Lower bound on quantum full mixed-state tomography

arXiv:2207.08800

Joran van Apeldoorn[1,2], Arjan Cornelissen[1,4], András Gilyén[3], Giacomo Nannicini[4]

[1]QuSoft, University of Amsterdam, the Netherlands
[2]IViR, University of Amsterdam, the Netherlands
[3]Alfréd Rényi Institute of Mathematics, Budapest, Hungary
[4]IBM Quantum, IBM T.J. Watson research center, Yorktown Heights, NY, USA

August 18th, 2022

Quantum full state tomography overview

"Quantum full state tomography is learning a classical description of a quantum state."

Quantum full state tomography overview

"Quantum full state tomography is learning a classical description of a quantum state."

Full mixed-state tomography:

Full pure-state tomography:

Quantum full state tomography overview

"Quantum full state tomography is learning a classical description of a quantum state."

Full mixed-state tomography:

Full pure-state tomography:
Unknown: $|\psi\rangle \in \mathbb{C}^d$.
Goal: obtain $\left|\widetilde{\psi}\right\rangle \in \mathbb{C}^d$, s.t. $\left\|\left|\widetilde{\psi}\right\rangle - |\psi\rangle\right\|_2 \leq \varepsilon$.

Quantum full state tomography overview

"Quantum full state tomography is learning a classical description of a quantum state."

Full mixed-state tomography:

Full pure-state tomography:

Unknown: $|\psi\rangle \in \mathbb{C}^d$.

Goal: obtain $\left|\widetilde{\psi}\right\rangle \in \mathbb{C}^d$, s.t. $\left\|\left|\widetilde{\psi}\right\rangle - |\psi\rangle\right\|_2 \leq \varepsilon$.

1. Given access to conditional copies $(|0\rangle|0\rangle + |\psi\rangle|1\rangle)/\sqrt{2}$:
   1. $\widetilde{O}(\frac{d}{\varepsilon^2})$. [KP'20; This work]
   2. $\Omega(\frac{d}{\varepsilon^2})$. [This work]

Quantum full state tomography overview

"Quantum full state tomography is learning a classical description of a quantum state."

Full mixed-state tomography:

Full pure-state tomography:

Unknown: $|\psi\rangle \in \mathbb{C}^d$.

Goal: obtain $\left|\widetilde{\psi}\right\rangle \in \mathbb{C}^d$, s.t. $\left\|\left|\widetilde{\psi}\right\rangle - |\psi\rangle\right\|_2 \leq \varepsilon$.

1. Given access to conditional copies $(|0\rangle|0\rangle + |\psi\rangle|1\rangle)/\sqrt{2}$:
   1. $\widetilde{O}(\frac{d}{\varepsilon^2})$. [KP'20; This work]
   2. $\Omega(\frac{d}{\varepsilon^2})$. [This work]
2. Given (inverse) unitary access to $|\psi\rangle$:
   1. $\widetilde{O}(\frac{d}{\varepsilon})$. [This work]
   2. $\Omega(\frac{d}{\varepsilon})$. [This work]

Quantum full state tomography overview

"Quantum full state tomography is learning a classical description of a quantum state."

Full pure-state tomography:
Unknown: $|\psi\rangle \in \mathbb{C}^d$.
Goal: obtain $\left|\widetilde{\psi}\right\rangle \in \mathbb{C}^d$, s.t. $\left\|\left|\widetilde{\psi}\right\rangle - |\psi\rangle\right\|_2 \leq \varepsilon$.

1. Given access to conditional copies $(|0\rangle|0\rangle + |\psi\rangle|1\rangle)/\sqrt{2}$:
   1. $\widetilde{O}(\frac{d}{\varepsilon^2})$. [KP'20; This work]
   2. $\Omega(\frac{d}{\varepsilon^2})$. [This work]
2. Given (inverse) unitary access to $|\psi\rangle$:
   1. $\widetilde{O}(\frac{d}{\varepsilon})$. [This work]
   2. $\Omega(\frac{d}{\varepsilon})$. [This work]

Full mixed-state tomography:
Unknown: $\rho \in \mathbb{C}^{d\times d}$, with $\mathrm{rank}(\rho) \leq r$.
Goal: obtain $\widetilde{\rho} \in \mathbb{C}^{d\times d}$, s.t. $\|\widetilde{\rho} - \rho\|_1 \leq \varepsilon$.

Quantum full state tomography overview

"Quantum full state tomography is learning a classical description of a quantum state."

Full pure-state tomography:
Unknown: $|\psi\rangle \in \mathbb{C}^d$.
Goal: obtain $\left|\widetilde{\psi}\right\rangle \in \mathbb{C}^d$, s.t. $\left\|\left|\widetilde{\psi}\right\rangle - |\psi\rangle\right\|_2 \leq \varepsilon$.

1. Given access to conditional copies $(|0\rangle|0\rangle + |\psi\rangle|1\rangle)/\sqrt{2}$:
   1. $\widetilde{O}(\frac{d}{\varepsilon^2})$. [KP'20; This work]
   2. $\Omega(\frac{d}{\varepsilon^2})$. [This work]
2. Given (inverse) unitary access to $|\psi\rangle$:
   1. $\widetilde{O}(\frac{d}{\varepsilon})$. [This work]
   2. $\Omega(\frac{d}{\varepsilon})$. [This work]

Full mixed-state tomography:
Unknown: $\rho \in \mathbb{C}^{d\times d}$, with $\mathrm{rank}(\rho) \leq r$.
Goal: obtain $\widetilde{\rho} \in \mathbb{C}^{d\times d}$, s.t. $\|\widetilde{\rho} - \rho\|_1 \leq \varepsilon$.

1. Given access to single copies of ρ:
   1. $O(\frac{dr^2}{\varepsilon^2})$. [HHJ+'17]
   2. $\Omega(\frac{dr^2}{\varepsilon^2})$. [HHJ+'17; CHL+'22]

Quantum full state tomography overview

"Quantum full state tomography is learning a classical description of a quantum state."

Full pure-state tomography:
Unknown: $|\psi\rangle \in \mathbb{C}^d$.
Goal: obtain $\left|\widetilde{\psi}\right\rangle \in \mathbb{C}^d$, s.t. $\left\|\left|\widetilde{\psi}\right\rangle - |\psi\rangle\right\|_2 \leq \varepsilon$.

1. Given access to conditional copies $(|0\rangle|0\rangle + |\psi\rangle|1\rangle)/\sqrt{2}$:
   1. $\widetilde{O}(\frac{d}{\varepsilon^2})$. [KP'20; This work]
   2. $\Omega(\frac{d}{\varepsilon^2})$. [This work]
2. Given (inverse) unitary access to $|\psi\rangle$:
   1. $\widetilde{O}(\frac{d}{\varepsilon})$. [This work]
   2. $\Omega(\frac{d}{\varepsilon})$. [This work]

Full mixed-state tomography:
Unknown: $\rho \in \mathbb{C}^{d\times d}$, with $\mathrm{rank}(\rho) \leq r$.
Goal: obtain $\widetilde{\rho} \in \mathbb{C}^{d\times d}$, s.t. $\|\widetilde{\rho} - \rho\|_1 \leq \varepsilon$.

