Matrix Rigidity

Shoup-Smolensky dimension and Rigidity

Sasha Golovnev

September 23, 2020

Goal

- Know: n^2 algebraically independent entries form rigid matrix

Goal

- Know: n^2 algebraically independent entries form rigid matrix
- Will show: just n algebraically independent entries are sufficient for (moderate) rigidity

n^2 random entries $\rightarrow$ rigid

n random bits - dream $\rightarrow$ 2^n brute force

GOAL

- Know: n^2 algebraically independent entries form rigid matrix

I

- Will show: just n algebraically independent entries are sufficient for (moderate) rigidity

II

- Will show: linear independence is sufficient for (high) rigidity

ne

$\sqrt{2}$ $\sqrt{3}$ $\sqrt{5}$ $\sqrt{6}$ $\sqrt{7}$ – lin

$e^{\sqrt{2}}$ $e^{\sqrt{3}}$ $e^{\sqrt{5}}$ $e^{\sqrt{6}}$ $e^{\sqrt{7}}$

Linearly Independent Numbers

Definition

$x_1, \ldots, x_n \in \mathbb{R}$ are linearly independent over $\mathbb{Q}$ if they do not satisfy any non-trivial linear equation with coefficient in $\mathbb{Q}$:

$$k_1 x_1 + \ldots + k_n x_n \neq 0 \,.$$

for all $k_1, \ldots, k_n \in \mathbb{Q}$ except $k_1 = \ldots = k_n = 0$.

Linearly Independent Numbers

Definition

$x_1, \ldots, x_n \in \mathbb{R}$ are linearly independent over $\mathbb{Q}$ if they do not satisfy any non-trivial linear equation with coefficient in $\mathbb{Q}$:

$$k_1 x_1 + \ldots + k_n x_n \neq 0\,.$$

for all $k_1, \ldots, k_n \in \mathbb{Q}$ except $k_1 = \ldots = k_n = 0$.

Example

$\{1, \alpha\}$ are linearly independent over $\mathbb{Q}$ iff α is irrational.

$k_1 \cdot 1 + k_2 \cdot \alpha = 0$ $\quad k_1, k_2 \in \mathbb{Q}$

$\Rightarrow \alpha = \frac{-k_1}{k_2} \in \mathbb{Q}$

Besicovitch Theorem

Theorem (Besicovitch)

Let $a_1, a_2, \dots, a_m$ be m distinct square roots of square-free integers, then they are all linearly independent over $\mathbb{Q}$.

$1 \quad \sqrt{2} \quad \sqrt{3} \quad \sqrt{5} \quad \sqrt{6} \quad \sqrt{7} \quad \sqrt{10}$

Algebraically Independent Numbers

Definition

$x_1, \ldots, x_n \in \mathbb{R}$ are algebraically independent over $\mathbb{Q}$ if they do not satisfy any non-trivial polynomial equation with coefficient in $\mathbb{Q}$.

Algebraically Independent Numbers

Definition

$x_1, \ldots, x_n \in \mathbb{R}$ are algebraically independent over $\mathbb{Q}$ if they do not satisfy any non-trivial polynomial equation with coefficient in $\mathbb{Q}$.

Examples

- $\{\pi, e^\pi\}$ are algebraically independent over $\mathbb{Q}$

Algebraically Independent Numbers

Definition

$x_1, \ldots, x_n \in \mathbb{R}$ are algebraically independent over $\mathbb{Q}$ if they do not satisfy any non-trivial polynomial equation with coefficient in $\mathbb{Q}$.

Examples

- $\{\pi, e^\pi\}$ are algebraically independent over $\mathbb{Q}$
- $\{\overset{x_1=}{\sqrt{e+7}}, \overset{x_2=}{e^3+1}\}$ are not algebraically independent over $\mathbb{Q}$

$P_1(x_1, x_2) = (x_1^2 - 7)^3 + 1 - x_2$

Algebraically Independent Numbers

Definition

$x_1, \ldots, x_n \in \mathbb{R}$ are algebraically independent over $\mathbb{Q}$ if they do not satisfy any non-trivial polynomial equation with coefficient in $\mathbb{Q}$.

