Stopping by Matrix Rigidity on a snowy day

Introduction to Matrix Rigidity - I

C Ramya
Tata Institute of Fundamental Research
Mumbai, INDIA

Workshop on Matrix Rigidity
FSTTCS 2020

Matrix Rigidity

- *Matrix Rigidity* was introduced by Valiant(1977) in the context of computing linear transformations and was studied independently by Grigoriev(1976).

Matrix Rigidity

- *Matrix Rigidity* was introduced by Valiant(1977) in the context of computing linear transformations and was studied independently by Grigoriev(1976).

Rigidity of a matrix

Rigidity of a matrix A for rank r is the minimum number of entries to be changed in A so that $\text{rank}(A)$ is at most r.

Matrix Rigidity

- *Matrix Rigidity* was introduced by Valiant(1977) in the context of computing linear transformations and was studied independently by Grigoriev(1976).

Rigidity of a matrix

Rigidity of a matrix A for rank r is the minimum number of entries to be changed in A so that $\mathrm{rank}(A)$ is at most r.

- *Rigidity* of a matrix $A \in \mathbb{F}^{n\times n}$ for rank r is denoted by $R_A^{\mathbb{F}}(r)$.

Matrix Rigidity

- *Matrix Rigidity* was introduced by Valiant(1977) in the context of computing linear transformations and was studied independently by Grigoriev(1976).

Rigidity of a matrix

Rigidity of a matrix A for rank r is the minimum number of entries to be changed in A so that $\text{rank}(A)$ is at most r.

- *Rigidity* of a matrix $A \in \mathbb{F}^{n \times n}$ for rank r is denoted by $R_A^{\mathbb{F}}(r)$. For the $n \times n$ identity matrix I_n, $R_{I_n}^{\mathbb{F}}(r) \leq (n-r)$.

Matrix Rigidity

- *Matrix Rigidity* was introduced by Valiant(1977) in the context of computing linear transformations and was studied independently by Grigoriev(1976).

Rigidity of a matrix

Rigidity of a matrix A for rank r is the minimum number of entries to be changed in A so that rank(A) is at most r.

- *Rigidity* of a matrix $A \in \mathbb{F}^{n \times n}$ for rank r is denoted by $R_A^{\mathbb{F}}(r)$. For the $n \times n$ identity matrix I_n, $R_{I_n}^{\mathbb{F}}(r) \leq (n - r)$.
- A matrix is *rigid* if it is *far* from any matrix of *low* rank.

Matrix Rigidity

- *Matrix Rigidity* was introduced by Valiant(1977) in the context of computing linear transformations and was studied independently by Grigoriev(1976).

Rigidity of a matrix

Rigidity of a matrix A for rank r is the minimum number of entries to be changed in A so that rank(A) is at most r.

- *Rigidity* of a matrix $A \in \mathbb{F}^{n \times n}$ for rank r is denoted by $R_A^{\mathbb{F}}(r)$. For the $n \times n$ identity matrix I_n, $R_{I_n}^{\mathbb{F}}(r) \leq (n - r)$.
- A matrix is *rigid* if it is *far* from any matrix of *low* rank.
- $R_A(r)$ is hamming distance between A and rank $\leq r$ matrices.

Matrix Rigidity

- *Matrix Rigidity* was introduced by Valiant(1977) in the context of computing linear transformations and was studied independently by Grigoriev(1976).

Rigidity of a matrix

Rigidity of a matrix A for rank r is the minimum number of entries to be changed in A so that rank(A) is at most r.

- *Rigidity* of a matrix $A \in \mathbb{F}^{n \times n}$ for rank r is denoted by $R_A^{\mathbb{F}}(r)$. For the $n \times n$ identity matrix I_n, $R_{I_n}^{\mathbb{F}}(r) \leq (n - r)$.
- A matrix is *rigid* if it is *far* from any matrix of *low* rank.
- $R_A(r)$ is hamming distance between A and rank $\leq r$ matrices.

- Rigidity intertwines *combinatorial* & *algebraic* property.

Matrix Rigidity

- *Matrix Rigidity* was introduced by Valiant(1977) in the context of computing linear transformations and was studied independently by Grigoriev(1976).

Rigidity of a matrix

Rigidity of a matrix A for rank r is the minimum number of entries to be changed in A so that rank(A) is at most r.

- *Rigidity* of a matrix $A \in \mathbb{F}^{n \times n}$ for rank r is denoted by $R_A^{\mathbb{F}}(r)$. For the $n \times n$ identity matrix I_n, $R_{I_n}^{\mathbb{F}}(r) \leq (n - r)$.
- A matrix is *rigid* if it is *far* from any matrix of *low* rank.
- $R_A(r)$ is hamming distance between A and rank $\leq r$ matrices.

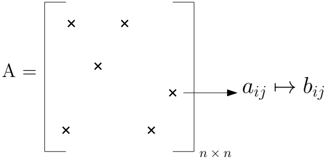
- Rigidity intertwines *combinatorial* & *algebraic* property.
- Rigidity has connections to communication complexity, data structure lower bounds and coding theory.

Interpreting Matrix Rigidity

Let $A \in \mathbb{F}^{n \times n}$. Suppose rigidity of matrix A for rank r is $\leq s$.

Interpreting Matrix Rigidity

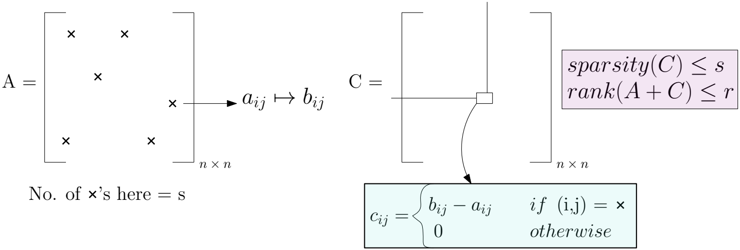
Let $A \in \mathbb{F}^{n \times n}$. Suppose rigidity of matrix A for rank r is $\leq s$.



No. of ×'s here = s

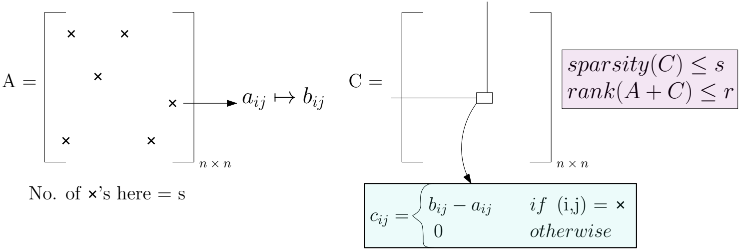
Interpreting Matrix Rigidity

Let $A \in \mathbb{F}^{n\times n}$. Suppose rigidity of matrix A for rank r is $\leq s$.



Interpreting Matrix Rigidity

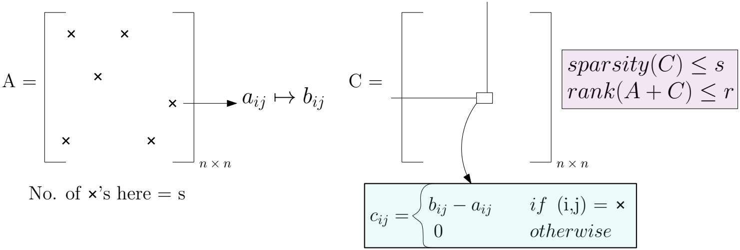
Let $A \in \mathbb{F}^{n \times n}$. Suppose rigidity of matrix A for rank r is $\leq s$.



- When $R_A^{\mathbb{F}}(r) \leq s$, there is a matrix $C \in \mathbb{F}^{n \times n}$ of sparsity $\leq s$ such that $\text{rank}(A + C) \leq r$.

Interpreting Matrix Rigidity

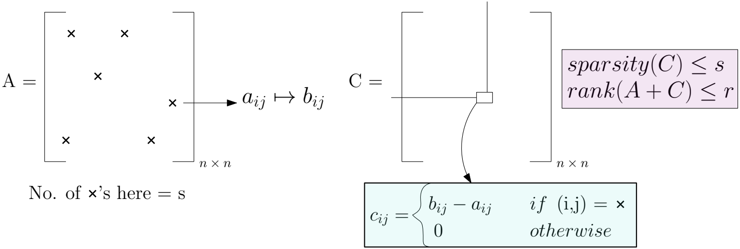
Let $A \in \mathbb{F}^{n\times n}$. Suppose rigidity of matrix A for rank r is $\leq s$.