1. Given access to single copies of ρ:
   1. $O(\frac{dr^2}{\varepsilon^2})$. [HHJ+'17]
   2. $\Omega(\frac{dr^2}{\varepsilon^2})$. [HHJ+'17; CHL+'22]
2. Given access to simultaneous copies of ρ:
   1. $\widetilde{O}(\frac{dr}{\varepsilon^2})$. [HHJ+'17]
   2. $\Omega(\frac{dr}{\varepsilon^2})$. [HHJ+'17; Yue'22]

Quantum full state tomography overview

"Quantum full state tomography is learning a classical description of a quantum state."

Full pure-state tomography:
Unknown: $|\psi\rangle \in \mathbb{C}^d$.
Goal: obtain $\left|\widetilde{\psi}\right\rangle \in \mathbb{C}^d$, s.t. $\left\|\left|\widetilde{\psi}\right\rangle - |\psi\rangle\right\|_2 \leq \varepsilon$.

1. Given access to conditional copies $(|0\rangle|0\rangle + |\psi\rangle|1\rangle)/\sqrt{2}$:
   1. $\widetilde{O}(\frac{d}{\varepsilon^2})$. [KP'20; This work]
   2. $\Omega(\frac{d}{\varepsilon^2})$. [This work]
2. Given (inverse) unitary access to $|\psi\rangle$:
   1. $\widetilde{O}(\frac{d}{\varepsilon})$. [This work]
   2. $\Omega(\frac{d}{\varepsilon})$. [This work]

Full mixed-state tomography:
Unknown: $\rho \in \mathbb{C}^{d\times d}$, with $\mathrm{rank}(\rho) \leq r$.
Goal: obtain $\widetilde{\rho} \in \mathbb{C}^{d\times d}$, s.t. $\|\widetilde{\rho} - \rho\|_1 \leq \varepsilon$.

1. Given access to single copies of ρ:
   1. $O(\frac{dr^2}{\varepsilon^2})$. [HHJ+'17]
   2. $\Omega(\frac{dr^2}{\varepsilon^2})$. [HHJ+'17; CHL+'22]
2. Given access to simultaneous copies of ρ:
   1. $\widetilde{O}(\frac{dr}{\varepsilon^2})$. [HHJ+'17]
   2. $\Omega(\frac{dr}{\varepsilon^2})$. [HHJ+'17; Yue'22]
3. Given (inverse) unitary access to a purification:
   1. $\widetilde{O}(\frac{dr}{\varepsilon})$. [This work]
   2. $\Omega(\frac{dr}{\varepsilon})$. [This talk – yet to be included]

Aside: other quantum state tomography results

"Quantum state tomography is learning properties of a quantum state."

Aside: other quantum state tomography results

"Quantum state tomography is learning properties of a quantum state."

Learning observables:
$O_1, \dots, O_M$ with $\|O_j\| \leq 1$.
Unknown: $|\psi\rangle \in \mathbb{C}^d$.
Goal: obtain $\widetilde{o}_j$ s.t. $|\widetilde{o}_j - \langle\psi| O_j |\psi\rangle| \leq \varepsilon$.

Aside: other quantum state tomography results

"Quantum state tomography is learning properties of a quantum state."

Learning observables:
$O_1, \dots, O_M$ with $\|O_j\| \leq 1$.
Unknown: $|\psi\rangle \in \mathbb{C}^d$.
Goal: obtain $\widetilde{o}_j$ s.t. $|\widetilde{o}_j - \langle\psi| O_j |\psi\rangle| \leq \varepsilon$.

1. Given copies of $|\psi\rangle$:
   1. $O(\frac{\log(M)}{\varepsilon^2})$. *(if they commute)*
   2. $O(\frac{\log(M)}{\varepsilon^4})$. *(shadow tomgoraphy)* [HKP'20]

Aside: other quantum state tomography results

"Quantum state tomography is learning properties of a quantum state."

Learning observables:
$O_1, \ldots, O_M$ with $\|O_j\| \leq 1$.
Unknown: $|\psi\rangle \in \mathbb{C}^d$.
Goal: obtain $\widetilde{o}_j$ s.t. $|\widetilde{o}_j - \langle\psi| O_j |\psi\rangle| \leq \varepsilon$.

1. Given copies of $|\psi\rangle$:
   1. $O(\frac{\log(M)}{\varepsilon^2})$. *(if they commute)*
   2. $O(\frac{\log(M)}{\varepsilon^4})$. *(shadow tomgoraphy)* [HKP'20]
2. Given unitary access to $|\psi\rangle$:
   1. $\widetilde{O}(\frac{\sqrt{\sum_{j=1}^M \|O_j\|^2}}{\varepsilon}) = \widetilde{O}(\frac{\sqrt{M}}{\varepsilon})$. [HWC+'22]
   2. $\widetilde{O}(\frac{\sqrt{\|\sum_{j=1}^M O_j^2\|}}{\varepsilon}) = \widetilde{O}(\frac{\sqrt{M}}{\varepsilon})$. [This work]

Aside: other quantum state tomography results

"Quantum state tomography is learning properties of a quantum state."

Learning observables:

$O_1, \dots, O_M$ with $\|O_j\| \leq 1$.

Unknown: $|\psi\rangle \in \mathbb{C}^d$.

Goal: obtain $\widetilde{o}_j$ s.t. $|\widetilde{o}_j - \langle\psi| O_j |\psi\rangle| \leq \varepsilon$.

1. Given copies of $|\psi\rangle$:
   1. $O(\frac{\log(M)}{\varepsilon^2})$. *(if they commute)*
   2. $O(\frac{\log(M)}{\varepsilon^4})$. *(shadow tomgoraphy)* [HKP'20]
2. Given unitary access to $|\psi\rangle$:
   1. $\widetilde{O}(\frac{\sqrt{\sum_{j=1}^M \|O_j\|^2}}{\varepsilon}) = \widetilde{O}(\frac{\sqrt{M}}{\varepsilon})$. [HWC+'22]
   2. $\widetilde{O}(\frac{\sqrt{\|\sum_{j=1}^M O_j^2\|}}{\varepsilon}) = \widetilde{O}(\frac{\sqrt{M}}{\varepsilon})$. [This work]

Specific observables and other norms:

1. $O_j = |j\rangle\langle j|$, for $j = 1, \dots, d$.
2. $p_j = |\langle j|\psi\rangle|^2$.

Unknown: $|\psi\rangle \in \mathbb{C}^d$.

Goal: obtain $\widetilde{p}$ s.t. $\|\widetilde{p} - p\|_q \leq \varepsilon$.

Aside: other quantum state tomography results

"Quantum state tomography is learning properties of a quantum state."

Learning observables:

$O_1, \dots, O_M$ with $\|O_j\| \leq 1$.

Unknown: $|\psi\rangle \in \mathbb{C}^d$.

Goal: obtain $\widetilde{o}_j$ s.t. $|\widetilde{o}_j - \langle\psi| O_j |\psi\rangle| \leq \varepsilon$.

