Matrix rigidity and elimination theory

Abhinav Kumar
joint work with Satya Lokam, Vijay Patankar and Jalayal Sarma M.N.

MIT

April 25, 2012

Rigidity of a matrix

Definition

Let A be an $n \times n$ matrix with entries in a field F. The rigidity $\mathrm{Rig}(A, r)$ of A for target rank r is the smallest number of entries of A that need to be changed to make the rank at most r.

Most of the time we'll work with $F = \mathbb{C}$. If F is a subfield of $\mathbb{C}$ (e.g. $\mathbb{Q}$) we may want to consider changes in some finite extension field L/F, and define $\mathrm{Rig}(A, r, L)$.

Rigidity of a matrix

Definition

Let A be an $n \times n$ matrix with entries in a field F. The rigidity $\mathrm{Rig}(A, r)$ of A for target rank r is the smallest number of entries of A that need to be changed to make the rank at most r.

Most of the time we'll work with $F = \mathbb{C}$. If F is a subfield of $\mathbb{C}$ (e.g. $\mathbb{Q}$) we may want to consider changes in some finite extension field L/F, and define $\mathrm{Rig}(A, r, L)$.

Rigidity of a matrix

Definition

Let A be an $n \times n$ matrix with entries in a field F. The rigidity $\mathrm{Rig}(A, r)$ of A for target rank r is the smallest number of entries of A that need to be changed to make the rank at most r.

Most of the time we'll work with $F = \mathbb{C}$. If F is a subfield of $\mathbb{C}$ (e.g. $\mathbb{Q}$) we may want to consider changes in some finite extension field L/F, and define $\mathrm{Rig}(A, r, L)$.

Valiant's theorem

Valiant defined matrix rigidity in his study of lower bounds on complexity for computing linear forms in n variables, for circuits using gates which can compute linear combinations of two variables.

To compute one such linear combination, we can use a binary tree to get a circuit of depth $\log_2(n)$ and size n.

But: say we want to use such a circuit to simultaenously compute n linear forms in n variables, given by the entries of the vector Ax, where $x = (x_1, \ldots, x_n)$ is the column vector of inputs.

Valiant showed that this cannot be done with circuits which are both shallow (of depth $O(\log n)$) and small (of size $O(n)$).

Valiant's theorem

Valiant defined matrix rigidity in his study of lower bounds on complexity for computing linear forms in n variables, for circuits using gates which can compute linear combinations of two variables.

To compute one such linear combination, we can use a binary tree to get a circuit of depth $\log_2(n)$ and size n.

But: say we want to use such a circuit to simultaenously compute n linear forms in n variables, given by the entries of the vector Ax, where $x = (x_1, \ldots, x_n)$ is the column vector of inputs.

Valiant showed that this cannot be done with circuits which are both shallow (of depth $O(\log n)$) and small (of size $O(n)$).

Valiant's theorem

Valiant defined matrix rigidity in his study of lower bounds on complexity for computing linear forms in n variables, for circuits using gates which can compute linear combinations of two variables.

To compute one such linear combination, we can use a binary tree to get a circuit of depth $\log_2(n)$ and size n.

But: say we want to use such a circuit to simultaenously compute n linear forms in n variables, given by the entries of the vector Ax, where $x = (x_1, \ldots, x_n)$ is the column vector of inputs.

Valiant showed that this cannot be done with circuits which are both shallow (of depth $O(\log n)$) and small (of size $O(n)$).

Valiant's theorem II

More precisely,

Theorem

Let $A_1, A_2, \ldots$ be an infinite family of matrices, where A_n is an $n \times n$ real matrix and for some $\kappa, c, \epsilon > 0$, we have $\mathrm{Rig}(A, \kappa n) \geq cn^{1+\epsilon}$. Then given any fixed $c_1, c_2 > 0$, there does not exist a family of straight line programs for the corresponding sets of linear forms that achieve size $c_1 n$ and depth $c_2 \log n$ simultaneously for all n.

Remarks:

- The proof uses some graph theoretic property of the circuit (namely, that it's a *grate*.
- We'll see that most matrices have quadratic rigidity, so asking for super-linear rigidity is perhaps not so bad.