- When $R_A^{\mathbb{F}}(r) \leq s$, there is a matrix $C \in \mathbb{F}^{n\times n}$ of sparsity $\leq s$ such that $\text{rank}(A + C) \leq r$.
- If there is a matrix $C \in \mathbb{F}^{n\times n}$ of sparsity $\leq s$ such that $\text{rank}(A + C) \leq r$ then $R_A^{\mathbb{F}}(r) \leq s$.

Interpreting Matrix Rigidity

Let $A \in \mathbb{F}^{n\times n}$. Suppose rigidity of matrix A for rank r is $\leq s$.



- When $R_A^{\mathbb{F}}(r) \leq s$, there is a matrix $C \in \mathbb{F}^{n\times n}$ of sparsity $\leq s$ such that rank$(A + C) \leq r$.
- If there is a matrix $C \in \mathbb{F}^{n\times n}$ of sparsity $\leq s$ such that rank$(A + C) \leq r$ then $R_A^{\mathbb{F}}(r) \leq s$.

Rigidity of a matrix A for rank r

$$R_A^{\mathbb{F}}(r) = \min_C \{\text{sparsity(C)} \mid C \in \mathbb{F}^{n\times n},\ \text{rank}_{\mathbb{F}}(A + C) \leq r\}.$$

Toy Example I: Identity Matrix

$$R_A^{\mathbb{F}}(r) = \min_C \{\text{sparsity}(\mathrm{C}) \mid C \in \mathbb{F}^{n\times n},\ \text{rank}_{\mathbb{F}}(A + C) \leq r\}$$

Toy Example I: Identity Matrix

$$R_A^{\mathbb{F}}(r) = \min_C\{\text{sparsity(C)} \mid C \in \mathbb{F}^{n\times n},\ \text{rank}_{\mathbb{F}}(A + C) \leq r\}$$

- If $R_A(r) \leq s$ then $A = S + L$ such that S has sparsity $\leq s$ and L has rank $\leq r$.

Toy Example I: Identity Matrix

$$R_A^{\mathbb{F}}(r) = \min_C \{\text{sparsity(C)} \mid C \in \mathbb{F}^{n\times n},\ \text{rank}_{\mathbb{F}}(A+C) \le r\}$$

- If $R_A(r) \le s$ then $A = S + L$ such that S has sparsity $\le s$ and L has rank $\le r$.
- If $A = S + L$ with S has sparsity of $S \le s$ and $\text{rank}(L) \le r$ then $R_A(r) \le s$.

Toy Example I: Identity Matrix

$$R_A^{\mathbb{F}}(r) = \min_C\{\text{sparsity(C)} \mid C \in \mathbb{F}^{n\times n},\ \text{rank}_{\mathbb{F}}(A+C) \leq r\}$$

- If $R_A(r) \leq s$ then $A = S + L$ such that S has sparsity $\leq s$ and L has rank $\leq r$.
- If $A = S + L$ with S has sparsity of $S \leq s$ and $\text{rank}(L) \leq r$ then $R_A(r) \leq s$.

Example

Rigidity of $n \times n$ identity matrix is $(n-r)$ for any $r \leq n$.

- For any $r \leq n$, $R_{I_n}(r) \leq (n-r)$.

Toy Example I: Identity Matrix

$$R_A^{\mathbb{F}}(r) = \min_C \{\text{sparsity(C)} \mid C \in \mathbb{F}^{n\times n},\ \text{rank}_{\mathbb{F}}(A+C) \leq r\}$$

- If $R_A(r) \leq s$ then $A = S + L$ such that S has sparsity $\leq s$ and L has rank $\leq r$.
- If $A = S + L$ with S has sparsity of $S \leq s$ and $\text{rank}(L) \leq r$ then $R_A(r) \leq s$.

Example

Rigidity of $n \times n$ identity matrix is $(n - r)$ for any $r \leq n$.

- For any $r \leq n$, $R_{I_n}(r) \leq (n - r)$.
- Suppose, $R_{I_n}(r) < (n - r)$.

Toy Example I: Identity Matrix

$$R_A^{\mathbb{F}}(r) = \min_C \{\text{sparsity(C)} \mid C \in \mathbb{F}^{n \times n},\ \text{rank}_{\mathbb{F}}(A + C) \leq r\}$$

- If $R_A(r) \leq s$ then $A = S + L$ such that S has sparsity $\leq s$ and L has rank $\leq r$.
- If $A = S + L$ with S has sparsity of $S \leq s$ and $\text{rank}(L) \leq r$ then $R_A(r) \leq s$.

Example

Rigidity of $n \times n$ identity matrix is $(n - r)$ for any $r \leq n$.

- For any $r \leq n$, $R_{I_n}(r) \leq (n - r)$.
- Suppose, $R_{I_n}(r) < (n - r)$. Then, there exists $C \in \mathbb{F}^{n \times n}$ of sparsity $< (n - r)$ such that $\text{rank}(I_n + C) \leq r$.

Toy Example I: Identity Matrix

$$R_A^{\mathbb{F}}(r) = \min_C \{\text{sparsity(C)} \mid C \in \mathbb{F}^{n\times n},\ \text{rank}_{\mathbb{F}}(A + C) \leq r\}$$

- If $R_A(r) \leq s$ then $A = S + L$ such that S has sparsity $\leq s$ and L has rank $\leq r$.
- If $A = S + L$ with S has sparsity of $S \leq s$ and $\text{rank}(L) \leq r$ then $R_A(r) \leq s$.

Example

Rigidity of $n \times n$ identity matrix is $(n - r)$ for any $r \leq n$.

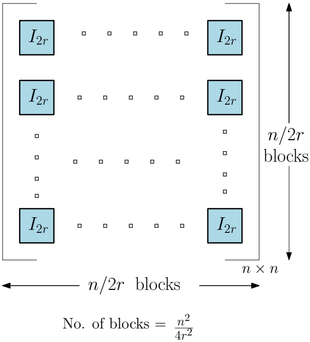
- For any $r \leq n$, $R_{I_n}(r) \leq (n - r)$.
- Suppose, $R_{I_n}(r) < (n - r)$. Then, there exists $C \in \mathbb{F}^{n\times n}$ of sparsity $< (n - r)$ such that $\text{rank}(I_n + C) \leq r$.

$$\text{rank}(I_n + C) \geq \text{rank}(I_n) - \text{rank}(C) \geq n - (n - r) > r (\Leftarrow\!\!\Rightarrow)$$

Toy Example II: Building over Identity matrices

Theorem (Midrijānis (2005))

For any n divisible by $2r$, $R^{\mathbb{F}}_{M_n}(r) = \frac{n^2}{4r}$.



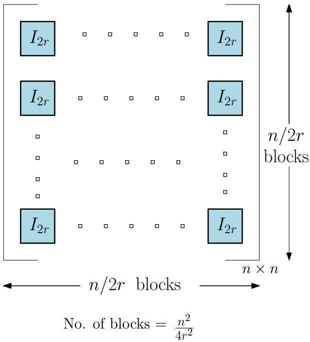
Toy Example II: Building over Identity matrices

Theorem (Midrijānis (2005))

For any n divisible by $2r$, $R^{\mathbb{F}}_{M_n}(r) = \frac{n^2}{4r}$.

Proof.

- By changing r entries in each block *consistently*, $\mathrm{rank}(M_n)$ is at most r. Thus, $R_{M_n}(r) \leq \frac{n^2}{4r}$.



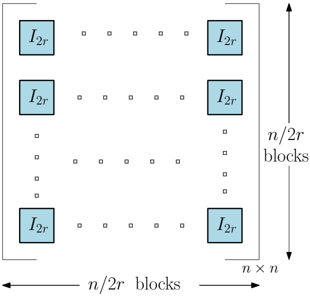
Toy Example II: Building over Identity matrices

Theorem (Midrijānis (2005))

For any n divisible by $2r$, $R^{\mathbb{F}}_{M_n}(r) = \frac{n^2}{4r}$.

Proof.

- Clearly, by changing r entries in each block *consistently* $\text{rank}(M_n) \leq r$. Thus, $R_{M_n}(r) \leq \frac{n^2}{4r}$.
- Suppose, $rank(M_n)$ can be reduced to r by changing fewer than $\frac{n^2}{4r}$ entries. Then, $\exists\ I_{2r}$ block whose rank can be reduced to r by changing fewer than r entries. $(\Leftarrow\Rightarrow)$



No. of blocks $= \frac{n^2}{4r^2}$

Upper Bounds on Matrix Rigidity

Theorem (Valiant(1977))

For any matrix $A \in \mathbb{F}^{n\times n}$ *and any* $r \leq n$, $R_A^{\mathbb{F}}(r) \leq (n-r)^2$.

