, pick an arbitrary $x \in \widehat{\mathbb{C}}$. ◀

▶ **Lemma 45.** *Let $r \geq 3$. Let $j_1 \notin \{1,2\}$ and $j_2 \notin \{2, j_1\}$ be elements of $[r]$. Let $E_1, E_2 \subseteq \mathbb{K}$ be unbounded sets. For $v_1, v_2, w_1, w_2 \in \mathbb{K}^r$, $A_1 \in \mathbb{K}^{r\times r}$, an invertible matrix $A_2 \in \mathbb{K}^{r\times r}$, $x_1, x_2 \in \mathbb{K}$, $z_1, z_2 \in \mathbb{C}$ and a diagonal matrix $Z \in \mathbb{C}^{r\times r}$ consider*

$$T(x_1, x_2, Z, z_1, z_2) = \begin{pmatrix} A_1 + Z & v_1 & v_2 \\ A_2 & w_1 + z_1 e_1 + x_1 e_{j_1} & w_2 + z_2 e_2 + x_2 e_{j_2} \end{pmatrix}.$$

The set of $(A_1, A_2) \in \mathbb{K}^{2r^2}$, for which there exist v_1, v_2, w_1, w_2, s.t. for all $x_1 \in E_1$, $x_2 \in E_2$ there exist $Z \in \mathrm{Diag}(\mathbb{C}^{r\times r})$, $z_1, z_2 \in \mathbb{C}$ s.t. $\mathrm{rank}(T(x_1, x_2, Z, z_1, z_2)) \leq r$, is small in $\mathbb{K}^{2r^2}$.

Proof. Since A_2 is invertible and the rank of $T(x_1, x_2, Z, z_1, z_2)$ is $\leq r$, $\forall i \in \{1,2\}$ we have

$$(A_1 + Z)A_2^{-1}(w_i + z_i e_i + x_i e_{j_i}) = v_i,$$

$$A_1 A_2^{-1}(z_i e_i + x_i e_{j_i}) + Z A_2^{-1}(w_i + z_i e_i + x_i e_{j_i}) = v_i - A_1 A_2^{-1} w_i.$$

Denote $\gamma_i = v_i - A_1 A_2^{-1} w_i$, $\alpha_i = A_1 A_2^{-1} e_i$, $\beta_i = A_2^{-1} e_i$ and $\phi_i = A_2^{-1} w_i$. Then

$$Z_{kk} = \frac{\gamma_{ik} - z_i \alpha_{ik} - x_i \alpha_{j_i k}}{\phi_{ik} + z_i \beta_{ik} + x_i \beta_{j_i k}}, \qquad \forall k \in [r], \forall i \in \{1,2\}, \quad \text{so} \tag{11}$$

$$\frac{\gamma_{1k} - z_1 \alpha_{1k} - x_1 \alpha_{j_1 k}}{\phi_{1k} + z_1 \beta_{1k} + x_1 \beta_{j_1 k}} = \frac{\gamma_{2k} - z_2 \alpha_{2k} - x_2 \alpha_{j_2 k}}{\phi_{2k} + z_2 \beta_{2k} + x_2 \beta_{j_2 k}} \qquad \forall k \in [r]. \tag{12}$$

Fix $x_2 \in E_2$. By passing to a subsequence for $x_1 \in E_1$ we may assume that $\lim_{E_1 \ni x_1 \to \infty} z_1(x_1, x_2)/x_1 = c \in \widehat{\mathbb{C}}$ is well-defined. For this subsequence,

$$\lim_{E_1 \ni x_1 \to \infty} \frac{\gamma_{2k} - z_2 \alpha_{2k} - x_2 \alpha_{j_2 k}}{\phi_{2k} + z_2 \beta_{2k} + x_2 \beta_{j_2 k}} = -\frac{\alpha_{1k} c + \alpha_{j_1 k}}{\beta_{1k} c + \beta_{j_1 k}} \qquad \forall k \in [r].$$

Hence, using Observation 44, there exists $z_2 = z_2(x_2)$ such that

$$\frac{\gamma_{2k} - z_2 \alpha_{2k} - x_2 \alpha_{j_2 k}}{\phi_{2k} + z_2 \beta_{2k} + x_2 \beta_{j_2 k}} = -\frac{\alpha_{1k} c + \alpha_{j_1 k}}{\beta_{1k} c + \beta_{j_1 k}} \qquad \forall k \in [r].$$

By passing to a subsequence for $x_2 \in E_2$ we may assume that $\lim_{E_2 \ni x_2 \to \infty} z_2(x_2)/x_2 = c' \in \widehat{\mathbb{C}}$. Then

$$\lim_{E_2 \ni x_2 \to \infty} \frac{\alpha_{1k} c(x_2) + \alpha_{j_1 k}}{\beta_{1k} c(x_2) + \beta_{j_1 k}} = \frac{c' \alpha_{2k} + \alpha_{j_2 k}}{c' \beta_{2k} + \beta_{j_2 k}} \qquad \forall k \in [r].$$

Hence, using Observation 44, there exists c'' such that

$$\frac{\alpha_{1k} c'' + \alpha_{j_1 k}}{\beta_{1k} c'' + \beta_{j_1 k}} = \frac{c' \alpha_{2k} + \alpha_{j_2 k}}{c' \beta_{2k} + \beta_{j_2 k}} \qquad \forall k \in [r]. \tag{13}$$

Since $j_2 \neq 2$, this gives a dependence for $\alpha_{j_2 k}$ on other variables with last index k and 2 parameters c', c'', if $c' \neq \infty$. If $c' = \infty$, we get a dependence for α_{2k} on other variables with last index k and a parameter c''. Hence for $r \geq 3$ the set of matrices $(A_1, A_2) \in \mathbb{K}^{2r^2}$ that satisfy Eq. (13) is small in $\mathbb{K}^{2r^2}$. ◀

The next two lemmas can be proved in a similar fashion, so we defer their proofs to Appendix B.

▶ **Lemma 46.** *Let $r \geq 3$. Consider $A_1 \in \mathbb{K}^{r\times r}$ and an invertible matrix $A_2 \in \mathbb{K}^{r\times r}$. Define*

$$v_i = -A_1^2 A_2^{-1} e_i + \omega^2 A_2^{-1} e_i \quad \text{and} \quad w_i = -A_2 A_1 A_2^{-1} e_i$$

Let $E_2 \subseteq \mathbb{K}$ be an unbounded set. For a diagonal matrix $Z \in \mathbb{C}^{r\times r}$ and $z_1, z_2 \in \mathbb{C}$, $x_2 \in \mathbb{K}$, consider

$$T(x_2, Z, z_1, z_2) = \begin{pmatrix} A_1 + Z & v_1 & v_2 \\ A_2 & w_1 + z_1 e_1 & w_2 + z_2 e_3 + x_2 e_2 \end{pmatrix}.$$

The set of matrices $(A_1, A_2) \in \mathbb{K}^{2r^2}$, such that for all $x_2 \in E_2$ there exist $Z \in \operatorname{Diag}(\mathbb{C}^{r\times r})$, and $z_1, z_2 \in \mathbb{C}$ such that $\operatorname{rank}(T(x_2, Z, z_1, z_2)) \leq r$, is small in $\mathbb{K}^{2r^2}$.