1. Given copies of $|\psi\rangle$:
   1. $O(\frac{\log(M)}{\varepsilon^2})$. *(if they commute)*
   2. $O(\frac{\log(M)}{\varepsilon^4})$. *(shadow tomgoraphy)* [HKP'20]
2. Given unitary access to $|\psi\rangle$:
   1. $\widetilde{O}(\frac{\sqrt{\sum_{j=1}^M \|O_j\|^2}}{\varepsilon}) = \widetilde{O}(\frac{\sqrt{M}}{\varepsilon})$. [HWC+'22]
   2. $\widetilde{O}(\frac{\sqrt{\|\sum_{j=1}^M O_j^2\|}}{\varepsilon}) = \widetilde{O}(\frac{\sqrt{M}}{\varepsilon})$. [This work]

Specific observables and other norms:

1. $O_j = |j\rangle\langle j|$, for $j = 1, \dots, d$.
2. $p_j = |\langle j|\psi\rangle|^2$.

Unknown: $|\psi\rangle \in \mathbb{C}^d$.

Goal: obtain $\widetilde{p}$ s.t. $\|\widetilde{p} - p\|_q \leq \varepsilon$.

Given unitary access to $|\psi\rangle$:

$$\widetilde{\Theta}\left(\min\left\{\frac{d^{\frac{1}{q}}}{\varepsilon}, \frac{1}{\varepsilon^{\frac{1}{1-\frac{1}{q}}}}\right\}\right).$$ [vA'21; This work]

Probably many more...

Problem statement

Problem statement

Full mixed-state tomography (d, r, ε):

1. *Parameters:* $1 \leq r \leq d$, and $\varepsilon \in [0, 1/256]$.
2. *Input:* $U : |0\rangle \mapsto |\psi\rangle = \sum_{j=1}^{r} \alpha_j |\psi_j\rangle_A |\chi_j\rangle_B$.
3. $\rho = \mathrm{Tr}_B[|\psi\rangle\langle\psi|] = \sum_{j=1}^{r} |\alpha_j|^2 |\psi_j\rangle\langle\psi_j|$.
4. *Goal:* output $\widetilde{\rho} \in \mathbb{C}^{d \times d}$ s.t. $\|\widetilde{\rho} - \rho\|_1 \leq \varepsilon$.

Problem statement

Full mixed-state tomography (d, r, ε):

1. *Parameters:* $1 \leq r \leq d$, and $\varepsilon \in [0, 1/256]$.
2. *Input:* $U : |0\rangle \mapsto |\psi\rangle = \sum_{j=1}^{r} \alpha_j |\psi_j\rangle_A |\chi_j\rangle_B$.
3. $\rho = \mathrm{Tr}_B[|\psi\rangle\langle\psi|] = \sum_{j=1}^{r} |\alpha_j|^2 |\psi_j\rangle\langle\psi_j|$.
4. *Goal:* output $\widetilde{\rho} \in \mathbb{C}^{d \times d}$ s.t. $\|\widetilde{\rho} - \rho\|_1 \leq \varepsilon$.

Question: Optimal number of (inverse) calls to U?

Problem statement

Full mixed-state tomography (d, r, ε):

1. *Parameters:* $1 \leq r \leq d$, and $\varepsilon \in [0, 1/256]$.
2. *Input:* $U : |0\rangle \mapsto |\psi\rangle = \sum_{j=1}^{r} \alpha_j |\psi_j\rangle_A |\chi_j\rangle_B$.
3. $\rho = \mathrm{Tr}_B[|\psi\rangle\langle\psi|] = \sum_{j=1}^{r} |\alpha_j|^2 |\psi_j\rangle\langle\psi_j|$.
4. *Goal:* output $\widetilde{\rho} \in \mathbb{C}^{d \times d}$ s.t. $\|\widetilde{\rho} - \rho\|_1 \leq \varepsilon$.

Question: Optimal number of (inverse) calls to U?
Remainder of this talk: $\Omega(\frac{dr}{\varepsilon})$ queries are required.

Lower bound – approximate string recovery

Idea: "Embed the approximate string recovery problem into the full mixed-state tomography problem."

Lower bound – approximate string recovery

Idea: "Embed the approximate string recovery problem into the full mixed-state tomography problem."

Ingredients:

1. Absolute constants $c, C \in (0, 1)$.
2. $D \subseteq \{0, 1\}^{dr}$ with $|D| \geq C \cdot 2^{dr}$.
3. For all $b \in D$, let $S_b \subseteq |D|$, with $b \in S_b$.
   (horizontal edges)
4. For all $\widetilde{b} \in D$, $|\{b \in D : \widetilde{b} \in S_b\}| \leq 2^{cdr}$.
   (right degree bounded by 2^{cdr})

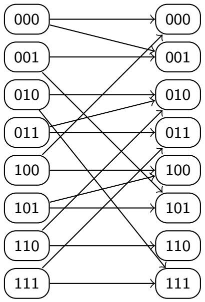
Lower bound – approximate string recovery

Idea: "Embed the approximate string recovery problem into the full mixed-state tomography problem."

Ingredients:

1. Absolute constants $c, C \in (0,1)$.
2. $D \subseteq \{0,1\}^{dr}$ with $|D| \geq C \cdot 2^{dr}$.
3. For all $b \in D$, let $S_b \subseteq |D|$, with $b \in S_b$. *(horizontal edges)*
4. For all $\widetilde{b} \in D$, $|\{b \in D : \widetilde{b} \in S_b\}| \leq 2^{cdr}$. *(right degree bounded by 2^{cdr})*

Input: $b \in \{0,1\}^{dr}$ Output: $\widetilde{b} \in \{0,1\}^{dr}$



Lower bound – approximate string recovery

Idea: "Embed the approximate string recovery problem into the full mixed-state tomography problem."

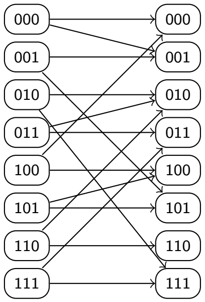
Ingredients:

1. Absolute constants $c, C \in (0,1)$.
2. $D \subseteq \{0,1\}^{dr}$ with $|D| \geq C \cdot 2^{dr}$.
3. For all $b \in D$, let $S_b \subseteq |D|$, with $b \in S_b$. *(horizontal edges)*
4. For all $\widetilde{b} \in D$, $|\{b \in D : \widetilde{b} \in S_b\}| \leq 2^{cdr}$. *(right degree bounded by 2^{cdr})*

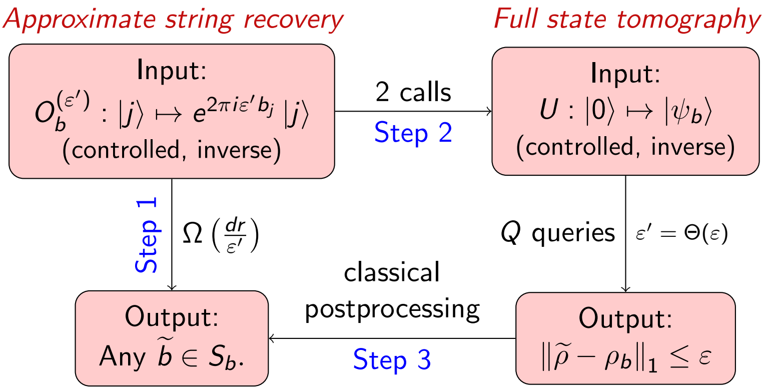
Approximate string recovery (ε, D, $b \mapsto S_b$):

1. *Input:* $O_b^{(\varepsilon)} : |j\rangle \mapsto e^{2\pi i \varepsilon b_j} |j\rangle$ with $b \in D$.
2. *Output:* any $\widetilde{b} \in S_b$.

