Lower Bounds on Matrix Rigidity via a Quantum Argument

Ronald de Wolf

CWI Amsterdam

Rigidity: What and why?

- Consider full-rank $n \times n$ matrix M

Rigidity: What and why?

- Consider full-rank $n \times n$ matrix M
- How many of its entries do we need to change if we want to lower its rank to r?

Rigidity: What and why?

- Consider full-rank $n \times n$ matrix M
- How many of its entries do we need to change if we want to lower its rank to r?
- $R_M(r) = \min\{\Delta(M, \widetilde{M}) \mid \text{rank}(\widetilde{M}) \leq r\}$

Rigidity: What and why?

- Consider full-rank $n \times n$ matrix M
- How many of its entries do we need to change if we want to lower its rank to r?
- $R_M(r) = \min\{\Delta(M, \widetilde{M}) \mid \text{rank}(\widetilde{M}) \leq r\}$
- Example:
  $R_I(r) = n - r$

Rigidity: What and why?

- Consider full-rank $n \times n$ matrix M
- How many of its entries do we need to change if we want to lower its rank to r?
- $R_M(r) = \min\{\Delta(M, \widetilde{M}) \mid \text{rank}(\widetilde{M}) \leq r\}$
- Example:
  $R_I(r) = n - r$
  $R_M(r) \approx (n - r)^2$ for random M

Rigidity: What and why?

- Consider full-rank $n \times n$ matrix M
- How many of its entries do we need to change if we want to lower its rank to r?
- $R_M(r) = \min\{\Delta(M, \widetilde{M}) \mid \text{rank}(\widetilde{M}) \leq r\}$
- Example:
  $R_I(r) = n - r$
  $R_M(r) \approx (n-r)^2$ for random M
- Motivation (Valiant 77):

Rigidity: What and why?

- Consider full-rank $n \times n$ matrix M
- How many of its entries do we need to change if we want to lower its rank to r?
- $R_M(r) = \min\{\Delta(M, \widetilde{M}) \mid \text{rank}(\widetilde{M}) \leq r\}$
- Example:
  $R_I(r) = n - r$
  $R_M(r) \approx (n-r)^2$ for random M
- Motivation (Valiant 77): Explicit matrix with high rigidity implies size-depth tradeoffs for arithmetic circuits

Rigidity: What and why?

- Consider full-rank $n \times n$ matrix M
- How many of its entries do we need to change if we want to lower its rank to r?
- $R_M(r) = \min\{\Delta(M, \widetilde{M}) \mid \text{rank}(\widetilde{M}) \leq r\}$
- Example:
  $R_I(r) = n - r$
  $R_M(r) \approx (n-r)^2$ for random M
- Motivation (Valiant 77): Explicit matrix with high rigidity implies size-depth tradeoffs for arithmetic circuits
- Good candidate: $n \times n$ Hadamard matrix H

Connection with quantum

- Renormalized rows $|\widetilde{H}_i\rangle$ of matrix $\widetilde{H} \approx H$ form a quantum communication system!

Connection with quantum

- Renormalized rows $|\widetilde{H}_i\rangle$ of matrix $\widetilde{H} \approx H$ form a quantum communication system!
- To communicate i:

Connection with quantum

- Renormalized rows $|\widetilde{H}_i\rangle$ of matrix $\widetilde{H} \approx H$ form a quantum communication system!
- To communicate i:

  (1) Alice sends $|\widetilde{H}_i\rangle$ in r dimensions

Connection with quantum

- Renormalized rows $|\widetilde{H}_i\rangle$ of matrix $\widetilde{H} \approx H$ form a quantum communication system!
- To communicate i:

  (1) Alice sends $|\widetilde{H}_i\rangle$ in r dimensions
  (2) Bob measures in Hadamard basis

Connection with quantum

- Renormalized rows $|\widetilde{H}_i\rangle$ of matrix $\widetilde{H} \approx H$ form a quantum communication system!
- To communicate i:

  (1) Alice sends $|\widetilde{H}_i\rangle$ in r dimensions
  (2) Bob measures in Hadamard basis
- Success probability $p_i = |\langle\widetilde{H}_i|H_i\rangle|^2$

Connection with quantum

- Renormalized rows $|\widetilde{H}_i\rangle$ of matrix $\widetilde{H} \approx H$ form a quantum communication system!
- To communicate i:

  (1) Alice sends $|\widetilde{H}_i\rangle$ in r dimensions
  (2) Bob measures in Hadamard basis
- Success probability $p_i = |\langle\widetilde{H}_i|H_i\rangle|^2$ is higher if $\widetilde{H}_i$ is a better approximation of H_i.