Examples

- $\{\pi, e^\pi\}$ are algebraically independent over $\mathbb{Q}$
- $\{\sqrt{e+7}, e^3+1\}$ are not algebraically independent over $\mathbb{Q}$

$\{e, \pi\}$—open question!

LW

$x_1, \ldots, x_n$ – lin ind

e^{x_1} ... e^{x_n} – alg ind

Construction I: n algebraically independent entries

Vandermonde Matrix

$x_1, \dots, x_n \in \mathbb{F}$

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \hdotsfor{5} \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{pmatrix}$$

$$V_{i,j} = x_i^{j-1}$$

Vandermonde determinant

$$\det(V) = \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \hdotsfor{5} \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix} = \prod_{1 \le j < i \le n} (x_i - x_j)$$

Vandermonde determinant

$$\det(V) = \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \hdotsfor{5} \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix} = \prod_{1 \leq j < i \leq n} (x_i - x_j)$$

If x_i are distinct, then $\det(V) \neq 0$

Rigidity of Vandermonde

Theorem

Let $\mathbb{F}$ be a field containing at least n distinct elements $x_1, \ldots, x_n$. Let V be a Vandermond matrix with $V_{i,j} = x_i^{j-1}$. Then

$$\mathcal{R}_V^{\mathbb{F}}(r) \geq \Omega(n^2/r) \,.$$

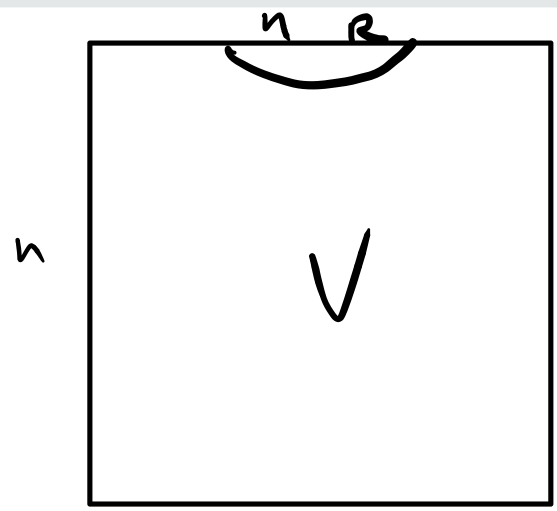
Theorem

Let $\mathbb{F}$ be a field containing at least n distinct elements $x_1, \ldots, x_n$. Let V be a Vandermond matrix with $V_{i,j} = x_i^{j-1}$. Then

$$\mathcal{R}_V^{\mathbb{F}}(r) \geq \Omega(n^2/r).$$

Change S entries in V.

R consecutive cols with a few changes.



$1 \leq k \leq n-R+1$ s.t.

$\mathrm{Col}_k, \mathrm{Col}_{k+1}, \ldots, \mathrm{Col}_{k+R-1}$

together have $\leq \dfrac{S \cdot R}{n-R+1}$ changes

$i \in [n]$ $\quad C_i = \#$ changes in Col_i.

$T_1 = \{C_1, \ldots, C_R\}$ $\quad$ - - - -

$T_2 = \{C_2, \ldots, C_{R+1}\}$ $\quad T_{n-R+1} = \{C_{n-R+1}, \ldots, C_n$

$T_3 = \{C_3, \ldots, C_{R+2}\}$

$i \in [n]$ $\quad C_i = \#$ changes in Col i.