Input: $b \in \{0,1\}^{dr}$ Output: $\widetilde{b} \in \{0,1\}^{dr}$



Idea: "Embed the approximate string recovery problem into the full state-tomography problem."



Lower bound – approximate string recovery

Case: $\varepsilon' = 1/2$

Case: $\varepsilon' \in (0, 1/2)$

Lower bound – approximate string recovery

Case: $\varepsilon' = 1/2$

1. $O_b^{(\varepsilon')} : |j\rangle \mapsto e^{2\pi i b_j} |j\rangle = (-1)^{b_j} |j\rangle$.

Case: $\varepsilon' \in (0, 1/2)$

Lower bound – approximate string recovery

Case: $\varepsilon' = 1/2$

1. $O_b^{(\varepsilon')} : |j\rangle \mapsto e^{2\pi i b_j} |j\rangle = (-1)^{b_j} |j\rangle$.
2. Algorithm:
   1. Run the algorithm that outputs any $\widetilde{b} \in S_b$ with Q queries.
   2. Output any $b \in D$ such that $\widetilde{b} \in S_b$ uniformly at random.

Case: $\varepsilon' \in (0, 1/2)$

Lower bound – approximate string recovery

Case: $\varepsilon' = 1/2$

1. $O_b^{(\varepsilon')} : |j\rangle \mapsto e^{2\pi i b_j} |j\rangle = (-1)^{b_j} |j\rangle$.
2. Algorithm:
   1. Run the algorithm that outputs any $\widetilde{b} \in S_b$ with Q queries.
   2. Output any $b \in D$ such that $\widetilde{b} \in S_b$ uniformly at random.
3. Recovers b with probability at least $2/3 \cdot 2^{-cdr}$.

Case: $\varepsilon' \in (0, 1/2)$

Lower bound – approximate string recovery

Case: $\varepsilon' = 1/2$

1. $O_b^{(\varepsilon')} : |j\rangle \mapsto e^{2\pi i b_j} |j\rangle = (-1)^{b_j} |j\rangle$.
2. Algorithm:
    1. Run the algorithm that outputs any $\widetilde{b} \in S_b$ with Q queries.
    2. Output any $b \in D$ such that $\widetilde{b} \in S_b$ uniformly at random.
3. Recovers b with probability at least $2/3 \cdot 2^{-cdr}$.
4. Polynomial method: [FGGS'99] $C \cdot 2^{dr} \leq |D| \leq \frac{3}{2} \cdot 2^{cdr} \cdot 2^{drH(Q/dr)}$.

Case: $\varepsilon' \in (0, 1/2)$

Lower bound – approximate string recovery

Case: $\varepsilon' = 1/2$

1. $O_b^{(\varepsilon')} : |j\rangle \mapsto e^{2\pi i b_j} |j\rangle = (-1)^{b_j} |j\rangle$.
2. Algorithm:
   1. Run the algorithm that outputs any $\widetilde{b} \in S_b$ with Q queries.
   2. Output any $b \in D$ such that $\widetilde{b} \in S_b$ uniformly at random.
3. Recovers b with probability at least $2/3 \cdot 2^{-cdr}$.
4. Polynomial method: [FGGS'99] $C \cdot 2^{dr} \leq |D| \leq \frac{3}{2} \cdot 2^{cdr} \cdot 2^{drH(Q/dr)}$.

Thus, $Q = \Omega(dr)$.

Case: $\varepsilon' \in (0, 1/2)$

Lower bound – approximate string recovery

Case: $\varepsilon' = 1/2$

1. $O_b^{(\varepsilon')} : |j\rangle \mapsto e^{2\pi i b_j} |j\rangle = (-1)^{b_j} |j\rangle$.
2. Algorithm:
   1. Run the algorithm that outputs any $\widetilde{b} \in S_b$ with Q queries.
   2. Output any $b \in D$ such that $\widetilde{b} \in S_b$ uniformly at random.
3. Recovers b with probability at least $2/3 \cdot 2^{-cdr}$.
4. Polynomial method: [FGGS'99] $C \cdot 2^{dr} \leq |D| \leq \frac{3}{2} \cdot 2^{cdr} \cdot 2^{drH(Q/dr)}$.

Thus, $Q = \Omega(dr)$.

Case: $\varepsilon' \in (0, 1/2)$

Idea: Any problem becomes $1/\varepsilon'$ harder when switching from O_b to $O_b^{(\varepsilon')}$.

Lower bound – approximate string recovery

Case: $\varepsilon' = 1/2$

1. $O_b^{(\varepsilon')} : |j\rangle \mapsto e^{2\pi i b_j} |j\rangle = (-1)^{b_j} |j\rangle$.
2. Algorithm:
    1. Run the algorithm that outputs any $\widetilde{b} \in S_b$ with Q queries.
    2. Output any $b \in D$ such that $\widetilde{b} \in S_b$ uniformly at random.
3. Recovers b with probability at least $2/3 \cdot 2^{-cdr}$.
4. Polynomial method: [FGGS'99] $C \cdot 2^{dr} \leq |D| \leq \frac{3}{2} \cdot 2^{cdr} \cdot 2^{drH(Q/dr)}$.

Thus, $Q = \Omega(dr)$.

Case: $\varepsilon' \in (0, 1/2)$

Idea: Any problem becomes $1/\varepsilon'$ harder when switching from O_b to $O_b^{(\varepsilon')}$.

Technical difficulties:

1. Proof for functions. [LMRŠS'11]
    1. Proof via adversary method.
    2. Approximate string recovery is not a function.

Lower bound – approximate string recovery

Case: $\varepsilon' = 1/2$

1. $O_b^{(\varepsilon')} : |j\rangle \mapsto e^{2\pi i b_j} |j\rangle = (-1)^{b_j} |j\rangle$.
2. Algorithm:
    1. Run the algorithm that outputs any $\widetilde{b} \in S_b$ with Q queries.
    2. Output any $b \in D$ such that $\widetilde{b} \in S_b$ uniformly at random.
3. Recovers b with probability at least $2/3 \cdot 2^{-cdr}$.
4. Polynomial method: [FGGS'99]
$C \cdot 2^{dr} \leq |D| \leq \frac{3}{2} \cdot 2^{cdr} \cdot 2^{drH(Q/dr)}$.

Thus, $Q = \Omega(dr)$.

Case: $\varepsilon' \in (0, 1/2)$

Idea: Any problem becomes $1/\varepsilon'$ harder when switching from O_b to $O_b^{(\varepsilon')}$.

Technical difficulties:

1. Proof for functions. [LMRŠS'11]
    1. Proof via adversary method.
    2. Approximate string recovery is not a function.
2. Adversary method for relations: [Bel'15]
    1. Approximate string recovery is a relation.

