Matrix Rigidity

Shoup-Smolensky dimension and Circuits

Sasha Golovnev

September 28, 2020

Goal

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

Goal

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

$x_1, \dots, x_n$ alg. ind over $\mathbb{Q}$

$$V = \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & & & & \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{bmatrix}$$

$R = \sqrt{n}$

$$R_V(R) \geq \Omega(n^2)$$

To compare w/ expl. bounds:

$$R_V \geq \frac{n^2}{R} \log\left(\frac{n}{R}\right)$$

Goal

- Know: n^2 algebraically independent entries form rigid matrix
- Previous class: just n algebraically independent entries are sufficient for (moderate) rigidity
- Will show: $\overset{n^2}{\text{linear}}$ independence is sufficient for (high) rigidity

$$A \in \mathbb{C}^{n \times n}$$

$$R_A(r) \geq \Omega(n^2) \quad \forall r < \frac{n}{100}$$

Construction I: n algebraically independent entries

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* $1 \leq r \leq \frac{\sqrt{n}}{10}$,

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

Proof Outline

- Define a complexity measure ($\mathbf{dim}_t^{SS}$)

Proof Outline

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

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

$V \neq S + L \Rightarrow$ V is Rigid

Shoup-Smolensky Dimension

Definition

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

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

$t = 2$

$2\text{-}\dim^{ss}(A)$ = dim over $\mathbb{Q}$

$B_2 = \{\sqrt{2}, \sqrt{3}, 2, \sqrt{6}, 2\sqrt{2}, 2\sqrt{3}\}$

$1, \sqrt{2}, \sqrt{3}, \sqrt{6}$

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

Construction II: n^2 linearly independent entries

Main Theorem

Theorem

Let $A \in \mathbb{C}^{n\times n}$ be a matrix with square roots of n^2 distinct primes as its entries. For any $1 \le r \le \frac{n}{32}$,

$$\mathcal{R}_A^{\mathbb{C}}(r) \geq n(n-16r)\,.$$

Theorem

Let $A \in \mathbb{C}^{n\times n}$ be a matrix with square roots of n^2 distinct primes as its entries. For any $1 \le r \le \frac{n}{32}$,

$$\mathcal{R}_A^{\mathbb{C}}(r) \ge n(n-16r)\,.$$

$$A = \begin{bmatrix} 1 & \sqrt{2} & \sqrt{3} & \cdots \\ \sqrt{7} & \sqrt{5} & \sqrt{11} & \\ \sqrt{13} & & & \\ & & & \\ & - & - - - & \end{bmatrix}$$

$R = \frac{n}{32}$

$\mathcal{R}_A^{\mathbb{C}} \geqslant \Omega(n^2)$

Compare it to what we need

for ckt lower bounds: $R = \frac{n}{32}$

$\mathcal{R} \geqslant n^{1+\delta}$

A cannot be computed by linear-size ckts.

But A is not completely explicit, because every entry requires large/infinite precision.

But A has a simple/short description

Proof outline:

1. $\dim_{ss}(L)$ is low ✓
2. $\dim_{ss}(A-S)$ is high
3. $A \neq L+S \Rightarrow$ A is rigid.

SS Dimension of L

Recall from last class:

Lemma

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

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

\# monomials of ~~deg~~ deg t of nr vars is

$\le \binom{nr+t}{t}$; $\dim^{ss}(L) \le (\#\text{ of mons})^2$

SS Dimension of $A - S$

Lemma

Let A be an $n \times n$ matrix with square roots of n^2 distinct primes as its entries, and $S \in \mathbb{C}^{n\times n}$ such that $\|S\|_0 \le s$. For any $1 \le s, t \le n^2$,

$$\mathrm{dim}_t^{SS}(A - S) \ge \binom{n^2 - s}{t}.$$

Besicovitch Theorem

$1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}$ - lin ind over $\mathbb{Q}$

Theorem (Besicovitch)

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

Lemma

Let A be an $n \times n$ matrix with square roots of n^2 distinct primes as its entries, and $S \in \mathbb{C}^{n\times n}$ such that $\|S\|_0 \le s$. For any $1 \le s, t \le n^2$,

$$\dim_t^{SS}(A - S) \ge \binom{n^2 - s}{t}.$$

$A-S$ still has $\geq n^2-s$ square roots of distinct primes.

---

t-SS : t-wise products of entries of $A-S$.

$\binom{n^2-s}{t}$ t-wise products where all t els are square roots of distinct primes.

