USING ELIMINATION THEORY TO CONSTRUCT RIGID MATRICES

Abhinav Kumar, Satyanarayana V. Lokam,
Vijay M. Patankar, and Jayalal Sarma M.N.

September 23, 2012

Abstract. The rigidity of a matrix A for target rank r is the minimum number of entries of A that must be changed to ensure that the rank of the altered matrix is at most r. Since its introduction by Valiant (1977), rigidity and similar rank-robustness functions of matrices have found numerous applications in circuit complexity, communication complexity, and learning complexity. Almost all $n \times n$ matrices over an infinite field have a rigidity of $(n-r)^2$. It is a long-standing open question to construct infinite families of *explicit* matrices even with superlinear rigidity when $r = \Omega(n)$.

In this paper, we construct an infinite family of complex matrices with the largest possible, i.e., $(n-r)^2$, rigidity. The entries of an $n \times n$ matrix in this family are distinct primitive roots of unity of orders roughly $\exp(n^2 \log n)$. To the best of our knowledge, this is the first family of concrete (but not entirely explicit) matrices having maximal rigidity and a succinct algebraic description.

Our construction is based on elimination theory of polynomial ideals. In particular, we use results on the existence of polynomials in elimination ideals with effective degree upper bounds (effective Nullstellensatz). Using elementary algebraic geometry, we prove that the dimension of the affine variety of matrices of rigidity at most k is exactly $n^2-(n-r)^2+k$. Finally, we use elimination theory to examine whether the rigidity function is semicontinuous.

Keywords. Matrix Rigidity, Elimination Theory.

Subject classification. Lower Bounds, Arithmetic Circuits.

1. Introduction

Valiant (Valiant 1977) introduced the notion of matrix rigidity. The rigidity function $\mathrm{Rig}(A, r)$ of a matrix A for target rank r is defined to be the smallest number of entries of A that must be changed to ensure that the altered matrix has rank at most r. It is easy to see that for every $n \times n$ matrix A (over any field), $\mathrm{Rig}(A, r) \leqslant (n - r)^2$. Valiant also showed that, over an infinite field, almost all matrices have rigidity exactly $(n - r)^2$. It is a long-standing open question to construct infinite families of *explicit* matrices with superlinear rigidity for $r = \Omega(n)$. Here, by an explicit family, we mean that the $n \times n$ matrix in the family is computable by a deterministic Turing machine in time polynomial in n or by a Boolean circuit of size polynomial in n. Lower bounds on rigidity of explicit matrices are motivated by their numerous applications in complexity theory. In particular, Valiant showed that lower bounds of the form $\mathrm{Rig}(A, \epsilon n) = n^{1+\delta}$ (where ϵ and δ are some positive constants) imply that the linear transformation defined by A cannot be computed by arithmetic circuits of linear size and logarithmic depth consisting of gates that compute linear functions of their inputs. Since then, applications of lower bounds on rigidity and similar rank-robustness functions have been found in circuit complexity, communication complexity, and learning complexity (Forster (2002); Forster *et al.* (2001); Linial & Shraibman (2009); Lokam (2001); Paturi & Pudlák (2004); Razborov (1989)). For comprehensive surveys on this topic, see Cheraghchi (2005); Codenotti (2000); Lokam (2009). Over finite fields, the best known lower bound for explicit A was first proved by Friedman (Friedman (1993)) and is $\mathrm{Rig}(A, r) = \Omega(\frac{n^2}{r} \log \frac{n}{r})$ for parity check matrices of good error-correcting codes. Over infinite fields, the same lower bound was proved by Shokrollahi, Spielman, and Stemann (Spielman *et al.* (1997)) for Cauchy matrices, Discrete Fourier Transform matrices of prime order (see Lokam (2000)), and other families. Note that this type of lower bound reduces to the trivial $\mathrm{Rig}(A, r) = \Omega(n)$ when $r = \Omega(n)$. In Lokam (2006), lower bounds of the form $\mathrm{Rig}(A, \epsilon n) = \Omega(n^2)$ were proved when $A = (\sqrt{p_{jk}})$ or when $A = (\exp(2\pi \mathrm{i}/p_{jk}))$, where p_{jk} are the first n^2 primes. These matrices, however, are not explicit in the sense defined above.

In this paper, we construct an infinite family of complex matrices with the highest possible, i.e., $(n-r)^2$, rigidity. The entries of the $n \times n$ matrix in this family are primitive roots of unity of orders roughly $\exp(n^2 \log n)$. We show that the real parts of these matrices are also maximally rigid. Like the matrices in Lokam (2006), this family of matrices is not explicit in the sense of efficient computability described earlier. However, one of the motivations for studying rigidity comes from algebraic complexity. In the world of algebraic complexity, any element of the ground field (in our case $\mathbb{C}$) is considered a primitive or atomic object. In this sense, the matrices we construct are explicitly described algebraic entities. To the best of our knowledge, this is the first construction giving an infinite family of non-generic/concrete matrices with maximum rigidity. It is still unsatisfactory, though, that the roots of unity in our matrices have orders exponential in n. Earlier constructions in Lokam (2006) use roots of unity of orders $O(n^2)$ but the bounds on rigidity proved there are weaker: $n(n-cr)$ for some constant $c > 2$.

We pursue a general approach to studying rigidity based on elementary algebraic geometry and elimination theory. To set up the formalism of this approach, we begin by reproving Valiant's result that the set of matrices of rigidity less than $(n-r)^2$ is contained in[1] a proper Zariski closed set in $\mathbb{C}^{n \times n}$, i.e., such matrices are solutions of a finite system of polynomial equations. Hence a generic matrix has rigidity at least $(n-r)^2$. In fact, we prove a more general statement: the set of $n \times n$ matrices of rigidity at most k for target rank r has dimension (as an affine variety) exactly $n^2-(n-r)^2+k$. This sheds light on the geometric structure of rigid matrices. We believe that our argument in this context is clearer and cleaner than an earlier work in the projective setting by Landsberg *et al.* (2003). To look for specific matrices of high rigidity, we consider certain elimination ideals associated to matrices with rigidity at most k. A result in Dickenstein *et al.* (1991) using effective Null-

[1]We note that this set itself may not be Zariski closed, as was mistakenly claimed in some earlier results, e.g., Lokam (2001), Landsberg *et al.* (2003). The example in Section 5.1.1 shows that the set of matrices of rigidity less than $(n-r)^2$ is not Zariski closed.

stellensatz bounds (for instance, as in Brownawell (1987); Kollár (1988)) shows that an elimination ideal of a polynomial ideal must always contain a nonzero polynomial with an explicit degree upper bound (Theorem 3.13). We then use simple facts from algebraic number theory to prove that a matrix whose entries are primitive roots of unity of sufficiently high orders cannot satisfy any polynomial with such a degree upper bound. This gives us the claimed family of matrices of maximum rigidity.

Our primary objects of interest in this paper are the varieties of matrices with rigidity at most k. For a fixed k, we have a natural decomposition of this variety based on the patterns of changes. We prove that this natural decomposition is indeed a decomposition into *irreducible* components (Corollary 4.3). In fact, these components are defined by elimination ideals of determinantal ideals generated by all the $(r+1) \times (r+1)$ minors of an $n \times n$ matrix of indeterminates. Better effective upper bounds on the degree of a nonzero polynomial in the elimination ideal of determinantal ideals than those given by Theorem 3.13 would lead to similar improvements in the bound on the order of the primitive roots of unity we use to construct our rigid matrices. While determinantal ideals have been well-studied in mathematical literature, their elimination theory does not seem to have been as well-studied. The application to rigidity might be a natural motivation for further investigating the elimination ideals that arise in this situation.

We next consider the question: given a matrix A, is there a small neighborhood of A within which the rigidity function is nondecreasing, i.e. such that every matrix in this neighborhood has rigidity at least equal to that of A? This is related to the notion of *semicontinuity* of the rigidity function. We give a family of examples to show that the rigidity function is in general not semicontinuous. However, the *specific* matrices we produce with entries being roots of unity as above, by their very construction, have neighborhoods within which rigidity is nondecreasing.

The rest of the paper is organized as follows. In Section 2, we introduce some definitions and notations and recall a basic result from elimination theory. Much of the necessary background from basic algebraic geometry is reviewed in Appendix A. We intro-

duce our main approach in Section 3, reprove Valiant's theorem, and compute the dimension of the variety of matrices of rigidity at most k. We present our new construction of maximally rigid matrices in Section 3.3. Connection to the elimination ideals of determinantal ideals is established in Section 4. In Section 5, we study semicontinuity of the rigidity function through examples and counterexamples.

2. Preliminaries

2.1. Definitions and Notations. Let F be a field[2]. Then, by $M_n(F)$ we denote the algebra of $n \times n$ matrices over F. At times, when it is clear from the context, we will denote $M_n(F)$ by M_n. We use $M_{m\times n}(F)$ to denote the set of $m \times n$ matrices over F. For $X \in M_n(F)$, by X_{ij} we will denote the (i, j)-th entry of X. Given $X \in M_n(F)$, the support of X is defined as $\mathrm{Supp}(X) := \{(i, j) \mid X_{ij} \neq 0 \in F\}$. Given a non-negative integer k, we define

$$S(k) := \{X \in M_n(F) : |\mathrm{Supp}(X)| \leqslant k\}.$$

Thus, $S(k)$ is the set of matrices over F with at most k non-zero entries.

A *pattern* π is a subset of the positions of an $n \times n$ matrix. Then, we define:

$$S(\pi) := \{X \in M_n(F) : \ \mathrm{Supp}(X) \subseteq \pi\}.$$

Note that $S(k) = \bigcup_{|\pi|=k} S(\pi)$.