$T_1 = \{C_1, \ldots, C_R\}$ $\quad - - - -$

$T_2 = \{C_2, \ldots, C_{R+1}\}$ $\quad T_{n-R+1} = \{C_{n-R+1}$

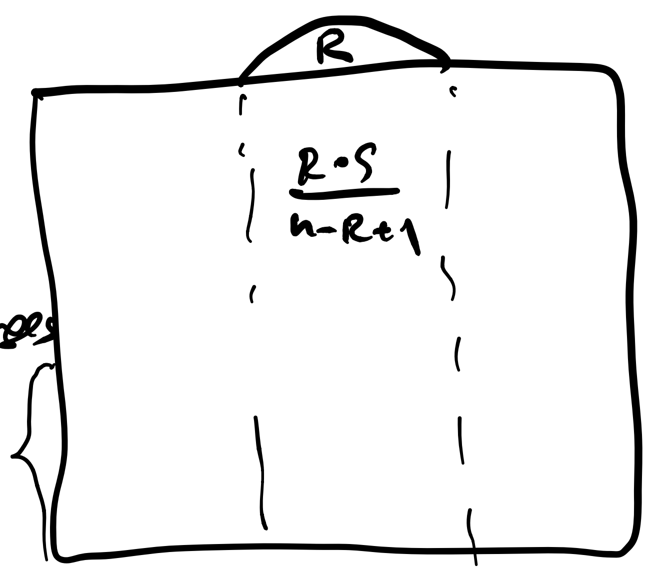
$T_3 = \{C_3, \ldots, C_{R+2}\}$

$$\sum_{i=1}^{n-R+1} T_i \le R \cdot \sum_{i=1}^{n} C_i = R \cdot S$$

= total # of changes

$$\Downarrow \ \exists k \in \{1, \ldots, n-R+1\}$$

$$T_i \le \frac{R \cdot S}{n-R+1}$$



pick rows without changes

at least $n - \frac{S \cdot R}{n-R+1}$ such rows

If $n - \frac{S \cdot R}{n-R+1} \geq R$

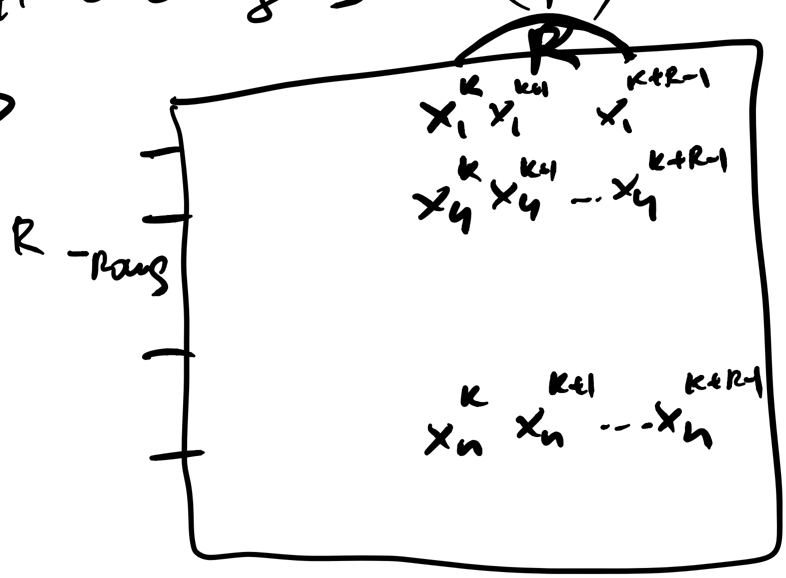
$$\Updownarrow$$

$$\frac{S \cdot R}{n-R+1} \leq n-R$$

$$S \leq \frac{(n-R)(n-R+1)}{R} = \Theta\left(\frac{n^2}{R}\right)$$

If # changes $\leq \Theta\left(\frac{n^2}{R}\right)$

$\Rightarrow$



$$\mathrm{Rk}\begin{pmatrix} x_1^k & x_1^{k+1} & \cdots & x_1^{k+R-1} \\ \\ x_R^k & x_R^{k+1} & \cdots & x_R^{k+R-1} \end{pmatrix} =$$