Lower bound – approximate string recovery

Case: $\varepsilon' = 1/2$

1. $O_b^{(\varepsilon')} : |j\rangle \mapsto e^{2\pi i b_j} |j\rangle = (-1)^{b_j} |j\rangle$.
2. Algorithm:
    1. Run the algorithm that outputs any $\widetilde{b} \in S_b$ with Q queries.
    2. Output any $b \in D$ such that $\widetilde{b} \in S_b$ uniformly at random.
3. Recovers b with probability at least $2/3 \cdot 2^{-cdr}$.
4. Polynomial method: [FGGS'99]
$C \cdot 2^{dr} \leq |D| \leq \frac{3}{2} \cdot 2^{cdr} \cdot 2^{drH(Q/dr)}$.

Thus, $Q = \Omega(dr)$.

Case: $\varepsilon' \in (0, 1/2)$

Idea: Any problem becomes $1/\varepsilon'$ harder when switching from O_b to $O_b^{(\varepsilon')}$.

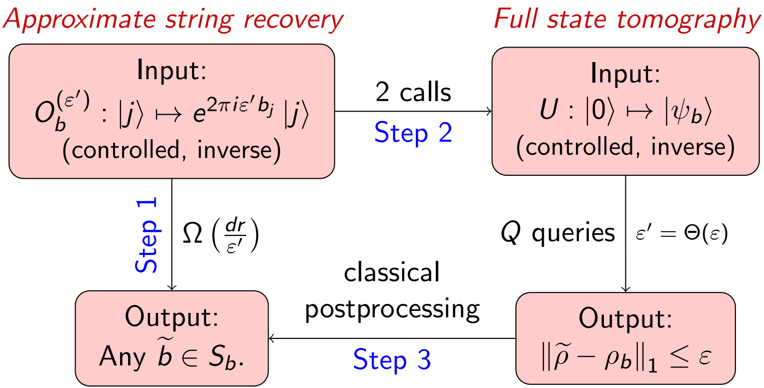
Technical difficulties:

1. Proof for functions. [LMRŠS'11]
    1. Proof via adversary method.
    2. Approximate string recovery is not a function.
2. Adversary method for relations: [Bel'15]
    1. Approximate string recovery is a relation.
3. Combine both: [CJ'21].

Thus, $Q = \Omega(\frac{dr}{\varepsilon'})$.

Lower bound – proof overview

Idea: "Embed the approximate string recovery problem into the full state-tomography problem."

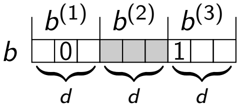


Lower bound – embedding

Embedding: ($\varepsilon < 1/256$)

1. Let $U^{(1)}, \ldots, U^{(r)} \in \mathbb{C}^{d \times d}$ unitaries.
2. Let $b \in \{0,1\}^{dr}$.
3. Define
$$\left|\psi_b^{(j)}\right\rangle = \frac{1}{\sqrt{d}} \sum_{k=1}^{d} \sum_{c \in \{0,1\}} \sqrt{\frac{1}{2} + 128\varepsilon(-1)^{c+b_k^{(j)}}} \left|c\right\rangle \left|k\right\rangle.$$
4. Let $\left|\psi_b\right\rangle = \frac{1}{\sqrt{r}} \sum_{j=1}^{r} (I \otimes U^{(j)}) \left|\psi_b^{(j)}\right\rangle_A \left|j\right\rangle_B$
5. Let $\rho_b = \mathrm{Tr}_B[\left|\psi_b\right\rangle\!\left\langle\psi_b\right|]$.

Lower bound – embedding



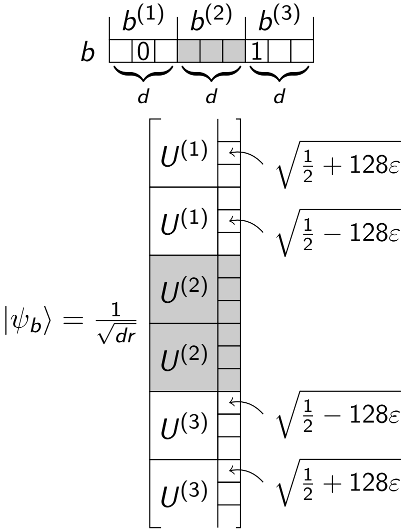
Embedding: $(\varepsilon < 1/256)$

1. Let $U^{(1)}, \ldots, U^{(r)} \in \mathbb{C}^{d \times d}$ unitaries.
2. Let $b \in \{0,1\}^{dr}$.
3. Define
$$\left|\psi_b^{(j)}\right\rangle = \frac{1}{\sqrt{d}} \sum_{k=1}^{d} \sum_{c \in \{0,1\}} \sqrt{\frac{1}{2} + 128\varepsilon(-1)^{c+b_k^{(j)}}} \, |c\rangle \, |k\rangle .$$
4. Let $|\psi_b\rangle = \frac{1}{\sqrt{r}} \sum_{j=1}^{r} (I \otimes U^{(j)}) \left|\psi_b^{(j)}\right\rangle_A |j\rangle_B$
5. Let $\rho_b = \mathrm{Tr}_B[|\psi_b\rangle\langle\psi_b|]$.

Lower bound – embedding

Embedding: ($\varepsilon < 1/256$)

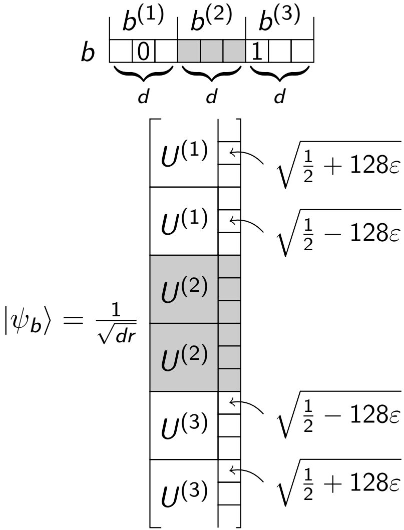
1. Let $U^{(1)}, \ldots, U^{(r)} \in \mathbb{C}^{d\times d}$ unitaries.
2. Let $b \in \{0,1\}^{dr}$.
3. Define
$$\left|\psi_b^{(j)}\right\rangle = \frac{1}{\sqrt{d}} \sum_{k=1}^{d} \sum_{c\in\{0,1\}} \sqrt{\frac{1}{2} + 128\varepsilon(-1)^{c+b_k^{(j)}}} \left|c\right\rangle \left|k\right\rangle.$$
4. Let $|\psi_b\rangle = \frac{1}{\sqrt{r}} \sum_{j=1}^{r} (I \otimes U^{(j)}) \left|\psi_b^{(j)}\right\rangle_A |j\rangle_B$
5. Let $\rho_b = \mathrm{Tr}_B[|\psi_b\rangle\langle\psi_b|]$.