Valiant's theorem II

More precisely,

Theorem

Let $A_1, A_2, \ldots$ be an infinite family of matrices, where A_n is an $n \times n$ real matrix and for some $\kappa, c, \epsilon > 0$, we have $\mathrm{Rig}(A, \kappa n) \geq cn^{1+\epsilon}$. Then given any fixed $c_1, c_2 > 0$, there does not exist a family of straight line programs for the corresponding sets of linear forms that achieve size $c_1 n$ and depth $c_2 \log n$ simultaneously for all n.

Remarks:

- The proof uses some graph theoretic property of the circuit (namely, that it's a *grate*.
- We'll see that most matrices have quadratic rigidity, so asking for super-linear rigidity is perhaps not so bad.

Valiant's theorem II

More precisely,

Theorem

Let $A_1, A_2, \ldots$ be an infinite family of matrices, where A_n is an $n \times n$ real matrix and for some $\kappa, c, \epsilon > 0$, we have $\mathrm{Rig}(A, \kappa n) \geq cn^{1+\epsilon}$. Then given any fixed $c_1, c_2 > 0$, there does not exist a family of straight line programs for the corresponding sets of linear forms that achieve size $c_1 n$ and depth $c_2 \log n$ simultaneously for all n.

Remarks:

- The proof uses some graph theoretic property of the circuit (namely, that it's a *grate*.
- We'll see that most matrices have quadratic rigidity, so asking for super-linear rigidity is perhaps not so bad.

Valiant's theorem II

More precisely,

Theorem

Let $A_1, A_2, \ldots$ be an infinite family of matrices, where A_n is an $n \times n$ real matrix and for some $\kappa, c, \epsilon > 0$, we have $\mathrm{Rig}(A, \kappa n) \geq cn^{1+\epsilon}$. Then given any fixed $c_1, c_2 > 0$, there does not exist a family of straight line programs for the corresponding sets of linear forms that achieve size $c_1 n$ and depth $c_2 \log n$ simultaneously for all n.

Remarks:

- The proof uses some graph theoretic property of the circuit (namely, that it's a *grate*.
- We'll see that most matrices have quadratic rigidity, so asking for super-linear rigidity is perhaps not so bad.

Easy upper bound

Proposition

Any $n \times n$ matrix X has rigidity at most $(n-r)^2$ for target rank r.

Proof.

If the rank less than r, rigidity is zero. Else assume w.lo.g. that the top left $r \times r$ block is nonsingular. Write X as

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

Modify D to $CA^{-1}B$. □

Easy upper bound

Proposition

Any $n \times n$ matrix X has rigidity at most $(n-r)^2$ for target rank r.

Proof.

If the rank less than r, rigidity is zero. Else assume w.lo.g. that the top left $r \times r$ block is nonsingular. Write X as

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

Modify D to $CA^{-1}B$. □

Generic rigidity

An extension of this argument shows that *generic* matrices have maximal rigidity, i.e. the subset of matrices of rigidity less than $(n-r)^2$ is contained in a proper Zariski-closed subset.

Proof: if rigidity is $k < (n-r)^2$, then the matrix is in the image of a map from a variety of matrices of the form

$$\begin{pmatrix} A & B \\ C & CA^{-1}B \end{pmatrix}.$$

(which has dimension $\leq n^2 - (n-r)^2$) times $\mathbb{A}^k$. Since $k + n^2 - (n-r)^2 < n^2 = \dim \mathrm{Mat}_n$, the image is contained in a proper closed subset.

Generic rigidity

An extension of this argument shows that *generic* matrices have maximal rigidity, i.e. the subset of matrices of rigidity less than $(n-r)^2$ is contained in a proper Zariski-closed subset.

Proof: if rigidity is $k < (n-r)^2$, then the matrix is in the image of a map from a variety of matrices of the form

$$\begin{pmatrix} A & B \\ C & CA^{-1}B \end{pmatrix}.$$

(which has dimension $\leq n^2 - (n-r)^2$) times $\mathbb{A}^k$. Since $k + n^2 - (n-r)^2 < n^2 = \dim \mathrm{Mat}_n$, the image is contained in a proper closed subset.