Vandermonde

$$= \mathrm{Rk}\begin{pmatrix} 1 & x_1 & x_1^{R-1} \\ \\ 1 & x_R & x_R^{R-1} \end{pmatrix} = R$$

We assumed that we made $s = O\left(\frac{n^2}{R}\right)$ changes, then found full-rank $R \times R$ submatrix $\Rightarrow$ Even after s changes rank $\geq R$ $\Rightarrow$

$$\mathrm{Rig}(V) \geq \left(R, \frac{n^2}{R}\right)$$

Main Theorem

Best expl rig $\frac{n^2}{R}\log\left(\frac{n}{R}\right)$

Ex. $R=\sqrt{n}$, best $n^{3/2}\log n$

Theorem

Let $x_1, \ldots, x_n$ be algebraically independent over $\mathbb{Q}$, and $V_{i,j} = x_i^{j-1}$. Then for every $1 \leq r \leq \frac{\sqrt{n}}{10}$,

$$\mathcal{R}_V^{\mathbb{C}}(r) \geq n(n - 100 \cdot r^2)/2\,.$$

$R = \frac{\sqrt{n}}{100}$ $\quad R(R) \geq \Omega(n^2)$

Proof Outline

t-Shoup-Smolensky

- Define a complexity measure (dim_t^{SS})

Proof Outline

- Define a complexity measure (dim_t^{SS})
- Prove that for low $\mathsf{rank}(L) \implies$ low $\mathsf{dim}_t^{SS}(L)$

Proof Outline

- Define a complexity measure ($\mathbf{dim}_t^{SS}$) ✓
- Prove that for low $\mathbf{rank}(L) \implies$ low $\mathbf{dim}_t^{SS}(L)$
- Prove that for any sparse S, $\mathbf{dim}_t^{SS}(V - S)$ is high

Shoup-Smolensky Dimension

measures "algebraic independence"

polys of degree t of entries A.

Definition

For any $t, n \in \mathbb{N}$ and $A \in \mathbb{C}^{n \times n}$. The *$t$-Shoup-Smolensky dimension of A*, $\dim_t^{SS}(A)$, is the dimension of the vector space over $\mathbb{Q}$ spanned by product of t distinct elements of A.

$A = \{\sqrt{2}\}$ $\quad \dim_{\mathbb{Q}} = 1$, because $\sqrt{2}$ spans A.

$A = \{\sqrt{2}, \sqrt{8}\}$ $\quad \dim_{\mathbb{Q}} = 1$, $\sqrt{2}$ spans A.

$A = \{\sqrt{2}, \sqrt{3}\}$ $\quad \dim_{\mathbb{Q}} = 2$, $\{\sqrt{2}, \sqrt{3}\}$ spans A.

t- SS dim

$\boxed{A}$, take products of t- tuples of els A.

$\Downarrow$

gives a set of numbers.

$$\dim_t^{ss}(A) = \dim_{\mathbb{Q}} \text{ of this set of numbers.}$$

$$A = \begin{bmatrix} 1 & \sqrt{2} \\ \sqrt{3} & 2 \end{bmatrix}$$

1-SS-dim $\quad B_1 = \{1, \sqrt{2}, \sqrt{3}, 2\}$

$$\dim_1^{ss}(A) = \dim(B_1) = 3$$

2-SS-dim $\quad B_2 = \{1, \sqrt{2}, \sqrt{3}, 2, \sqrt{6}, 2\sqrt{2}, 2\sqrt{3}\}$

$$\dim_2^{ss}(A) = \dim(B_2) = 4$$

$$A = \begin{bmatrix} 1 & \sqrt{2} \\ \sqrt{3} & \sqrt{6} \end{bmatrix}$$

1-SS-dim $\quad B_1 = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$

$$\dim_1^{SS}(A) = \dim(B_1) = 4$$

2-SS-dim $\quad B_2 = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}, \sqrt{6}, \sqrt{12} = 2\sqrt{3}, \sqrt{18} = 3\sqrt{2}\}$