Upper Bounds on Matrix Rigidity

Theorem (Valiant(1977))

For any matrix $A \in \mathbb{F}^{n \times n}$ and any $r \leq n$, $R_A^{\mathbb{F}}(r) \leq (n-r)^2$.

Proof.

- If $\text{rank}(A) \leq r$ then $R_A(r) = 0$.
- If $\text{rank}(A) > r$ there exists an full rank $r \times r$ submatrix B in A.

Upper Bounds on Matrix Rigidity

Theorem (Valiant(1977))

For any matrix $A \in \mathbb{F}^{n\times n}$ and any $r \leq n$, $R_A^{\mathbb{F}}(r) \leq (n-r)^2$.

Proof.

- If $\operatorname{rank}(A) \leq r$ then $R_A(r) = 0$.
- If $\operatorname{rank}(A) > r$ there exists an full rank $r \times r$ submatrix B in A.

$$\begin{array}{c} \begin{matrix} r & (n-r) \end{matrix} \\ \begin{matrix} r \\ (n-r) \end{matrix} \begin{bmatrix} B & C \\ D & E \end{bmatrix} \begin{matrix} r \\ (n-r) \end{matrix} \\ \begin{matrix} r & (n-r) \end{matrix} \end{array}$$

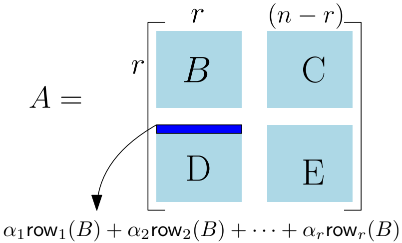
Upper Bounds on Matrix Rigidity

Theorem (Valiant(1977))

For any matrix $A \in \mathbb{F}^{n \times n}$ *and any* $r \leq n$, $R_A^{\mathbb{F}}(r) \leq (n-r)^2$.

Proof.

- If $\text{rank}(A) \leq r$ then $R_A(r) = 0$.
- If $\text{rank}(A) > r$ there exists an full rank $r \times r$ submatrix B in A.
- Every row of D can be expressed as a linear combination of the r rows of B.



Upper Bounds on Matrix Rigidity

Theorem (Valiant(1977))

For any matrix $A \in \mathbb{F}^{n\times n}$ and any $r \le n$, $R_A^{\mathbb{F}}(r) \le (n-r)^2$.

Proof.

- If $\mathrm{rank}(A) \le r$ then $R_A(r) = 0$.
- If $\mathrm{rank}(A) > r$ there exists an full rank $r \times r$ submatrix B in A.
- Every row of D can be expressed as a linear combination of the r rows of B.
- Edit every row of E by corresponding linear combination of the r rows of C.

$$A = \begin{array}{cc} & \begin{array}{cc} r & (n-r) \end{array} \\ r & \begin{bmatrix} B & C \\ D & E \end{bmatrix} \end{array}$$

$$\alpha_1 \mathrm{row}_1(C) + \alpha_2 \mathrm{row}_2(C) + \cdots + \alpha_r \mathrm{row}_r(C)$$

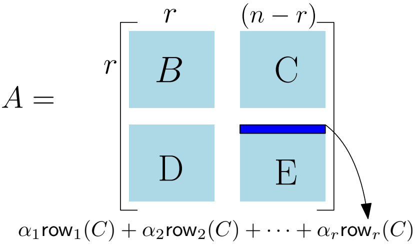
Upper Bounds on Matrix Rigidity

Theorem (Valiant(1977))

For any matrix $A \in \mathbb{F}^{n \times n}$ and any $r \leq n$, $R_A^{\mathbb{F}}(r) \leq (n-r)^2$.

Proof.

- If $\text{rank}(A) \leq r$ then $R_A(r) = 0$.
- If $\text{rank}(A) > r$ there exists an full rank $r \times r$ submatrix B in A.
- Every row of D can be expressed as a linear combination of the r rows of B.
- Edit every row of E by corresponding linear combination of the r rows of C.



Now, every row of A is a linear combination of the first r rows.
By changing $(n-r)^2$ entries in E, $\text{rank}(A)$ is reduced to r.
Thus, $R_A^{\mathbb{F}}(r) \leq (n-r)^2$.

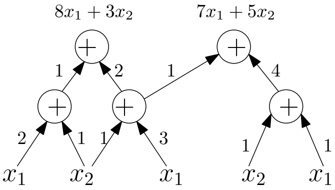
Linear Circuits

- *Linear circuits* are a computational model involving additions and scalar multiplications.

Linear Circuits

- *Linear circuits* are a computational model involving additions and scalar multiplications.

- A linear circuit $\mathcal{C}$ over $\mathbb{F}$ is a DAG where
  - in-degree 0 gates: labelled by variables;
  - internal gates: labelled by $+$;
  - edges: labelled by constants in $\mathbb{F}$.



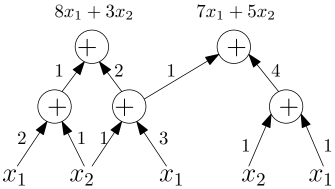
$$x \mapsto A \cdot x \qquad x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

$$A = \begin{bmatrix} 8 & 3 \\ 7 & 5 \end{bmatrix}$$

Linear Circuits

- *Linear circuits* are a computational model involving additions and scalar multiplications.

- A linear circuit $\mathcal{C}$ over $\mathbb{F}$ is a DAG where
  - in-degree 0 gates: labelled by variables;
  - internal gates: labelled by $+$;
  - edges: labelled by constants in $\mathbb{F}$.



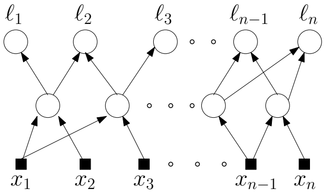
$$x \mapsto A \cdot x \qquad x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

$$A = \begin{bmatrix} 8 & 3 \\ 7 & 5 \end{bmatrix}$$

- Linear circuits have *n* inputs, *n* outputs and fan-in 2 gates.

Linear Circuits

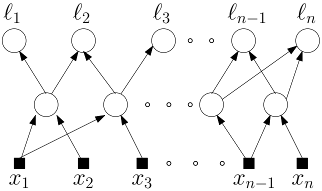
- *Linear circuits* are a computational model involving additions and scalar multiplications.
- A linear circuit $\mathcal{C}$ over $\mathbb{F}$ is a DAG where
  - in-degree 0 gates: labelled by variables;
  - internal gates: labelled by $+$;
  - edges: labelled by constants in $\mathbb{F}$.



- Linear circuits have *n* inputs, *n* outputs and fan-in 2 gates.

Linear Circuits

- *Linear circuits* are a computational model involving additions and scalar multiplications.
- A linear circuit $\mathcal{C}$ over $\mathbb{F}$ is a DAG where
  - in-degree 0 gates: labelled by variables;
  - internal gates: labelled by $+$;
  - edges: labelled by constants in $\mathbb{F}$.

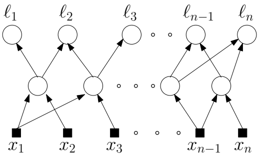


$$A = \begin{bmatrix} \longleftarrow & \ell_1 & \longrightarrow \\ \longleftarrow & \ell_2 & \longrightarrow \\ & \vdots & \\ \longleftarrow & \ell_n & \longrightarrow \end{bmatrix}$$

- Linear circuits have n inputs, n outputs and fan-in 2 gates.
- $\mathcal{C}$ computes a linear transformation represented by $A \in \mathbb{F}^{n \times n}$.

Linear Circuits

- A linear circuit $\mathcal{C}$ over $\mathbb{F}$ is a DAG where
  - in-degree 0 gates: labelled by variables;
  - internal gates: labelled by $+$;
  - edges: labelled by constants in $\mathbb{F}$.



$$A = \begin{bmatrix} \longleftarrow & \ell_1 & \longrightarrow \\ \longleftarrow & \ell_2 & \longrightarrow \\ & \vdots & \\ \longleftarrow & \ell_n & \longrightarrow \end{bmatrix}$$

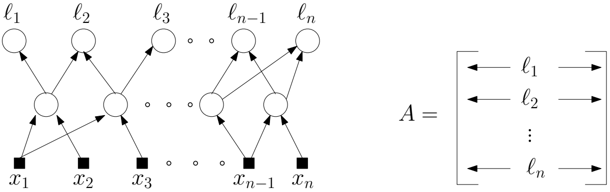
- Linear circuits have n inputs, n outputs and fan-in 2 gates.
- $\mathcal{C}$ computes a linear transformation represented by $A \in \mathbb{F}^{n \times n}$.

