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 $r$. 

$R_{\mathbb{F}}A(r)$ is the 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 $\text{rank}(A)$ is at most $r$.

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

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

▶ 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 $\text{rank}(A)$ is at most $r$.

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

\[
A = \begin{bmatrix}
\times & \times & \times \\
\times & \times & \\
\times & \times & \times
\end{bmatrix}_{n \times n}
\]

No. of \( \times \)'s here = \( s \)
Interpreting Matrix Rigidity

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

No. of $\times$’s here $= s$
Let $A \in \mathbb{F}^{n \times n}$. Suppose rigidity of matrix $A$ for rank $r$ is \( \leq s \).

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

\[
C = \begin{bmatrix}
\cdots & 0 & \cdots \\
0 & \cdots & 0 \\
\cdots & 0 & \cdots
\end{bmatrix}
\]

\[
c_{ij} = \begin{cases} 
    b_{ij} - a_{ij} & \text{if } (i,j) = x \\
    0 & \text{otherwise}
\end{cases}
\]
Interpreting Matrix Rigidity

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

$A = \begin{bmatrix} \times & \times & \times \\ \times & \times & \times \\ \times & \times & \times \end{bmatrix}_{n \times n}$

No. of $\times$'s here = $s$

$a_{ij} \mapsto b_{ij}$

$C = \begin{bmatrix} \end{bmatrix}_{n \times n}$

$\text{sparsity}(C) \leq s \quad \text{rank}(A + C) \leq r$

$c_{ij} = \begin{cases} b_{ij} - a_{ij} & \text{if } (i,j) = \times \\ 0 & \text{otherwise} \end{cases}$

▶ 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 \( \leq s \).

\[
A = \begin{bmatrix}
\times & \times & \times \\
\times & \times & \times \\
\times & \times & \times \\
n \times n
\end{bmatrix}
\]

No. of \( \times \)'s here = \( s \)

\[
C = \begin{bmatrix}
\vdots \\
\vdots \\
\vdots \\
n \times n
\end{bmatrix}
\]

\[
c_{ij} = \begin{cases} 
    b_{ij} - a_{ij} & \text{if } (i,j) = \times \\
    0 & \text{otherwise}
\end{cases}
\]

\( \text{sparsity}(C) \leq s \)

\( \text{rank}(A + C) \leq r \)

- 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 \( R_{A}^{\mathbb{F}}(r) \leq s \).

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

\[ R^F_A(r) = \min_C \{ \text{sparsity}(C) \mid C \in \mathbb{F}^{n \times n}, \text{rank}_\mathbb{F}(A + C) \leq r \} \]
Toy Example I: Identity Matrix

\[ R_F^A(r) = \min_C \{ \text{sparsity}(C) \mid C \in \mathbb{F}^{n \times n}, \ \text{rank}_F(A + C) \leq r \} \]

▶ 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

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

- 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 \( R_A(r) \leq s \).
Toy Example I: Identity Matrix

\[ R^F_A(r) = \min_C \{ \text{sparsity}(C) \mid C \in \mathbb{F}^{n \times n}, \ \text{rank}_F(A + C) \leq r \} \]

- 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

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

- 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

\[ R_A^F(r) = \min_{C} \{ \text{sparsity}(C) \mid C \in \mathbb{F}^{n \times n}, \ \text{rank}_F(A + C) \leq r \} \]

- 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 $2r$, $R_{M_n}^{F}(r) = \frac{n^2}{4r}$. 

```
\begin{array}{c}
\begin{bmatrix}
I_{2r} & \cdots & \cdots & I_{2r} \\
\vdots & \ddots & \vdots & \vdots \\
I_{2r} & \cdots & \cdots & I_{2r}
\end{bmatrix}
\end{array}
```

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

$n \times n$ blocks

$n/2r$ blocks
Theorem (Midrijānis (2005))

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

Proof.

- By changing $r$ entries in each block consistently, $\text{rank}(M_n)$ 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 $2r$, $R_{M_n}^F(r) = \frac{n^2}{4r}$.