Proof. See Appendix B, Lemma 88. ◀

▶ **Lemma 47.** *Let $r \geq 3$. Let $j_1 \notin \{1, 2\}$ be an element of $[r]$. Let $E_1, E_2 \subseteq \mathbb{K}$ be unbounded sets. For $v_1, v_2, w_1, w_2 \in \mathbb{K}^r$, $A_1 \in \mathbb{K}^{r\times r}$, an invertible matrix $A_2 \in \mathbb{K}^{r\times r}$, $x_1, x_2 \in \mathbb{K}$, $z_1, z_2 \in \mathbb{C}$ and a diagonal matrix $Z \in \mathbb{C}^{r\times r}$ consider*

$$T(x_1, x_2, Z, z_1, z_2) = \begin{pmatrix} A_1 + Z & v_1 & v_2 + x_2 e_1 \\ A_2 & w_1 + z_1 e_1 + x_1 e_{j_1} & w_2 + z_2 e_2 \end{pmatrix}.$$

The set of matrices $(A_1, A_2) \in \mathbb{K}^{2r^2}$, for which there exist $v_1, v_2, w_1, w_2 \in \mathbb{K}^r$, s.t. for all $x_1 \in E_1$ and $x_2 \in E_2$ there exist $Z \in \operatorname{Diag}(\mathbb{C}^{r\times r})$, $z_1, z_2 \in \mathbb{C}$ s.t. $\operatorname{rank}(T(x_1, x_2, Z, z_1, z_2)) \leq r$, is small in $\mathbb{K}^{2r^2}$.

Proof. See Appendix B, Lemma 89. ◀

▶ Remark 48. Note that in Lemmas 43 and 46 we assume that v_1, v_2, w_1 and w_2 have the specific form given by Lemma 24, while in Lemmas 45 and 47 we cannot make such assumption. The reason is that Lemmas 45 and 47 treat matrices obtained from $M \in \mathcal{D}_r$ after its rows and columns are permuted in the way that does not respect the diagonal. And so, in this case, Lemma 24 cannot be applied.

3.5 Proof of Theorem 33

Finally, we are ready to prove Theorem 33.

Proof of Theorem 33. Let $\mathcal{P}$ denote the collection of the subsets of $[2r] \times [2r]$ with precisely $3r - 3$ elements. Let $\mathcal{P}_0 \subset \mathcal{P}$ denote the set of well-distributed $\pi \in \mathcal{P}$.

Recall that $\mathcal{D}_r^{\#}$ denotes the set of matrices $M \in \mathcal{D}_r^*$ such that for all $k \leq r$ every $k \times k$ minor of M is non-singular.

Fix $M \in \mathcal{D}_r^{\#}$. Assume that for every $D \in \operatorname{Diag}(\mathbb{K}^{2r\times 2r})$ we have $R_{\mathbb{K}}(M + D, r) \leq 3r - 3$. This means that for every $D \in \operatorname{Diag}(\mathbb{K}^{2r\times 2r})$ there exists $\pi \in \mathcal{P}$ and $Z \in \mathbb{K}^{(\pi)}$ such that

$$\operatorname{rank}(M + D + Z) \leq r.$$

Let $\mathcal{L}_M$ be the set of $D \in \operatorname{Diag}(\mathbb{K}^{2r\times 2r}) \cong \mathbb{K}^{2r}$ such that some $(r + 1) \times (r + 1)$ minor of $M + D$ is singular. By Lemma 32, $\mathcal{L}_M$ is a proper Zariski-closed subset of $\operatorname{Diag}(\mathbb{K}^{2r\times 2r})$. Define $\Omega_M = \operatorname{Diag}(\mathbb{K}^{2r\times 2r}) \setminus \mathcal{L}_M$.

Observe that for all $D \in \Omega_M$, for all $\pi \in \mathcal{P} \setminus \mathcal{P}_0$ and for all $Z \in \mathbb{C}^{(\pi)}$ we have

$$\operatorname{rank}(M + D + Z) \geq r + 1.$$

From now on we restrict ourself to taking $D \in \Omega_M$. Hence, in the rest of the proof we may assume that π is well-distributed.

Let $S \subseteq [2r]$ denote the set of indices of columns that have at most 1 element of π. Then, by Lemma 37, $|S| \geq r+2$, and if there is no column with 0 elements, then $|S| \geq r+3$.

Now we want to pick a subset S' of $r+2$ indices from S. We use the following rules.

1. If there is a column with index in S that contains 0 elements of π, select S' to be an arbitrary subset of S of size $r+2$ that contains this index.
2. Otherwise, every column with index in S has precisely 1 element of π and $|S| \geq r+3$.
   - **a.** If $\pi = \{(i,i) \mid i \in S\}$ pick S' to be an arbitrary subset of S of size $r+2$.
   - **b.** If π disagrees with the diagonal in precisely 1 position, choose S' to consist of columns where π agrees with the diagonal.
   - **c.** If π disagrees with the diagonal in precisely 2 positions, choose S' to contain only one column where they disagree. Moreover, using Lemma 39, we can pick such S' so that π restricted to columns in S' defines a matching.
   - **d.** Else, π has at least 3 elements not on the diagonal. We claim that it is always possible to pick S' so that
     - π defines a matching, when it is restricted to the columns in S'.
     - π disagrees with the diagonal in at least 2 positions when it is restricted to the columns with indices in S'.
     - π contains an element with column index in S' and row index not in S'.

     To justify that, first shrink S to be of size $r+3$ by preserving the condition that π disagrees with the diagonal in at least 3 columns. If π is a matching on S, choose any $(i,j) \in \pi$ with $i \neq j$ and define $S' = S \setminus \{i\}$. Otherwise, by Lemma 39, π contains a matching of size $r+2$, so there is precisely one row i with 2 elements in columns j_1 and j_2. Moreover, there is $j \in S$ such that the row with index j has no element of π. To get S' delete from S any of the elements j_1, j_2 that is different from j. Such S' satisfies all the desired properties.

Let $\pi' \subseteq [2r] \times S'$ denote the restriction of π to the columns in S' and define a matrix $B = \mathrm{proj}_{S'}(M)$. If there is a column of B with no element of π' we add an element to π' in this column to the row that has no element of π', and if possible, with an index not in S'. Thus, we may assume that every column of B contains precisely one element of π', and π' defines a matching.

By permuting the rows and columns of M in a way that preserves the diagonal, we may assume that $S' = [r+2]$. We also assume that coordinates in Ω_M are permuted accordingly.

We want to show that for almost all M and all $\pi \in \mathcal{P}_0$ there is no "large set" (in the sense of Lemma 42) of diagonal matrices $D \in \mathrm{Diag}(\mathbb{K}^{2r\times 2r})$ such that for arbitrary D in this set $\mathrm{rank}(M+D+Z) \leq r$ for some $Z \in \mathbb{K}^{(\pi)}$.

To do this, we show how to permute rows and columns of B in order to apply one of the lemmas proved in Sections 3.3 and 3.4. We have three cases for π'.

(A) If π' coincides with the diagonal, then by Lemma 43 for almost all matrices $M \in \mathcal{D}_r^{\#}$ there is no diagonal matrix $Y \in \mathrm{Diag}(\mathbb{K}^{2r\times(r+2)})$ such that $B+Y$ has rank at most r.

(B) If π' disagrees with the diagonal in precisely one column, then by the choice of S', π' has an element in a row that is not in $S' = [r+2]$. We may permute the rows and the columns of B, so that the diagonal is preserved and $\pi' = \{(i,i) \mid i \in [r+1]\} \cup \{(r+3, r+2)\}$. Then it follows from Lemma 46 that for almost all matrices $M \in \mathcal{D}_r^{\#}$ there are no unbounded sets $E_1, E_2, \ldots, E_{r+2}$ such that for every matrix $D \in \mathrm{Diag}(\mathbb{C}^{2r\times r})$ with $D_{ii} \in E_i$ for $i \in [r+2]$ there exists $Y \in \mathbb{C}^{(\pi')}$ for which $B+D+Y$ has rank at most r.

(C) If π' disagrees with the diagonal in at least 2 columns, then, by the choice of S', there is a row with index $j_1 > r+2$ that has an element of π' in the column $i_1 \in S' = [r+2]$. Moreover, there is at least one other column i_2 with an element of π not on a diagonal. Since π' defines a matching, we can permute the rows and the columns of B so that π' becomes the diagonal and columns i_1, i_2 are mapped to columns $r+1$ and $r+2$. Let $\sigma \subseteq [2r] \times [r+2]$ be the the image of the diagonal after such permutation. By the construction of π', σ has the entry in column $r+1$ in the row with index $\geq r+3$ and the entry in column $r+2$ in the row distinct from $r+2$. If the entry of σ in the last column is in the row with index $\leq r$ we can further permute the first r columns and rows in the way that preserves the diagonal, so that the entry of σ in the last column becomes in the first row.