Definition 2.1. *The rigidity function* $\mathrm{Rig}(X, r)$ *is the minimum number of entries we need to change in the matrix* X *so that the rank becomes at most* r*:*

$$\mathrm{Rig}(X, r) := \min\{\mathrm{Supp}(T) \ : \ \mathrm{rank}(X + T) \leqslant r\}.$$

Sometimes, we will allow T *to be chosen in* $M_n(L)$ *for* L *an extension field of* F*. In this case we will denote the rigidity by* $\mathrm{Rig}(X, r, L)$*.*

[2]For the most part, we will use the field of complex numbers $\mathbb{C}$. However, many of our definitions make sense over an arbitrary field and the theorems we use from algebraic geometry hold over any algebraically closed field.

Let $\mathsf{RIG}(n, r, k)$ denote the set of $n \times n$ matrices X such that $\mathrm{Rig}(X, r) = k$. Similarly, we define $\mathsf{RIG}(n, r, \geqslant k)$ to be the set of matrices of rigidity at least k and $\mathsf{RIG}(n, r, \leqslant k)$ to be the set of matrices of rigidity at most k. For a pattern π of size k, let $\mathsf{RIG}(n, r, \pi)$ be the set of matrices X such that for some $T_\pi \in S(\pi)$ we have $\mathrm{rank}(X + T_\pi) \leqslant r$. Then we have

$$\mathsf{RIG}(n, r, \leqslant k) = \bigcup_{\pi, |\pi|=k} \mathsf{RIG}(n, r, \pi).$$

2.2. Elimination Theory and the Closure Theorem. We review much of the necessary background from algebraic geometry in Appendix A. Here we recall a basic result from Elimination Theory. As the name suggests, Elimination Theory deals with elimination of a subset of variables from a given set of polynomial equations and finding the *reduced set* of polynomial equations (not involving the eliminated variables). The main results of Elimination Theory, especially the Closure Theorem, describe a precise relation between the reduced ideal and the given ideal, and its corresponding geometric interpretation.

Given an ideal $I = \langle f_1, \ldots, f_s \rangle \subseteq F[x_1, \ldots, x_n]$, the l-th *elimination ideal* I_l is the ideal of $F[x_{l+1}, \ldots, x_n]$ defined by $I_l := I \cap F[x_{l+1}, \ldots, x_n]$. We refer to page 125, Theorem 3 of Cox *et al.* (2007) for the following theorem.

THEOREM 2.2 (Closure Theorem). *Let I be an ideal of the ring $F[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and $I_n := I \bigcap F[y_1, \ldots, y_m]$ be the n-th elimination ideal associated to I. Let $V(I)$ and $V(I_n)$ be the subvarieties of $\mathbb{A}^{n+m}$ and $\mathbb{A}^m$ (the affine spaces over $\overline{F}$ of dimension $n + m$ and m respectively) defined by I and I_n respectively. Let p be the natural projection map from $\mathbb{A}^{n+m} \to \mathbb{A}^m$ (projection map onto the y-coordinates). Then,*

(i) $V(I_n)$ is the smallest (closed) affine variety containing the set $p(V(I)) \subseteq \mathbb{A}^m$. In other words, $V(I_n)$ is the Zariski closure of $p(V(I)(\overline{F})) \subseteq \overline{F}^m$.

(ii) When $V(I)(\overline{F}) \neq \phi$, there is an affine variety W strictly contained in $V(I_n)$ such that $V(I_n) - W \subseteq p(V(I))$.

3. Use of Elimination Theory

3.1. Determinantal Ideals and their Elimination Ideals. We would like to investigate the structure of the sets $\mathsf{RIG}(n, r, \leqslant k, \overline{F})$ and $\mathsf{RIG}(n, r, \pi, \overline{F})$ and their Zariski closures

$$\begin{aligned} \mathcal{W}(n, r, \leqslant k) &:= \overline{\mathsf{RIG}(n, r, \leqslant k, \overline{F})} \quad \text{and} \\ \mathcal{W}(n, r, \pi) &:= \overline{\mathsf{RIG}(n, r, \pi, \overline{F})} \end{aligned}$$

in the n^2-dimensional affine space of $n \times n$ matrices. Note that we have the "upper bound" $\mathsf{RIG}(n, r, \leqslant k) \subset \mathsf{RIG}(n, r, \leqslant k, \overline{F})$ and therefore $\overline{\mathsf{RIG}(n, r, \leqslant k)} \subset \mathcal{W}(n, r, \leqslant k)$. Let X be an $n \times n$ matrix with entries being indeterminates $x_1, \ldots, x_{n^2}$. For a pattern π of k positions, let T_π be the $n \times n$ matrix with indeterminates $t_1, \ldots, t_k$ in the positions given by π. Note that saying $X + T_\pi$ has rank at most r is equivalent to saying that all its $(r+1) \times (r+1)$ minors vanish. Let us consider the ideal generated by these minors:

$$I(n, r, \pi) := \left\langle \text{Minors}_{(r+1)\times(r+1)}(X + T_\pi) \right\rangle, \tag{3.1}$$

where $\left\langle \text{Minors}_{(r+1)\times(r+1)}(X + T_\pi) \right\rangle \subseteq F[x_1, \ldots, x_{n^2}, t_1, \ldots, t_k]$. It then follows from the definition of rigidity that $\mathsf{RIG}(n, r, \pi, \overline{F})$ is the projection from $\mathbb{A}^{n^2} \times \mathbb{A}^k$ to $\mathbb{A}^{n^2}$ of the set $V(I(n, r, \pi))(\overline{F})$. Thus, if we define the elimination ideal

$$EI(n, r, \pi) := I(n, r, \pi) \cap F[x_1, \ldots, x_{n^2}] \subseteq F[x_1, \ldots, x_{n^2}],$$

then by the Closure Theorem (Theorem 2.2), we obtain

$$\mathcal{W}(n, r, \pi) = V(EI(n, r, \pi)). \tag{3.2}$$

Note that

$$\mathcal{W}(n, r, \leqslant k) = \bigcup_{\pi, |\pi| = k} \mathcal{W}(n, r, \pi).$$

3.2. Valiant's Theorem. The following theorem due to Valiant (Valiant 1977, Theorem 6.4, page 172) says that a generic matrix has rigidity $(n - r)^2$. That is, for $k < (n - r)^2$, the dimension of $\mathcal{W}(n, r, \leqslant k)$ is strictly less than n^2.

A reader familiar with Valiant's proof will realize that our proof is basically a rephrasing of Valiant's proof in the language of algebraic geometry. The point of this proof is to set up the formalism and use it later; in particular, when we compute the exact dimension of the rigidity variety $\mathcal{W}(n, r, \leqslant k)$.

THEOREM 3.3 (Valiant 1977). *Let $n \geqslant 1, 0 < r < n$ and $0 \leqslant k < (n-r)^2$. Let $\mathcal{W} := \mathcal{W}(n, r, \leqslant k)$ be as above. Then,*

$$\dim(\mathcal{W}) < n^2.$$

PROOF. Let $\pi \subseteq \{(i,j) \mid 1 \leqslant i, j \leqslant n\}$ be a pattern of size k. For a choice of $0 \leqslant s \leqslant r$, we let τ denote a choice of s rows and s columns, and for a matrix B, let B_τ be the corresponding submatrix of B, whose determinant is one of the $s \times s$ minors of B. For $s = 0$, we let B_τ be the empty matrix, with determinant defined to be 1.

For $s \leqslant r$, define $\mathsf{RIG}(n, s, \pi, \tau)$ to be the set of all $n \times n$ matrices A that satisfy the following properties: there exists some $n \times n$ matrix T_π such that

1. $\mathrm{Supp}(T_\pi) \subseteq \pi$,
2. $\mathrm{rank}(A + T_\pi) = s$, and
3. $\det((A + T_\pi)_\tau) \neq 0$ where τ denotes the fixed $s \times s$ minor as above.

Recall that $S(\pi)$ is the set of matrices whose support is contained in π. Let us also define

$$\mathsf{RANK}(n, s, \tau) := \{C \in M_n \mid \mathrm{rank}(C) = s \text{ and } \det(C_\tau) \neq 0\}.$$

By definition, every element $A \in \mathsf{RIG}(n, s, \pi, \tau)$ can be written as $C - T_\pi$, with $C \in \mathsf{RANK}(n, s, \tau)$ and $T_\pi \in S(\pi)$.

We first prove the following lemma:

LEMMA 3.4. $\dim(\mathsf{RANK}(n, s, \tau)) = n^2 - (n-s)^2$.

PROOF. Without loss of generality we can assume that τ is the upper left $s \times s$-minor. Thus we can write a $C \in \mathsf{RANK}(n, s, \tau)$ as

$$C = \begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix},$$

where $\operatorname{rank}(C) = s$ and C_{11} is an $s \times s$ matrix whose determinant is non-zero.

Since the matrix C_{11} is nonsingular of dimension equal to $s = \operatorname{rank}(C)$, it follows that the first s columns are linearly independent and span the column space of C. Therefore each of the last $(n-s)$ columns is a linear combination of the first s columns in exactly one way, and the linear combination is determined by the entries of C_{12}. Formally, we have the equation

$$C_{22} = C_{21} C_{11}^{-1} C_{12}.$$

The set of all C_{11} is an affine open set of dimension s^2 and C_{12} and C_{21} can each range over $\mathbb{A}^{s(n-s)}$. Hence, the algebraic set $\mathsf{RANK}(n, s, \tau)$ has dimension exactly $s^2 + 2r(n-s) = n^2 - (n-s)^2$. □

Consider the following natural map Φ:

$$\mathbb{A}^{n^2-(n-s)^2} \times \mathbb{A}^k \supset \mathsf{RANK}(n, s, \tau) \times S(\pi) \xrightarrow{\Phi} M_n \cong \mathbb{A}^{n^2}, \tag{3.5}$$

taking (X, T_π) to $X + T_\pi$. The image of Φ is exactly $\mathsf{RIG}(n, r, \pi, \tau)$ as defined at the beginning of this proof.