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, $\text{rank}(M_n)$ 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. ($\iff$)
Theorem (Valiant(1977))

For any matrix $A \in \mathbb{F}^{n \times n}$ and any $r \leq n$, $R^F_A(r) \leq (n - r)^2$. 
Theorem (Valiant(1977))

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

**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 $A$. 
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 $A$. 

\[ \begin{bmatrix} 
    r & (n-r) \\
    D & E \\
    r & (n-r) \\
\end{bmatrix} \]
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 $B$.

\[
A = \begin{bmatrix}
B & C \\
D & E
\end{bmatrix}
\]

\[
\alpha_1\text{row}_1(B) + \alpha_2\text{row}_2(B) + \cdots + \alpha_r\text{row}_r(B)
\]
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 $C$. 

\[
A = \begin{bmatrix} B & C \\ D & E \end{bmatrix}
\]

\[
\text{row}_{1}(C) \alpha_{1} + \text{row}_{2}(C) \alpha_{2} + \cdots + \text{row}_{r}(C) \alpha_{r}
\]
Upper Bounds on Matrix Rigidity

**Theorem (Valiant(1977))**

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

**Proof.**

- If \( \text{rank}(A) \leq r \) then \( R^A_A(r) = 0 \).
- 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, \( R_{\mathbb{F}}^A(r) \leq (n - r)^2 \).
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 $C$ over $\mathbb{F}$ is a DAG where
  - in-degree 0 gates: labelled by variables;
  - internal gates: labelled by $+$;
  - edges: labelled by constants in $\mathbb{F}$.

\[
x \mapsto Ax
\]

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

\[
x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}
\]

8$x_1$ + 3$x_2$
7$x_1$ + 5$x_2$
**Linear Circuits**

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

- A linear circuit $C$ 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.

```
8x_1 + 3x_2
+ 7x_1 + 5x_2
+ 1 4
+ 1
+ 1
+ 1
2 1 1 3 1 1
x_1 x_2 x_1 x_2 x_1

x \mapsto A \cdot x
A = 8 3
  7 5
x = [x_1]
```
Linear Circuits

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

- A linear circuit $C$ 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 $C$ 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.
$C$ computes a linear transformation represented by $A \in \mathbb{F}^{n \times n}$.
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.
$\mathcal{C}$ 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 $\mathbb{F}^n \rightarrow \mathbb{F}^n$ can be computed by a linear circuit of size $O(n^2)$ and depth $O(\log n)$. 
Linear Circuits

- A linear circuit $C$ 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 of $C$: $\#$ of edges
- Depth of $C$: length of longest path from i/p to o/p.

- Best known size lower bound: $3n - o(n)$ (Chashkin 1994).
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.
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 $\Omega(n \log \log n)$. 
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* $\epsilon$ 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 (Erdős, 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 $\epsilon$ times, length of every path at most $d/2^\epsilon$ and no. of edges removed is $s\epsilon/\log d$.

\[
\ell_i \\
\quad b_2 \\
\quad \quad b_1 \\
\quad \quad \quad b_3 \\
---\text{removed edges} \\
b_1, \ldots, b_k: \text{tails of removed edges} \\
k \leq \frac{s\epsilon}{\log d}
\]
Proof (contd.)

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

\[
\ell_i = \sum_{j=1}^{k} \alpha_{ij} b_j + c_i
\]

\[
\alpha_{ij} \in F, \quad b_j \in F^n
\]

\[
c_i \in F^n, \quad 2^{d/2^\epsilon} \text{-sparse}
\]
Each \( \ell_i \) is a linear combination of the tails \( b_1, \ldots, b_k \) and at most \( 2^{d/2^\epsilon} \) input variables.

\[
\ell_i = \sum_{j=1}^k \alpha_{ij} b_j + c_i
\]
Each $\ell_i$ is a linear combination of the tails $b_1, \ldots, b_k$ and at most $2^{d/2^e}$ input variables.

