POLYNOMIAL DEGREE BOUNDS ON EQUATIONS FOR NON-RIGID MATRICES

WITH APPLICATIONS TO CIRCUIT LOWER BOUNDS

Mrinal Kumar
IIT Bombay

Ben Lee Volk
UT Austin

A NOTE ON EXPLICITNESS

In this talk, we'll study rigid matrices over $\mathbb{C}$.

(things also make sense over positive characteristic, but let's not worry about it.)

A necessary requirement for **explicitness** of a matrix is that its entries are integers or rationals with small bit complexity.

We want a matrix that can't be decomposed as low rank + sparse, even when "low rank" and "sparse" contain arbitrary complex entries.

The first step is to verify that such matrices even exist (non explicitly).

Fortunately, this is true, even for $\{0,1\}$ matrices. **[Pudlák-Rödl, Hrubeš-Yehudayoff]**

AN ALGEBRAIC GEOMETRIC APPROACH TO MATRIX RIGIDITY

What can we say about polynomials vanishing on $\overline{\text{non-rigid matrices}}$?

IDEALS AND VARIETIES

A set $V \subseteq \mathbb{C}^N$ is a **variety** if there are polynomials $f_1, \ldots, f_t \in \mathbb{C}[x_1, \ldots, x_N]$ such that

$$V = \left\{ x \in \mathbb{C}^N : f_1(x) = f_2(x) = \cdots = f_t(x) = 0 \right\}.$$

Each variety corresponds to an ideal

$$\mathbf{I}(V) = \{ f \in \mathbb{C}[x_1, \ldots, x_N] : f \text{ vanishes on } V \}.$$

Each ideal $I \subseteq \mathbb{C}[x_1, \ldots, x_N]$ corresponds to a variety

$$\mathbf{V}(I) = \{ x \in \mathbb{C}^n : f(x) = 0 \text{ for all } f \in I \}.$$

CLOSURE

Given an arbitrary set $A \subseteq \mathbb{C}^N$, similarly let $\mathbf{I}(A)$ be the ideal of polynomials vanishing on A.

The set $\mathbf{V}(\mathbf{I}(A))$ is called the **Zariski closure** of A, and denoted $\overline{A}$.

In words: $\overline{A}$ is the set of common zeros of all polynomials vanishing on A.

$\overline{A}$ is the smallest variety containing A.

In algebraic complexity we study sets A corresponding to low complexity objects: non-rigid matrices, low-rank tensors, polynomials with small circuits, ...

For such sets: $\overline{A} =$ Euclidean closure of A.

EQUATIONS FOR VARIETIES

$A \subseteq \mathbb{C}^N$ is a set of low complexity algebraic objects (non-rigid matrices, low-rank tensors, coefficient vectors of polynomials with small circuits)

A non-zero polynomial $P \in \mathbf{I}(A)$ is called an **equation** for A.

Such a P may serve as a "proof" that a point $v \in \mathbb{C}^N$ is **not** in A:

$$P(v) \neq 0 \implies v \text{ has high complexity}$$

This is an algebraic proof for a lower bound.

Note that $P(v) \neq 0$ actually implies $v \notin \overline{A}$.

ALGEBRAIC NATURAL PROOFS

An algebraic proof is **natural** if P has low complexity **[FSV17, GKSS17]**.

(Formally: P has degree $\mathsf{poly}(N)$ and can be computed by an arithmetic circuit of size $\mathsf{poly}(N)$, where $N =$ # vars of P)

Algebraic natural proofs exist for many limited models of computation. We don't know if they exist for strong classes of algebraic computation (for example, the class of polynomial size arithmetic circuits).

Some people conjecture they don't exist ("natural proofs barrier")

This question of whether they exists is also, in some sense, the algebraic analog of the boolean MCSP problem.

Are there natural proofs for rigidity?

PREVIOUS RESULTS

Thm: [KLPS14, GHIL16] there's an equation for rigidity of exponential degree.

More formally: whenever $s < (n-r)^2$, there's a nonzero n^2-variate polynomial of degree at most n^{4n^2} which is zero on all matrices which are not (r,s)-rigid.

As a corollary, they construct a matrix with algebraic numbers which is optimally rigid (just take n^2 numbers which don't have any low-degree polynomial relation).

Conjecture: [GHIL16] For some $\varepsilon > 0$, there's an equation for matrices which are not $(\varepsilon n, n^{1+\varepsilon})$-rigid, of degree $\mathrm{poly}(n)$.

This talk: the conjecture is true.

NEW DEGREE BOUNDS

Thm: there's an equation for matrices which are not $(\varepsilon n, \varepsilon n^2)$-rigid, of degree at most n^3.

In fact, a $\mathrm{poly}(n)$ degree bound applies to a much larger class of matrices:

Thm: there's an equation of degree $\mathrm{poly}(n)$ for matrices computed by a linear circuit of size at most εn^2.

Similar theorems for low-rank 3-dim tensors and other related models.

The proof is non-explicit and doesn't produce an explicit equation P.

If there's an explicit P, this is great news for circuit lower bounds.

If there isn't an explicit P, this is also great news for circuit lower bounds.

DEGREE BOUNDS FOR NON-RIGID MATRICES

Thm: there's an equation of deg $\leq n^3$ for non-$(\varepsilon n, \varepsilon n^2)$-rigid matrices.

Lemma: There's a polynomial map $Q : \mathbb{C}^{4\varepsilon n^2} \to \mathbb{C}^{n \times n}$ of degree n^2 whose image contains all matrices which are not $(\varepsilon n, \varepsilon n^2)$-rigid.