Questions

All this leads to the natural question:

Construct an explicit family of reasonably natural matrices of super-linear rigidity for target rank linear in the dimension n.

Remarks:

- Or even better, quadratic rigidity.
- Or better still, maximal rigidity $(n-r)^2$.

Note that these extensions will not give a better lower complexity bound, but they are natural questions from the algebraic point of view.

Questions

All this leads to the natural question:

Construct an explicit family of reasonably natural matrices of super-linear rigidity for target rank linear in the dimension n.

Remarks:

- Or even better, quadratic rigidity.
- Or better still, maximal rigidity $(n-r)^2$.

Note that these extensions will not give a better lower complexity bound, but they are natural questions from the algebraic point of view.

Questions

All this leads to the natural question:

Construct an explicit family of reasonably natural matrices of super-linear rigidity for target rank linear in the dimension n.

Remarks:

- Or even better, quadratic rigidity.
- Or better still, maximal rigidity $(n - r)^2$.

Note that these extensions will not give a better lower complexity bound, but they are natural questions from the algebraic point of view.

Questions

All this leads to the natural question:

Construct an explicit family of reasonably natural matrices of super-linear rigidity for target rank linear in the dimension n.

Remarks:

- Or even better, quadratic rigidity.
- Or better still, maximal rigidity $(n - r)^2$.

Note that these extensions will not give a better lower complexity bound, but they are natural questions from the algebraic point of view.

Questions

All this leads to the natural question:

Construct an explicit family of reasonably natural matrices of super-linear rigidity for target rank linear in the dimension n.

Remarks:

- Or even better, quadratic rigidity.
- Or better still, maximal rigidity $(n - r)^2$.

Note that these extensions will not give a better lower complexity bound, but they are natural questions from the algebraic point of view.

Examples I

One guess for highly rigid matrices: *totally regular matrices*, i.e. all minors are nonsingular.

This guess is not correct! Valiant shows:

Proposition

For each n there is an $n \times n$ totally regular matrix A such that

$$\mathrm{Rig}(A, n(\log\log\log n)/(\log\log n)) \leq n^{1+O(1/\log\log n)}.$$

Remarks:

- That is, one can bring rank down to $o(n)$ by changing $o(n^{1+\epsilon})$ entries.
- Proof uses *superconcentrators*, and is also non-explicit.

Examples I

One guess for highly rigid matrices: *totally regular matrices*, i.e. all minors are nonsingular.

This guess is not correct! Valiant shows:

Proposition

For each n there is an $n \times n$ totally regular matrix A such that

$$\mathrm{Rig}(A, n(\log\log\log n)/(\log\log n)) \leq n^{1+O(1/\log\log n)}.$$

Remarks:

- That is, one can bring rank down to $o(n)$ by changing $o(n^{1+\epsilon})$ entries.
- Proof uses *superconcentrators*, and is also non-explicit.

Examples I

One guess for highly rigid matrices: *totally regular matrices*, i.e. all minors are nonsingular.

This guess is not correct! Valiant shows:

Proposition

For each n there is an $n \times n$ totally regular matrix A such that

$$\mathrm{Rig}(A, n(\log\log\log n)/(\log\log n)) \leq n^{1+O(1/\log\log n)}.$$

Remarks:

- That is, one can bring rank down to $o(n)$ by changing $o(n^{1+\epsilon})$ entries.
- Proof uses *superconcentrators*, and is also non-explicit.

Examples I

One guess for highly rigid matrices: *totally regular matrices*, i.e. all minors are nonsingular.

This guess is not correct! Valiant shows:

Proposition

For each n there is an $n \times n$ totally regular matrix A such that

$$\mathrm{Rig}(A, n(\log\log\log n)/(\log\log n)) \leq n^{1+O(1/\log\log n)}.$$

Remarks:

- That is, one can bring rank down to $o(n)$ by changing $o(n^{1+\epsilon})$ entries.
- Proof uses *superconcentrators*, and is also non-explicit.