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

$A = B_1 B_2 + C$ 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 $\ell_i$ is a linear combination of the tails $b_1, \ldots, b_k$ and at most $2^{d/2^\epsilon}$ input variables.

\[ \ell_i = \sum_{j=1}^{k} \alpha_{ij} b_j + c_i \]

- $A = B_1 B_2 + C$ 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 $\text{sparsity}(C) \leq n 2^{d/2^\epsilon}$. 
Each $\ell_i$ is a linear combination of the tails $b_1, \ldots, b_k$ and at most $2^{d/2^\epsilon}$ input variables.

$$\ell_i = \sum_{j=1}^{k_i} \alpha_{ij} b_j + c_i$$

$A = B_1 B_2 + C$ 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 $n2^{d/2^\epsilon}$. 
Proof (contd.)

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

\[ \ell_i = \sum_{j=1}^{k} \alpha_{ij} b_j + c_i \]

- $A = B_1 B_2 + C$ 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 $\text{sparsity}(C) \leq n 2^{d/2^\epsilon}$.

- Thus, rigidity of $A$ for rank $\frac{s \epsilon}{\log d}$ is at most $n 2^{d/2^\epsilon}$.

- 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 $\Omega(n \log \log n)$. 

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).
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 $R_{M_n}^\mathbb{F}(\epsilon n) \geq \Omega(n^{1+\delta})$ for $\epsilon, \delta > 0$. 

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

Recent Progress towards answering Valiant’s Question (and beyond).
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 $\Omega(n \log \log n)$.

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

- \textit{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 $R^\mathbb{F}_q_M(r) = \Omega((n - r)^2 / \log n)$. 
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 $0 \leq r \leq n - \Omega(\sqrt{n})$ 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: 

$$\binom{n^2}{s} \cdot q^s \cdot \binom{n}{r}^2 \cdot q^{n^2-(n-r)^2}.$$  

- no. of $s$-sparse matrices  
- no. of rank-$r$ 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 $R_M^F(r) = \Omega((n - r)^2 / \log n)$.

**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: 
\[
\binom{n^2}{s} \cdot q^s \cdot \binom{n}{r}^2 \cdot q^{n^2 - (n-r)^2}.
\]

- No. of $s$-sparse matrices
- No. of rank-$r$ 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

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: $q^{O(n^2)} \cdot q^s \cdot n^{O(1)}$. 

Super-exponential time construction
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 $R^\mathbb{F}_M(r) = (n - r)^2$. 
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 $r$. 
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 \( x_1, \ldots, x_n, y_1, \ldots, y_n \in F \).

Theorem (Shokrollahi, Spielman, Stemann(1997))

Let \( F \) be a field with at least \( 2n \) distinct elements and \( M_n \) be \( n \times n \) Cauchy matrix. Then, \( R_{M_n}^{F}(r) = \Omega(\frac{n^2}{r} \log \frac{n}{r}) \) for \( \log n \leq r \leq n/2 \).
Proof of SSS‘97

Suppose not, $R_{M_n}^F(r) = o\left(\frac{n^2}{r} \log \frac{n}{r}\right)$. 

Consider a bipartite graph $G = (U, V, E)$ with $|U| = |V| = n$ such that $(i, j) \in E(G)$ iff $M_{ij}$ is untouched.

Theorem (Kovári-Sos-Turán (1954))

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

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

▶ If fewer than $n^2/4\left(\frac{r+1}{2}\right)\log \frac{n}{r}$ entries in $M_n$ are changed an $(r+1) \times (r+1)$ submatrix of $M_n$ remains untouched.
Proof of SSS‘97

Suppose not, \( R^F_{M_n}(r) = o\left(\frac{n^2}{r} \log \frac{n}{r}\right) \). That is, by changing \( o\left(\frac{n^2}{r} \log \frac{n}{r}\right) \) entries in \( M \), rank can be reduced to \( r \).
Proof of SSS‘97