> - size($\mathcal{C}$): # of edges
> - depth($\mathcal{C}$): length of longest path from i/p to o/p.

- Any linear transformation $\mathbb{F}^n \to \mathbb{F}^n$ can be computed by a linear circuit of size $O(n^2)$ and depth $O(\log n)$.

Linear Circuits

- A linear circuit $\mathcal{C}$ over $\mathbb{F}$ is a DAG where
  - in-degree 0 gates: labelled by variables;
  - internal gates: labelled by $+$;
  - edges: labelled by constants in $\mathbb{F}$.



- Linear circuits have n inputs, n outputs and fan-in 2 gates.

  - size($\mathcal{C}$): # of edges
  - depth($\mathcal{C}$): length of longest path from i/p to o/p.

- Best known size lower bound: $3n - o(n)$ (Chashkin 1994).

Linear Circuits and Matrix Rigidity

- Can we prove super-linear lower bounds for linear circuits of logarithmic depth?
- What is the linear circuit complexity of rigid matrices? Can a matrix of high rigidity be computed by linear size logarithmic depth linear circuits?

Linear Circuits and Matrix Rigidity

- Can we prove super-linear lower bounds for linear circuits of logarithmic depth?
- What is the linear circuit complexity of rigid matrices? Can a matrix of high rigidity be computed by linear size logarithmic depth linear circuits?

Theorem (Valiant(1977))

For any $A \in \mathbb{F}^{n \times n}$ if $R_A(\epsilon n) > n^{1+\delta}$ for some $\epsilon, \delta > 0$ then any linear circuit of depth $O(\log n)$ computing the transformation $A : x \mapsto A \cdot x$ must have size $\Omega(n \log \log n)$.

Linear Circuits and Matrix Rigidity

- Can we prove super-linear lower bounds for linear circuits of logarithmic depth?
- What is the linear circuit complexity of rigid matrices? Can a matrix of high rigidity be computed by linear size logarithmic depth linear circuits?

Theorem (Valiant(1977))

For any $A \in \mathbb{F}^{n\times n}$ if $R_A(\epsilon n) > n^{1+\delta}$ for some $\epsilon, \delta > 0$ then any linear circuit of depth $O(\log n)$ computing the transformation $A : x \mapsto A \cdot x$ must have size $\Omega(n \log\log n)$.

- *Rigid* matrices cannot be computed by linear circuits having *small* depth as well as *small* size.

Proof of Valiant's Theorem

- Consider a linear circuit of size s, depth d, n inputs, n outputs and fan-in 2.

Proof of Valiant's Theorem

- Consider a linear circuit of size s, depth d, n inputs, n outputs and fan-in 2.

Edge Removal Lemma (Erdös, Graham, and Szemerédi 1976)

Let G be a directed acyclic graph with s edges and every path having length at most d. Then, by removing at most $s/\log d$ edges every path in the resulting graph has length at most $d/2$.

Proof of Valiant's Theorem

- Consider a linear circuit of size s, depth d, n inputs, n outputs and fan-in 2.

Edge Removal Lemma (Erdös, Graham, and Szemerédi 1976)

Let G be a directed acyclic graph with s edges and every path having length at most d. Then, by removing at most $s/\log d$ edges every path in the resulting graph has length at most $d/2$.

- Repeating the *edge removal process* ϵ times, length of every path at most $d/2^{\epsilon}$ and no. of edges removed is $\frac{s\epsilon}{\log d}$.

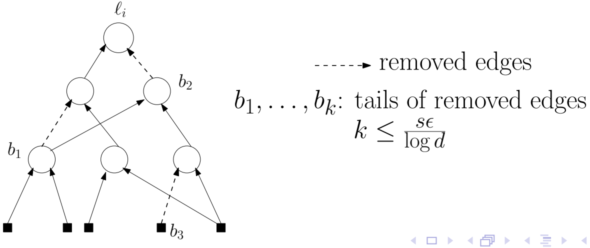
Proof of Valiant's Theorem

- Consider a linear circuit of size s, depth d, n inputs, n outputs and fan-in 2.

Edge Removal Lemma (Erdös, Graham, and Szemerédi 1976)

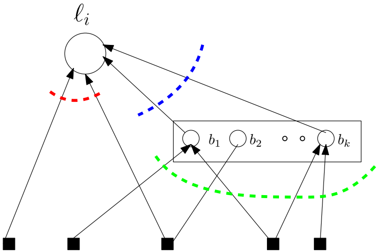
Let G be a directed acyclic graph with s edges and every path having length at most d. Then, by removing at most $s/\log d$ edges every path in the resulting graph has length at most $d/2$.

- Repeating the *edge removal process* ϵ times, length of every path at most $d/2^{\epsilon}$ and no. of edges removed is $\frac{s\epsilon}{\log d}$.



Proof(contd.)

- Each ℓ_i is a linear combination of the tails $b_1, \ldots, b_k$ and at most $2^{d/2^\epsilon}$ input variables.



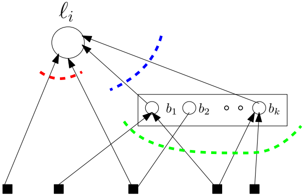
$$\ell_i = \Sigma_{j=1}^{k} \alpha_{ij} b_j + c_i$$

$$\alpha_{ij} \in F \;\; b_j \in F^n$$

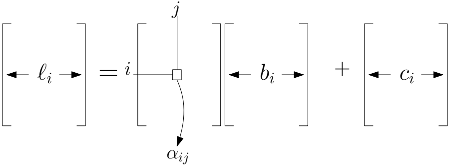
$$c_i \in F^n, \; 2^{d/2^\epsilon}\text{-sparse}$$

Proof(contd.)

- Each ℓ_i is a linear combination of the tails $b_1, \ldots, b_k$ and at most $2^{d/2^{\epsilon}}$ input variables.

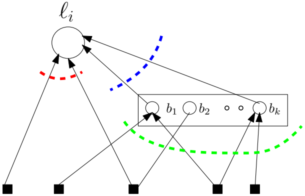


$$\ell_i = \Sigma_{j=1}^{k} \alpha_{ij} b_j + c_i$$

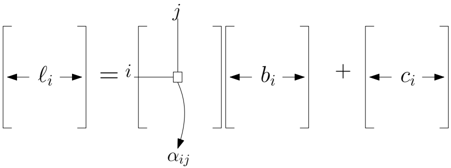


Proof(contd.)

- Each ℓ_i is a linear combination of the tails $b_1, \ldots, b_k$ and at most $2^{d/2^{\epsilon}}$ input variables.



$$\ell_i = \Sigma_{j=1}^{k} \alpha_{ij} b_j + c_i$$

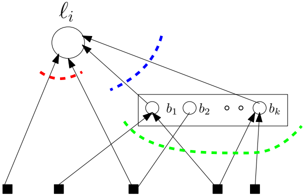


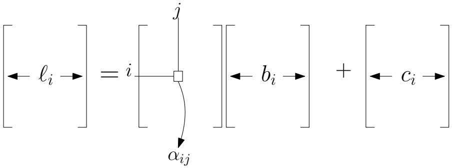
- $A = B_1 B_2 + C$ where $B_1 \in \mathbb{F}^{n \times k}$, $B_2 \in \mathbb{F}^{k \times n}$, $C \in \mathbb{F}^{n \times n}$.

Proof(contd.)

- Each ℓ_i is a linear combination of the tails $b_1, \ldots, b_k$ and at most $2^{d/2^{\epsilon}}$ input variables.

$$\ell_i = \Sigma_{j=1}^{k} \alpha_{ij} b_j + c_i$$

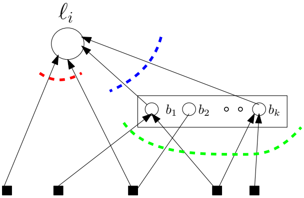




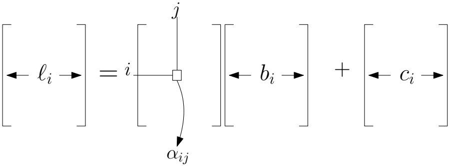
- $A = B_1 B_2 + C$ where $B_1 \in \mathbb{F}^{n \times k}$, $B_2 \in \mathbb{F}^{k \times n}$, $C \in \mathbb{F}^{n \times n}$.
- Then, $\text{rank}(B_1 B_2) \leq k \leq \frac{s\epsilon}{\log d}$ and $\text{sparsity}(C) \leq n 2^{d/2^{\epsilon}}$.