Let $E_1, E_2, \ldots, E_{r+2}$ be unbounded subsets of $\mathbb{K}$ (which may depend on M) and let $\sigma' = \sigma \setminus \{(i,i) \mid i \in [r]\}$. Let $D \in \mathbb{K}^{(\sigma)}$ be such that $D_{ij} \in E_j$ for all $(i,j) \in \sigma$ and let D' be a part of D supported on σ'. Then, by Lemma 45 and Lemma 47, if for every D there exists $Y \in \mathrm{Diag}(\mathbb{C}^{2r\times(r+2)})$ such that $B+D+Y$ has rank at most r, then for every D, $\mathrm{proj}_{[r]}(B) + D'$ belongs to a proper Zariski-closed subset $\mathcal{B}_{\pi'}$ of $\mathbb{K}^{2r\times r}$, which depends only on π'.

This means that there exists a non-trivial polynomial $f \in \mathbb{K}[x_{ij}]_{i\in[2r],\ j\in[r]}$ such that $f(\mathrm{proj}_{[r]}(B) + D') = 0$. Consider this as a polynomial with variables d_{ij}, which are the (i,j)-th entries of D' with $(i,j) \in \sigma'$. Since every variable d_{ij} independently can take infinitely many values we get that this is a trivial polynomial in variables d_{ij}. Since f is non-trivial, we get that entries of B satisfy some non-trivial polynomial.

Therefore, for almost all $M \in \mathcal{D}_r^{\#}$ there are no unbounded sets $E_1, E_2, \ldots, E_{r+2}$ such that for every matrix $D \in \mathrm{Diag}(\mathbb{C}^{2r\times r})$ with $D_{ii} \in E_i$ for $i \in [r+2]$ there exists $Y \in \mathbb{C}^{(\pi')}$ for which $B+D+Y$ has rank at most r.

We see from (A), that there is a set $\mathcal{M}$ of almost all matrices $M \in \mathcal{D}_r^{\#}$, such that for all $D \in \Omega_M$ and all well-distributed π, for which π' coincides with the diagonal, there is no $Z \in \mathbb{K}^{(\pi)}$ with $\mathrm{rank}(M+D+Z) \leq r$.

Let $\mathcal{P}_1 \subseteq \mathcal{P}_0$ be the set of well-distributed $\pi \subseteq [2r]\times[2r]$ for which the π', constructed by the rules above, does not end up in case (A), i.e. π' does not coincide with the diagonal.

Assume that $M \in \mathcal{M}$. Then for any $D \in \Omega_M$ there should exists a $\pi \in \mathcal{P}_1$ and $Z \in \mathbb{K}^{(\pi)}$ such that $\mathrm{rank}(M+D+Z) \leq r$. Using Lemma 42, applied with $P = \mathcal{P}_1$, we deduce that there exists a set $\pi \in \mathcal{P}_1$ and unbounded sets $E_1, E_2, \ldots, E_{2r} \subseteq \mathbb{K}$, such that for any $D \in \mathrm{Diag}(\mathbb{K}^{2r\times 2r})$ with $D_{ii} \in E_i$ for every $i \in [2r]$, there exists $Z \in \mathbb{C}^{(\pi)}$ with $\mathrm{rank}(M+D+Z) \leq r$. Let S' be as above and $B = \mathrm{proj}_{S'}(M)$. Then $\mathrm{rank}(B+\mathrm{proj}_{S'}(D)+\mathrm{proj}_{S'}(Z)) \leq r$. However, for almost all matrices M this gives a contradiction with (B) or (C).

Thus, for almost all $M \in \mathcal{D}_r^{\#}$ there is $D \in \mathrm{Diag}(\mathbb{K}^{2r\times 2r})$ with $R_{\mathbb{K}}(M+D,r) \geq 3r-2$. ◀

4 Field extension: avoiding transcendentals

In this section we prove that absolute rigidity can always be achieved over a finite extension. Recall that a field extension $\mathbb{L}/\mathbb{K}$ is *finite* if $\dim_{\mathbb{K}} \mathbb{L}$ is finite. Recall also that we wrote $R^*(A,r)$ to denote the absolute rigidity of A for target rank r.

▶ **Proposition 49.** *Let A be a matrix over the field $\mathbb{K}$. Then there exists a finite extension $\mathbb{L}/\mathbb{K}$ such that for all $r \geq 0$ we have $R^*(A,r) = R_{\mathbb{L}}(A,r)$.*

▶ **Notation 50** (weight). For a matrix A, let $w(A)$, the *weight* of A, denote the number of nonzero entries of A.

We begin with some simple observations.

▶ **Observation 51.** *If $\mathbb{L}/\mathbb{K}$ is a field extension and A is a matrix over $\mathbb{K}$, then, for all $r \geq 0$, we have $R_{\mathbb{K}}(A,r) \geq R_{\mathbb{L}}(A,r)$.* ◀

▶ **Definition 52.** *For a field $\mathbb{K}$ let $\mathrm{cl}(\mathbb{K})$ denote the algebraic closure of the pure transcendental extension of $\mathbb{K}$ of countably infinite transcendence degree.*

▶ **Observation 53.** *Let A be a matrix over the field $\mathbb{K}$. Then for all $r \geq 0$, we have $R^*(A,r) = R_{\mathrm{cl}(\mathbb{K})}(A,r)$.*

Proof. Fix r. By definition, $R^*(A,r) \leq R_{\mathrm{cl}(\mathbb{K})}(A,r)$. We need to prove the reverse inequality.

Let $\mathbb{L}$ be an extension of $\mathbb{K}$ such that $R^*(A,r) = R_{\mathbb{L}}(A,r)$. So there exists a matrix D over $\mathbb{L}$, of weight $R^*(A,r)$, such that $\mathrm{rank}(A-D) \leq r$. Let $\mathbb{M} \subseteq \mathbb{L}$ be the subfield generated by $\mathbb{K}$ and the elements of D. Then $R_{\mathbb{L}}(A,r) = R_{\mathbb{M}}(A,r)$. But $\mathbb{M}$ can be embedded in $\mathrm{cl}(\mathbb{K})$ and therefore, by Obs. 51, $R_{\mathbb{M}}(A,r) \geq R_{\mathrm{cl}(\mathbb{K})}(A,r)$. So $R^*(A,r) = R_{\mathbb{L}}(A,r) = R_{\mathbb{M}}(A,r) \geq R_{\mathrm{cl}(\mathbb{K})}(A,r)$. ◀

We shall need the following well-known result, which is often the first step in the proof of Hilbert's Nullstellensatz. See, e. g., Cor. 1.2 in Chap. 9, §1 of [9].

▶ **Fact 54.** Let $\mathbb{L}/\mathbb{K}$ be a field extension. Assume $\mathbb{L}$ is a finitely generated $\mathbb{K}$-algebra. Then the extension $\mathbb{L}/\mathbb{K}$ is finite.

Proof of Proposition 49. We need to achieve $R_{\mathbb{L}}(A,r) = R_{\mathrm{cl}(\mathbb{K})}(A,r)$ for all r. For each r we have a matrix Z_r over $\mathrm{cl}(\mathbb{K})$ of weight $\leq R^*(A,r)$ such that $\mathrm{rank}_{\mathrm{cl}(\mathbb{K})}(A - Z_r) \leq r$. Let $\mathcal{Z}$ denote the set of elements of the matrices Z_r, $r \geq 0$. This is a finite set. (If $r \geq \mathrm{rk}(A)$ then $Z_r = 0$.) Let $\mathcal{B} = \mathbb{K}[\mathcal{Z}]$ denote the $\mathbb{K}$-algebra generated by $\mathcal{Z}$. Let $\mathcal{M}$ be a maximal ideal of $\mathcal{B}$, and let $\mathbb{L} = \mathcal{B}/\mathcal{M}$. So $\mathbb{L}$ is an extension field of $\mathbb{K}$.