Also, note that $\dim(S(\pi)) = |\pi|$. We note that if there is a surjective morphism from an affine variety X to another affine variety Y, then $\dim Y \leqslant \dim X$ (a more formal statement appears as Lemma A.5 in Appendix A). Thus for $k \leqslant (n-s)^2 - 1$, we get

$$\dim(\overline{\operatorname{Im}(\Phi)}) = \dim(\overline{\mathsf{RIG}(n, s, \pi, \tau)}) \leqslant n^2 - (n-s)^2 + k < n^2. \tag{3.6}$$

Note that

$$\mathcal{W} = \bigcup_{s \leqslant r, \tau, \pi} \overline{\mathsf{RIG}(n, s, \pi, \tau)} \tag{3.7}$$

and that completes the proof of the theorem. □

Thus we have proved that the set of matrices of rigidity strictly smaller than $(n-r)^2$ is contained in a proper closed affine variety of $\mathbb{A}^{n^2}$, and thus is of dimension strictly less than n^2. In other words, a *generic matrix*, i.e. a matrix that lies outside a certain proper closed affine subvariety of $\mathbb{A}^{n^2}$, is *maximally rigid* (even if we allow changes by elements of $\overline{F}$, rather than just F). Therefore, over an infinite field F (for instance, an algebraically closed field), there always exist maximally rigid matrices.

We now refine Valiant's argument and prove the following exact bound on the dimension of $\mathcal{W}$. The main point of the proof is a *lower bound* on $\dim(\mathcal{W})$.

THEOREM 3.8. *Let $0 \leqslant r \leqslant n$ and $0 \leqslant k \leqslant (n-r)^2$. Then*

$$\dim(\mathcal{W}) = n^2 - (n-r)^2 + k.$$

PROOF. By the above proof of Theorem 3.3 (see Equation (3.6)), we only need to prove that the $\dim(\mathcal{W})$ is at least $n^2-(n-r)^2+k$. By Equation (3.7) as above,

$$\dim(\mathcal{W}) = \max_{s \leqslant r, \pi, \tau} \dim(\overline{\mathsf{RIG}(n, s, \pi, \tau)}).$$

Thus, to prove the theorem it is sufficient to prove that for some $r \leqslant s$, and some π and τ:

$$\dim(\mathsf{RIG}(n, s, \pi, \tau)) \geqslant n^2 - (n-r)^2 + k.$$

We take $s = r$ and choose π and τ as follows. Fix a pattern π of size k such that it is a subset of $\{(i,j) \mid r+1 \leqslant i, j \leqslant n\}$. This is possible because $k \leqslant (n-r)^2$. Let τ be the top left $r \times r$ minor. We now define:

(3.9)
$$U := \left\{ \begin{bmatrix} G & A \\ B & X_\pi + BG^{-1}A \end{bmatrix} \;:\; \begin{matrix} A \in M_{r\times(n-r)}, G \in GL_r \\ B \in M_{(n-r)\times r},\ X_\pi \in S(\pi) \end{matrix} \right\}.$$

As an affine algebraic variety, U is isomorphic to $GL(r) \times \mathbb{A}^{n\times(n-r)} \times \mathbb{A}^{(n-r)\times r} \times \mathbb{A}^k$, and thus $\dim(U) = r^2 + 2(n-r)r + k = n^2 - (n-r)^2 + k$. If we subtract the matrix

$$\begin{bmatrix} 0 & 0 \\ 0 & X_\pi \end{bmatrix}$$

from the matrix above, we get a matrix

$$\begin{bmatrix} G & A \\ B & BG^{-1}A \end{bmatrix}$$

of rank exactly r since the the first r columns are linearly independent (G being invertible) and the last $n-r$ columns are a linear combination of the first r, obtained by multiplying on the right by the matrix $G^{-1}A$. Therefore, $U \subseteq \mathsf{RIG}(n, r, \pi, \tau)$, and hence $\dim(\mathsf{RIG}(n, r, \pi, \tau)) \geqslant n^2 - (n-r)^2 + k$. □

Remark 3.10. A similar argument or line of study - though in the projective setting - is also found in Landsberg *et al.* (2003). Our formalism and proofs seem clearer and simpler. Our theorem is also very explicit.

3.3. Rigid Matrices over the field of Complex Numbers. Recall that to say that the rigidity of a matrix A for target rank r is at least k, it suffices to prove that the matrix A is not in $\mathcal{W}(n, r, \leqslant (k-1))$. We use this idea to achieve the maximum possible lower bound for the rigidity of a family of matrices over the field of complex numbers $\mathbb{C}$. As a matter of fact, we obtain matrices with real algebraic entries with rigidity $(n-r)^2$.

Theorem 3.11. *Let $\Delta(n) = n^{4n^2}$ and let $p_{i,j} > \Delta(n)$ be distinct primes for $1 \leqslant i, j \leqslant n$. Let $K = \mathbb{Q}(\zeta_{1,1}, \ldots, \zeta_{n,n})$ where $\zeta_{i,j} = e^{2\pi \mathrm{i}/p_{i,j}}$. Let $A(n) := [\zeta_{i,j}] \in M(n, K)$. Then, for any field L containing K,*

$$\mathrm{Rig}(A(n), r, L) = (n-r)^2.$$

Proof. For simplicity, we will index the $\zeta_{i,j}$ by ζ_α for $\alpha = 1$ to n^2, and similarly p_α. First, note that we may assume $1 \leqslant r \leqslant n-1$ since for $r = n$ the statement of the theorem is a tautology, and for $r = 0$, it is obvious. We prove the theorem by showing that

$$A(n) \notin \mathcal{W}(n, r, \leqslant (n-r)^2 - 1)(L).$$

Thus it is sufficient to prove that

$$A(n) \notin \mathcal{W}(n, r, \pi)(L)$$

for any pattern π with $|\pi| = k := (n-r)^2 - 1$. Let π be any such pattern. To simplify notation, let us define $\mathcal{W} := \mathcal{W}(n, r, \pi)(L)$. By Theorem 3.3 we have:

$$\dim(\mathcal{W}) \leqslant \dim(\mathcal{W}(n, r, \leqslant (n-r)^2 - 1)) < n^2.$$

Equivalently (by Hilbert's Nullstellensatz),

$$EI(n, r, \pi) \neq (0).$$

Proving that $A(n) \notin \mathcal{W}$ is equivalent to showing the existence of a $g \in EI(n, r, \pi)$ such that $g(A(n)) \neq 0$. The key to the proof of the theorem is to produce a polynomial g of sufficiently low degree.

Claim 3.12. *There is a polynomial $g \in EI(n, r, \pi)$ of total degree less than $\Delta(n)$.*

To prove the claim, we use the following theorem - see Proposition 1.7 and Remark 1.8 of Dickenstein *et al.* (1991):

Theorem 3.13 (Dickenstein *et al.* 1991). *Let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal in the polynomial ring $F[Y]$ over an infinite field F, where $Y = \{y_1, \ldots, y_m\}$. Let $d_{\max}$ be the maximum* total degree *of a generator f_i. Let $Z = \{y_{i_1}, \ldots, y_{i_\ell}\} \subseteq Y$ be a subset of indeterminates of Y. If $I \cap F[Z] \neq (0)$ then there exists a non-zero polynomial $g \in I \cap F[Z]$ such that, $g = \sum_{i=1}^{s} g_i f_i$, with $g_i \in F[Y]$ and $\deg(g_i f_i) \leqslant d^m(d^m + 1)$, where $d = \max(d_{\max}, 3)$.*

Remark 3.14. Note that the proof of Theorem 3.13 relies on a slightly different notion of the degree of a variety than the usual definition in projective algebraic geometry. This definition was used in Heintz (1983) to prove the *Bézout inequality*. For an explanation of how the first sentence of Remark 1.8 of Dickenstein *et al.* (1991) follows from this inequality, we refer the reader to Proposition 2.3 of Heintz & Schnorr (1980).

Let us apply Theorem 3.13 to our case - in the notation of this theorem, $F := \mathbb{Q}$, $Y := \{x_1, \ldots, x_{n^2}, t_1, \ldots, t_k\}$, $Z := \{x_1, \ldots, x_{n^2}\}$, Σ_{r+1} := set of all minors of size $(r+1)$, $f_\tau := \det((X + T_\pi)_\tau)$

for $\tau \in \Sigma_{r+1}$, where by Y_τ we denote the τ-th minor of Y, and $I := I(n, r, \pi) = \langle f_\tau : \tau \in \Sigma_{r+1} \rangle$ as defined in (3.1). We may as well assume $n \geqslant 3$, since for $n = 2$ the claim is easy to verify by explicit calculation. Then we have:

$$\begin{aligned} m &= n^2 + (n-r)^2 - 1 \leqslant 2n^2 - 2, \\ d &= \max(r+1, 3) \leqslant n, \quad \text{and} \\ I \cap F[Z] &= EI(n, r, \pi) \neq (0). \end{aligned}$$

By Theorem 3.13 there exists a

$$g \neq 0 \in EI(n, r, \pi) \subseteq \mathbb{Q}[x_1, \ldots, x_{n^2}]$$

such that

$$\deg(g) \leqslant d^m(d^m + 1) \leqslant n^{2n^2-2}(n^{2n^2-2} + 1) < n^{4n^2} = \Delta(n).$$

We will now apply the following Lemma 3.15, which we prove later, to this situation.