Lower bound – embedding

For a single bit $b \in \{0,1\}$, we can perform:

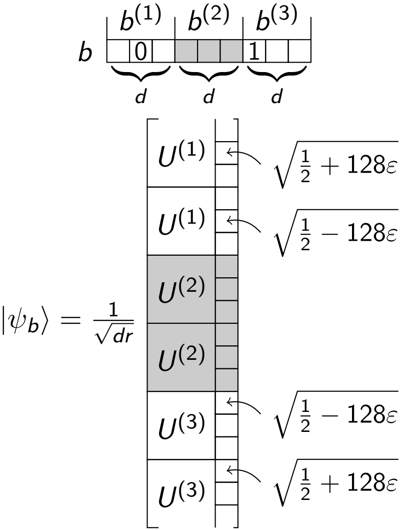
1. Let ξ, ε' to be fixed later.
2. Start with state
$$\frac{1}{\sqrt{2}}\begin{bmatrix} e^{\pi i(\xi+\varepsilon')} \\ e^{-\pi i(\xi+\varepsilon')} \end{bmatrix}$$



Lower bound – embedding

For a single bit $b \in \{0,1\}$, we can perform:

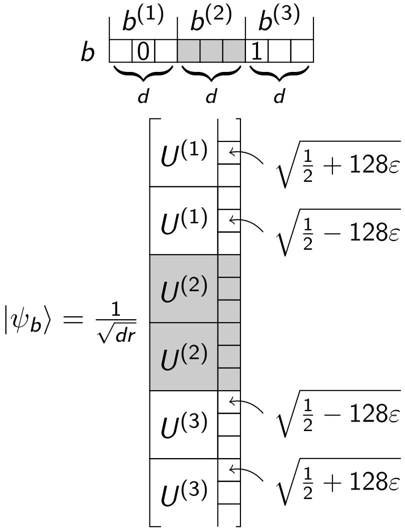
1. Let ξ, ε' to be fixed later.
2. Start with state
$$\frac{1}{\sqrt{2}}\begin{bmatrix} e^{\pi i(\xi+\varepsilon')} \\ e^{-\pi i(\xi+\varepsilon')} \end{bmatrix}$$
3. Apply $(O_b^{(\varepsilon')})^\dagger$ and $O_b^{(\varepsilon')}$ to first and second entry
$$\frac{1}{\sqrt{2}}\begin{bmatrix} e^{\pi i(\xi+(-1)^b\varepsilon')} \\ e^{-\pi i(\xi+(-1)^b\varepsilon')} \end{bmatrix}$$



Lower bound – embedding

For a single bit $b \in \{0,1\}$, we can perform:

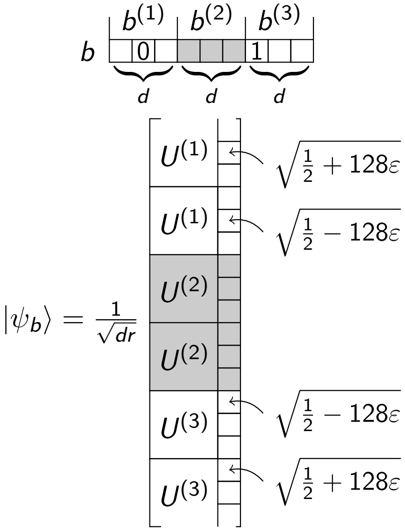
1. Let ξ, ε' to be fixed later.
2. Start with state
$$\frac{1}{\sqrt{2}}\begin{bmatrix} e^{\pi i(\xi+\varepsilon')} \\ e^{-\pi i(\xi+\varepsilon')} \end{bmatrix}$$
3. Apply $(O_b^{(\varepsilon')})^\dagger$ and $O_b^{(\varepsilon')}$ to first and second entry
$$\frac{1}{\sqrt{2}}\begin{bmatrix} e^{\pi i(\xi+(-1)^b\varepsilon')} \\ e^{-\pi i(\xi+(-1)^b\varepsilon')} \end{bmatrix}$$
4. Apply H and then S
$$\begin{bmatrix} \cos(\pi(\xi+(-1)^b\varepsilon')) \\ \sin(\pi(\xi+(-1)^b\varepsilon')) \end{bmatrix} = \begin{bmatrix} \sqrt{\frac{1}{2}+(-1)^b 128\varepsilon} \\ \sqrt{\frac{1}{2}-(-1)^b 128\varepsilon} \end{bmatrix}$$



Lower bound – embedding

For a single bit $b \in \{0,1\}$, we can perform:

1. Let ξ, ε' to be fixed later.
2. Start with state
   $$\frac{1}{\sqrt{2}}\begin{bmatrix} e^{\pi i(\xi+\varepsilon')} \\ e^{-\pi i(\xi+\varepsilon')} \end{bmatrix}$$
3. Apply $(O_b^{(\varepsilon')})^\dagger$ and $O_b^{(\varepsilon')}$ to first and second entry
   $$\frac{1}{\sqrt{2}}\begin{bmatrix} e^{\pi i(\xi+(-1)^b\varepsilon')} \\ e^{-\pi i(\xi+(-1)^b\varepsilon')} \end{bmatrix}$$
4. Apply H and then S
   $$\begin{bmatrix} \cos(\pi(\xi+(-1)^b\varepsilon')) \\ \sin(\pi(\xi+(-1)^b\varepsilon')) \end{bmatrix} = \begin{bmatrix} \sqrt{\frac{1}{2}+(-1)^b128\varepsilon} \\ \sqrt{\frac{1}{2}-(-1)^b128\varepsilon} \end{bmatrix}$$
5. Solve for ξ, ε', then $\varepsilon' = \Theta(\varepsilon)$.

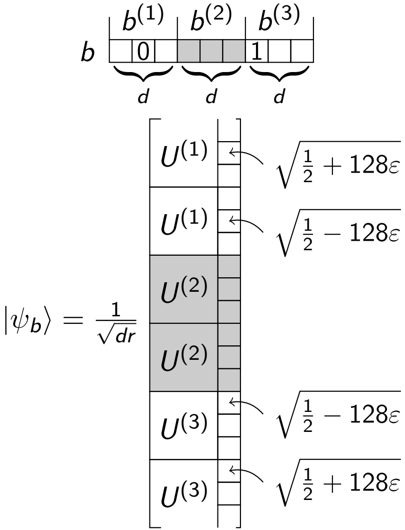


Lower bound – embedding

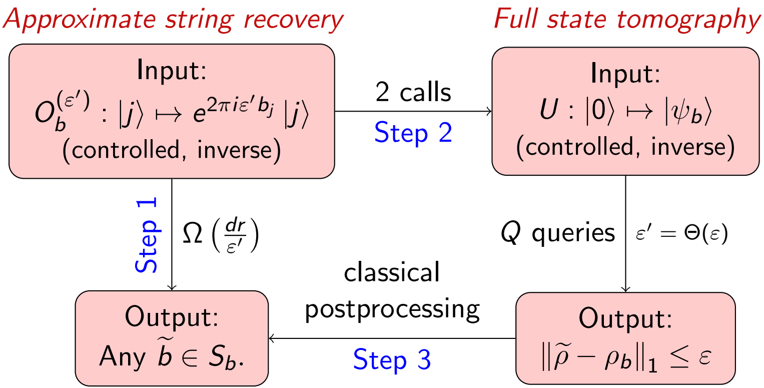
For a single bit $b \in \{0,1\}$, we can perform:

1. Let ξ, ε' to be fixed later.
2. Start with state
$$\frac{1}{\sqrt{2}}\begin{bmatrix} e^{\pi i(\xi+\varepsilon')} \\ e^{-\pi i(\xi+\varepsilon')} \end{bmatrix}$$
3. Apply $(O_b^{(\varepsilon')})^\dagger$ and $O_b^{(\varepsilon')}$ to first and second entry
$$\frac{1}{\sqrt{2}}\begin{bmatrix} e^{\pi i(\xi+(-1)^b\varepsilon')} \\ e^{-\pi i(\xi+(-1)^b\varepsilon')} \end{bmatrix}$$
4. Apply H and then S
$$\begin{bmatrix} \cos(\pi(\xi+(-1)^b\varepsilon')) \\ \sin(\pi(\xi+(-1)^b\varepsilon')) \end{bmatrix} = \begin{bmatrix} \sqrt{\frac{1}{2}+(-1)^b 128\varepsilon} \\ \sqrt{\frac{1}{2}-(-1)^b 128\varepsilon} \end{bmatrix}$$
5. Solve for ξ, ε', then $\varepsilon' = \Theta(\varepsilon)$.

Now perform in parallel to obtain $|\psi_b\rangle$.



Idea: "Embed the approximate string recovery problem into the full state-tomography problem."



Lower bound – postprocessing

Lower bound – postprocessing

1. Postprocessing algorithm:
   1. Run algorithm to obtain $\widetilde{\rho}$ s.t. $\|\widetilde{\rho} - \rho_b\|_1 \leq \varepsilon$.
   2. Output any $\widetilde{b} \in \{0,1\}^{dr}$ such that $\left\|\widetilde{\rho} - \rho_{\widetilde{b}}\right\|_1 \leq \varepsilon$.

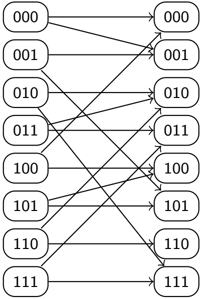
   It follows that $\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon$.

Lower bound – postprocessing

1. Postprocessing algorithm:
   1. Run algorithm to obtain $\widetilde{\rho}$ s.t. $\|\widetilde{\rho} - \rho_b\|_1 \leq \varepsilon$.
   2. Output any $\widetilde{b} \in \{0,1\}^{dr}$ such that $\left\|\widetilde{\rho} - \rho_{\widetilde{b}}\right\|_1 \leq \varepsilon$.

   It follows that $\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon$.
2. Thus, let $S_b = \{\widetilde{b} \in \{0,1\}^{dr} : \left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon\}$.

Input: $b \in \{0,1\}^{dr}$ Output: $\widetilde{b} \in \{0,1\}^{dr}$

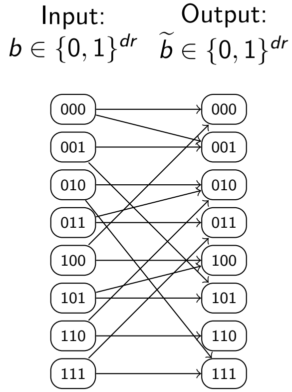


Edge when $\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon$.

Lower bound – postprocessing

1. Postprocessing algorithm:
   1. Run algorithm to obtain $\widetilde{\rho}$ s.t. $\|\widetilde{\rho} - \rho_b\|_1 \leq \varepsilon$.
   2. Output any $\widetilde{b} \in \{0,1\}^{dr}$ such that $\left\|\widetilde{\rho} - \rho_{\widetilde{b}}\right\|_1 \leq \varepsilon$.

   It follows that $\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon$.
2. Thus, let $S_b = \{\widetilde{b} \in \{0,1\}^{dr} : \left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon\}$.
3. Then $b \in S_b$.
   (horizontal edges)



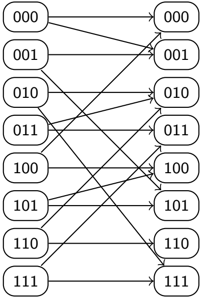
Edge when $\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon$.

Lower bound – postprocessing

1. Postprocessing algorithm:
    1. Run algorithm to obtain $\widetilde{\rho}$ s.t. $\|\widetilde{\rho} - \rho_b\|_1 \leq \varepsilon$.
    2. Output any $\widetilde{b} \in \{0,1\}^{dr}$ such that $\left\|\widetilde{\rho} - \rho_{\widetilde{b}}\right\|_1 \leq \varepsilon$.

    It follows that $\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon$.
2. Thus, let $S_b = \{\widetilde{b} \in \{0,1\}^{dr} : \left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon\}$.
3. Then $b \in S_b$.
   (horizontal edges)
4. Remains to show that $\exists c \in (0,1)$ s.t.
   $|\{b \in \{0,1\}^{dr} : \widetilde{b} \in S_b\}| \leq 2^{cdr}$.
   (bounded right degree)

Input: $b \in \{0,1\}^{dr}$ Output: $\widetilde{b} \in \{0,1\}^{dr}$



Edge when $\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon$.

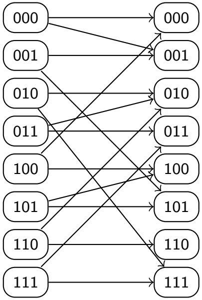
Lower bound – postprocessing

Let $b, \widetilde{b} \in \{0,1\}^{dr}$ uniformly at random.

Suppose that $\exists c \in (0,1)$ s.t.

$$\mathbb{P}\left[\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon\right] \leq 2^{-cdr}.$$

Input: $b \in \{0,1\}^{dr}$ Output: $\widetilde{b} \in \{0,1\}^{dr}$



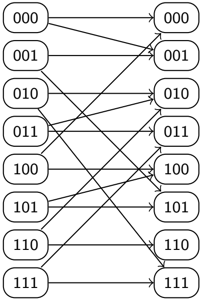
Edge when $\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon$.

Lower bound – postprocessing

Let $b, \widetilde{b} \in \{0,1\}^{dr}$ uniformly at random.
Suppose that $\exists c \in (0,1)$ s.t.
$$\mathbb{P}\left[\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon\right] \leq 2^{-cdr}.$$

1. $\#\{\text{edges}\} \leq 2^{-cdr} \cdot 2^{2dr}$.

Input: $b \in \{0,1\}^{dr}$ Output: $\widetilde{b} \in \{0,1\}^{dr}$



Edge when $\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon$.

Lower bound – postprocessing

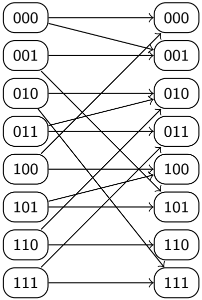
Let $b, \widetilde{b} \in \{0,1\}^{dr}$ uniformly at random.

Suppose that $\exists c \in (0,1)$ s.t.

$$\mathbb{P}\left[\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon\right] \leq 2^{-cdr}.$$

1. $\#\{\text{edges}\} \leq 2^{-cdr} \cdot 2^{2dr}$.
2. $\sum \deg(\widetilde{b}) \leq 2^{-cdr} \cdot 2^{2dr}$.

Input: $b \in \{0,1\}^{dr}$ Output: $\widetilde{b} \in \{0,1\}^{dr}$



Edge when $\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon$.