$\Downarrow$

square roots of distinct primes

By Besicovitch Thm, they all are lin ind over $\mathbb{Q}$

$\Rightarrow \dim_t^{SS}(A-S) \geq \binom{n^2-s}{t}$ $\square$

Main Theorem

Theorem

Let $A \in \mathbb{C}^{n \times n}$ be a matrix with square roots of n^2 distinct primes as its entries. For any $1 \leq r \leq \frac{n}{32}$,

$$\mathcal{R}_A^{\mathbb{C}}(r) \geq n(n - 16r)\,.$$

Theorem

Let $A \in \mathbb{C}^{n\times n}$ be a matrix with square roots of n^2 distinct primes as its entries. For any $1 \le r \le \frac{n}{32}$,

$$\mathcal{R}_A^{\mathbb{C}}(r) \ge n(n-16r)\,.$$

$$s = n(n-16R) = n^2 - 16nR$$

$$t = n\cdot R$$

$$\dim_t^{ss}(L) \le \binom{nR+t}{nR}^2 = \binom{2nR}{nR}^2 < \left(2^{2nR}\right)^2 = 2^{4nR} = 16^{nR}$$

$$\binom{k}{k/2} < 2^k$$

$$\dim_t^{ss}(A-S) \ge \binom{n^2-s}{t} = \binom{16nR}{t} = \binom{16nR}{nR} \ge (16)^{nR}$$

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

$$16^{nR} > \dim_t^{ss}(L)$$

$$\dim_t^{ss}(A-S) \geq 16^{nR} > \dim_t^{ss}(L)$$

$$\Downarrow$$

$$A - S \neq L \Rightarrow$$

A is Rigid $\square$

Shoup-Smolensky Dimension and Circuit Lower Bounds

Rigidity and Circuits

- We study rigidity to prove circuit lower bounds against linear circuits

Rigidity and Circuits

- We study rigidity to prove circuit lower bounds against linear circuits
- Rigidity for rank $n/100$ and sparsity $n^{1.01}$ implies super-linear circuit lower bounds

Rigidity and Circuits

- We study rigidity to prove circuit lower bounds against linear circuits
- Rigidity for rank $n/100$ and sparsity $n^{1.01}$ implies super-linear circuit lower bounds
- Shoup-Smolensky dimension can be directly used to prove a super-linear circuit lower bound against such circuits

Rigidity and Circuits

- We study rigidity to prove circuit lower bounds against linear circuits
- Rigidity for rank $n/100$ and sparsity $n^{1.01}$ implies super-linear circuit lower bounds
- Shoup-Smolensky dimension can be directly used to prove a super-linear circuit lower bound against such circuits $\boxed{\frac{n^2}{\log n}}$
- Alas, for linear functions that are not completely explicit

Shoup-Smolensky Lower Bound

$x \in \mathbb{C}^n$ $\quad$ $y \in \mathbb{C}^n$

$y = \underline{A} \cdot x$

Theorem

Let $A \in \mathbb{C}^{n \times n}$ be a matrix with square roots of n^2 distinct primes as its entries. Any linear circuit computing $x \to Ax$ must have size at least

$$s \geq \Omega(n^2 / \log n) .$$

Proof Outline

- Prove that our matrix A has high $\mathbf{dim}^{SS}_{t}$

$t = n^2$

$$A = \begin{bmatrix} \sqrt{p_1} & \sqrt{p_2} & \\ & & \\ & & \end{bmatrix}$$

t-products are square roots of squarefree numbers => lin ind.

$$\dim^{SS}_{n^2}(A) \geq 2^{n^2}$$

Proof Outline

- Prove that our matrix A has high $\mathbf{dim}^{SS}$
- Prove that small circuits compute $x \to Bx$ only for B with low $\mathbf{dim}^{SS}$

Proof Outline

- Prove that our matrix A has high $\mathbf{dim}^{SS}$
- Prove that small circuits compute $x \to Bx$ only for B with low $\mathbf{dim}^{SS}$
- Conclude that A requires large circuits

Proof

- Prove that $\mathbf{dim}^{SS}_{n^2}(A) \geq 2^{n^2}$ ✓

Proof

- Prove that $\mathbf{dim}_{n^2}^{SS}(A) \geq 2^{n^2}$
- Prove that circuits of size s compute $x \rightarrow Bx$ only for B with $\mathbf{dim}_{n^2}^{SS}(A) \leq (n^2 + s)^s$