Proof(contd.)

- Each ℓ_i is a linear combination of the tails $b_1, \ldots, b_k$ and at most $2^{d/2^\epsilon}$ input variables.



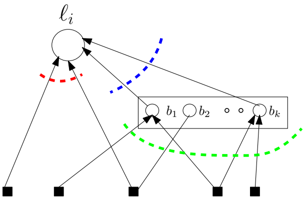
$$\ell_i = \Sigma_{j=1}^{k} \alpha_{ij} b_j + c_i$$



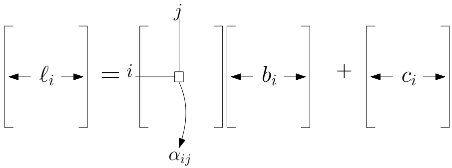
- $A = B_1 B_2 + C$ where $B_1 \in \mathbb{F}^{n \times k}$, $B_2 \in \mathbb{F}^{k \times n}$, $C \in \mathbb{F}^{n \times n}$.
- Then, $\mathrm{rank}(B_1 B_2) \leq k \leq \frac{s\epsilon}{\log d}$ and $\mathrm{sparsity}(C) \leq n2^{d/2^\epsilon}$.
- Thus, rigidity of A for rank $\frac{s\epsilon}{\log d}$ is at most $n2^{d/2^\epsilon}$.

Proof(contd.)

- Each ℓ_i is a linear combination of the tails $b_1, \ldots, b_k$ and at most $2^{d/2^\epsilon}$ input variables.



$$\ell_i = \Sigma_{j=1}^{k} \alpha_{ij} b_j + c_i$$



- $A = B_1 B_2 + C$ where $B_1 \in \mathbb{F}^{n \times k}$, $B_2 \in \mathbb{F}^{k \times n}$, $C \in \mathbb{F}^{n \times n}$.
- Then, $\text{rank}(B_1 B_2) \leq k \leq \frac{s\epsilon}{\log d}$ and $\text{sparsity}(C) \leq n2^{d/2^\epsilon}$.
- Thus, rigidity of A for rank $\frac{s\epsilon}{\log d}$ is at most $n2^{d/2^\epsilon}$.
- If $A \in \mathbb{F}^{n \times n}$ is computed by a linear circuit of size $n \log\log n$ and depth $\log n$ then $R_A(\epsilon n) \leq n^{1+\delta}$.

Valiant's Question

- For any $A \in \mathbb{F}^{n \times n}$ if $R_A(\epsilon n) > n^{1+\delta}$ for some $\epsilon, \delta > 0$ then any linear circuit of depth $O(\log n)$ computing A must have size $\Omega(n \log \log n)$.

Valiant's Question

- For any $A \in \mathbb{F}^{n\times n}$ if $R_A(\epsilon n) > n^{1+\delta}$ for some $\epsilon, \delta > 0$ then any linear circuit of depth $O(\log n)$ computing A must have size $\Omega(n \log\log n)$.

Valiant's Question

Find an *explicit* sequence of matrices $M_n \in \mathbb{F}^{n\times n}$ such that $R^{\mathbb{F}}_{M_n}(\epsilon n) \geq \Omega(n^{1+\delta})$ for $\epsilon, \delta > 0$.

Valiant's Question

- For any $A \in \mathbb{F}^{n\times n}$ if $R_A(\epsilon n) > n^{1+\delta}$ for some $\epsilon, \delta > 0$ then any linear circuit of depth $O(\log n)$ computing A must have size $\Omega(n \log\log n)$.

Valiant's Question

Find an *explicit* sequence of matrices $M_n \in \mathbb{F}^{n\times n}$ such that $R^{\mathbb{F}}_{M_n}(\epsilon n) \geq \Omega(n^{1+\delta})$ for $\epsilon, \delta > 0$.

- *Explicit*: There exists a poly(n) time deterministic algorithm on input 1^n outputs the $n \times n$ matrix M_n.

Valiant's Question

- For any $A \in \mathbb{F}^{n \times n}$ if $R_A(\epsilon n) > n^{1+\delta}$ for some $\epsilon, \delta > 0$ then any linear circuit of depth $O(\log n)$ computing A must have size $\Omega(n \log \log n)$.

Valiant's Question

Find an *explicit* sequence of matrices $M_n \in \mathbb{F}^{n \times n}$ such that $R^{\mathbb{F}}_{M_n}(\epsilon n) \geq \Omega(n^{1+\delta})$ for $\epsilon, \delta > 0$.

- *Explicit*: There exists a poly(n) time deterministic algorithm on input 1^n outputs the $n \times n$ matrix M_n.

This Workshop

Recent Progress towards answering Valiant's Question (and beyond).

Existence of Rigid Matrices

Theorem (Valiant(1977))

Let $\mathbb{F}_q$ *be a finite field. For any* $0 \leq r \leq n - \Omega(\sqrt{n})$ *there is a matrix* $M \in \mathbb{F}_q^{n \times n}$ *such that* $R_M^{\mathbb{F}_q}(r) = \Omega((n-r)^2 / \log n)$.

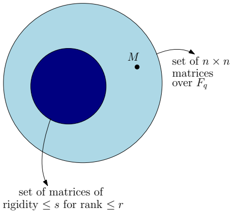
Existence of Rigid Matrices

Theorem (Valiant(1977))

Let $\mathbb{F}_q$ be a finite field. For any $0 \leq r \leq n - \Omega(\sqrt{n})$ there is a matrix $M \in \mathbb{F}_q^{n \times n}$ such that $R_M^{\mathbb{F}_q}(r) = \Omega((n-r)^2/\log n)$.

Proof. (via counting)

- Count no. of matrices $A \in \mathbb{F}_q^{n \times n}$ with $R_A(r) \leq s$.



Existence of Rigid Matrices

Theorem (Valiant(1977))

Let $\mathbb{F}_q$ be a finite field. For any $0 \leq r \leq n - \Omega(\sqrt{n})$ there is a matrix $M \in \mathbb{F}_q^{n \times n}$ such that $R_M^{\mathbb{F}_q}(r) = \Omega((n-r)^2 / \log n)$.

Proof. (via counting)

- Count no. of matrices $A \in \mathbb{F}_q^{n \times n}$ with $R_A(r) \leq s$.
- If $R_A(r) \leq s$ then $A = S + L$, sparsity$(S) \leq s$ and rank$(L) \leq r$.

Existence of Rigid Matrices

Theorem (Valiant(1977))

Let $\mathbb{F}_q$ be a finite field. For any $0 \le r \le n - \Omega(\sqrt{n})$ there is a matrix $M \in \mathbb{F}_q^{n\times n}$ such that $R_M^{\mathbb{F}_q}(r) = \Omega((n-r)^2/\log n)$.

Proof. (via counting)

- Count no. of matrices $A \in \mathbb{F}_q^{n\times n}$ with $R_A(r) \le s$.
- If $R_A(r) \le s$ then $A = S + L$, sparsity$(S) \le s$ and rank$(L) \le r$.

No.of $R_A(r) \le s$ matrices: $\underbrace{\binom{n^2}{s} \cdot q^s}_{\text{no. of } s\text{-sparse matrices}} \cdot \underbrace{\binom{n}{r}^2 \cdot q^{n^2-(n-r)^2}}_{\text{no. of rank-}r\text{ matrices}}.$

Existence of Rigid Matrices

Theorem (Valiant(1977))

Let $\mathbb{F}_q$ be a finite field. For any $0 \leq r \leq n - \Omega(\sqrt{n})$ there is a matrix $M \in \mathbb{F}_q^{n \times n}$ such that $R_M^{\mathbb{F}_q}(r) = \Omega((n-r)^2/\log n)$.

Proof. (via counting)

- Count no. of matrices $A \in \mathbb{F}_q^{n \times n}$ with $R_A(r) \leq s$.
- If $R_A(r) \leq s$ then $A = S + L$, sparsity$(S) \leq s$ and rank$(L) \leq r$.

No.of $R_A(r) \leq s$ matrices: $\underbrace{\binom{n^2}{s} \cdot q^s}_{\text{no. of } s\text{-sparse matrices}} \cdot \underbrace{\binom{n}{r}^2 \cdot q^{n^2-(n-r)^2}}_{\text{no. of rank-}r\text{ matrices}}$.