Connection with quantum

- Renormalized rows $|\widetilde{H}_i\rangle$ of matrix $\widetilde{H} \approx H$ form a quantum communication system!
- To communicate i:

  (1) Alice sends $|\widetilde{H}_i\rangle$ in r dimensions
  (2) Bob measures in Hadamard basis
- Success probability $p_i = |\langle \widetilde{H}_i | H_i \rangle|^2$ is higher if $\widetilde{H}_i$ is a better approximation of H_i.
- Nayak 99: $\sum_{i=1}^{n} p_i \leq r$

Connection with quantum

- Renormalized rows $|\widetilde{H}_i\rangle$ of matrix $\widetilde{H} \approx H$ form a quantum communication system!
- To communicate i:

  (1) Alice sends $|\widetilde{H}_i\rangle$ in r dimensions
  (2) Bob measures in Hadamard basis
- Success probability $p_i = |\langle\widetilde{H}_i|H_i\rangle|^2$ is higher if $\widetilde{H}_i$ is a better approximation of H_i.
- Nayak 99: $\sum_{i=1}^{n} p_i \leq r$
- Tradeoff between r and the quality of the approximation

Two applications

- $R_H(r) \geq \dfrac{n^2}{4r}$

Two applications

- $R_H(r) \geq \dfrac{n^2}{4r}$
- This improves Kashin & Razborov by factor 64

Two applications

- $R_H(r) \geq \dfrac{n^2}{4r}$
- This improves Kashin & Razborov by factor 64
- If we limit the change-per-entry to θ:

Two applications

- $R_H(r) \geq \dfrac{n^2}{4r}$
- This improves Kashin & Razborov by factor 64
- If we limit the change-per-entry to θ:
  $R_H(r,\theta) \geq \dfrac{n^2(n-r)}{2\theta n + r(\theta^2 + 2\theta)}$

Two applications

- $R_H(r) \geq \dfrac{n^2}{4r}$
- This improves Kashin & Razborov by factor 64
- If we limit the change-per-entry to θ:
  $$R_H(r,\theta) \geq \frac{n^2(n-r)}{2\theta n + r(\theta^2 + 2\theta)}$$
- Matches earlier results of Lokam and Kashin-Razborov

To be or not to be quantum

- Of course, this is all linear algebra

To be or not to be quantum

- Of course, this is all linear algebra

- An anonymous referee suggested an alternative linear algebra proof for the same bounds

To be or not to be quantum

- Of course, this is all linear algebra
- An anonymous referee suggested an alternative linear algebra proof for the same bounds
- Quantum method is potentially stronger

To be or not to be quantum

- Of course, this is all linear algebra
- An anonymous referee suggested an alternative linear algebra proof for the same bounds
- Quantum method is potentially stronger
- Simple proof of $R_M(r) \geq n^2/4r$ for $H_2^{\otimes \log n}$ (Midrijanis)

Summary

- Reproved best known bounds on rigidity of Hadamard matrix

Summary

- Reproved best known bounds on rigidity of Hadamard matrix using quantum information theory

Summary

- Reproved best known bounds on rigidity of Hadamard matrix using quantum information theory

- Fits in a sequence of quantum proofs for classical theorems

Summary

- Reproved best known bounds on rigidity of Hadamard matrix using quantum information theory
- Fits in a sequence of quantum proofs for classical theorems
- These rigidity bounds are not very good

Summary

- Reproved best known bounds on rigidity of Hadamard matrix using quantum information theory
- Fits in a sequence of quantum proofs for classical theorems
- These rigidity bounds are not very good
- But: the connection with quantum gives a fresh look at this 28-year old problem, and may yield more