Let $\varphi : \mathcal{B} \to \mathbb{L}$ denote the natural epimorphism. So φ fixes all elements of $\mathbb{K}$. Moreover, for every matrix B we have $w(\varphi(B)) \leq w(B)$ and $\mathrm{rank}(\varphi(B)) \leq \mathrm{rank}(B)$ (because singular minors are mapped to singular minors). Therefore $\mathrm{rank}(A - \varphi(Z_r)) = \mathrm{rank}\,\varphi(A - Z_r) \leq \mathrm{rank}(A - Z_r) \leq r$, and $w(\varphi(Z_r)) \leq w(Z_r)$. This proves that $R_{\mathbb{L}}(A,r) \leq R^*(A,r)$. The reverse inequality holds by definition.

Finally we need to show that the extension $\mathbb{L}/\mathbb{K}$ is finite. This is immediate from Fact 54, given that $\mathbb{L} = \mathbb{K}[\varphi(\mathcal{Z})]$ is a finitely generated $\mathbb{K}$-algebra which is a field. ◀

We observe that Prop. 49 is equivalent to saying that absolute rigidity is achieved over the algebraic closure of the field of definition of the matrix.

▶ **Corollary 55.** *Let A be a matrix over the field $\mathbb{K}$. Then $R^*(A,r) = R_{\overline{\mathbb{K}}}(A,r)$, where $\overline{\mathbb{K}}$ denotes the algebraic closure of $\mathbb{K}$. Moreover, this statement is equivalent to Prop. 49.*

Proof. Assume Prop. 49. Let $\mathbb{L}$ be a finite extension of $\mathbb{K}$ such that $R^*(A,r) = R_{\mathbb{L}}(A,r)$. Then $\mathbb{L}$ can be embedded in $\overline{\mathbb{K}}$, so a reference to Obs. 51 proves the Corollary.

Now suppose the Corollary is true. For every r, let B_r be the matrix over $\overline{\mathbb{K}}$ such that $\mathrm{rank}(B_r) \leq r$ and $w(A - B_r) = R^*(A,r)$. Let $S \subset \overline{\mathbb{K}}$ be the (finite) set of elements of the matrices B_r. Then, for all r, we have $R^*(A,r) = R_{\mathbb{K}[S]}(A,r)$. But $\mathbb{K}[S]$ is a finite extension, proving Prop. 49. ◀

A similar result holds for linear arithmetic circuits.

▶ **Proposition 56.** *Let $\mathbb{E}/\mathbb{K}$ be a field extension. Let $\mathcal{A}$ be a linear arithmetic circuit over the field $\mathbb{E}$ that computes a linear function $x \mapsto Ax$ over $\mathbb{K}$ (so A is a matrix over $\mathbb{K}$). Then $\mathcal{A}$ can be simulated by a linear arithmetic circuit $\mathcal{A}'$ over a finite extension of $\mathbb{K}$ such that $\mathcal{A}'$ has the same set of nodes and wires as $\mathcal{A}$.*

Proof. Each node of $\mathcal{A}$ computes an $\mathbb{E}$-linear combination of its inputs. Let $\mathcal{Z}$ denote the set of all the coefficients occurring at nodes. Let $\mathcal{B} = \mathbb{K}[\mathcal{Z}]$ denote the $\mathbb{K}$-algebra generated by $\mathcal{Z}$. Let $\mathcal{M}$ be a maximal ideal of $\mathcal{B}$, and let $\mathbb{L} = \mathcal{B}/\mathcal{M}$. So $\mathbb{L}$ is an extension field of $\mathbb{K}$. We shall define the linear arithmetic circuit $\mathcal{A}'$ over $\mathbb{L}$.

Let $\varphi : \mathcal{B} \to \mathbb{L}$ denote the natural epimorphism. So φ fixes all elements of $\mathbb{K}$. Now keep all nodes and links in $\mathcal{A}$ but replace each scalar $a \in \mathcal{Z}$ involved in $\mathcal{A}$ (as a coefficient of a linear combination at a gate) by $\varphi(a)$. So this circuit will compute the transformation $x \mapsto \varphi(A)x$. But $\varphi(A) = A$ (since φ fixes $\mathbb{K}$ pointwise), so the simulation is complete.

Finally, as before, the extension $\mathbb{L}/\mathbb{K} = \mathbb{K}[\varphi(\mathcal{Z})]/\mathbb{K}$ is finite by Fact 54. ◀

5 Refutation of more candidates for rigidity

In this section we show that, as corollaries to the results of Dvir and Liu [4], more long-running candidates for rigidity fail.

▶ **Definition 57** (G-circulants)**.** *Let G be a finite abelian group of order n, and let $A = (a_{ij})$ be an $n \times n$ matrix over a domain D. Let the rows and columns of A be labeled by the elements of G. We say that A is a G-circulant if there is a function $f : G \to D$ such that for all $i, j \in G$ we have $a_{ij} = f(i - j)$. A* circulant *matrix is a G-circulant where G is the cyclic group of order n.*

Recall that by a *family* of square matrices we mean a set of square matrices of unbounded order.

▶ **Theorem 58** (Dvir–Liu)**.**

(a) *No family of G-circulants over $\mathbb{C}$ (for variable G) is Valiant-rigid over $\mathbb{C}$.*

(b) *No family of circulants over a fixed finite field is strictly Valiant-rigid.*

Part (a) is stated in [4, Theorem 1.5]. Part (b) is stated in [4, Theorem 7.27].

5.1 Point–hyperplane incidence matrices

Finite projective geometries of dimension d are defined by geometric axioms. "Desargues' Theorem" is not one of the axioms; geometries satisfying this additional axiom are called Desarguesian. The Desarguesian finite projective geometries are precisely the *Galois geometries* $\mathrm{PG}(d, q)$ constructed from finite fields (q is the order of the field).

In fact, for $d \geq 3$, all projective spaces are Desarguesian. However, this is not the case for $d = 2$ (finite projective planes), so we need to make this distinction. Here we are interested only in Galois geometries.

Let q be a prime power and $d \geq 2$. The points as well as the hyperplanes of the d-dimensional Galois geometry $\mathrm{PG}(d, q)$ can be represented by equivalence classes of nonzero vectors in $\mathbb{F}_q^{d+1}$, where the equivalence relation is defined by scaling (one vector is a scalar multiple of the other). In particular, there are $N := (q^{d+1} - 1)/(q - 1)$ points and the same number of hyperplanes in this geometry. Let a be a point represented by a vector $x \in \mathbb{F}_q^{d+1} \setminus \{0\}$ and let b be a hypeplane represented by a vector $y \in \mathbb{F}_q^{d+1} \setminus \{0\}$. Then a and b are incident if and only if $x^T y = 0$ (x and y are "orthogonal"). (We view x, y as column vectors.)

The incidence matrix of this geometry is the $N \times N$ $(0,1)$ matrix of which the rows are labeled by the points, the columns are labeled by the hyperplanes, and an entry of 1 represents incidence.

▶ **Lemma 59.** *Let q be a prime power and $d \geq 2$. Under appropriate numbering of the points and hyperplanes, the point–hyperplane incidence matrix of the Galois geometry $\mathrm{PG}(d,q)$ is a circulant matrix.*

Proof. This is a consequence of the existence of a *Singer cycle* in $\mathrm{GL}(d+1,q)$, i. e., a linear transformation σ of $\mathbb{F}_q^{d+1}$ that cyclically permutes the nonzero vectors. The existence of such a transformation follows from the fact that the muliplicative group of $\mathbb{F}_{q^{d+1}}$ is cyclic: View $\mathbb{F}_q^{d+1}$ as the additive group of $\mathbb{F}_{q^{d+1}}$ and let σ be the multiplication by a generator of the multiplicative group of $\mathbb{F}_{q^{d+1}}$; this is a linear transformation of $\mathbb{F}_q^{d+1}$.