LEMMA 3.15. *Let N be a positive integer. Let $\theta_1, \cdots, \theta_m$ be m algebraic numbers such that for any $1 \leqslant i \leqslant m$, the field $\mathbb{Q}(\theta_i)$ is Galois over $\mathbb{Q}$ and such that*

$$[\mathbb{Q}(\theta_i) : \mathbb{Q}] \geqslant N \quad \text{and} \quad \mathbb{Q}(\theta_i) \cap \mathbb{Q}(\theta_1, \ldots, \theta_{i-1}, \theta_{i+1}, \ldots, \theta_m) = \mathbb{Q}.$$

Let $g(\underline{x}) \neq 0 \in \mathbb{Q}[x_1, \ldots, x_m]$ such that $\deg(g) < N$. Then, $g(\theta_1, \ldots, \theta_m) \neq 0$. □

Let us set $m = n^2, N = \Delta(n), l := \deg(g) \leqslant N$ in Lemma 3.15. It is now easy to check that

$$[\mathbb{Q}(\zeta_\alpha) : \mathbb{Q}] = p_\alpha - 1 \geqslant \Delta(n) = N$$

and

$$\mathbb{Q}(\zeta_\alpha) \cap \mathbb{Q}(\zeta_1, \ldots, \zeta_{\alpha-1}, \zeta_{\alpha+1}, \ldots, \zeta_{n^2}) = \mathbb{Q}.$$

The latter follows from the fact that the prime p_α is totally ramified in $\mathbb{Q}(\zeta_\alpha)$ and is unramified in $\mathbb{Q}(\zeta_1, \ldots, \zeta_{\alpha-1}, \zeta_{\alpha+1}, \ldots, \zeta_{n^2})$; see Theorem 4.10 in Narkiewicz (2004). Thus Lemma 3.15 is applicable and we get:

$$g(\zeta_1, \ldots, \zeta_{n^2}) \neq 0.$$

To complete the argument (for Theorem 3.11), now we prove Lemma 3.15.

Proof of Lemma 3.15: By induction on m. For $m = 1$ this is trivial. Now suppose that the statement is true when the number of variables is strictly less than m. Assuming that the statement is not true for m, we will arrive at a contradiction. This will prove the lemma.

Let $g \in \mathbb{Q}[\underline{x}]$ with $l := \deg(g) < N$ be such that

$$g(\theta_1, \ldots, \theta_m) = 0,$$

with θ_i, $1 \leqslant i \leqslant m$, satisfying the conditions as in the theorem. Since the statement is true for $(m-1)$ variables by the inductive hypothesis, without loss of generality, we can assume that all the variables and hence x_m appears in g. Let us denote x_m by x. Let us write

$$g(x_1, \ldots, x_m) = \sum_{i=0}^{l} f_i(x_1, \ldots, x_{m-1}) x^{l-i}.$$

Note that $l < N$ and $\deg(f_i) < N$ for $0 \leqslant i \leqslant l$. Since $g \neq 0$, for some i, $0 \leqslant i \leqslant l$ the polynomial $f_i \neq 0$. Thus, by the inductive hypothesis,

$$f_i(\theta_1, \ldots, \theta_{m-1}) \neq 0.$$

Thus $g(\theta_1, \ldots, \theta_{m-1})(x) \neq 0 \in \mathbb{Q}(\theta_1, \ldots, \theta_{m-1})[x]$. This implies that θ_m satisfies a non-zero polynomial over $\mathbb{Q}(\theta_1, \ldots, \theta_{m-1})$ of degree $\leqslant l < N$. Thus:

$$[\mathbb{Q}(\theta_1, \ldots, \theta_m) : \mathbb{Q}(\theta_1, \ldots, \theta_{m-1})] \leqslant l < N. \tag{3.16}$$

On the other hand, since $\mathbb{Q}(\theta_m) \cap \mathbb{Q}(\theta_1, \ldots, \theta_{m-1}) = \mathbb{Q}$ and the fields $\mathbb{Q}(\theta_i)$ are Galois over $\mathbb{Q}$, by Theorem 3.17 (stated below), we conclude that

$$[\mathbb{Q}(\theta_1, \ldots, \theta_{m-1})(\theta_m) : \mathbb{Q}(\theta_1, \ldots, \theta_{m-1})] = [\mathbb{Q}(\theta_m) : \mathbb{Q}] \geqslant N.$$

This contradicts (3.16) above and proves the lemma.

THEOREM 3.17 (Lang 2004, Theorem 1.12, page 266). *Let K be a Galois extension of k, let F be an arbitrary extension of k, and assume that K, F are subfields of some other field. Then KF (the compositum of K and F) is Galois over F, and K is Galois over $K \bigcap F$. Let H be the Galois group of KF over F, and G the Galois group of K over k. If $\sigma \in H$ then the restriction of σ to K is in G, and the map $\sigma \mapsto \sigma|_K$ gives an isomorphism of H on the Galois group of K over $K \cap F$. In particular, $[KF : F] = [K : K \cap F]$.*

This concludes the proof of Theorem 3.11. □

Note that Theorem 3.11 is true for any family of matrices $A(n) = [\theta_{i,j}]$ provided the $\theta_{i,j}$ satisfy Lemma 3.15. Hence, we have:

COROLLARY 3.18. *Let $A(n) := [\zeta_{i,j} + \overline{\zeta_{i,j}}]$, where $\zeta_{i,j}$ are primitive roots of unity of order $p_{i,j}$ such that $p_{i,j} - 1 \geqslant 2\Delta(n)$ (here $\overline{\zeta_{i,j}}$ denotes the complex conjugate of $\zeta_{i,j}$). Then, $A(n) \in M(n, \mathbb{R})$ has* $\mathrm{Rig}(A(n), r) = (n - r)^2$.

PROOF. We apply the remark above with $\theta_{i,j} = \zeta_{i,j} + \overline{\zeta_{i,j}}$, which generates the maximal real subfield of $\mathbb{Q}(\zeta_{i,j})$. These fields are Galois over $\mathbb{Q}$, and since $\mathbb{Q}(\theta_{i,j}) \subset \mathbb{Q}(\zeta_{i,j})$, they satisfy the linear disjointness property which forms the second part of the assumption of Lemma 10. □

4. Reduction to Determinantal Ideals

In this section, we show that the natural decomposition of the rigidity varieties $\mathcal{W}(n, r, \leqslant k) = \bigcup_{|\pi|=k} \mathcal{W}(n, r, \pi)$ is indeed a decomposition into *irreducible* affine algebraic varieties. In fact, these components turn out to be varieties defined by elimination ideals of determinantal ideals generated by all the $(r+1) \times (r+1)$ minors.

To improve the bounds on the orders of primitive roots of unity in Theorem 3.11, it suffices to improve the degree bounds given by Theorem 3.13 for the special case when I is a determinantal ideal. However, we do not know of such an improvement even for the special case when I is the determinantal ideal of a generic Vandermonde matrix.

To show the decomposition, we will continue to use the notation from Section 3. Consider the matrix $X + T_\pi$. Let $x = \{x_1, \ldots, x_{n^2}\} = x_{\bar{\pi}} \cup x_\pi$, where x_π is the set of variables that are indexed by π and $x_{\bar{\pi}}$ is the set of remaining variables.

Let

$$J := I(n, r, \pi) = \left\langle \text{Minors}_{(r+1)\times(r+1)}(X + T_\pi) \right\rangle$$

be the ideal of $\mathbb{Q}[x, t] = \mathbb{Q}[x_\pi, x_{\bar{\pi}}, t_\pi]$ generated by the $(r+1) \times (r+1)$ minors of $X + T_\pi$. Let

$$\begin{aligned} J_1 &:= J \cap \mathbb{Q}[x_\pi, x_{\bar{\pi}}] \subseteq \mathbb{Q}[x_1, \ldots, x_{n^2}], \\ J_2 &:= J_1 \cap \mathbb{Q}[x_{\bar{\pi}}], \\ I_{r+1} &:= \left\langle \text{Minors}_{(r+1)\times(r+1)}(X) \right\rangle \subseteq \mathbb{Q}[x], \quad \text{and} \\ EI_{r+1} &:= I_{r+1} \cap \mathbb{Q}[x_{\bar{\pi}}] \subseteq \mathbb{Q}[x_{\bar{\pi}}]. \end{aligned}$$

Notice that since J_1 is the elimination ideal of J w.r.t. eliminating variables t_π, a matrix A lies in $\mathcal{W}(n, r, \pi) = \overline{\mathsf{RIG}(n, r, \pi, \overline{F})}$ if and only if its entries lie in the variety defined by the ideal J_1. Therefore, J_1 equals the elimination ideal $EI(n, r, \pi)$ defined in Section 3.1, by definition. Also, I_{r+1} is the ideal generated by the $(r+1) \times (r+1)$ minors of X and EI_{r+1} its elimination ideal for the polynomial ring over the rationals generated by the variables $x_{\bar{\pi}}$.