- When $r < n - c_1\sqrt{n}$ and $s < c_2(n-r)^2/\log n$ almost all matrices have rigidity $(n-r)^2$.

Super-exponential time construction of Rigid Matrices

Super-exponential time construction

- For every $n \times n$ matrices A with entries in $\mathbb{F}_q$, test if there exists any s-sparse matrix C such that $\mathrm{rank}_{\mathbb{F}_q}(A + C) \leq r$.
- Running time: $q^{O(n^2)} \cdot q^s \cdot n^{O(1)}$.

Super-exponential time construction of Rigid Matrices

Super-exponential time construction

- For every $n \times n$ matrices A with entries in $\mathbb{F}_q$, test if there exists any s-sparse matrix C such that $\text{rank}_{\mathbb{F}_q}(A + C) \leq r$.
- Running time: $q^{O(n^2)} \cdot q^s \cdot n^{O(1)}$.

Theorem (Valiant(1977))

Let $\mathbb{F}$ be an infinite field. For any $0 \leq r \leq n$ there is a matrix $M \in \mathbb{F}^{n \times n}$ such that $R_M^{\mathbb{F}}(r) = (n - r)^2$.

Untouched Minor Argument

- Consider an $n \times n$ matrix M all of whose $r \times r$ submatrices have full rank.

Untouched Minor Argument

- Consider an $n \times n$ matrix M all of whose $r \times r$ submatrices have full rank.
- Suppose *few* entries of M are changed, there is at least one untouched submatrix contributing rank r.

Untouched Minor Argument

- Consider an $n \times n$ matrix M all of whose $r \times r$ submatrices have full rank.
- Suppose *few* entries of M are changed, there is at least one untouched submatrix contributing rank r.

- Cauchy matrix: $C = \{c_{ij}\}_{i,j=1}^{n}; c_{ij} = \frac{1}{x_i + y_j}$ for $2n$ distinct elements $x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbb{F}$.

Untouched Minor Argument

- Consider an $n \times n$ matrix M all of whose $r \times r$ submatrices have full rank.
- Suppose *few* entries of M are changed, there is at least one untouched submatrix contributing rank r.

- Cauchy matrix: $C = \{c_{ij}\}_{i,j=1}^{n}; c_{ij} = \frac{1}{x_i + y_j}$ for $2n$ distinct elements $x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbb{F}$.

Theorem (Shokrollahi, Spielman, Stemann(1997))

Let $\mathbb{F}$ be a field with at least $2n$ distinct elements and M_n be $n \times n$ Cauchy matrix. Then, $R_{M_n}^{\mathbb{F}}(r) = \Omega(\frac{n^2}{r} \log \frac{n}{r})$ for $\log n \leq r \leq n/2$.

Proof of SSS‘97

Suppose not, $R^{\mathbb{F}}_{M_n}(r) = o(\frac{n^2}{r} \log \frac{n}{r})$.

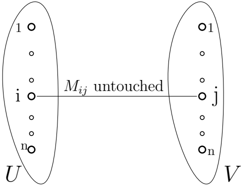
Proof of SSS‘97

Suppose not, $R^{\mathbb{F}}_{M_n}(r) = o(\frac{n^2}{r}\log\frac{n}{r})$. That is, by changing $o(\frac{n^2}{r}\log\frac{n}{r})$ entries in M, rank can be reduced to r.

Proof of SSS'97

Suppose not, $R^{\mathbb{F}}_{M_n}(r) = o(\frac{n^2}{r}\log\frac{n}{r})$. That is, by changing $o(\frac{n^2}{r}\log\frac{n}{r})$ entries in M, rank can be reduced to r.

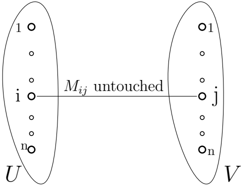
- Consider a bipartite graph $G = (U, V, E)$ with $|U| = |V| = n$ such that $(i, j) \in E(G)$ iff M_{ij} is untouched.
- G has at least $n^2 - o(\frac{n^2}{r}\log\frac{n}{r})$ edges.



Proof of SSS'97

Suppose not, $R^{\mathbb{F}}_{M_n}(r) = o(\frac{n^2}{r}\log\frac{n}{r})$. That is, by changing $o(\frac{n^2}{r}\log\frac{n}{r})$ entries in M, rank can be reduced to r.

- Consider a bipartite graph $G = (U, V, E)$ with $|U| = |V| = n$ such that $(i,j) \in E(G)$ iff M_{ij} is untouched.
- G has at least $n^2 - o(\frac{n^2}{r}\log\frac{n}{r})$ edges.



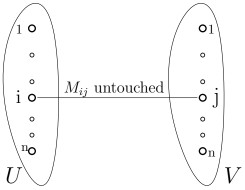
Theorem (Kovári-Sós-Turán (1954))

The maximum number of edges in any $n \times n$ bipartite graph without $K_{r+1,r+1}$ is at most $n^2 - \frac{n(n-r)}{2(r+1)}\log\frac{n}{r}$.

Proof of SSS'97

Suppose not, $R^{\mathbb{F}}_{M_n}(r) = o(\frac{n^2}{r}\log\frac{n}{r})$. That is, by changing $o(\frac{n^2}{r}\log\frac{n}{r})$ entries in M, rank can be reduced to r.

- Consider a bipartite graph $G = (U, V, E)$ with $|U| = |V| = n$ such that $(i, j) \in E(G)$ iff M_{ij} is untouched.
- G has at least $n^2 - o(\frac{n^2}{r}\log\frac{n}{r})$ edges.



Theorem (Kovári-Sós-Turán (1954))

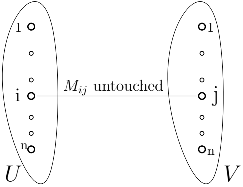
The maximum number of edges in any $n \times n$ bipartite graph without $K_{r+1,r+1}$ is at most $n^2 - \frac{n(n-r)}{2(r+1)}\log\frac{n}{r}$.

- G contains a $(r+1) \times (r+1)$ complete bipartite subgraph.

Proof of SSS‘97

Suppose not, $R^{\mathbb{F}}_{M_n}(r) = o(\frac{n^2}{r}\log\frac{n}{r})$. That is, by changing $o(\frac{n^2}{r}\log\frac{n}{r})$ entries in M, rank can be reduced to r.

- Consider a bipartite graph $G = (U, V, E)$ with $|U| = |V| = n$ such that $(i, j) \in E(G)$ iff M_{ij} is untouched.
- G has at least $n^2 - o(\frac{n^2}{r}\log\frac{n}{r})$ edges.



Theorem (Kovári-Sós-Turán (1954))

The maximum number of edges in any $n \times n$ bipartite graph without $K_{r+1,r+1}$ is at most $n^2 - \frac{n(n-r)}{2(r+1)}\log\frac{n}{r}$.

- G contains a $(r+1) \times (r+1)$ complete bipartite subgraph.
- If fewer than $\frac{n^2}{4(r+1)}\log\frac{n}{r}$ entries in M are changed an $(r+1) \times (r+1)$ submatrix of M_n remains untouched.

Matrices with Algebraically Independent Entries

- $a_1, \ldots, a_n \in \mathbb{R}$ are *algebraically independent* over $\mathbb{Q}$ if there is no polynomial $P \in \mathbb{Q}[x_1, \ldots, x_n]$ such that $P(a_1, \ldots, a_n) = 0$.

Matrices with Algebraically Independent Entries

- $a_1, \ldots, a_n \in \mathbb{R}$ are *algebraically independent* over $\mathbb{Q}$ if there is no polynomial $P \in \mathbb{Q}[x_1, \ldots, x_n]$ such that $P(a_1, \ldots, a_n) = 0$.
- $\{\pi, e^\pi\}$ are algebraically independent over $\mathbb{Q}$.

Matrices with Algebraically Independent Entries

- $a_1, \ldots, a_n \in \mathbb{R}$ are *algebraically independent* over $\mathbb{Q}$ if there is no polynomial $P \in \mathbb{Q}[x_1, \ldots, x_n]$ such that $P(a_1, \ldots, a_n) = 0$.
- $\{\pi, e^\pi\}$ are algebraically independent over $\mathbb{Q}$.
- Any set of $n+1$ polynomials $p_1, \ldots, p_{n+1}$ on n variables is algebraically dependent.