Examples I

One guess for highly rigid matrices: *totally regular matrices*, i.e. all minors are nonsingular.

This guess is not correct! Valiant shows:

Proposition

For each n there is an $n \times n$ totally regular matrix A such that

$$\mathrm{Rig}(A, n(\log\log\log n)/(\log\log n)) \leq n^{1+O(1/\log\log n)}.$$

Remarks:

- That is, one can bring rank down to $o(n)$ by changing $o(n^{1+\epsilon})$ entries.
- Proof uses *superconcentrators*, and is also non-explicit.

Examples II

Nevertheless, here are some natural familes.

- Vandermonde matrices: row j is $1, x_j, x_j^2, \ldots, x_j^n$.
- Discrete Fourier transform matrices: $n = p$ prime say, Vandermonde with $x_j = e^{2\pi\sqrt{-1}j/p}$.
- Generalized Hadamard matrices H: entries complex numbers h_{ij} of absolute value 1, and such that $HH^\dagger = nI_n$.
- Circulant matrices: each row is a shift of the previous one.
- Cauchy matrix $C_{ij} = 1/(i + j - 1)$.

Examples II

Nevertheless, here are some natural familes.

- Vandermonde matrices: row j is $1, x_j, x_j^2, \ldots, x_j^n$.
- Discrete Fourier transform matrices: $n = p$ prime say, Vandermonde with $x_j = e^{2\pi\sqrt{-1}j/p}$.
- Generalized Hadamard matrices H: entries complex numbers h_{ij} of absolute value 1, and such that $HH^\dagger = nI_n$.
- Circulant matrices: each row is a shift of the previous one.
- Cauchy matrix $C_{ij} = 1/(i + j - 1)$.

Examples II

Nevertheless, here are some natural familes.

- Vandermonde matrices: row j is $1, x_j, x_j^2, \ldots, x_j^n$.
- Discrete Fourier transform matrices: $n = p$ prime say, Vandermonde with $x_j = e^{2\pi\sqrt{-1}j/p}$.
- Generalized Hadamard matrices H: entries complex numbers h_{ij} of absolute value 1, and such that $HH^\dagger = nI_n$.
- Circulant matrices: each row is a shift of the previous one.
- Cauchy matrix $C_{ij} = 1/(i + j - 1)$.

Examples II

Nevertheless, here are some natural familes.

- Vandermonde matrices: row j is $1, x_j, x_j^2, \ldots, x_j^n$.
- Discrete Fourier transform matrices: $n = p$ prime say, Vandermonde with $x_j = e^{2\pi\sqrt{-1}j/p}$.
- Generalized Hadamard matrices H: entries complex numbers h_{ij} of absolute value 1, and such that $HH^\dagger = nI_n$.
- Circulant matrices: each row is a shift of the previous one.
- Cauchy matrix $C_{ij} = 1/(i + j - 1)$.

Examples II

Nevertheless, here are some natural familes.

- Vandermonde matrices: row j is $1, x_j, x_j^2, \ldots, x_j^n$.
- Discrete Fourier transform matrices: $n = p$ prime say, Vandermonde with $x_j = e^{2\pi\sqrt{-1}j/p}$.
- Generalized Hadamard matrices H: entries complex numbers h_{ij} of absolute value 1, and such that $HH^\dagger = nI_n$.
- Circulant matrices: each row is a shift of the previous one.
- Cauchy matrix $C_{ij} = 1/(i + j - 1)$.

Progress so far

Matrices	$\Omega(.)$	References
Vandermonde	$\frac{n^2}{r}$	Razborov '89, Pudlak '94 Shparlinsky '97, Lokam '99
Hadamard	$\frac{n^2}{r}$	Kashin-Razborov '98
Parity Check	$\frac{n^2}{r}\log(\frac{n}{r})$	Friedman '93 Pudlak-Rodl '94
Totally regular	$\frac{n^2}{r}\log(\frac{n}{r})$	Shokrallahi-Spielmann-Stemann '97
$\sqrt{p_{ij}}$	$n(n-16r)$	Lokam '06
$\zeta_{ij} = e^{\frac{2\pi\sqrt{-1}}{p_{ij}}}$	$(n-r)^2$	This work.