PROPOSITION 4.1. *$J_1 = J_2\mathbb{Q}[x]$ (the ideal generated by J_2 in $\mathbb{Q}[x]$) and $J_2 = EI_{r+1}$. In particular, $EI(n, r, \pi) = EI_{r+1}\mathbb{Q}[x]$ considered as ideals in $\mathbb{Q}[x]$.*

PROOF. First, notice that in the $(r+1)\times(r+1)$ minors of $X+T_\pi$, the variable $t_{i,j}$, for $(i, j) \in \pi$, always occurs in combination with $x_{i,j}$ as $t_{i,j} + x_{i,j}$. Therefore, eliminating the variables t_π will also automatically eliminate the variables x_π, giving the equality of the generators of the ideals J_1 and J_2. Therefore $J_1 = J_2\mathbb{Q}[x]$. More formally, consider the automorphism ϕ of $\mathbb{Q}[x_\pi, x_{\bar{\pi}}, t_\pi]$ defined by letting $\phi(t_{i,j}) = x_{i,j} + t_{i,j}$ for each $(i, j) \in \pi$ and $\phi(x_{i,j}) = x_{i,j}$ for all (i, j). The ideal $J_1 = J \cap \mathbb{Q}[x_\pi, x_{\bar{\pi}}] \subseteq \mathbb{Q}[x_1, \ldots, x_{n^2}]$ must equal the ideal $\phi(\phi^{-1}(J) \cap \phi^{-1}\mathbb{Q}[x_1, \ldots, x_{n^2}])$, since ϕ is an isomorphism. But $\phi^{-1}(J)$ is generated by determinants of matrices only involving the

variables t_π and $x_{\bar{\pi}}$, whereas $\phi^{-1}\mathbb{Q}[x_1, \ldots, x_{n^2}]) = \mathbb{Q}[x_1, \ldots, x_{n^2}]$, so that $\phi^{-1}(J) \cap \phi^{-1}\mathbb{Q}[x_1, \ldots, x_{n^2}]$ is generated by polynomials only involving the variables of $x_{\bar{\pi}}$. Therefore,

$$\phi^{-1}(J_1) = \phi^{-1}(J) \cap \phi^{-1}\mathbb{Q}[x_1, \ldots, x_{n^2}] = J_2\mathbb{Q}[x].$$

Taking the image under ϕ, we get $J_1 = J_2\mathbb{Q}[x]$.

The equation $J_2 = EI_{r+1}$ follows from similar considerations, noting that the variables $x_{i,j}$ for $(i,j) \in \pi$ always occur in the combination $x_{i,j} + t_{i,j}$ in the minors which generate J. Therefore eliminating them eliminates $t_{i,j}$ as well. More formally, consider the isomorphism $\psi : \mathbb{Q}[x_\pi, x_{\bar{\pi}}, t_\pi] \to \mathbb{Q}[x_\pi, x_{\bar{\pi}}, t_\pi]$ defined by letting $\psi(x_{i,j}) = x_{i,j} + t_{i,j}$ for each $(i,j) \in \pi$, while $\psi(t_{i,j}) = t_{i,j}$ for $(i,j) \in \pi$ and $\psi(x_{i,j}) = x_{i,j}$ for $(i,j) \notin \pi$. Then again we have :

$$\begin{aligned} J_2 = J_1 \cap \mathbb{Q}[x_{\bar{\pi}}] = J \cap \mathbb{Q}[x_{\bar{\pi}}] &= \psi(\psi^{-1}(J) \cap \psi^{-1}(\mathbb{Q}[x_{\bar{\pi}}])) \\ &= \phi(I_{r+1}\mathbb{Q}[x, t_\pi] \cap \mathbb{Q}[x_{\bar{\pi}}]) \\ &= \phi(EI_{r+1}) = EI_{r+1} \subset \mathbb{Q}[x_{\bar{\pi}}]. \end{aligned}$$

□

The following is a well-known theorem; see (Hochster & Eagon 1971, Theorem 1) and (Bruns & Vetter 1980, Chapter 2).

THEOREM 4.2. *Let* $\mathsf{RANK}(n, \leqslant r)$ *be the set of all rank* $\leqslant r$ *matrices of* $M_n \cong \mathbb{A}^{n^2}$. *Then*

(i) $I(\mathsf{RANK}(n, \leqslant r)) = I_{r+1}$ *and* $\mathsf{RANK}(n, \leqslant r) = V(I_{r+1})$.

(ii) I_{r+1} *is a prime ideal of* $\mathbb{Q}[X]$. *In particular,* $\mathsf{RANK}(n, \leqslant r)$ *is an irreducible variety.*

COROLLARY 4.3. *In the natural decomposition* $\mathcal{W}(n, r, \leqslant k) = \bigcup_{|\pi|=k} \mathcal{W}(n, r, \pi)$, *the* $\mathcal{W}(n, r, \pi)$ *are irreducible varieties.*

PROOF. In general if J is a prime ideal of a commutative ring S and if R is a subring of S, then $I = J \cap R$ is prime ideal of R. Using this, it follows that the elimination ideal $EI_{r+1} \subseteq \mathbb{Q}[x_{\bar{\pi}}]$ is a prime ideal since $I_{r+1} \subseteq \mathbb{Q}[x]$ is a prime ideal by Theorem 4.2.

By Lemma 4.1, $EI(n, r, \pi) = EI_{r+1}\mathbb{Q}[x]$ considered as ideals in $\mathbb{Q}[x]$. We need to prove that $EI(n, r, \pi)$ is a prime ideal in $\mathbb{Q}[x]$. To prove this we use the following general fact: if $S = R[y]$ where y is transcendental over an integral domain R then, IS, the ideal generated by I in S, is a prime ideal of S. To see this, note that $S/IS \cong (R/I)[y]$. Now, R/I is an integral domain (this is equivalent to I being prime), therefore so is $(R/I)[y]$. Therefore IS is a prime ideal. Now let $R = \mathbb{Q}[x_{\bar{\pi}}]$ and $S = \mathbb{Q}[x] = R[x_\pi]$. Let $I = EI_{r+1}$ which is a prime ideal of R. Then, $IS = EI_{r+1}\mathbb{Q}[x] = EI(n, r, \pi)$ (Lemma 4.1) and further more, from the general comments as above, it follows that the latter is a prime ideal in $\mathbb{Q}[x]$. Thus, $W(n, r, \pi) = V(EI(n, r, \pi)) = V(EI_{r+1})$ (by (3.2)) is an irreducible subvariety of $\mathbb{A}^{n^2}$. □

Finally, we end with the observation that Proposition 4.1 gives us a slight improvement on Theorem 3.11.

THEOREM 4.4. *Let $\Delta(n) = 2n^{2n^2}$. Let $p_{i,j}$ for $1 \leqslant i,\ j \leqslant n$ be distinct primes such that $p_{i,j} > \Delta(n)$. Let $K = \mathbb{Q}(\zeta_{1,1}, \ldots, \zeta_{n,n})$ where $\zeta_{i,j} = e^{2\pi \mathrm{i}/p_{i,j}}$. Let $A(n) := [\zeta_{i,j}] \in M(n, K)$. Then, for any field L containing K,*

$$\mathrm{Rig}(A(n), r, L) = (n - r)^2.$$

PROOF. The only change is the improvement on $\Delta(n)$, which follows from Theorem 3.13 as before, using the fact that $EI(n, r, \pi) = EI_{r+1}\mathbb{Q}[x]$ by Proposition 4.1 above. Since now there are only $m = n^2$ variables in all, we easily get the bound $\deg(g) \leqslant n^{n^2}(n^{n^2} + 1) < \Delta(n)$. (As before, we have assumed $n \geqslant 3$.) □

5. Topology of Rigidity with some Examples

In this section, we make some observations about the topological behavior of the rigidity function in $M_n(\mathbb{C})$. The main motivation is to examine if all matrices within a small neighborhood of a matrix A are at least as rigid as A. For instance, the matrices $A(n)$ from Theorem 3.11 have an open neighborhood around them within which the rigidity function is constant. This is a direct consequence of their very construction since they are outside the

closed sets $\mathcal{W}(n, r, \leqslant (n-r)^2 - 1)$. We ask if this is a general property of the rigidity function itself. The notion of *semicontinuity* of a function captures this property.

5.1. Semicontinuity of Rigidity. Intuitively, if a function is (lower) semicontinuous at a given point, then within a small neighborhood of that point, the function is nondecreasing. Formally,

DEFINITION 5.1 (Semicontinuity). *Let Y be a topological space. A function $\phi : Y \to \mathbb{Z}$ is* (lower) semicontinuous *if, for each n, the set $\{y \in Y : \phi(y) \leqslant n\}$ is a closed subset of Y. That is, for each y there is a neighbourhood U of y such that for $y' \in U, \phi(y') \geqslant \phi(y)$.*

The rank function of a matrix, for example, is a lower semicontinuous function on the space of all $n \times n$ complex matrices. Unfortunately, the rigidity function does not in general have this nice property. We now show below that that there is an infinite family of matrices $\{A_n\}_{n \geqslant 1}$ such that, for all n and any $\epsilon_n > 0$, there is a matrix B_n that is ϵ_n-close to A_n but having rigidity strictly *smaller* than that of A_n.

We start with a 3×3 example. Let a, b, c, d, e be non-zero rational numbers and consider

$$A = \begin{bmatrix} a & b & c \\ d & 0 & 0 \\ e & 0 & 0 \end{bmatrix} \in M_3(\mathbb{C}). \tag{5.2}$$

Observe that $\operatorname{rank}(A) = 2$ and by changing two (and no fewer) entries its rank can be brought down to 1. Hence, $\operatorname{Rig}(A, 1) = 2$.

Now for any $\epsilon > 0$, let

$$A(\delta) = \begin{bmatrix} a & b & c \\ d & bd\delta & cd\delta \\ e & be\delta & ce\delta \end{bmatrix},$$

where $\delta \neq 0$ and $\delta \neq 1/a$, be such that $\epsilon \geqslant \max\{bd\delta, cd\delta, be\delta, ce\delta\}$. Note that $\operatorname{rank}(A(\delta)) = 2$. Also $\operatorname{Rig}(A(\delta), 1) = 1$ because changing a to $\frac{1}{\delta}$ will make all the 2×2 sub-determinants of $A(\delta)$ zero. Thus, we have a matrix $A(\delta)$ which is in the open ϵ-ball around

A such that $\mathrm{Rig}(A,1) > \mathrm{Rig}(A(\delta),1)$. This proves conditions for semicontinuity of rigidity do *not* hold at A.
To produce an infinite family for any given n, choose $\alpha, a_1, a_2, \ldots, a_{n-1}$ and $b_1, b_2, \ldots, b_{n-1}$ to be non-zero rational numbers, and let

$$A_n := \begin{bmatrix} \alpha & a_1 & a_2 & \ldots & a_{n-1} \\ b_1 & 0 & 0 & \ldots & 0 \\ b_2 & 0 & 0 & \ldots & 0 \\ . & . & . & \ldots & . \\ . & . & . & \ldots & . \\ b_{n-1} & 0 & 0 & \ldots & 0 \end{bmatrix} \in M_n(\mathbb{C}).$$

Then, it is easy to show by induction that for $n \geqslant 3$, $\mathrm{rank}(A_n) = 2$, and $\mathrm{Rig}(A_n, 1) = n - 1$.