Matrices with Algebraically Independent Entries

- $a_1, \ldots, a_n \in \mathbb{R}$ are *algebraically independent* over $\mathbb{Q}$ if there is no polynomial $P \in \mathbb{Q}[x_1, \ldots, x_n]$ such that $P(a_1, \ldots, a_n) = 0$.
- $\{\pi, e^\pi\}$ are algebraically independent over $\mathbb{Q}$.
- Any set of $n+1$ polynomials $p_1, \ldots, p_{n+1}$ on n variables is algebraically dependent.

Theorem

Let $A \in \mathbb{R}^{n \times n}$ with n^2 algebraically independent elements over $\mathbb{Q}$ as its entries. Then, for any $r \leq n$, $R_A^{\mathbb{R}}(r) = (n-r)^2$.

Proof. Upper bound via Valiant's theorem.

Matrices with Algebraically Independent Entries

Lower Bound: Suppose not, $R_A^{\mathbb{R}}(r) < (n-r)^2$. Then $A = S + L$ such that S has sparsity $s < (n-r)^2$ and L has rank $\leq r$.

Matrices with Algebraically Independent Entries

Lower Bound: Suppose not, $R_A^{\mathbb{R}}(r) < (n-r)^2$. Then $A = S + L$ such that S has sparsity $s < (n-r)^2$ and L has rank $\leq r$.

- Every entry of A is a function of the $n^2 - (n-r)^2$ many entries of L and s entries of S.

Matrices with Algebraically Independent Entries

Lower Bound: Suppose not, $R_A^{\mathbb{R}}(r) < (n-r)^2$. Then $A = S + L$ such that S has sparsity $s < (n-r)^2$ and L has rank $\leq r$.

- Every entry of A is a function of the $n^2 - (n-r)^2$ many entries of L and s entries of S.
- These are n^2 polynomials each on $n^2 - (n-r)^2 + s$ variables.

Matrices with Algebraically Independent Entries

Lower Bound: Suppose not, $R_A^{\mathbb{R}}(r) < (n-r)^2$. Then $A = S + L$ such that S has sparsity $s < (n-r)^2$ and L has rank $\leq r$.

- Every entry of A is a function of the $n^2 - (n-r)^2$ many entries of L and s entries of S.
- These are n^2 polynomials each on $n^2 - (n-r)^2 + s$ variables.
- The entries of A are algebraically dependent. $(\Rightarrow\Leftarrow)$

Matrices with Algebraically Independent Entries

Lower Bound: Suppose not, $R_A^{\mathbb{R}}(r) < (n-r)^2$. Then $A = S + L$ such that S has sparsity $s < (n-r)^2$ and L has rank $\leq r$.

- Every entry of A is a function of the $n^2 - (n-r)^2$ many entries of L and s entries of S.
- These are n^2 polynomials each on $n^2 - (n-r)^2 + s$ variables.
- The entries of A are algebraically dependent. $(\Rightarrow\Leftarrow)$

- The matrix A is not explicit. The degree of the extension $[\mathbb{Q}(a_{11}, \ldots, a_{nn}) : \mathbb{Q}] = 2^{n^2}$.

Matrices with Algebraically Independent Entries

Lower Bound: Suppose not, $R_A^{\mathbb{R}}(r) < (n-r)^2$. Then $A = S + L$ such that S has sparsity $s < (n-r)^2$ and L has rank $\leq r$.

- Every entry of A is a function of the $n^2 - (n-r)^2$ many entries of L and s entries of S.
- These are n^2 polynomials each on $n^2 - (n-r)^2 + s$ variables.
- The entries of A are algebraically dependent. ($\Rightarrow\Leftarrow$)

- The matrix A is not explicit. The degree of the extension $[\mathbb{Q}(a_{11}, \ldots, a_{nn}) : \mathbb{Q}] = 2^{n^2}$.
- Can we reduce the amount of algebraic independence among the entries while maintaining rigidity?

Non-explicit Rigid Matrices

Theorem (Lokam(2000, 2006))

- *Let* $x_1, \ldots, x_n \in \mathbb{C}$ *be algebraically independent over* $\mathbb{Q}$ *and* $V = (x_i^j)_{1 \le i,j \le n}$ *be Vandermonde matrix in* $\mathbb{C}^{n \times n}$*. Then,* $R_V^{\mathbb{C}}(r) = \Omega(n^2)$ *for* $r \le O(\sqrt{n})$*.*

Non-explicit Rigid Matrices

Theorem (Lokam(2000, 2006))

- *Let* $x_1, \ldots, x_n \in \mathbb{C}$ *be algebraically independent over* $\mathbb{Q}$ *and* $V = (x_i^j)_{1 \leq i,j \leq n}$ *be Vandermonde matrix in* $\mathbb{C}^{n \times n}$*. Then,* $R_V^{\mathbb{C}}(r) = \Omega(n^2)$ *for* $r \leq O(\sqrt{n})$*.*
- *Let* $A \in \mathbb{C}^{n \times n}$ *with* $a_{ij} = \sqrt{p_{ij}}$ *for distinct primes* $p_{11}, \ldots, p_{nn}$*. Then,* $R_A^{\mathbb{C}}(r) = \Omega(n^2)$ *for* $r \leq n/32$*.*

Non-explicit Rigid Matrices

Theorem (Lokam(2000, 2006))

- *Let* $x_1, \ldots, x_n \in \mathbb{C}$ *be algebraically independent over* $\mathbb{Q}$ *and* $V = (x_i^j)_{1 \leq i,j \leq n}$ *be Vandermonde matrix in* $\mathbb{C}^{n \times n}$. *Then,* $R_V^{\mathbb{C}}(r) = \Omega(n^2)$ *for* $r \leq O(\sqrt{n})$.
- *Let* $A \in \mathbb{C}^{n \times n}$ *with* $a_{ij} = \sqrt{p_{ij}}$ *for distinct primes* $p_{11}, \ldots, p_{nn}$. *Then,* $R_A^{\mathbb{C}}(r) = \Omega(n^2)$ *for* $r \leq n/32$.

- Square root of distinct primes are linearly independent over $\mathbb{Q}$.

Non-explicit Rigid Matrices

Theorem (Lokam(2000, 2006))

- *Let* $x_1, \ldots, x_n \in \mathbb{C}$ *be algebraically independent over* $\mathbb{Q}$ *and* $V = (x_i^j)_{1 \le i,j \le n}$ *be Vandermonde matrix in* $\mathbb{C}^{n \times n}$. *Then,* $R_V^{\mathbb{C}}(r) = \Omega(n^2)$ *for* $r \le O(\sqrt{n})$.
- *Let* $A \in \mathbb{C}^{n \times n}$ *with* $a_{ij} = \sqrt{p_{ij}}$ *for distinct primes* $p_{11}, \ldots, p_{nn}$. *Then,* $R_A^{\mathbb{C}}(r) = \Omega(n^2)$ *for* $r \le n/32$.

- Square root of distinct primes are linearly independent over $\mathbb{Q}$.
- Proof via *algebraic dimension* argument(Shoup, Smolensky).

- Random matrices are rigid with high probability.

Rigidity of Random Matrices

- Random matrices are rigid with high probability.

[Goldreich, Tal 2013] Rigidity of Random Toeplitz matrix

For every $r \in [\sqrt{n}, n/32]$, $\mathcal{R}_T^{\mathbb{F}_2}(r) = \Omega\left(\frac{n^3}{r^2 \log n}\right)$ with probability $1 - o(1)$ where $T \in \mathbb{F}_2^{n \times n}$ is a random Toeplitz/Hankel matrix.

Toeplitz $T = \begin{bmatrix} a_0 & a_1 & a_2 \\ a_{-1} & a_0 & a_1 \\ a_{-2} & a_{-1} & a_0 \end{bmatrix}$ and Hankel $H = \begin{bmatrix} a_{-2} & a_{-1} & a_0 \\ a_{-1} & a_0 & a_1 \\ a_0 & a_1 & a_2 \end{bmatrix}$

Rigidity of Random Matrices

- Random matrices are rigid with high probability.

[Goldreich, Tal 2013] Rigidity of Random Toeplitz matrix

For every $r \in [\sqrt{n}, n/32]$, $\mathcal{R}_T^{\mathbb{F}_2}(r) = \Omega\left(\frac{n^3}{r^2 \log n}\right)$ with probability $1 - o(1)$ where $T \in \mathbb{F}_2^{n \times n}$ is a random Toeplitz/Hankel matrix.