Proof of Thm (assuming Lemma):

n^2-variate polynomials of degree $\leq n^3$	$\longrightarrow$	$4\varepsilon n^2$-variate polynomials of degree $\leq n^5$
P	$\mapsto$	$P \circ Q$
dim = $\binom{n^3+n^2}{n^2}$	$>$	dim = $\binom{n^5+4\varepsilon n^2}{4\varepsilon n^2}$

$\implies \exists P_0 \neq 0$ such that $P_0 \circ Q \equiv 0$. So $\forall$ non-rigid M, $P_0(M) = P_0(Q(v)) = 0$. $\square$

UNIVERSAL MAPS FOR NON-RIGID MATRICES

Lemma: There's a polynomial map $Q : \mathbb{C}^{4\varepsilon n^2} \to \mathbb{C}^{n \times n}$ of degree n^2 whose image contains all matrices which are not $(\varepsilon n, \varepsilon n^2)$-rigid.

Part 1: Construct $Q_1 : \mathbb{C}^{2\varepsilon n^2} \to \mathbb{C}^{n \times n}$ of degree 2 whose image contains all matrices of rank at most εn.

Part 2: Construct $Q_2 : \mathbb{C}^{2\varepsilon n^2} \to \mathbb{C}^{n \times n}$ of degree n^2 whose image contains all εn^2-sparse matrices.

Then $Q = Q_1 + Q_2$.

Construction of Q_1: Let U be an $n \times \varepsilon n$ matrix of formal variables, and similarly V an $\varepsilon n \times n$. Define Q_1 as matrix multiplication UV.

i.e., $Q_1 : \mathbb{C}^{2\varepsilon n^2} \to \mathbb{C}^{n \times n}$ defined by $(Q_1)_{i,j} = \sum_{k=1}^{\varepsilon n} u_{i,k} v_{k,j}$ for $i, j \in [n]$.

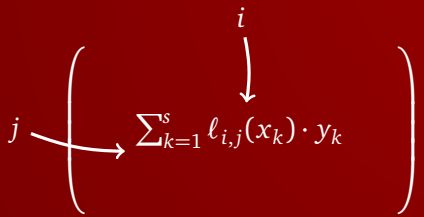
UNIVERSAL MAP FOR SPARSE MATRICES

Part 2: $Q_2 : \mathbb{C}^{2s} \to \mathbb{C}^{n \times n}$, deg $\leq n^2$, image contains all s-sparse matrices.

Turns out this is already done by **[Shpilka-Volkovich]**

Pick distinct $\alpha_{i,j} \in \mathbb{C}$ and let $\ell_{i,j}(z)$ be the Lagrange interpolation polynomials

$$\ell_{i,j}(z) = \begin{cases} 1 & \text{if } z = \alpha_{i,j} \\ 0 & \text{if } z = \alpha_{i',j'} \text{ for } (i',j') \neq (i,j) \end{cases} = \frac{\prod_{(i',j') \neq (i,j)} (z - \alpha_{i',j'})}{\prod_{(i',j') \neq (i,j)} (\alpha_{i,j} - \alpha_{i',j'})}$$



vars: $x_1, \ldots, x_s, y_1, \ldots, y_s$
to put $\beta_1, \ldots \beta_s$ in $(i_1, j_1), \ldots, (i_s, j_s)$
(and zero elsewhere):
set $x_k = \alpha_{i_k, j_k}$ and $y_k = \beta_k$.

UNIVERSAL MAP FOR LINEAR CIRCUITS

We construct a map $Q : \mathbb{C}^{2\varepsilon n^2} \to \mathbb{C}^{n \times n}$ of degree $\leq n^{10}$ whose image contains all matrices which can be computed by a linear circuit of size at most εn^2.

(As before, this implies a polynomial degree bound for equations for this variety)

The idea is to use a **universal circuit** for size s: this is a "generic" circuit graph with fresh variables as edge labels, that contains all size s circuits as subcircuits.

This results in a $\mathrm{poly}(s)$ blow-up in the circuit size, which is usually fine but not in this case, since we must keep the number of variables significantly smaller than n^2.

But a similar idea using the Shpilka-Volkovich map solves this problem.

Exactly the same idea also works for 3d tensors of small rank, small slice rank, etc.

CIRCUIT LOWER BOUNDS

Thm: Suppose PIT ∈ P. Then at least one of the following is true:

1. There's a PSPACE algorithm which outputs a polynomial family not in VP.
2. There's an efficient construction of $(\varepsilon n, \varepsilon n^2)$-rigid matrices, with an NP oracle.

(compare with **[Kabanets-Impagliazzo]**)

(also compare with recent constructions of somewhat-rigid matrices with an NP oracle: **[Alman-Chen, Bhangale-Harsha-Paradise-Tal]**)

Option 1 is true if the equations we found for non-rigid matrices are hard.

Option 2 is true if PIT ∈ P and these equations are easy.

(actually even if PIT ∈ NP)

PROOF SKETCH

The equations we find are solutions to a linear system of exponential size and we can output a solution in PSPACE using standard small-space algorithm for linear algebra.

If this is a family of hard polynomials, we're done.

If they are easy and PIT $\in$ P:

1. guess a small circuit for the equation P
2. verify (deterministically) using PIT algorithm
3. find a matrix M such that $P(M) \neq 0$

all can be done deterministically using an NP oracle

(there are some technical problems to solve)

OPEN PROBLEMS

- are there explicit equations?
- even if not, can the degree bound help in construction of rigid matrices?
- first step could be figuring out equations for very small instances and trying to generalize
- further applications of “border rigidity?”

Thank You.