Proof

- Prove that $\mathbf{dim}^{SS}_{n^2}(A) \geq 2^{n^2}$ ✓

- Prove that circuits of size s compute $x \to Bx$ only for B with $\mathbf{dim}^{SS}_{n^2}(A) \leq (n^2 + s)^s$

- Conclude that $s \geq \Omega(n^2/\log n)$ ✓

$$(n^2+s)^s \geq \dim^{ss}_{n^2}(A) \geq 2^{n^2}$$

$$\wedge$$

$$(2n^2)^s = 2^{O(s\log n)}$$

$$2^{O(s\log n)} \geq 2^{n^2}$$

$$\Rightarrow s \geq \Omega\left(\frac{n^2}{\log n}\right)$$

Proof

- Prove that $\mathbf{dim}^{SS}_{n^2}(A) \geq 2^{n^2}$
- Prove that circuits of size s compute $x \to Bx$ only for B with $\mathbf{dim}^{SS}_{n^2}(A) \leq (n^2 + s)^s$
- Conclude that $s \geq \Omega(n^2 / \log n)$

Technical Lemma

Lemma

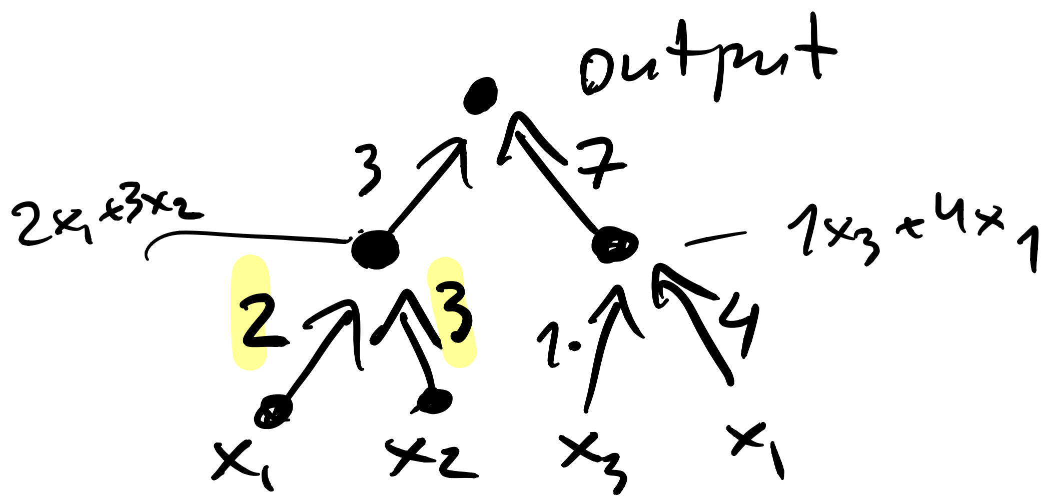
Let C be a linear circuit of size s computing $x \to Bx$ for $B \in \mathbb{C}^{n \times n}$. Then

$$\dim_{n^2}^{SS}(A) \leq \left(n^2 + s\right)^s .$$

Lemma

Let C be a linear circuit of size s computing $x \to Bx$ for $B \in \mathbb{C}^{n \times n}$. Then