Toeplitz $T = \begin{bmatrix} a_0 & a_1 & a_2 \\ a_{-1} & a_0 & a_1 \\ a_{-2} & a_{-1} & a_0 \end{bmatrix}$ and Hankel $H = \begin{bmatrix} a_{-2} & a_{-1} & a_0 \\ a_{-1} & a_0 & a_1 \\ a_0 & a_1 & a_2 \end{bmatrix}$

- Asymptotically better than $\Omega(\frac{n^2}{r} \log \frac{n}{r})$ if $r = o(\frac{n}{\log n \log\log n})$.

Rigidity of Random Matrices

- Random matrices are rigid with high probability.

[Goldreich, Tal 2013] Rigidity of Random Toeplitz matrix

For every $r \in [\sqrt{n}, n/32]$, $\mathcal{R}_T^{\mathbb{F}_2}(r) = \Omega\left(\frac{n^3}{r^2 \log n}\right)$ with probability $1 - o(1)$ where $T \in \mathbb{F}_2^{n \times n}$ is a random Toeplitz/Hankel matrix.

Toeplitz $T = \begin{bmatrix} a_0 & a_1 & a_2 \\ a_{-1} & a_0 & a_1 \\ a_{-2} & a_{-1} & a_0 \end{bmatrix}$ and Hankel $H = \begin{bmatrix} a_{-2} & a_{-1} & a_0 \\ a_{-1} & a_0 & a_1 \\ a_0 & a_1 & a_2 \end{bmatrix}$

- Asymptotically better than $\Omega(\frac{n^2}{r} \log \frac{n}{r})$ if $r = o(\frac{n}{\log n \log \log n})$.

Explicit construction in E^{NP}

- Run over all $n \times n$ Hankel/Toeplitz matrices with $\{0, 1\}$ entries.
- For each such matrix test if $\mathcal{R}_T^{\mathbb{F}_2}(r) = \Omega\left(\frac{n^3}{r^2 \log n}\right)$.

Designing $\mathrm{TEST}_{s,r}(H)$

$\mathrm{TEST}_{s,r}(H)$

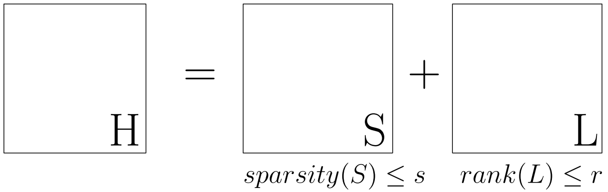
(1) If H is not rigid then reject H.
(2) If H is random Hankel matrix, accept H w.p $1 - o(1)$.

Designing $\text{TEST}_{s,r}(H)$

$\text{TEST}_{s,r}(H)$

(1) If H is not rigid then reject H.

(2) If H is random Hankel matrix, accept H w.p $1 - o(1)$.

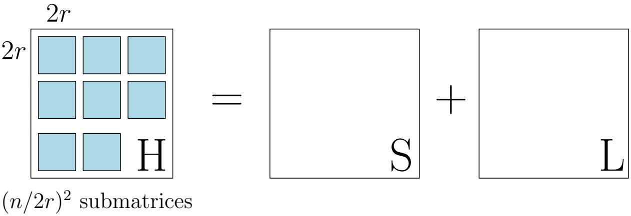


Designing $\mathsf{TEST}_{s,r}(H)$

$\mathsf{TEST}_{s,r}(H)$

(1) If H is not rigid then reject H.

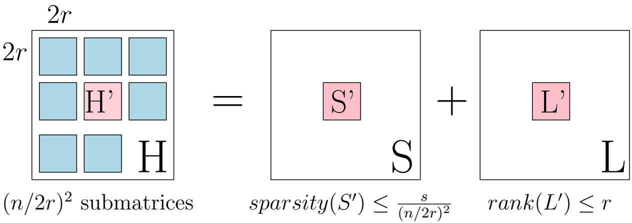
(2) If H is random Hankel matrix, accept H w.p $1 - o(1)$.



Designing $\mathsf{TEST}_{s,r}(H)$

$\mathsf{TEST}_{s,r}(H)$

(1) If H is not rigid then reject H.
(2) If H is random Hankel matrix, accept H w.p $1 - o(1)$.



Designing $\mathrm{TEST}_{s,r}(H)$

$\mathrm{TEST}_{s,r}(H)$

(1) If H is not rigid then reject H.
(2) If H is random Hankel matrix, accept H w.p $1 - o(1)$.

$\mathrm{TEST}_{s,r}(H)$

Partition H into submatrices of dimension $2r \times 2r$ each.
For every such submatrix H' of H
  For every $\frac{s}{(n/2r)^2}$-sparse matrix S' in $\mathbb{F}_2^{2r \times 2r}$
    If $\mathrm{rank}(H' - S') \le r$ then `reject` H
`Accept` H

Designing TEST$_{s,r}(H)$

TEST$_{s,r}(H)$

(1) If H is not rigid then reject H.
(2) If H is random Hankel matrix, accept H w.p $1 - o(1)$.

TEST$_{s,r}(H)$

Partition H into submatrices of dimension $2r \times 2r$ each.
For every such submatrix H' of H
  For every $\frac{s}{(n/2r)^2}$-sparse matrix S' in $\mathbb{F}_2^{2r \times 2r}$
    If $\mathrm{rank}(H' - S') \leq r$ then `reject` H
`Accept` H

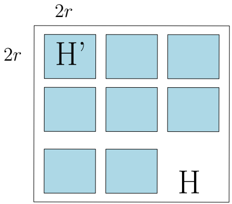
$\Pr[\text{TEST rejects } H] = \Pr[\exists H' \exists S' \ \mathrm{rank}(H'\text{-}S') \leq r]$
Need to bound $\Pr[\mathrm{rank}(H'\text{-}S') \leq r]$.

Designing $\text{TEST}_{s,r}(H)$

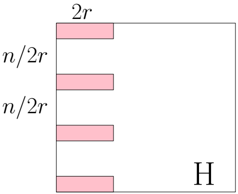
$\text{TEST}_{s,r}(H)$

Partition H into submatrices of dimension $2r \times 2r$ each.
For every such submatrix H' of H
  For every $\frac{s}{(n/2r)^2}$-sparse matrix S' in $\mathbb{F}_2^{2r\times 2r}$
    If $\text{rank}(H' - S') \le r$ then `reject` H
`Accept` H

$\Pr[\text{TEST rejects } H] = \Pr[\exists H' \exists S' \ \text{rank}(H'\text{-}S') \le r]$
Need to bound $\Pr[\text{rank}(H'\text{-}S') \le r]$.



$(n/2r)^2$ submatrices



Explicit Rigid matrices beyond exponential time

- (Folklore) Sub-exponential time construction of $M \in \mathbb{F}_2^{n \times n}$ with $R_M^{\mathbb{F}_2}(n^{1/2-\epsilon}) \geq \Omega(n^2/\log n)$.
- (Alman, Chen '20) $M \in \mathbb{F}_2^{n \times n}$ in P^{NP} such that there exists a $\delta > 0$ with $R_M(2^{(\log n)^{1/4-\epsilon}}) \geq \delta n^2$ for all $\epsilon > 0$.
- (Bhangale, Harsha, Paradise, Tal '20) $M \in \mathbb{F}_2^{n \times n}$ in P^{NP} such that there exists a $\delta > 0$ with $R_M(2^{\log n/\Omega(\log\log n)}) \geq \delta n^2$.

- Works for any finite field for large n.
- Proof via linear circuit lower bounds & PCPs.

The Road Thus Taken

1977	$R_A(\epsilon n) = n^{1+\delta}$	GOAL
1977	$\exists M\ R_A(r) = (n-r)^2/\log n$	Existence
1997	A in P, $R_A(r) = \Omega\left(\frac{n^2}{r}\log\frac{n}{r}\right)$	Untouched Minor argument
2000,2006	Non-explicit $R_A(r) = \Omega(n^2)$	Shoup-Smolensky Dimension
2013	A in E^{NP}, $R_A(r) = \Omega\left(\frac{n^3}{r^2 \log n}\right)$	Rigidity of Random Toeplitz matrices
2020	A in $2^{o(n)}$-time, $R_A(n^{0.5-\epsilon}) = \Omega\left(\frac{n^2}{\log n}\right)$	Talk by Ben Lee Volk
2020	A in P^{NP}, $R_A\left(2^{\log n/\Omega(\log\log n)}\right) \geq \delta n^2$	Talk by Amey Bhangale

Thank You! Questions?