Any linear transformation of $\mathbb{F}_q^{d+1}$ preserves the "scaling" equivalence relation, so σ also gives a cyclic permutation of the points and the hyperplanes.

Let $A \in GL(d+1,q)$ be an invertible matrix and let let B denote its inverse-transpose. Then, for any $x, y \in \mathbb{F}_q^{d+1}$ we have $x^T y = 0$ if and only if $(Ax)^T(By) = 0$. So in this sense, the pair (A,B) preserves orthogonality.

Let now A be the matrix of a Singer cycle and let B denote its inverse-transpose. Let a_0 be a point represented by the vector $x \neq 0$ and b_0 a hyperplane represented by the vector $y \neq 0$. For $k \in \mathbb{Z}$, let a_k be the point represented by $A^k x$ and let b_k be the hyperplane represented by the vector $B^k y$. So $a_i = a_j$ if and only if $i \equiv j \pmod{N}$, and the same holds for the b_i. We also note by the foregoing that a_i and b_j are incident if and only if a_{i+1} and b_{j+1} are incident. This means that arranging the points in the order $a_0, \dots, a_{N-1}$ and the hyperplanes in the order $b_0, \dots, b_{N-1}$, the incidence matrix becomes a circulant. ◀

We obtain the following two corollaries from Theorem 58.

▶ **Corollary 60.** *For no family of Galois geometries is the corresponding family of point–hyperplane incidence matrices absolutely Valiant-rigid in characteristic zero.*

▶ **Corollary 61.** *For no family of Galois geometries is the corresponding family of point–hyperplane incidence matrices strictly Valiant-rigid over any fixed finite field.*

Galois planes are the Galois geometries $\mathrm{PG}(2,q)$. It follows from Corollary 61 that for no family of Galois planes is the corresponding family of point-line incidence matrices Valiant-rigid over $\mathbb{F}_2$. This is noteworthy because Valiant [16] suggested (without making a distinction between Desarguesian and non-Desarguesian planes) that the incidence matrices of finite projective planes might be candidates for rigidity over $\mathbb{F}_2$.

5.2 Vandermonde matrices

In this section we show that Vandermonde matrices of which the generators form a geometric progression are not absolutely Valiant-rigid.

▶ **Definition 62** (G-Hankel matrices)**.** *Let G be a finite abelian group of order n. Let $f : G \to \mathbb{F}$ be a function from G to a field $\mathbb{F}$. We define the G-Hankel matrix corresponding to f as the $n \times n$ matrix, whose rows and columns are labeled by the elements of G, and the element in position (g,h) is $f(g+h)$.*

As pointed out in [4], by permuting the rows of a G-Hankel matrix one can get a G-circulant matrix. Therefore such a pair of matrices has the same rigidity.

The classical *Hankel matrices* are the special case of G-Hankel matrices where G is the cyclic group of order n.

▶ **Observation 63.** *Let V be a Vandermonde matrix over a field $\mathbb{K}$ with generators that form a geometric progression. Then there exist diagonal matrices D_1 and D_2 over $\mathbb{K}$ such that D_1VD_2 is a Hankel matrix.*

Proof. Assume that the generators of V are sa^{i-1} for $i = 1, 2, \ldots, n$. Then the (i, j)-th entry of V is $s^{(j-1)}a^{(i-1)(j-1)}$. Define a pair of diagonal matrices with entries

$$(D_1)_{ii} = a^{i(i-1)/2} \quad \text{and} \quad (D_2)_{jj} = s^{-(j-1)}a^{j(j-1)/2}.$$

Clearly, the entries of D_1 and D_2 belong to K. Moreover,

$$(D_1VD_2)_{ij} = a^{1+(i+j)(i+j-3)/2}.$$

Thus, D_1VD_2 is a Hankel matrix. ◀

This observation, combined with part (a) of Theorem 58 by Dvir and Liu, yields the following corollary.

▶ **Corollary 64.** *Let $\mathcal{F}$ be a family of Vandermonde matrices over fields of characteristic zero, with generators that form a geometric progression. Then $\mathcal{F}$ is not absolutely Valiant-rigid.*

Proof. Note that multiplication by a diagonal matrix with non-zero entries does not change rigidity, so for D_1 and D_2 defined as above, $R_{\mathbb{K}}(V, r) = R_{\mathbb{K}}(D_1VD_2, r)$. ◀

5.3 Paley–Hadamard matrices

Hadamard matrices have for decades been considered candidates for rigidity. To everyone's surprise, Alman and Williams [2] recently showed that the Walsh–Hadamard matrices are not strictly Valiant-rigid.

In this section we remove a lot more Hadamard matrices from the list of rigidity candidates.

▶ **Corollary 65.** *No family of Paley–Hadamard matrices is absolutely Valiant-rigid.*

While the orders of the Walsh–Hadamard matrices are the powers of 2, the Paley–Hadamard matrices are exponentially more frequent: for every prime power $q \equiv -1 \pmod 4$ there is a Paley–Hadamard matrix of order $q + 1$, and for every prime power $q \equiv 1 \pmod 4$ there is a Paley–Hadamard matrix of order $2q + 2$.

Let q be an odd prime power and let $\chi : \mathbb{F}_q \to \{0, 1, -1\} \subseteq \mathbb{C}$ denote the quadratic character over $\mathbb{F}_q$. So for $x \in \mathbb{F}_q$, we have $\chi(x) = 0$ if $x = 0$; $\chi(x) = 1$ if $x \neq 0$ is a square in $\mathbb{F}_q$ and $\chi(x) = -1$ if x is not a square.

▶ **Definition 66** (Paley–Hadamard matrices). *For an odd prime power q define a $q \times q$ matrix Q with $Q_{i,j} = \chi(i - j)$.*

- *if $q \equiv -1 \mod 4$, consider a matrix $H = I + \begin{pmatrix} 0 & \mathbf{1^T} \\ \mathbf{1} & Q \end{pmatrix}$, where $\mathbf{1}$ is an all-ones vector.*
- *if $q \equiv 1 \mod 4$, consider a matrix H obtained by replacing each entry of $\begin{pmatrix} 0 & \mathbf{1^T} \\ \mathbf{1} & Q \end{pmatrix}$ with a 2×2 matrix in the following way.*
  1. *Each entry 0 is replaced with $\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$;*
  2. *Each entry ± 1 is replaced with $\pm \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.*

The matrix H is a Hadamard matrix and is called a Paley–Hadamard matrix.

▶ **Observation 67.** *Let q be an odd prime power and let Q be the corresponding Paley–Hadamard matrix.*

- *If $q \equiv -1 \mod 4$, then the lower right $q \times q$ submatrix of H is a G-circulant matrix, where G is the additive group of $\mathbb{F}_q$.*
- *If $q \equiv 1 \mod 4$, then the lower right $2q \times 2q$ submatrix of H consists of 4 blocks that are G-circulants for the additive group of $\mathbb{F}_q$.*

Proof. If $q \equiv -1 \mod 4$, the statement immediately follows from the definition of the matrix Q. If $q \equiv 1 \mod 4$, denote by H_0 the right-lower $2q \times 2q$ submatrix. Note that the matrix obtained from H_0 by looking at the entries on the intersection of odd rows and odd columns is $Q + I$, and so is a circulant. Similarly, the matrices obtained by looking at the intersection of even rows and even columns, odd rows and even columns, and even rows and odd columns are circulants. ◀

This observation, combined with Theorem 58, proves Corollary 65.

References

1 Josh Alman. Kronecker products, low-depth circuits, and matrix rigidity. In *Proc. 53rd ACM Symp. on Theory of Computing (STOC'21)*, pages 772–785, 2021. arXiv:2102.11992. doi:10.1145/3406325.3451008.

2 Josh Alman and Ryan Williams. Probabilistic rank and matrix rigidity. In *Proc. 49th STOC*, pages 17:1–17:23. ACM Press, 2017. doi:10.1145/3055399.3055484.