Statement of our result

We construct matrices with maximal rigidity, but over a number field of relatively high degree.

Theorem

Let $\Delta(n) = 2n^{2n^2}$ *and let* $p_{ij} > \Delta(n)$ *be distinct primes for* $1 \leq i, j \leq n$. *Let* $A(n)$ *have* (i,j) *entry* $\zeta_{ij} = e^{2\pi\sqrt{-1}/p_{ij}}$. *Then* $\mathrm{Rig}(A(n), r) = (n-r)^2$.

Determinantal ideal

Recall that the variety of matrices of rank at most r is defined by the determinantal ideal $I(n, r)$ with generators all $(r+1) \times (r+1)$ minors of

$$\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & & \vdots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{pmatrix}$$

It's an irreducible variety of dimension $n^2 - (n-r)^2$.

Elimination ideals

Let π be a *pattern* (Valiant calles it a mask) of positions where we allow changes, of cardinality k strictly less than $(n-r)^2$ say. The set of matrices whose rank can be brought down to at most r by changing entries in π lie in the image of a variety of dimension $n^2 - (n-r)^2 + k$.

Its closure is defined by the *elimination ideal* $I(n, r, \pi) = I(n, r) \cap Q[x_{\overline{\pi}}]$ where $\overline{\pi}$ means positions not in π.

Elimination ideals

Let π be a *pattern* (Valiant calles it a mask) of positions where we allow changes, of cardinality k strictly less than $(n-r)^2$ say. The set of matrices whose rank can be brought down to at most r by changing entries in π lie in the image of a variety of dimension $n^2 - (n-r)^2 + k$.

Its closure is defined by the *elimination ideal* $I(n, r, \pi) = I(n, r) \cap Q[x_{\overline{\pi}}]$ where $\overline{\pi}$ means positions not in π.

Sketch of proof

As a generic matrix has maximal rigidity, these elimination ideals $I(n, r, \pi)$ are all non-zero, as π runs over all patterns of size strictly less than $(n - r)^2$.

So the ideal $I(n, r, \pi)$ is nonzero. We'll use effective Nullstellensatz bounds to show that there's a multivariate polynomial of low enough degree, and then use Galois theory to show that it cannot vanish on the roots of unity constructed. Therefore, the matrix with entries $A_{ij} = e^{2\pi\sqrt{-1}/p_{ij}}$ does not lie in $V(I(n, r, \pi))$ for any π, and therefore has maximal rigidity.

Sketch of proof

As a generic matrix has maximal rigidity, these elimination ideals $I(n, r, \pi)$ are all non-zero, as π runs over all patterns of size strictly less than $(n - r)^2$.

So the ideal $I(n, r, \pi)$ is nonzero. We'll use effective Nullstellensatz bounds to show that there's a multivariate polynomial of low enough degree, and then use Galois theory to show that it cannot vanish on the roots of unity constructed. Therefore, the matrix with entries $A_{ij} = e^{2\pi\sqrt{-1}/p_{ij}}$ does not lie in $V(I(n, r, \pi))$ for any π, and therefore has maximal rigidity.

Hypersurfaces

In fact, we can show pretty easily that the corresponding union of subvarieties $V(I(n, r, \pi))$ is a (reducible) hypersurface.

Explicit equations for these, or understanding of their geometry, might be useful in trying to understand why some families of matrices (e.g. Vandermonde) seem to have maximal rigidity.

Hypersurfaces

In fact, we can show pretty easily that the corresponding union of subvarieties $V(I(n, r, \pi))$ is a (reducible) hypersurface.

Explicit equations for these, or understanding of their geometry, might be useful in trying to understand why some families of matrices (e.g. Vandermonde) seem to have maximal rigidity.