Suppose not, $R_{M_n}^{\text{F}}(r) = o\left(\frac{n^2}{r} \log \frac{n}{r}\right)$. That is, by changing $o\left(\frac{n^2}{r} \log \frac{n}{r}\right)$ 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 $n^2 - o\left(\frac{n^2}{r} \log \frac{n}{r}\right)$ edges.
Proof of SSS‘97

Suppose not, $R_{M_n}^F(r) = o\left(\frac{n^2}{r} \log \frac{n}{r}\right)$. That is, by changing $o\left(\frac{n^2}{r} \log \frac{n}{r}\right)$ 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 $n^2 - o\left(\frac{n^2}{r} \log \frac{n}{r}\right)$ 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, \( R^F_{M_n}(r) = o\left(\frac{n^2}{r} \log \frac{n}{r}\right) \). That is, by changing \( o\left(\frac{n^2}{r} \log \frac{n}{r}\right) \) 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 \( n^2 - o\left(\frac{n^2}{r} \log \frac{n}{r}\right) \) 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, \( R^F_{M_n}(r) = o\left(\frac{n^2}{r} \log \frac{n}{r}\right) \). That is, by changing \( o\left(\frac{n^2}{r} \log \frac{n}{r}\right) \) 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 \( n^2 - o\left(\frac{n^2}{r} \log \frac{n}{r}\right) \) 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 $P(a_1, \ldots, a_n) = 0$. 

{\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 $r \leq n$, $\det(R^n(A) \cap \mathbb{R}^r) = (n-r)^2$. 

Proof. Upper bound via Valiant's theorem.
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 \textit{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 \textit{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 \( r \leq n \), \( R_A^R(r) = (n - r)^2 \).

**Proof.** Upper bound via Valiant’s theorem.
Matrices with Algebraically Independent Entries

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

The entries of $A$ are algebraically dependent. ($\Rightarrow \Leftrightarrow$) The matrix $A$ is not explicit. The degree of the extension $\mathbb{Q}(a_{11},...,a_{nn}) : \mathbb{Q}$ = 2 $n^2$. Can we reduce the amount of algebraic independence among the entries while maintaining rigidity?
Lower Bound: Suppose not, $R^\mathbb{R}_A(r) < (n - r)^2$. 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 $S$. 

Every entry of $A$ is a function of the $n^2 - (n - r)^2$ many entries of $L$ and $s$ entries of $S$.
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. (\( \Rightarrow \equiv \))
Matrices with Algebraically Independent Entries

Lower Bound: Suppose not, $R^\mathbb{R}_A(r) < (n - r)^2$. 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, $R^\mathbb{R}_A(r) < (n - r)^2$. 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?
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, $R_V^C(r) = \Omega(n^2)$ for $r \leq O(\sqrt{n})$. 

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

Proof via algebraic dimension argument (Shoup, Smolensky).
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 $\mathbb{Q}$. Proof via algebraic dimension argument (Shoup, Smolensky).
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, $R^C_V(r) = \Omega(n^2)$ 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, $R^C_A(r) = \Omega(n^2)$ for $r \leq n/32$.

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

Proof via algebraic dimension argument (Shoup, Smolensky).
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 $\mathbb{Q}$.
- Proof via algebraic dimension argument(Shoup, Smolensky).
Random matrices are rigid with high probability.
Random matrices are rigid with high probability.

[Goldreich, Tal 2013] Rigidity of Random Toeplitz matrix

For every $r \in [\sqrt{n}, n/32]$, $\mathcal{R}_T^F(r) = \Omega\left(\frac{n^3}{r^2 \log n}\right)$ 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 $H = \begin{bmatrix} a_{-2} & a_{-1} & a_0 \\ a_{-1} & a_0 & a_1 \\ a_0 & a_1 & a_2 \end{bmatrix}$
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 $\Omega \left( \frac{n^2}{r} \log \frac{n}{r} \right)$ if $r = o \left( \frac{n}{\log n \log \log n} \right)$.
Rigidity of Random Matrices

- Random matrices are rigid with high probability.