3 Zeev Dvir and Benjamin Edelman. Matrix rigidity and the Croot-Lev-Pach lemma. *Theory of Computing*, 15(8):1–7, 2019. doi:10.4086/toc.2019.v015a008.

4 Zeev Dvir and Allen Liu. Fourier and circulant matrices are not rigid. *Theory of Computing*, 16(20):1–48, 2020. doi:10.4086/toc.2020.v016a020.

5 Joel Friedman. A note on matrix rigidity. *Combinatorica*, 13(2):235–239, 1993. doi:10.1007/BF01303207.

6 Oded Goldreich and Avishay Tal. Matrix rigidity of random Toeplitz matrices. *Comput. Complexity*, 27(2):305–350, 2018. Preliminary version in STOC'16. doi:10.1007/s00037-016-0144-9.

7 Robin Hartshorne. *Algebraic geometry.* Graduate texts in mathematics (52) Springer, 1977.

8 Bohdan Kivva. Improved upper bounds for the rigidity of Kronecker products. *arXiv*, 2021. arXiv:2103.05631.

9 Serge Lang. *Algebra*, volume 211 of *Grad. Texts in Math.* Springer, 3rd edition, 1996.

10 Satyanarayana V. Lokam. On the rigidity of Vandermonde matrices. *Theoret. Comput. Sci.*, 237(1–2):477–483, 2000. doi:10.1016/S0304-3975(00)00008-6.

11 Satyanarayana V. Lokam. Quadratic lower bounds on matrix rigidity. In *Internat. Conf. on Theory and Appl. of Models of Computation (TAMC'06)*, pages 295–307. Springer, 2006. doi:10.1007/11750321_28.

12 Alexander Razborov. On Rigid Matrices. Technical report, Steklov Mathematical Institute, 1989.

13 Alex Samorodnitsky, Ilya Shkredov, and Sergey Yekhanin. Kolmogorov width of discrete linear spaces: an approach to matrix rigidity. *Computational Complexity*, 25(2):309–348, 2016.

14 Mohammad Amin Shokrollahi, Daniel A. Spielman, and Volker Stemann. A remark on matrix rigidity. *Inform. Process. Lett.*, 64(6):283–285, 1997. doi:10.1016/S0020-0190(97)00190-7.

15 Victor Shoup and Roman Smolensky. Lower bounds for polynomial evaluation and interpolation. *Computational Complexity*, 6(4):301–311, 1997.

16 Leslie G. Valiant. Graph-theoretic arguments in low-level complexity. In *Math. Found. Comp. Sci. (MFCS'77)*, pages 162–176. Springer, 1977. doi:10.1007/3-540-08353-7_135.

A Basic concepts of algebraic geometry

In this appendix we review basic notions of the algebraic geometry that are needed in this paper. Our definitions follow [7], but, critically, we do not make the assumption that a field is algebraically closed.

Let $\mathbb{F}$ be an infinite field. $\mathbb{F}[x_1, x_2, \ldots, x_n]$ denotes the ring of polynomials in variables $x_1, x_2, \ldots, x_n$, with coefficients in $\mathbb{F}$.

▶ **Definition 68** (Affine algebraic set [7, p.2]). *A set $V \subseteq \mathbb{F}^n$ is called an (affine)* algebraic set *if it is the set of common zeros of a set of polynomials, $P \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$.*

▶ **Theorem 69** (Hilbert basis theorem). *Every affine algebraic set in $\mathbb{F}^n$ can be defined by a finite set of polynomials in $\mathbb{F}[x_1, x_2, \ldots, x_n]$.*

▶ **Definition 70** (Irreduciblility). *A topological space is* irreducible *if it is not a union of two nonempty proper closed subsets.*

▶ **Observation 71.** *The intersection of a finite number of non-empty open subsets of an irreducible topological space is non-empty (and open).*

Proof. For two sets this is equivalent to the definition of irreducibility; the full statement follows by induction. ◀

▶ **Definition 72** (Zariski topology 1 [7, p.2]). *The* Zariski topology *on $\mathbb{F}^n$ is the topology in which the closed sets are precisely the affine algebraic sets of $\mathbb{F}^n$.*

▶ **Proposition 73.** *The Zariski topology on $\mathbb{F}^n$ is a topology, and $\mathbb{F}^n$ is irreducible.*

Proof. To prove irreducibility, let A_1 and A_2 be two Zariski-closed proper subsets of $\mathbb{F}^n$. Let the nonzero polynomial f_i vanish on A_i. Let $a \in \mathbb{F}^n$ be a point at which $(f_1 f_2)(a) \neq 0$. It follows that $a \notin A_1 \cup A_2$. ◀

▶ **Definition 74** (Locally closed set). *In a topological space, a set is called* locally closed *if it can be written as an intersection of an open set and a closed set.*

▶ **Definition 75** (Zariski topology 2). *Let $V \subseteq \mathbb{F}^n$ be a locally closed set in the Zariski topology. The Zariski topology on V is the restriction of the Zariski topology on $\mathbb{F}^n$ to V.*

▶ **Observation 76.** *Let V and W be topological spaces. Let $f : V \to W$ be a continuous surjective map. If V is irreducible, then W is irreducible.*

▶ **Definition 77** ((Quasi-)affine variety [7, p.3]). *An irreducible affine algebraic set is called an* affine variety*. A Zariski-open subset of an affine variety is called a* quasi-affine variety.

It is easy to see that a quasi-affine variety is irreducible by definition.

▶ **Definition 78** (Almost all). *We say that some property holds for* almost all *points in a (quasi-)affine variety if it holds for some non-empty Zariski-open subset of the variety.*

We now restate Obs. 71.

▶ **Observation 79.** *If each of a finite number of properties holds for almost all points of a quasi-variety V, then they all hold simultaneously for almost all points of V.*

▶ **Definition 80** (Regular function [7, p.15]). *Let V be a quasi-affine variety in $\mathbb{F}^n$. A function $f : V \to \mathbb{F}$ is* regular at a point $p \in V$ *if there exists a Zariski-open neighbourhood $p \in U \subset V$ and polynomials $g, h \in \mathbb{F}[x_1, x_2, \dots, x_n]$ such that h is nowhere zero on U and $f = g/h$ on U. We say that f is* regular *on V if it is regular at every point of V.*

▶ **Lemma 81** ([7, Lemma 3.1]). *A regular function $f : V \to \mathbb{F}$ is continuous.*

▶ **Definition 82** (Morphism [7, p.15]). *Let V, W be a pair of quasi-affine varieties. A* morphism *(or a* regular map*) $\phi : V \to W$ is a continuous map such that for every open set $U \in W$, and for every regular function $f : U \to \mathbb{F}$ the function $f \circ \phi : \phi^{-1}(U) \to \mathbb{F}$ is regular.*

Clearly, the composition of two morphisms is a morphism.