$$\underline{\underline{\dim^{SS}_{n^2}(A) \le (n^2+s)^s}}\,.$$



$$\text{output} = 3(2x_1 + 3x_2) + 7(x_3 + 4x_1)$$

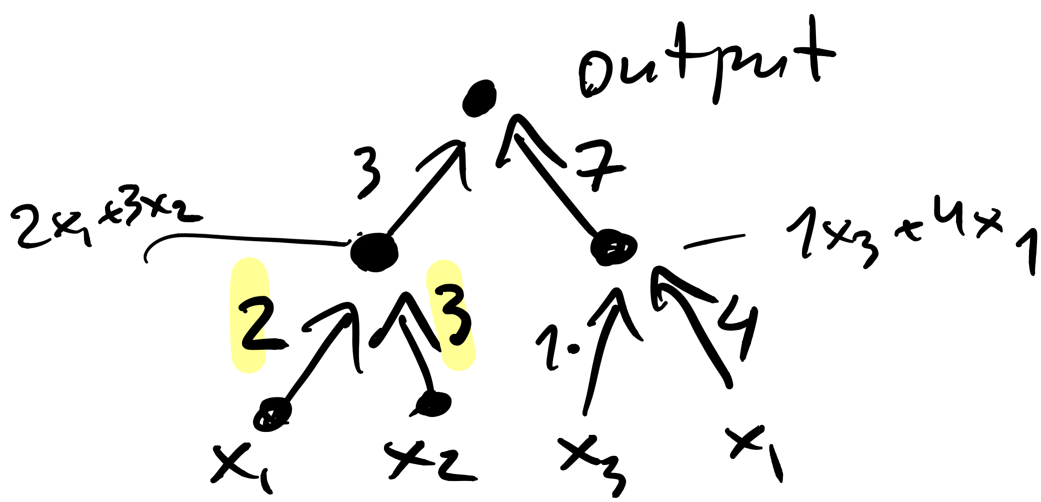
$$x \longrightarrow Bx$$

$$B = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ & & & \\ b_{n1} & & \cdots & b_{nn} \end{bmatrix}$$

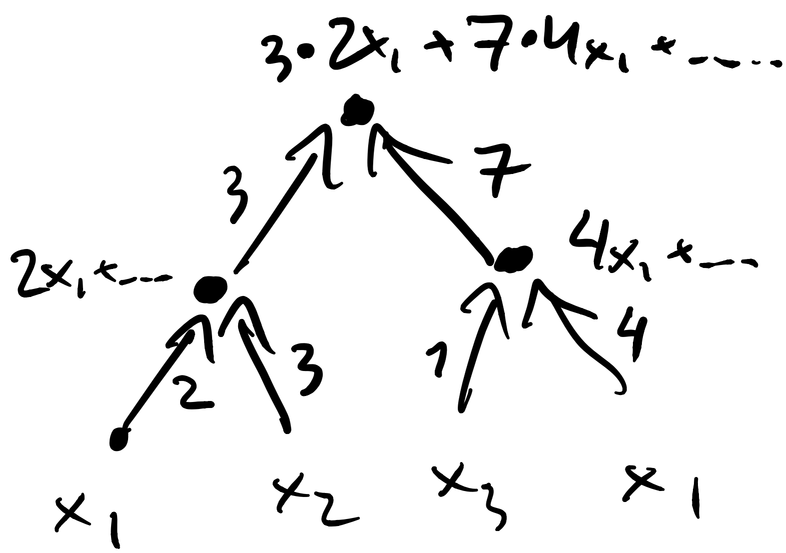
$$Bx = \begin{bmatrix} b_{11}x_1 + b_{12}x_2 + \dots + b_{1n}x_n \\ b_{21}x_1 + \dots \quad + b_{2n}x_n \\ \vdots \\ \\ \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}$$

b_{11} – the coef of x_1 in the first output

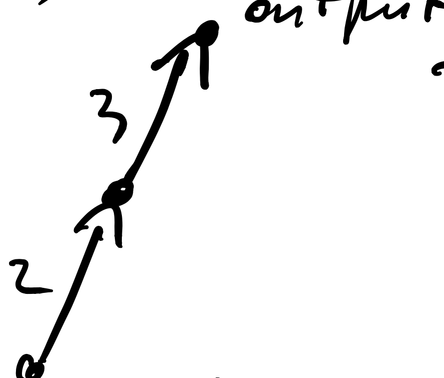
b_{ij} – coef of $\underline{\underline{x_i}}$ in $\underline{\underline{y_j}}$



$$\text{output} = 3(2x_1 + 3x_2) + 7(x_3 + 4x_1)$$



path from x_1 to output
multiply labels along the path



$2 \cdot 3$

take another path

$4 \cdot 7$

coeff of x_1 in this $= \sum$

$2 \cdot 3 + 4 \cdot 7$

Coeff of x_i in output j

$$\sum_{\substack{\text{all paths} \\ \text{from } x_i \text{ to } y_j}} \lambda_1 \cdot \lambda_2 \cdot \ldots \cdot \lambda_d$$

d = depth of circuit

$$B = \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ b_{n1} & \cdots & b_{nn} \end{bmatrix}$$

$$b_{ij} = \sum_{\text{paths}} \lambda_1 \cdot \lambda_2 \cdot \ldots \cdot \lambda_d$$

t-SS dim: looking at t-products of b_{ij}

$$\left(\sum_{\text{paths}} \lambda_1^{(1)} \cdots \lambda_d^{(1)}\right) \cdot$$