On the other hand, for a given ϵ, choose a δ such that $\epsilon \geqslant \max_{i,j}\{a_i b_j \delta\}$ with $\delta \neq 0,\ 1/\alpha$ and let

$$A_n(\delta) = \begin{bmatrix} \alpha & a_1 & a_2 & \ldots & a_n \\ b_1 & a_1 b_1 \delta & a_2 b_1 \delta & \ldots & a_n b_1 \delta \\ b_2 & a_1 b_2 \delta & a_2 b_2 \delta & \ldots & a_n b_2 \delta \\ . & . & . & \ldots & . \\ . & . & . & \ldots & . \\ b_n & a_1 b_n \delta & a_2 b_n \delta & \ldots & a_n b_n \delta \end{bmatrix}.$$

Observe that for every sub-determinant of A_n that is non-zero, the corresponding sub-determinant of $A_n(\delta)$ will also remain non-zero. Thus $\mathrm{rank}(A_n(\delta)) = 2$. But $\mathrm{Rig}(A_n(\delta), 1) = 1$ because if one changes α to $\frac{1}{\delta}$ then every 2×2 sub-determinant becomes zero.

To summarize, we exhibited an infinite family $\{A_n\}$ of matrices such that $\mathrm{Rig}(A_n, 1) = n-1$ and, given any $\epsilon_n > 0$, we constructed an infinite family $\{A_n(\delta_n)\}$ such that $A_n(\delta_n)$ is ϵ_n-close to A_n but $\mathrm{Rig}(A_n(\delta_n), 1) = 1$. This shows that the rigidity function is in general not semicontinuous.

5.1.1. Examples which are maximally rigid. The above example matrices are not maximally rigid. Might it be that for matrices of highest rigidity, semicontinuity holds? We now produce examples of matrices with maximum rigidity where the semi-

continuity property of rigidity fails. Let

$$A = \begin{bmatrix} a & b & c \\ d & e & 0 \\ g & 0 & i \end{bmatrix},$$

where $a, b, \ldots, i$ are non-zero rational numbers. Notice that changing 4 entries (namely a, b, d, e) will be enough to bring the rank down to 1. It is easy to verify that changing 3 entries will not suffice for a general choice of $a, \ldots, i$. Thus, $\mathrm{Rig}(A, 1) = 4 = (3-1)^2 = (n-r)^2$, with $n = 3$ and $r = 1$.

Let M be a generic matrix and let π be the diagonal pattern of size 3 (represented by variables t_1, t_2, t_3). Consider

$$M + T_\pi = \begin{bmatrix} a + t_1 & b & c \\ d & e + t_2 & f \\ g & h & i + t_3 \end{bmatrix}.$$

It can be checked that the elimination ideal for target rank $r = 1$ is generated by $bfg - cdh$. Note that A satisfies this equation and thus it follows that $A \in \overline{\mathsf{RIG}(3, 1, 3, \pi)}$. This implies that any Zariski open neighborhood of A intersects $\mathsf{RIG}(3, 1, 3, \pi)$. This is a straightforward consequence of the definitions. In fact, for any $\epsilon > 0$, consider the matrix

$$A(\delta) = \begin{bmatrix} a & b & c \\ d & e & cd\delta \\ g & bg\delta & i \end{bmatrix},$$

where $\delta \neq 0$ is chosen such that $\epsilon \geqslant \max\{cd\delta, bg\delta\}$. Then $A(\delta)$ is within the open ball of radius ϵ around A. Also, $\mathrm{Rig}(A(\delta), 1) \leqslant 3$ because we may change the diagonal entries to get the matrix

$$B = \begin{bmatrix} \delta^{-1} & b & c \\ d & bd\delta & cd\delta \\ g & bg\delta & cg\delta \end{bmatrix}$$

which has rank 1. Thus we have explicitly demonstrated that A is in the Euclidean closure of $\mathsf{RIG}(3, 1, 3, \pi)$.

5.2. Euclidean vs. Zariski Topology When defining semi-continuity, it is more natural to consider the Euclidean topology. On the other hand, for algebraically defined classes of matrices such as those in Section 3.3, it is more natural to study the Zariski closure. It is easy to see that the Euclidean topology is in general finer than the Zariski topology, i.e., closed sets in the latter are also closed in the former. Interestingly, these two notions coincide in our context: we show that the closures of the rigidity loci are equal in the Zariski and Euclidean topology.

PROPOSITION 5.3. *The Euclidean Closure of* $\mathsf{RIG}(n, r, \leqslant k)(\mathbb{C})$ *equals its Zariski Closure.*

PROOF. Recall that $\mathsf{RIG}(n, r, \leqslant k) = \bigcup_{\pi,\ |\pi|=k} \mathsf{RIG}(n, r, \pi)$. Thus, to prove the proposition, it is sufficient to prove that for any pattern π, the Euclidean closure of $\mathsf{RIG}(n, r, \pi)$ equals its Zariski Closure. By Closure Theorem, there exists a subvariety V strictly contained in $\mathcal{W} := \overline{\mathsf{RIG}(n, r, \pi)}$ such that

$$\mathcal{W}(\mathbb{C}) - V(\mathbb{C}) \subseteq \mathsf{RIG}(n, r, \pi)(\mathbb{C}) \subseteq \mathcal{W}(\mathbb{C})$$

. Since $\mathcal{W}(\mathbb{C})$ is closed in the Euclidean topology, we will be done if we prove that the Euclidean closure of $\mathcal{W}(\mathbb{C}) - V(\mathbb{C})$ is $\mathcal{W}(\mathbb{C})$. This is precisely the statement of the following lemma from Shafarevich (1994), which we state below for easy reference. Also note that, by Corollary 4.3, W is an irreducible variety for every pattern π and hence the lemma is applicable. □

LEMMA 5.4 (Shafarevich 1994, Lemma 1, page 124). *If X is an irreducible algebraic variety and Y a proper subvariety of X then the set $X(\mathbb{C}) - Y(\mathbb{C})$ is dense in $X(\mathbb{C})$.*

Let us consider the matrix A in (5.2). We showed earlier that $A \in \mathsf{RIG}(3, 1, 2)$ and yet there are matrices arbitrarily close to it that belong to $\mathsf{RIG}(3, 1, 1)$. Thus A is in the Euclidean closure of $\mathsf{RIG}(3, 1, 1)$, hence it is also in the Zariski closure of $\mathsf{RIG}(3, 1, 1)$. Let us verify this directly.

We want to check that $A \in \mathcal{W}(3,1,\leqslant 1)$. We do this by showing a pattern π such that $A \in \mathcal{W}(3,1,\pi)$. Let $\pi := \{(1,1)\}$. Let us write:

$$X + t_1 := \begin{bmatrix} x_1 + t_1 & x_2 & x_3 \\ x_3 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{bmatrix},$$

where t_1 is the variable associate to π. We obtain

$$\begin{aligned} I(3,1,1,\pi) \;=\; & \langle t_1x_5 + x_1x_5 - x_2x_4, t_1x_6 + x_1x_6 - x_3x_4, \\ & t_1x_8 + x_1x_8 - x_2x_7, t_1x_9 + x_1x_9 - x_3x_7, \\ & x_2x_6 - x_3x_5, x_2x_9 - x_3x_8, x_4x_8 - x_5x_7, \\ & x_4x_9 - x_6x_7, x_5x_9 - x_6x_8\rangle. \end{aligned}$$

Eliminating t_1 from $I(3,1,1,\pi)$ using the Gröbner Basis algorithm we get

$$\begin{aligned} EI(3,1,1,\pi) \;=\; & \langle x_2x_6 - x_3x_5, x_2x_9 - x_3x_8, x_4x_8 - x_5x_7, \\ & x_4x_9 - x_6x_7, x_5x_9 - x_6x_8\rangle. \end{aligned}$$

It is now easy to verify that A satisfies these generating polynomials and hence $A \in \mathcal{W}(3,1,\pi)$.

5.3. Some matrices with good neighborhoods. Although the semicontinuity property fails for the rigidity function over the entire space of matrices, we observe below that around certain nice matrices the rigidity function does remain nondecreasing within a small neighborhood.

In fact, the examples above suggest a technique for proving that there is an ϵ such that the ϵ-neighborhood of some explicitly constructed matrix does not contain matrices of strictly smaller rigidity. For this, we consider the Zariski closure of matrices of rigidity at most $k-1$ (for some k). For a matrix M of rigidity at least k, if we prove that it does not lie in the above closure, then it means that it is in the complement of a Zariski closed set, and hence in a Euclidean open set. Thus there must be an ϵ such that the ϵ-neighborhood of M does not contain matrices of rigidity smaller than k.

We illustrate the above technique by an example: Consider the matrix

$$M := \begin{bmatrix} 2 & 3 & 5 \\ 7 & 11 & 13 \\ 17 & 19 & 23 \end{bmatrix} \in M_3(\mathbb{C}).$$

This is a matrix all of whose entries are distinct prime numbers. We will show below that $M \in \mathsf{RIG}(3, 1, 4)$, but $M \notin \mathcal{W}(3, 1, 3)$.