▶ **Lemma 83** ([7, Lemma 3.6]). *Let X be a quasi-affine variety and $Y \subseteq \mathbb{F}$ be an affine variety. A map (of sets) $\phi : X \to Y$ is a morphism if and only if $x_i \circ \phi$ is a regular function on X for each i, where $x_1, x_2, \dots, x_n$ are the coordinate functions on $\mathbb{F}^n$.*

▶ **Observation 84.** *Let $E_1, E_2, \dots, E_n$ be infinite subsets of $\mathbb{F}$. Suppose the polynomial $f \in \mathbb{F}[x_1, x_2, \dots, x_n]$ vanishes on the Cartesian product $E_1 \times \cdots \times E_n$. Then f is the zero polynomial.*

▶ **Lemma 85.** *Let U be a non-empty Zariski-open subset of $\mathbb{F}^n$, where $\mathbb{F}$ is a subfield of $\mathbb{C}$. Then there exist $E_1, E_2, \dots E_n \subseteq \mathbb{F}$ such that $E_1 \times \cdots \times E_n \subseteq U$ and each E_i is an unbounded set in $\mathbb{C}$.*

Proof. Since U is Zariski-open, there exists a polynomial $f \in \mathbb{F}[x_1, \dots, x_n]$, such that if $f(a_1, \dots a_n) \neq 0$, then $(a_1, \dots, a_n) \in U$. Let $E_1', E_2', \dots E_n' \subseteq \mathbb{F}$ be finite sets, such that for all $a_i \in E_i'$, $i \in [n]$ we have $f(a_1, a_2, \dots, a_n) \neq 0$. Then it is easy to see that for an arbitrary j there exists $b_j \notin E_j'$ such that the same condition holds when E_j' is replaced with $E_j' \cup \{b_j\}$. Moreover, such b_j can be taken so that its complex norm is greater than 1 plus the maximum of the norms of all elements that are currently in E_j'. Since we can in turn increment the size of each E_i, the claim follows by passing to the limit. ◀

▶ **Definition 86** (Constructible set). *In a topological space, a set is called* constructible *if it is a finite union of locally closed sets.*

▶ **Theorem 87** (Chevalley's theorem). *Let $f : V \to W$ be a regular map between algebraic sets over $\mathbb{F}$. Then $f(V)$ is a constructible set in the Zariski topology on W.*

B Omitted proofs

In this appendix we provide the proofs of Lemmas 46 and 47.

▶ **Lemma 88.** *Let $r \geq 3$. Consider $A_1 \in \mathbb{K}^{r \times r}$ and an invertible matrix $A_2 \in \mathbb{K}^{r \times r}$. Define*

$$v_i = -A_1^2 A_2^{-1} e_i + \omega^2 A_2^{-1} e_i \quad \text{and} \quad w_i = -A_2 A_1 A_2^{-1} e_i$$

Let $E_2 \subseteq \mathbb{K}$ be an unbounded set. For a diagonal matrix $Z \in \mathbb{C}^{r \times r}$ and $z_1, z_2 \in \mathbb{C}$, $x_2 \in \mathbb{K}$ consider

$$T(x_2, Z, z_1, z_2) = \begin{pmatrix} A_1 + Z & v_1 & v_2 \\ A_2 & w_1 + z_1 e_1 & w_2 + z_2 e_3 + x_2 e_2 \end{pmatrix}.$$

The set of matrices $(A_1, A_2) \in \mathbb{K}^{2r^2}$ such that for all $x_2 \in E_2$ there exist $Z \in \mathrm{Diag}(\mathbb{C}^{r \times r})$, and $z_1, z_2 \in \mathbb{C}$ such that $\mathrm{rank}(T(x_2, Z, z_1, z_2)) \leq r$ is small in $\mathbb{K}^{2r^2}$.

Proof. Assume $\operatorname{rank}(T(x_2, Z, z_1, z_2)) \leq r$. Since A_2 is invertible, the last two columns of $B(x_2, Z, z_1, z_2)$ can be expressed as a linear combination of the first r columns.

For convenience, define $x_1 = 0$, $j_1 = 1$ and $j_2 = 3$. Let $y_i \in \mathbb{K}^r$ satisfy

$$\begin{pmatrix} A_1 + Z \\ A_2 \end{pmatrix} y_i = \begin{pmatrix} v_i \\ w_i + z_i e_{j_i} + x_i e_2 \end{pmatrix}.$$

Then

$$y_i = A_2^{-1}(w_i + z_i e_{j_i} + x_i e_2) \quad \Rightarrow \quad (A_1 + Z)A_2^{-1}(w_i + z_i e_{j_i} + x_i e_2) = v_i,$$

$$-A_1^2 A_2^{-1} e_i + z_i A_1 A_2^{-1} e_{j_i} + x_i A_1 A_2^{-1} e_2 + Z(-A_1 A_2^{-1} e_i + z_i A_2^{-1} e_{j_i} + x_i A_2^{-1} e_2) = -A_1^2 A_2^{-1} e_i + \omega^2 A_2^{-1} e_i.$$

Let $\alpha_i = A_1 A_2^{-1} e_i$ and $\beta_i = A_2^{-1} e_i$. Then for all $k \in [r]$ we have

$$Z_{kk} = \frac{\omega^2 \beta_{1k} - z_1 \alpha_{1k}}{-\alpha_{1k} + z_1 \beta_{1k}} \quad \text{and} \quad Z_{kk} = \frac{\omega^2 \beta_{2k} - z_2 \alpha_{3k} - x_2 \alpha_{2k}}{-\alpha_{2k} + z_2 \beta_{3k} + x_2 \beta_{2k}}.$$

Hence, for all $k \in [r]$,

$$\frac{\omega^2 \beta_{1k} - z_1 \alpha_{1k}}{-\alpha_{1k} + z_1 \beta_{1k}} = \frac{\omega^2 \beta_{2k} - z_2 \alpha_{3k} - x_2 \alpha_{2k}}{-\alpha_{2k} + z_2 \beta_{3k} + x_2 \beta_{2k}}. \tag{14}$$

By passing to a subsequence for $x_2 \in E_2$ we may assume that $\lim\limits_{E_2 \ni x_2 \to \infty} z_2(x_2)/x_2 = c \in \widehat{\mathbb{C}}$ and $\lim\limits_{E_2 \ni x_2 \to \infty} z_1(x_2) = c' \in \widehat{\mathbb{C}}$ are well-defined. Then we must have

$$\frac{\omega^2 \beta_{1k} - c' \alpha_{1k}}{-\alpha_{1k} + c' \beta_{1k}} = -\frac{c\alpha_{3k} + \alpha_{2k}}{c\beta_{3k} + \beta_{2k}} \qquad \forall k \in [r].$$

If $c \neq \infty$, for every k this gives a non-trivial rational equation for α_{2k} in terms of other variables α_{ik}, β_{ik} and c, c'. If $c = \infty$, for every k we get a nontrivial rational equation for α_{3k} in terms of other variables and c'. In any case, for $r \geq 3$ the set of matrices $(A_1, A_2) \in \mathbb{K}^{2r^2}$ that satisfy Eq. (14) is small in $\mathbb{K}^{2r^2}$. ◀

▶ **Lemma 89.** *Let $r \geq 3$. Let $j_1 \notin \{1, 2\}$ be an element of $[r]$. Let $E_1, E_2 \subseteq \mathbb{K}$ be unbounded sets. For $v_1, v_2, w_1, w_2 \in \mathbb{K}^r$, $A_1 \in \mathbb{K}^{r \times r}$, an invertible matrix $A_2 \in \mathbb{K}^{r \times r}$, $x_1, x_2 \in \mathbb{K}$, $z_1, z_2 \in \mathbb{C}$ and a diagonal matrix $Z \in \mathbb{C}^{r \times r}$ consider*

$$T(x_1, x_2, Z, z_1, z_2) = \begin{pmatrix} A_1 + Z & v_1 & v_2 + x_2 e_1 \\ A_2 & w_1 + z_1 e_1 + x_1 e_{j_1} & w_2 + z_2 e_2 \end{pmatrix}.$$

The set of matrices $(A_1, A_2) \in \mathbb{K}^{2r^2}$, for which there exist $v_1, v_2, w_1, w_2 \in \mathbb{K}^r$, s.t. for all $x_1 \in E_1$ and $x_2 \in E_2$ there exist $Z \in \operatorname{Diag}(\mathbb{C}^{r \times r})$, $z_1, z_2 \in \mathbb{C}$ s.t. $\operatorname{rank}(T(x_1, x_2, Z, z_1, z_2)) \leq r$, is small in $\mathbb{K}^{2r^2}$.