Effective Nullstellensatz

We'll use the following bounds, which rely on the *Bezout inequality* for degrees proved by Heintz (1983)

Theorem (Dickenstein, Fitchas, Giusti, Sessa '91)

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 $Z = \{y_{i_1}, \ldots, y_{i_\ell}\} \subset Y$ 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 $\deg(g_i f_i) \leq d^m(d^m + 1)$, where $d = \max(d_{max}, 3)$.

Applying it to our situation, where $d = r + 1$ and $m = n^2$, we get a bound of $\Delta(n) = 2n^{2n^2}$ for the total degree of g.

Effective Nullstellensatz

We'll use the following bounds, which rely on the *Bezout inequality* for degrees proved by Heintz (1983)

Theorem (Dickenstein, Fitchas, Giusti, Sessa '91)

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 $Z = \{y_{i_1}, \ldots, y_{i_\ell}\} \subset Y$ 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 $\deg(g_i f_i) \leq d^m(d^m + 1)$, where $d = \max(d_{max}, 3)$.

Applying it to our situation, where $d = r + 1$ and $m = n^2$, we get a bound of $\Delta(n) = 2n^{2n^2}$ for the total degree of g.

Roots of unity

Finally, we have the following lemma.

Lemma

Let N be a positive integer, and $\theta_1, \ldots, \theta_m$ be algebraic numbers such that $\mathbb{Q}(\theta_i)$ is Galois over $\mathbb{Q}$ and such that

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

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

The proof is easy by induction, using the linear disjointness property.

Conclusion of proof

To finish the proof of the theorem, we note that choosing distinct primes p_{ij} for $1 \leq i, j \leq n$, and setting $\theta_{ij} = \zeta_{p_{ij}} := e^{2\pi\sqrt{-1}/p_{ij}}$, the linear disjointness property is satisfied. So we just need to make sure that $p_{ij} - 1 > \Delta(n) := 2n^{2n^2}$.

If we want real matrices, we can take $\theta_{ij} = \zeta_{p_{ij}} + \zeta_{p_{ij}}^{-1}$, these generate the totally real subfields of the cyclotomic fields, so we just need to ensure, $(p_{ij} - 1)/2 > \Delta(n)$.

Of course, this falls far short of our desired goal, since the roots of unity have very high degree. What we would like is to have rational entries, and preferably some systematic family of these.

Conclusion of proof

To finish the proof of the theorem, we note that choosing distinct primes p_{ij} for $1 \leq i, j \leq n$, and setting $\theta_{ij} = \zeta_{p_{ij}} := e^{2\pi\sqrt{-1}/p_{ij}}$, the linear disjointness property is satisfied. So we just need to make sure that $p_{ij} - 1 > \Delta(n) := 2n^{2n^2}$.

If we want real matrices, we can take $\theta_{ij} = \zeta_{p_{ij}} + \zeta_{p_{ij}}^{-1}$, these generate the totally real subfields of the cyclotomic fields, so we just need to ensure, $(p_{ij} - 1)/2 > \Delta(n)$.

Of course, this falls far short of our desired goal, since the roots of unity have very high degree. What we would like is to have rational entries, and preferably some systematic family of these.

Conclusion of proof

To finish the proof of the theorem, we note that choosing distinct primes p_{ij} for $1 \leq i, j \leq n$, and setting $\theta_{ij} = \zeta_{p_{ij}} := e^{2\pi\sqrt{-1}/p_{ij}}$, the linear disjointness property is satisfied. So we just need to make sure that $p_{ij} - 1 > \Delta(n) := 2n^{2n^2}$.

If we want real matrices, we can take $\theta_{ij} = \zeta_{p_{ij}} + \zeta_{p_{ij}}^{-1}$, these generate the totally real subfields of the cyclotomic fields, so we just need to ensure, $(p_{ij} - 1)/2 > \Delta(n)$.

Of course, this falls far short of our desired goal, since the roots of unity have very high degree. What we would like is to have rational entries, and preferably some systematic family of these.

Semicontinuity?

One approach to constructing rigid matrices over the rationals is by constructing rigid matrices over some totally real extension (as we have just done), and then approximating these real numbers by rational numbers, hoping that rigidity does not change.