We will prove this by ruling out all possible patterns π of size 3. We can quickly rule out some of these patterns as follows. Consider the pattern matrix T_π such that

$$M + T_\pi = \begin{bmatrix} a + t_1 & b + t_2 & c + t_3 \\ d & e & f \\ g & h & i \end{bmatrix}.$$

Then the equation $\begin{vmatrix} e & f \\ h & i \end{vmatrix} = 0$ belongs to the associated elimination ideal. Note here that the matrix M, due to its choice of entries, has the property that all the submatrices have full rank. Hence the above equation is obviously not satisfied by M. Similarly, we can rule out patterns π of size 3 for which either any row or any column contains at least two non-zero entries. Thus, to prove the claim we need to only rule out patterns T_π that touch all 2×2 minors. Thus, up to permutations (since choice of primes in M could be arbitrary but distinct) we need to check the case when T_π has the variables on the diagonal:

$$M + T_\pi = \begin{bmatrix} a + t_1 & b & c \\ d & e + t_2 & f \\ g & h & i + t_3 \end{bmatrix}.$$

In this case, the elimination ideal is generated by a single polynomial, namely $bfg - cdh$, which again M does not satisfy. Since up to permutations, all patterns of size 3 can be written as one of the above, we conclude that $M \notin \mathcal{W}(3, 1, 3)$. In addition, by the argument outlined earlier, this also implies that for the matrix M, there is an ϵ such that all the matrices in the ϵ-neighborhood are outside $\mathcal{W}(3, 1, 3)$.

Note that for the purposes of this argument, we can get by with much less: instead of populating the matrix with distinct primes, we could take a Vandermonde matrix

$$\begin{bmatrix} 1 & p & p^2 \\ 1 & q & q^2 \\ 1 & r & r^2 \end{bmatrix},$$

where p, q, r are distinct primes.

6. Conclusions and Further Research

In this paper, we considered the problem of finding $n \times n$ matrices of highest possible rigidity, i.e. $(n-r)^2$, for target rank r. In the first part, we presented a proof in the language of algebraic geometry, of Valiant's classical theorem that most matrices over $\mathbb{C}$ have rigidity exactly $(n-r)^2$. In addition, we are able to compute the exact dimension of the variety of matrices of rigidity strictly less than $(n-r)^2$. A natural question is to ask for the degrees and other geometrical properties of the loci $\overline{\mathrm{Rig}(n, r, \leqslant k)}$ of matrices with rigidity at most k (we computed the dimensions in Theorem 3.8).

Our second and main contribution is to construct certain explicit matrices of highest possible rigidity over $\mathbb{C}$. Entries of these matrices are primitive roots of unity of orders $\exp(n^2 \log n)$. While these matrices have a concrete and succinct algebraic description, they are still not explicit from a computational complexity perspective. In particular, the main open question of constructing polynomial time computable matrices of even superlinear rigidity is still wide open.

It is unclear whether the exponential orders, $\exp(n^2 \log n)$, for the roots of unity used in the matrices of Theorem 3.11 are necessary. It would be interesting to obtain matrices of *optimal* rigidity using roots of polynomial, or even $\exp(n)$, orders. Results on effective Nullstellensatz used in the proof of Theorem 3.13 show exponential degree bounds for polynomials in elimination ideals are in general unavoidable. Thus any improvements may have to exploit the special nature of the elimination ideals of matrices of rigidity less than $(n-r)^2$. In particular, as remarked in earlier sections,

elimination ideals of determinantal varieties are objects worthy of study in this context. Note that Lokam (2006) constructs matrices of *asymptotically optimal* rigidity using roots of unity of polynomial orders, using different and more elementary arguments.

Both our lower bound and the one from Lokam (2006) rely on the fact that the corresponding matrices live in number fields of at least exponentially large dimensions. This dimension can be viewed as an algebraic measure of explicitness of the matrix; the lower the dimension, the more explicit the matrix. Constructing matrices of high rigidity whose entries come from number fields of polynomial dimension is an open question.

A particularly interesting problem is whether a Vandermonde matrix $V = \left(x_i^{j-1}\right)_{ij}$ with algebraically independent coordinates $\{x_i\}$ has maximal rigidity. To analyze this question, one would look at the rigidity loci restricted to the subvariety of Vandermonde matrices. If this question has an affirmative answer, we believe that one may proceed using the Nullstellensatz (as we have done in here) to construct explicit Vandermonde matrices with entries being algebraic numbers, of significantly smaller complexity than those in this paper. We mention in passing that the finite Fourier transform matrix $\mathcal{F} = (\zeta_n^{(i-1)(j-1)})_{ij}$, which is a Vandermonde matrix, does *not* have maximal rigidity (for instance, for target rank $\lfloor 3n/4 \rfloor$, as long as $n > 4$).

In the final part of the paper, we try to understand the topological behavior of the rigidity function in the neighborhood of highly rigid matrices. Our main motivation for this line of investigation comes from the intuition that we may be able to find sufficiently explicit rational matrices of (moderately) high rigidity that approximate the complex matrices of (very) high rigidity that seem easier to find. We give examples to show that the rigidity function is in general not semi-continuous, meaning that within a small (Zariski or Euclidean) neighborhood of certain matrices, the rigidity function can strictly decrease. On the other hand, around many "natural and interesting" matrices, we find that the rigidity function is actually nondecreasing within a small neighborhood. We think that a better understanding of the topology of the stratification of $M_n(\mathbb{C})$ by the subsets $\mathrm{Rig}(n, r, k)$ will have a bearing on

the complexity-theoretic problem of constructing matrices of high rigidity.

Acknowledgements

AK was at Microsoft Research, Redmond, when this work was started, and later supported by NSF CAREER grant DMS-0952486. VMP was at Microsoft Research India, Bangalore, for the duration of most of this project. JSMN was at the Institute of Mathematical Sciences, Chennai, and Institute for Theoretical Computer Science, Tsinghua University, Beijing, China for the duration of this project.

References

W. D. Brownawell (1987). Bounds for the degrees in the Nullstellensatz. *Annals of Mathematics* **126**(3), 577–591.

W. Bruns & U. Vetter (1980). *Determinantal Rings*, volume 1327 of *Lecture Notes in Mathematics*. Springer-Verlag.

M. Cheraghchi (2005). On matrix rigidity and the complexity of linear forms. *Electronic Colloquium on Computational Complexity (ECCC)* (070).

B. Codenotti (2000). Matrix rigidity. *Linear Algebra and its Applications* **304**(1–3), 181–192.

D. Cox, J. Little & D. O'Shea (2007). *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer, New York, 3rd edition.

A. Dickenstein, N. Fitchas, M. Giusti & C. Sessa (1991). The membership problem for unmixed polynomial ideals is solvable in single exponential time. *Discrete Appl. Math.* **33**(1-3), 73–94. Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes (Toulouse, 1989).

D. Eisenbud & J. Harris (2000). *The Geometry of Schemes*, volume 197 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

J. Forster (2002). A linear lower bound on the unbounded error probabilistic communication complexity. *Journal of Computer and System Sciences* **65**(4), 612–625. Special issue of papers from Conf. on Computational Complexity (CCC), 2001 (Chicago, IL).

J. Forster, M. Krause, S. V. Lokam, R. Mubarakzjanov, N. Schmitt & H. U. Simon (2001). Relations between communication complexity, linear arrangements, and computational complexity. In *FSTTCS 2001: Foundations of Software Technology and Theoretical Computer Science*, volume 2245 of *Lecture Notes in Comput. Sci.*, 171–182. Springer, Berlin.

J. Friedman (1993). A note on matrix rigidity. *Combinatorica* **13**(2), 235 – 239.

R. Hartshorne (1977). *Algebraic Geometry*. Springer-Verlag, New York. Graduate Texts in Mathematics, No. 52.

J. Heintz (1983). Definability and fast quantifier elimination in algebraically closed fields. *Theoret. Comput. Sci.* **24**(3), 239–277.

J. Heintz & C.-P. Schnorr (1980). Testing polynomials which are easy to compute (extended abstract). In *Proceedings of the 12th Annual ACM Symposium on Theory of Computing*, 262–272. ACM.

M. Hindry & J. H. Silverman (2000). *Diophantine Geometry: An Introduction*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

M. Hochster & J.A. Eagon (1971). Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci. *American Journal of Mathematics* **93**, 1020–1058.

J. Kollár (1988). Sharp effective Nullstellensatz. *Journal of American Mathematical Society* **1**(4), 963–975.

J. M. Landsberg, J. Taylor & N. K. Vishnoi (2003). The geometry of matrix rigidity. Technical Report GIT-CC-03-54, Georgia Institute of Technology, http://smartech.gatech.edu/handle/1853/6514.

S. Lang (2004). *Algebra*. Springer-Verlag, revised third edition.

N. Linial & A. Shraibman (2009). Learning complexity vs. communication complexity. *Combinatorics, Probability & Computing* **18**(1-2), 227–245.

S. V. Lokam (2000). On the rigidity of Vandermonde matrices. *Theoretical Computer Science* **237**(1-2), 477–483.

S. V. Lokam (2001). Spectral methods for matrix rigidity with applications to size-depth tradeoffs and communication complexity. *Journal of Computer and System Sciences* **63**(3), 449–473.

S. V. Lokam (2006). Quadratic lower bounds on matrix rigidity. In *Proceedings of International Conference on Theory and Applications of Models of Computation (TAMC 2006)*, volume 3959 of *Lecture Notes in Computer Science*.

S. V. Lokam (2009). Complexity Lower Bounds using Linear Algebra. *Foundations and Trends in Theoretical Computer Science* **4**(1-2), 1–155.

W. Narkiewicz (2004). *Elementary and Analytic Theory of Algebraic Numbers*, volume XI of *Springer Monographs in Mathematics*. Springer.