$$\dim_2^{SS}(A) = \dim(B_2) = 4$$

SS Dimension of L

Step 1: $\dim_t^{SS}$ of low-rank is low

Lemma

For any $t, n \in \mathbb{N}$ and $L \in \mathbb{C}^{n\times n}$. Let $r = \operatorname{rank}(L)$, we have

$$\dim_t^{SS}(L) \leq \binom{nr+t}{t}^2.$$

Lemma

For any $t, n \in \mathbb{N}$ and $L \in \mathbb{C}^{n\times n}$. Let $r = \mathrm{rank}(L)$, we have

$$\dim_t^{SS}(L) \le \binom{nr+t}{t}^2.$$

$$ {}_{n}\overset{n}{\boxed{L}} = {}_{n}\overset{R}{\boxed{X}} \cdot {}_{R}\overset{n}{\boxed{Y}} $$

$$L_{ij} = \sum_{k=1}^{R} x_{ik} \cdot y_{kj}$$

$$\prod_{\{i,j\}\in T} L_{i,j} = \prod_{t} \sum x_{ik} y_{kj} =$$

$$= \sum \text{monomials}$$

each mon is of deg $2t$, t xs, t ys.

$$\dim_t^{SS}(L) = \dim \prod_{\{i,j\}\in T} L_{i,j} \le$$

$$\le \dim \left[\begin{array}{l}\text{monomials of deg } 2t, \\ t \ x\text{s} \ \& \ t \ y\text{s}\end{array}\right]$$

deg $2t$ mon with t xs and t ys
= product of degree-t monomial in x
and degree-t monomial in y.

$$\left(\le \dim \begin{bmatrix} \text{degree-}t \text{ monomials} \\ \text{in } x \end{bmatrix} \cdot \dim \begin{bmatrix} \text{degree-}t \text{ monomials} \\ \text{in } y \end{bmatrix} \right)$$

$\le$ # of distinct monomials of deg $2t$
w/ t xs and t ys.
$\le$ (# of degree-t mon in x)
$\cdot$ (# of degree-t mon in y).

m variables, monomials of deg $\leq t$.

$x_1, \ldots, x_m, 1$

exactly t from here with repetitions.

x_1, x_1, x_2 $\quad$ $x_1^2 \cdot x_2$

$x_1, 1, 1$ $\quad$ x_1

Choose t from $m+1$ objects
with repetitions.

Combinations with repetitions

$$\left(\!\!\binom{m+1}{t}\!\!\right)$$

$$\left(\!\!\binom{n}{k}\!\!\right) = \binom{n+k-1}{k}$$

$n=4$ $\quad$ $k=2$

Combinations

12 $\quad$ 23
13 $\quad$ 24
14 $\quad$ 34

$$\binom{4}{2} = \frac{4!}{2!\,2!} = 6$$

$$\left(\!\!\binom{4}{2}\!\!\right)$$

11 22 34
12 23 44
13 24
14 33

$$\left(\!\!\binom{4}{2}\!\!\right) = \binom{4+2-1}{2} = \binom{5}{2} = \frac{5!}{3!\,2!} = 10$$

$$\left(\!\!\binom{n}{k}\!\!\right) = \binom{n+k-1}{k}$$

# of mon of m vars of deg $\le t$ is

Combinations with repetitions

$$\left(\!\!\binom{m+1}{t}\!\!\right) \le \binom{m+1+t-1}{t} = \binom{m+t}{t}$$

$$\dim_t^{ss}(L) \leq \binom{\#\text{ mon of } Rn \text{ var of}}{\deg t}^2$$

$$= \binom{Rn+t}{t}^2$$

<u>Thm</u> $\quad rk(L) = R$

$$\Downarrow$$

$$\dim_t^{ss}(L) \leq \binom{Rn+t}{t}^2$$

SS DIMENSION OF $V - S$

Lemma

For any $n \in \mathbb{N}$, $1 \leq t \leq \frac{n}{2}$, and $1 \leq s < tn$. Let V be a Vandermonde matrix with algebraically independent entries and $S \in \mathbb{C}^{n \times n}$ such that $\|S\|_0 \leq s$, then