[Goldreich, Tal 2013] Rigidity of Random Toeplitz matrix

For every $r \in [\sqrt{n}, n/32]$, $\mathcal{R}^{\mathbb{F}_2}_T(r) = \Omega \left( \frac{n^3}{r^2 \log n} \right)$ 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 $r = o\left(\frac{n}{\log n \log \log n}\right)$.

**Explicit construction in $E^{NP}$**

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

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

\[
H = S + L
\]

$\text{sparsity}(S) \leq s$ \hspace{1cm} $\text{rank}(L) \leq r$
Designing $\text{TEST}_{s,r}(H)$

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

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

\[
\begin{align*}
\text{(2r) \times \text{2r submatrices}} & = S + L \\
\end{align*}
\]
Designing $\text{TEST}_{s,r}(H)$

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

\[
\begin{align*}
\text{TEST}_{s,r}(H) & = S' + L' \\
\text{sparsity}(S') & \leq \frac{s}{(n/2r)^2} \\
\text{rank}(L') & \leq r
\end{align*}
\]
Designing $\text{TEST}_{s,r}(H)$

<table>
<thead>
<tr>
<th>Test $\text{TEST}_{s,r}(H)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) If $H$ is not rigid then reject $H$.</td>
</tr>
<tr>
<td>(2) If $H$ is random Hankel matrix, accept $H$ w.p $1 - o(1)$.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test $\text{TEST}_{s,r}(H)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition $H$ into submatrices of dimension $2r \times 2r$ each.</td>
</tr>
<tr>
<td>For every such submatrix $H'$ of $H$</td>
</tr>
<tr>
<td>For every $\frac{s}{(n/2r)^2}$-sparse matrix $S'$ in $F_{2}^{2r \times 2r}$</td>
</tr>
<tr>
<td>If $\text{rank}(H' - S') \leq r$ then reject $H$</td>
</tr>
<tr>
<td>Accept $H$</td>
</tr>
</tbody>
</table>
Designing $\text{TEST}_{s,r}(H)$

**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 $\text{rank}(H' - S') \leq r$ then reject $H$

Accept $H$

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

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

![Diagram of submatrices](image-url)
Explicit Rigid matrices beyond exponential time

- **(Folklore)** Sub-exponential time construction of $M \in \mathbb{F}_2^{n \times n}$ with $R_M(\frac{n^{1/2}}{\log n}) \geq \Omega(n^2 / \log n)$.

- **(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

<table>
<thead>
<tr>
<th>Year</th>
<th>Equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1977</td>
<td>$R_A(\epsilon n) = n^{1+\delta}$</td>
</tr>
<tr>
<td>1977</td>
<td>$\exists M R_A(r) = (n-r)^2/\log n$</td>
</tr>
<tr>
<td>1997</td>
<td>$A$ in P, $R_A(r) = \Omega\left(\frac{n^2 \log n}{r}\right)$</td>
</tr>
<tr>
<td>2000, 2006</td>
<td>Non-explicit $R_A(r) = \Omega(n^2)$</td>
</tr>
<tr>
<td>2013</td>
<td>$A$ in $E^{NP}$, $R_A(r) = \Omega\left(\frac{n^3}{r^2 \log n}\right)$</td>
</tr>
<tr>
<td>2020</td>
<td>$A$ in $2^{o(n)}$-time, $R_A(n^{0.5-\epsilon}) = \Omega\left(\frac{n^2}{\log n}\right)$</td>
</tr>
<tr>
<td>2020</td>
<td>$A$ in $P^{NP}$, $R_A(2^{\log n/\Omega(\log \log n)}) \geq \delta n^2$</td>
</tr>
</tbody>
</table>

### GOAL
- Existence
- Untouched Minor argument
- Shoup-Smolensky Dimension
- Rigidity of Random Toeplitz matrices

#### Talk by Ben Lee Volk
- 2020

#### Talk by Amey Bhangale
- 2020

---

**Thank You! Questions?**