R. Paturi & P. Pudlák (2004). Circuit lower bounds and linear codes. In *Notes of Mathematical Seminars of St.Petersburg Department of Steklov Institute of Mathematics*, E. A. Hirsch, editor, volume 316 of *Teoria slozhnosti vychislenij IX*, 188–204. Technical Report appeared in ECCC : TR04-04.

A. A. Razborov (1989). On rigid matrices. Manuscript, (Russian).

I. R. Shafarevich (1994). *Basic Algebraic Geometry. 1. Varieties in Projective Space*. Springer Verlag, 2nd edition.

D. A. Spielman, V. Stemann & M. A. Shokhrollahi (1997). A remark on matrix rigidity. *Information Processing Letters* **64**(6), 283 – 285.

L. G. Valiant (1977). Graph-theoretic arguments in low-level complexity. In *Proceedings of the 6th Symposium on Mathematical Foundations of Computer Science*, volume 53 of *Lecture Notes in Computer Science*, 162–176. Springer Verlag.

A. Background on Algebraic Geometry

In this section, we recall some basic notions from algebraic geometry. Much of this background can be found in Hindry & Silverman (2000) and Eisenbud & Harris (2000).

We aim for a relatively elementary description: in particular, we will identify a variety with the set of its points over the algebraic closure, rather than thinking of its points as the prime ideals of a ring (the scheme-theoretic point of view).

Let F be a field. Let $\overline{F}$ denote a fixed algebraic closure of F. Let $x_1, \cdots, x_n$ be n algebraically independent variables over F. Let $F[x_1, \cdots, x_n]$ be the polynomial ring in n variables over F. An ideal I is by definition a sub-module of the ring $F[x_1, \cdots, x_n]$. More explicitly, I is a subset of $F[x_1, \cdots, x_n]$ which is a subgroup of $F[x_1, \cdots, x_n]$ under addition, and which is also closed under multiplication by elements of $F[x_1, \cdots, x_n]$. The ideal I is *prime* if whenever $rs \in I$ with $r, s \in F[x_1, \cdots, x_n]$, either $r \in I$ or $s \in I$.

An *affine algebraic variety* $S \subset \overline{F}^n$ is a subset

$$V(\Sigma) = \{(a_1, \ldots, a_n) \in \overline{F}^n : f(a_1, \ldots, a_n) = 0 \text{ for all } f \in \Sigma\}$$

for some subset Σ of $\overline{F}[x_1, \ldots x_n]$. In particular, Σ may consist of polynomials with coefficients in F, in which case we say that $V(\Sigma)$ is defined over F. In particular, we have *affine n-space* $\mathbb{A}^n = V(\{0\})$, and any affine algebraic variety is a subset of some $\mathbb{A}^n$ cut out by a set of polynomials.

If I_Σ is the ideal generated by Σ in $\overline{F}[x_1, \ldots, x_n]$ (or in $F[x_1, \ldots, x_n]$ if $\Sigma \subset F[x_1, \ldots, x_n]$), it is clear $V(I_\Sigma) = V(\Sigma)$. Therefore we may restrict attention to zero sets of ideals from now on. The Hilbert Basis theorem says that every ideal of a polynomial ring over a field is finitely generated, so we observe that we could always have started with a finite set of generators Σ. Since each generator is a polynomial with finitely many coefficients, it follows that any algebraic variety $V(I)$ may be defined over some finite extension of F.

For an affine variety $V(I)$ and an extension L of F, we define its L-rational points to be

$$V(I)(L) := \{(a_1, \ldots, a_n) \in L^n : f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}.$$

The algebraic variety $V(I)$ is a geometric object with a natural structure of a topological space, where the closed subsets are $V(J)$ for ideals $J \subseteq \overline{F}[x_1, \ldots, x_n]$ containing I. This is called the *Zariski topology*.

On the other hand, given a subset S of $\overline{F}^n$, let us define $I(S)$ to be the set of polynomials $f \in \overline{F}[x_1, \cdots, x_n]$ such that $f(s) = 0 \; \forall s \in S$; it follows that $I(S)$ is an ideal of $\overline{F}[x_1, \cdots, x_n]$. If $S \subset F^n$, then it is not hard to see that one can choose generators of $I(S)$ to lie in $F[x_1, \ldots, x_n]$. We can then associate the ideal $I_F(S) = I(S) \cap F[x_1, \ldots, x_n]$ to S. Note that $I_F(S) \cdot \overline{F}[x_1, \ldots, x_n] = I(S)$.

For any ideal $I \subset \overline{F}[x_1, \ldots, x_n]$, let us define

$$\sqrt{I} := \{f \in \overline{F}[x_1, \cdots, x_n] : \exists m \in \mathbb{N} \text{ such that } f^m \in I\}.$$

$\sqrt{I}$ is called the *radical* of the ideal I. We then have the following fundamental theorem.

THEOREM A.1. *(Hilbert's Nullstellensatz)*
For an ideal I of $\overline{F}[x_1, \cdots, x_n]$, $\sqrt{I} = I(V(I))$.

We will always deal with radical ideals, namely those I which are equal to $\sqrt{I}$.

Given a subset S of $\overline{F}^n$, the Zariski-closure of S, denoted by $\overline{S}$, is the smallest *algebraic* variety of $\overline{F}^n$ containing S. In other words, we have $\overline{S} = V(I(S))$.

We say that an algebraic variety X is *irreducible* if it can not be written as a union of two algebraic varieties X_1 and X_2 properly contained in X. Note that X is irreducible if and only if $I(X)$ is a prime ideal.

A morphism $\phi : X \subseteq \mathbb{A}^n \to \mathbb{A}^1$ from an affine closed subvariety of affine n-space to the affine line is a polynomial map $(x_1, \ldots x_n) \mapsto p(x_1, \ldots, x_n)$ where p is a polynomial. We naturally extend this to a morphism between affine varieties.

DEFINITION A.2. *Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be two closed affine varieties. A morphism $\phi : X \to Y$ is defined to be a map ϕ whose components are polynomials. In other words, ϕ has the form:*

$$\phi(x_1, \ldots x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_m))$$

where $f_1, \ldots f_m$ are polynomials, and with the property that it maps the subset X to Y.

The morphism ϕ is called dominant *if $\phi(X)$ is dense in Y.*

Let $X = V(I) \subset \mathbb{A}^n$ be an affine algebraic variety, where $I \subset \overline{F}[x_1, \ldots, x_n]$, and let $\overline{F}(X)$ denote the ring of fractions of the quotient ring $R = \overline{F}[x_1, \ldots, x_n]/I(X)$. If $I(X)$ is a prime ideal, $\overline{F}(X)$ is a field and is called the *function field* of X. Elements of the function field $\overline{F}(X)$ are called the set of *rational functions* on the variety X.

Definition A.3. *Let K be a finitely generated extension field over a base field F. Let T be a maximal set of algebraically independent elements of K over F. Such a T is called a* transcendence basis *of K over F. It can be proved that the cardinality $|T|$ is independent of T, and is called the* transcendence degree *of K over F and will be denoted by* $\text{tr deg}(K/F)$.

Definition A.4. *The dimension of an irreducible affine variety $X \subseteq \overline{F}^n$, denoted by* $\dim(X)$, *is the transcendence degree of the function field $\overline{F}(X)$ of the variety X over the base field $\overline{F}$. Thus,* $\dim(X) := \text{tr deg}(\overline{F}(X)/\overline{F})$.

For easy reference we state a lemma below that is an immediate consequence of Theorem 4.4, Chapter 1, of Hartshorne (1977).

Lemma A.5. *Let $\phi : X \to Y$ be a dominant morphism of irreducible varieties over F. Then ϕ induces a natural embedding $\phi^* : \overline{F}(Y) \hookrightarrow \overline{F}(X)$. In particular,*

$$\dim(Y) = \text{tr deg}(\overline{F}(Y)/\overline{F}) \leqslant \text{tr deg}(\overline{F}(X)/\overline{F}) = \dim(X).$$

If a variety X is not irreducible, we define its dimension to be the maximum of the dimensions of its (finitely many) irreducible components. The conclusion of Lemma A.5 that $\dim(Y) \leqslant \dim(X)$ continues to hold for a dominant morphism $X \to Y$ of varieties which may be reducible.

We have described closed affine subvarieties of affine n-space. In particular, a closed subset of $\mathbb{A}^n$ that is defined by a single

polynomial f in n variables is called a hypersurface $V(f)$. Now, it can be shown that the Zariski topology of $\mathbb{A}^n$ has a basis of open sets given by the complements of these hypersurfaces, $D(f) = \mathbb{A}^n \backslash V(f)$. In fact, $D(f)$ is itself isomorphic to an affine variety, namely the hypersurface $fy = 1$ in $\mathbb{A}^n \times \mathbb{A}^1_y$. In general, a space which we can thus identify naturally with a closed affine subvariety in some affine space (in a sense that we will not make precise here) is called an affine variety. An important example of this is the open subset $GL_n = D(\det) = M_n \backslash V(\det)$ of invertible matrices in M_n, where det stands for the determinant polynomial.

A general algebraic variety X is obtained by glueing together various pieces X_i such that X_i is an affine variety. The notion of gluing means that there are open varieties $U_{ij} \subset X_i$ and compatible isomorphisms $U_{ij} \to U_{ji}$ between them (so that we can think of U_{ij} as the intersection of X_i and X_j).

Manuscript received 12 December 2010

Abhinav Kumar
Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA, USA.
abhinav@math.mit.edu

Satyanarayana V. Lokam
Microsoft Research India
Bangalore, India.
satya@microsoft.com

Vijay M. Patankar
Indian Statistical Institute
Chennai Centre
Chennai, India.
vijay@isichennai.res.in

Jayalal Sarma M.N.
Department of Computer Science & Engineering
Indian Institute of Technology Madras
Chennai, India.
jayalal@cse.iitm.ac.in