This will work reasonably well in our situation, since we've actually constructed a matrix with a Zariski neighborhood (and therefore Euclidean neighborhood) disjoint from the less-than-maximally-rigid locus.

But one might wonder whether some kind of semicontinuity property holds for rigidity in general, as it holds for the rank function of matrices. We would like it if $\mathrm{Rig}(A, r) \geq \ell$, that the same held true in a neighborhood of A.

Semicontinuity?

One approach to constructing rigid matrices over the rationals is by constructing rigid matrices over some totally real extension (as we have just done), and then approximating these real numbers by rational numbers, hoping that rigidity does not change.

This will work reasonably well in our situation, since we've actually constructed a matrix with a Zariski neighborhood (and therefore Euclidean neighborhood) disjoint from the less-than-maximally-rigid locus.

But one might wonder whether some kind of semicontinuity property holds for rigidity in general, as it holds for the rank function of matrices. We would like it if $\mathrm{Rig}(A, r) \geq \ell$, that the same held true in a neighborhood of A.

Semicontinuity?

One approach to constructing rigid matrices over the rationals is by constructing rigid matrices over some totally real extension (as we have just done), and then approximating these real numbers by rational numbers, hoping that rigidity does not change.

This will work reasonably well in our situation, since we've actually constructed a matrix with a Zariski neighborhood (and therefore Euclidean neighborhood) disjoint from the less-than-maximally-rigid locus.

But one might wonder whether some kind of semicontinuity property holds for rigidity in general, as it holds for the rank function of matrices. We would like it if $\mathrm{Rig}(A, r) \geq \ell$, that the same held true in a neighborhood of A.

Examples I

Unfortunately, this expectation is false. Let a, b, c, d, e be non-zero rational numbers. Consider

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

We have $\text{rank}(A) = 2$; $\text{Rig}(A, 1) = 2$.

Examples II

Now, for any $\epsilon > 0$ let

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

Change a to $\frac{1}{\delta}$, rank of the matrix goes down to 1. $\mathrm{Rig}(A(\delta), 1) = 1$.

Examples III

One can even produce such counterexamples which are maximally rigid. For instance,

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

has $\mathrm{Rig}(A, 1) = 4 = (3-1)^2$.

Examples IV

But

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

has rigidity $\mathrm{Rig}(A(\delta), 1) = 3$, since one can change the diagonal entries to get

$$B = \begin{bmatrix} 1/\delta & b & c \\ d & bd\delta & cd\delta \\ e & bg\delta & cg\delta \end{bmatrix}$$

Some more thoughts, questions

Perhaps we can try to use similar techniques to show that the elimination ideals do not contain the ideal of the locus of Vandermonde matrices. Rational normal curves?

Can we systematically improve the bounds for effective Nullstellensatz, with some hypothesis on the degrees or type of generators. For example, for elimination ideals of determinantal ideals.

Coming back to the Valiant example of totally regular matrices with low rigidity, can we find explicit examples of these, using algebraic geometry rather than graph theory?

Some more thoughts, questions

Perhaps we can try to use similar techniques to show that the elimination ideals do not contain the ideal of the locus of Vandermonde matrices. Rational normal curves?

Can we systematically improve the bounds for effective Nullstellensatz, with some hypothesis on the degrees or type of generators. For example, for elimination ideals of determinantal ideals.

Coming back to the Valiant example of totally regular matrices with low rigidity, can we find explicit examples of these, using algebraic geometry rather than graph theory?

Some more thoughts, questions

Perhaps we can try to use similar techniques to show that the elimination ideals do not contain the ideal of the locus of Vandermonde matrices. Rational normal curves?

Can we systematically improve the bounds for effective Nullstellensatz, with some hypothesis on the degrees or type of generators. For example, for elimination ideals of determinantal ideals.

Coming back to the Valiant example of totally regular matrices with low rigidity, can we find explicit examples of these, using algebraic geometry rather than graph theory?

Reference: "Using Elimination Theory to construct Rigid Matrices", Abhinav Kumar, Satya V. Lokam, Vijay M. Patankar and Jayalal Sarma M.N. arXiv:0910.5301.

Thank you!