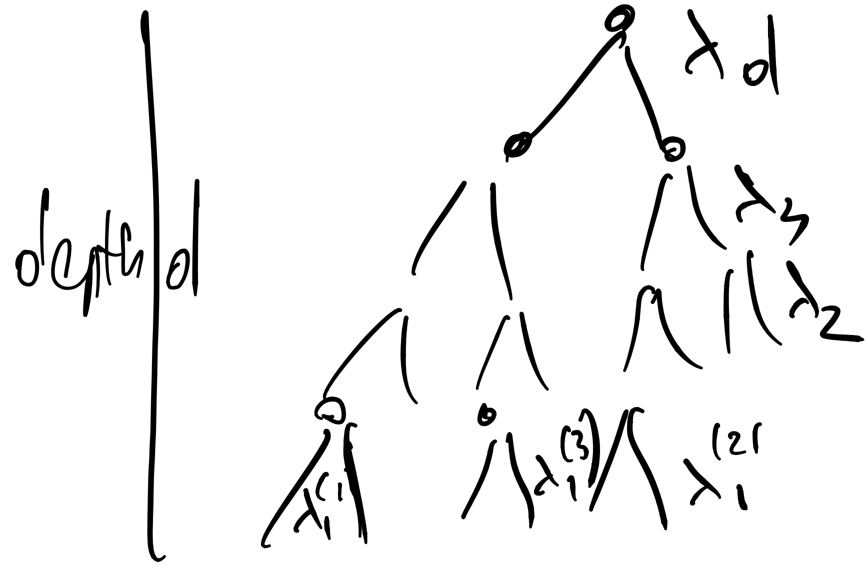
$$\left(\sum_{\text{paths}} \lambda_1^{(2)} \cdots \lambda_d^{(2)}\right) \cdot$$

$$\cdots$$

$$\left(\sum_{\text{paths}} \lambda_1^{(t)} \cdots \lambda_d^{(t)}\right) =$$

$$\sum \lambda_1^{(1)} \cdot \ldots \lambda_d^{(1)} \cdot \lambda_1^{(2)} \ldots \lambda_d^{(2)} \cdot \sim\ldots\ldots \lambda_1^{(t)} \cdot \ldots \lambda_d^{(t)}$$

$$= \sum \lambda_1^{(1)} \cdot \lambda_1^{(2)} \cdot \ldots \cdot \lambda_1^{(t)} \cdot \lambda_2^{(1)} \cdot \lambda_2^{(2)} \ldots \lambda_2^{(t)} \cdot \ldots \lambda_d^{(1)} \cdot \lambda_d^{(2)} \ldots \lambda_d^{(t)}$$



ckt size S

S_1 nodes at 1st level

S_2 nodes 2

S_d d level

$\sum S_i = S$

$2s_1$ different labels at the first level

$\underline{2s_1}$ diff for $\lambda_1^{(i)}$

$$\sum \boxed{\left(\lambda_1^{(1)} \circ \lambda_1^{(2)} \circ \cdots \circ \lambda_1^{(t)}\right)} \bullet \left(\lambda_2^{(1)} \circ \lambda_2^{(2)} \circ \cdots \circ \lambda_2^{(t)}\right) \circ$$

$$\cdots\cdots$$

$$\lambda_d^{(1)} \circ \lambda_d^{(2)} \cdots \lambda_d^{(t)}$$

# of such terms $\leq$

$$\leq \binom{2s_1}{t}$$

Hamon $\le \binom{2s_1}{t} \cdot \binom{2s_2}{t} \cdot \ldots \cdot \binom{2s_d}{t}$

$$\sum s_i = S.$$

$$\binom{2s_1}{t} \cdot \binom{2s_2}{t} \cdot \ldots \cdot \binom{2s_d}{t}$$

convexity

$$\le \binom{\frac{2S}{d}}{t} \cdot \binom{\frac{2S}{d}}{t} \cdot \ldots \cdot \binom{\frac{2S}{d}}{t}$$

$$\le \binom{\frac{2s}{d}+t}{t}^{d} \cdot$$

$$\binom{n}{k} = \binom{n}{n-k}$$

$$= \binom{\frac{2s}{d}+t}{\frac{2s}{d}}^{d}$$

$$\binom{n}{k} \le n^{k}$$

$$= \left(\left(\frac{2s}{d}+t\right)^{\frac{2s}{d}} \right)^{d} =$$

$$= \left(\frac{2s}{d} + t\right)^{2s}$$

$t = n^2 \quad \frac{2s}{d} \le 2s$

$$\le \left(2s + n^2\right)^{2s}$$

what we wanted $\square$