$$\dim_t^{SS}(V - S) \geq \left(n - \frac{s}{t}\right)^t.$$

Lemma

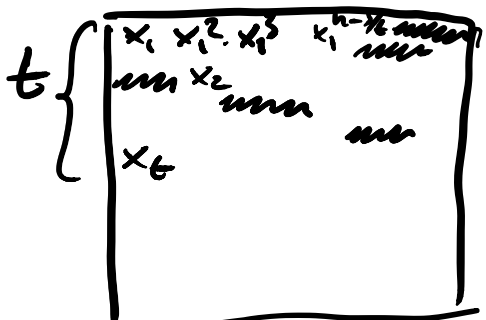
For any $n \in \mathbb{N}$, $1 \le t \le \frac{n}{2}$, and $1 \le s < tn$. Let V be a Vandermonde matrix with algebraically independent entries and $S \in \mathbb{C}^{n\times n}$ such that $\|S\|_0 \le s$, then

$$\dim_t^{SS}(V - S) \ge \left(n - \frac{s}{t}\right)^t.$$

s changes in V

I choose t rows with fewest # of changes.

t rows, each having $\le \frac{s}{t}$ changes



$\le \frac{s}{t}$ changes in these rows

Want take a large system of t-products that are lin ind.

Take any unchanged entry from 1st row

* any unchanged entry 2nd row

* 3rd row

t^{th} row

*

$$\left(n - \frac{s}{t}\right) \cdot \left(n - \frac{s}{t}\right) \cdot \ldots \cdot \left(n - \frac{s}{t}\right) =$$

$$= \left(n - \frac{s}{t}\right)^t$$

x_1 x_1^7

x_2^3 x_2^9

$$\begin{aligned}
&\alpha_1 \cdot x_1 \cdot x_2^3 + \\
&\alpha_2 \cdot x_1 \cdot x_2^9 + \\
&\alpha_3 \cdot x_1^7 \cdot x_2^3 + \\
&\alpha_4 \cdot x_1^7 \cdot x_2^9 = 0
\end{aligned}$$

lin comb

a polynomial in x_1 & x_2

$\Downarrow$

contradicts assumption that x_1 & x_2 are alg ind $\square$

Main Theorem

Theorem

Let $x_1, \ldots, x_n$ be algebraically independent over $\mathbb{Q}$, and $V_{i,j} = x_i^{j-1}$. Then for every $1 \leq r \leq \frac{\sqrt{n}}{10}$,

$$\mathcal{R}_V^{\mathbb{C}}(r) \geq n(n - 100 \cdot r^2)/2 \, .$$

$$\dim_t^{ss}(L) \le \binom{nR+t}{t}^2 \quad (*) \quad \text{Lemma 1}$$

$$\dim_t^{ss}(V-S) \geq \left(n - \frac{s}{t}\right)^t \quad (**) \quad \text{Lemma2}$$

$$t = \frac{n}{2} \qquad s = n(n-100R^2)/2$$

$$(**) > (*)$$

$$(**) = \left(n - \frac{s}{t}\right)^t = \left(n - (n-100R^2)\right)^t$$

$$= (100R^2)^t = (100R^2)^{n/2}$$

$$(*) \le \binom{nR+t}{t}^2 = \binom{nR+\frac{n}{2}}{\frac{n}{2}}^2$$

$$\binom{n}{k} \le \left(\frac{en}{k}\right)^k$$

$$\le \left(\frac{nR+\frac{n}{2}}{\frac{n}{2}}\right)^{2\cdot\frac{n}{2}} = (2R+1)^n$$

$$\le (90R^2)^{n/2} << (**)$$

$\square$