Proof. Similarly, as in Lemma 45, Eq. (11) holds for $i = 1$. For the second column we get

$$(A_1 + Z)A_2^{-1}(w_2 + z_2 e_2) = v_2 + x_2 e_1.$$

Denote $\gamma_i = v_i - A_1 A_2^{-1} w_i$, $\alpha_i = A_1 A_2^{-1} e_i$, $\beta_i = A_2^{-1} e_i$ and $\phi_i = A_2^{-1} w_i$, then

$$Z_{kk} = \frac{\gamma_{2k} - x_2 \mathbf{1}[k = 1] - z_2 \alpha_{2k}}{\phi_{2k} + z_2 \beta_{2k}}.$$

Combining this with Eq. (11) for $i = 1$, we get

$$\frac{\gamma_{1k} - z_1\alpha_{1k} - x_1\alpha_{j_1k}}{\phi_{1k} + z_1\beta_{1k} + x_1\beta_{j_1k}} = \frac{\gamma_{2k} - x_2\mathbf{1}[k=1] - z_2\alpha_{2k}}{\phi_{2k} + z_2\beta_{2k}}.$$

Similarly, as in Lemma 45, by fixing $x_2 \in E_2$ and passing to the subsequence for $x_1 \in E_1$, we deduce that there exist $c(x_2) \in \widehat{\mathbb{C}}$ and $z_2 = z_2(x_2) \in \widehat{\mathbb{C}}$ such that

$$\frac{\gamma_{2k} - x_2\mathbf{1}[k=1] - z_2\alpha_{2k}}{\phi_{2k} + z_2\beta_{2k}} = -\frac{\alpha_{1k}c(x_2) + \alpha_{j_1k}}{\beta_{1k}c(x_2) + \beta_{j_1k}} \qquad \forall k \in [r].$$

Again, as in Lemma 45, by passing to the subsequence for $x_2 \in E_2$ we may deduce that there exist c' and c'' in $\widehat{\mathbb{C}}$ such that

$$\frac{\mathbf{1}[k=1] + c'\alpha_{2k}}{c'\beta_{2k}} = \frac{\alpha_{1k}c'' + \alpha_{j_1k}}{\beta_{1k}c'' + \beta_{j_1k}} \qquad \forall k \in [r]. \tag{15}$$

If $c'' \neq 0$, then α_{1k} can be expressed through other variables α_{ik}, β_{ik} and c', c''. Since $j_1 \neq 2$, if $c'' = 0$, then α_{j_1k} can be expressed in terms of other variables α_{ik}, β_{ik} and c'. Thus, the set of matrices (A_1, A_2) that satisfy Eq. (15) is small in $\mathbb{K}^{2r^2}$. ◀

C Reduction to countable fields

In this section we outline the basic model theory that allows us to consider countable fields only for our main result.

▶ **Proposition 90.** *Let us fix positive integers n, r, s. Let $X = (x_{ij})$ be an $n \times n$ matrix of variables. Then there is a first-order formula $\varphi(x_{ij})$ in the language of fields that expresses, over any field $\mathbb{F}$, the statement that $R_{\mathbb{F}}(X, r) = s$.*

Proof. Rank is first-order expressible (look at a finite number of determinants). There is a finite number of s-tuples where the matrix can be changed. Combine these. ◀

Let us fix positive integers n, r, s, t. We wish to prove a statement of the following form:

$(**)$ If $\mathbb{K}$ is a field of characteristic zero and $\mathbb{L}/\mathbb{K}$ is a quadratic extension then there exists an $n \times n$ matrix A over $\mathbb{K}$ such that $R_{\mathbb{K}}(A, r) \geq s$ and $R_{\mathbb{L}}(A, r) \leq t$.

▶ **Proposition 91.** *If statement $(**)$ holds whenever $\mathbb{K}$ is countable then it always holds.*

Proof. Let $\mathbb{L} = \mathbb{K}[\omega]$ where $\omega^2 =: u \in \mathbb{K}$. Let us add a name for u as a constant to the signature of rings, so we talk about the model $(\mathbb{K}, u)$. By the downward Löwenheim–Skolem theorem, this model has a countable elementary submodel $(\mathbb{K}', u)$. Let now $\mathbb{L}' = \mathbb{K}'[\omega]$. So $\mathbb{L}'/\mathbb{K}'$ is a quadratic extension (because $u \in \mathbb{K}'$).

Let us now apply $(**)$ to this extension. Let A be a matrix over $\mathbb{K}'$ with the required properties: $R_{\mathbb{K}'}(A, r) \geq s$ and $R_{\mathbb{L}'}(A, r) \leq t$.

Now $R_{\mathbb{L}}(A, r) \leq t$ follows immediately because $\mathbb{L}' \subseteq \mathbb{L}$. On the other hand, in the light of Prop. 90, $R_{\mathbb{K}'}(A, r) = R_{\mathbb{K}}(A, r)$, because $\mathbb{K}'$ is an elementary submodel of $\mathbb{K}$. ◀

D A 5×5 matrix with different strict and absolute rigidity

In this appendix we provide a concrete example of a matrix that shows a difference between strict and absolute rigidity. Specifically, we exhibit a matrix $A \in \mathbb{Q}^{5\times 5}$ such that $R_{\mathbb{Q}}(A, 2) = 9$ and $R_{\mathbb{Q}[\sqrt{2}]}(A, 2) = 8$. Consider the 5×2 and 2×5 matrices

$$L = \begin{pmatrix} 1 & -\sqrt{2} \\ \sqrt{2} & -1 \\ 3-\sqrt{2} & 1 \\ 12-7\sqrt{2} & 1 \\ 10-7\sqrt{2} & 1+2\sqrt{2} \end{pmatrix} \quad \text{and} \quad R = \begin{pmatrix} 1 & 0 & 2+\sqrt{2} & 3+2\sqrt{2} & 1 \\ \sqrt{2} & 1 & 1+2\sqrt{2} & 2-3\sqrt{2} & 3+\sqrt{2} \end{pmatrix}.$$

The product LR has 8 irrational entries:

$$L \cdot R = \begin{pmatrix} -1 & -\sqrt{2} & -2 & 9 & -1-3\sqrt{2} \\ 0 & -1 & 1 & 2+6\sqrt{2} & -3 \\ 3 & 1 & 5+3\sqrt{2} & 7 & 6 \\ 12-6\sqrt{2} & 1 & 11 & 10 & 15-6\sqrt{2} \\ 14-6\sqrt{2} & 1+2\sqrt{2} & 15 & -8 & 17 \end{pmatrix}$$

The following matrix, $A \in \mathbb{Q}^{5\times 5}$, differs from LR in only these 8 entries.

$$A = \frac{1}{16} \begin{pmatrix} -16 & 34 & -32 & 144 & 67 \\ 0 & -16 & 16 & -89 & -48 \\ 48 & 16 & 43 & 112 & 96 \\ 137 & 16 & 176 & 160 & -92 \\ 39 & 73 & 240 & -128 & 272 \end{pmatrix} \tag{16}$$

In other words,

$$A - LR = \begin{pmatrix} 0 & * & 0 & 0 & * \\ 0 & 0 & 0 & * & 0 \\ 0 & 0 & * & 0 & 0 \\ * & 0 & 0 & 0 & * \\ * & * & 0 & 0 & 0 \end{pmatrix}, \tag{17}$$

where each $*$ hides some non-zero entry. We selected every entry of A at positions marked by $*$ independently uniformly at random from $\{-135/16, -134/16, \ldots, 135/16\}$.

Note that Eq. (17) immediately implies that $R_{\mathbb{Q}[\sqrt{2}]}(A, 2) \leq 8$.

We use exhaustive computer search to verify that $R_{\mathbb{Q}}(A, 2) > 8$. We consider all the $\binom{25}{8} = 1{,}081{,}575$ combinations of 8 cells among the 5×5 cells. Having fixed a set of 8 cells, we introduce variables for their entries, and use Matlab to verify that the system of $\binom{5}{3}^2 = 100$ polynomial equations, saying that the determinant of every 3×3 minor is zero, has no rational solutions. In fact, we obtain the following stronger result.

▶ **Proposition 92.** *If a 5×5 complex matrix B of rank ≤ 2 differs from A in at most 8 positions then B is either LR or its algebraic conjugate (replace every occurrence of $\sqrt{2}$ by $-\sqrt{2}$).*