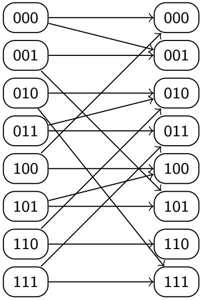
Lower bound – postprocessing

Let $b, \widetilde{b} \in \{0,1\}^{dr}$ uniformly at random.
Suppose that $\exists c \in (0,1)$ s.t.

$$\mathbb{P}\left[\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon\right] \leq 2^{-cdr}.$$

1. $\#\{\text{edges}\} \leq 2^{-cdr} \cdot 2^{2dr}$.
2. $\sum \deg(\widetilde{b}) \leq 2^{-cdr} \cdot 2^{2dr}$.
3. $|\{\widetilde{b} : \deg(\widetilde{b}) \geq 2^{-cdr/2} \cdot 2^{dr}\}| \leq 2^{-cdr/2} \cdot 2^{dr}$.

Input: $b \in \{0,1\}^{dr}$ Output: $\widetilde{b} \in \{0,1\}^{dr}$



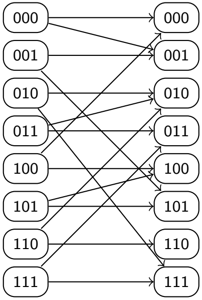
Edge when $\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon$.

Lower bound – postprocessing

Let $b, \widetilde{b} \in \{0,1\}^{dr}$ uniformly at random.
Suppose that $\exists c \in (0,1)$ s.t.
$\mathbb{P}\left[\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon\right] \leq 2^{-cdr}$.

1. $\#\{\text{edges}\} \leq 2^{-cdr} \cdot 2^{2dr}$.
2. $\sum \deg(\widetilde{b}) \leq 2^{-cdr} \cdot 2^{2dr}$.
3. $|\{\widetilde{b} : \deg(\widetilde{b}) \geq 2^{-cdr/2} \cdot 2^{dr}\}| \leq 2^{-cdr/2} \cdot 2^{dr}$.
4. $|\{\widetilde{b} : \deg(\widetilde{b}) \leq 2^{-cdr/2} \cdot 2^{dr}\}| \geq 2^{dr}(1 - 2^{-cdr/2})$.

Input: $b \in \{0,1\}^{dr}$ Output: $\widetilde{b} \in \{0,1\}^{dr}$



Edge when $\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon$.

Lower bound – postprocessing

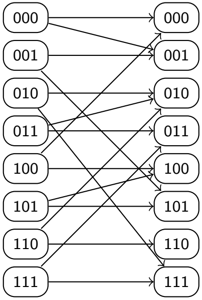
Let $b, \widetilde{b} \in \{0,1\}^{dr}$ uniformly at random.

Suppose that $\exists c \in (0,1)$ s.t.

$\mathbb{P}\left[\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon\right] \leq 2^{-cdr}$.

1. $\#\{\text{edges}\} \leq 2^{-cdr} \cdot 2^{2dr}$.
2. $\sum \deg(\widetilde{b}) \leq 2^{-cdr} \cdot 2^{2dr}$.
3. $|\{\widetilde{b} : \deg(\widetilde{b}) \geq 2^{-cdr/2} \cdot 2^{dr}\}| \leq 2^{-cdr/2} \cdot 2^{dr}$.
4. $|\{\widetilde{b} : \deg(\widetilde{b}) \leq 2^{-cdr/2} \cdot 2^{dr}\}| \geq 2^{dr}(1 - 2^{-cdr/2})$.
5. Let $D \subseteq \{0,1\}^{dr}$ be the set for all these $\widetilde{b}$'s: $|D| \geq C \cdot 2^{dr}$, with $C \in (0,1)$.

Input: $b \in \{0,1\}^{dr}$ Output: $\widetilde{b} \in \{0,1\}^{dr}$



Edge when $\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon$.

Lower bound – postprocessing

Let $b, \widetilde{b} \in \{0,1\}^{dr}$ uniformly at random.

Suppose that $\exists c \in (0,1)$ s.t.

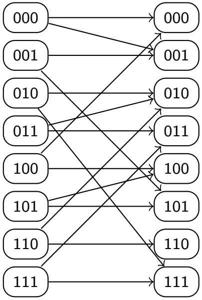
$$\mathbb{P}\left[\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon\right] \leq 2^{-cdr}.$$

1. $\#\{\text{edges}\} \leq 2^{-cdr} \cdot 2^{2dr}$.
2. $\sum \deg(\widetilde{b}) \leq 2^{-cdr} \cdot 2^{2dr}$.
3. $|\{\widetilde{b} : \deg(\widetilde{b}) \geq 2^{-cdr/2} \cdot 2^{dr}\}| \leq 2^{-cdr/2} \cdot 2^{dr}$.
4. $|\{\widetilde{b} : \deg(\widetilde{b}) \leq 2^{-cdr/2} \cdot 2^{dr}\}| \geq 2^{dr}(1 - 2^{-cdr/2})$.
5. Let $D \subseteq \{0,1\}^{dr}$ be the set for all these $\widetilde{b}$'s:
   $|D| \geq C \cdot 2^{dr}$, with $C \in (0,1)$.

Thus it remains to show $\exists c \in (0,1)$ s.t.

$$\mathbb{P}\left[\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon\right] \leq 2^{-cdr}.$$

Input: $b \in \{0,1\}^{dr}$ Output: $\widetilde{b} \in \{0,1\}^{dr}$



Edge when $\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon$.

Lower bound – proximity probability analysis

Remains to prove: $\exists c \in (0,1)$ s.t.
$\mathbb{P}\left[\left\|\rho_b - \rho_{\tilde{b}}\right\|_1 \leq 2\varepsilon\right] \leq 2^{-cdr}$.

Lower bound – proximity probability analysis

Remains to prove: $\exists c \in (0,1)$ s.t.
$\mathbb{P}\left[\left\|\rho_b - \rho_{\tilde{b}}\right\|_1 \leq 2\varepsilon\right] \leq 2^{-cdr}$.

Approximation: $\sqrt{\frac{1}{2} \pm 128\varepsilon} \approx \frac{1}{\sqrt{2}}(1 \pm 128\varepsilon)$.

Lower bound – proximity probability analysis

Remains to prove: $\exists c \in (0,1)$ s.t.
$\mathbb{P}\left[\left\|\rho_b - \rho_{\tilde{b}}\right\|_1 \leq 2\varepsilon\right] \leq 2^{-cdr}$.

Approximation: $\sqrt{\frac{1}{2} \pm 128\varepsilon} \approx \frac{1}{\sqrt{2}}(1 \pm 128\varepsilon)$.

1. *Total error:* $2(256\varepsilon)^2$.

Lower bound – proximity probability analysis

Remains to prove: $\exists c \in (0,1)$ s.t.

$$\mathbb{P}\left[\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon\right] \leq 2^{-cdr}.$$

Approximation: $\sqrt{\frac{1}{2} \pm 128\varepsilon} \approx \frac{1}{\sqrt{2}}(1 \pm 128\varepsilon)$.

1. *Total error:* $2(256\varepsilon)^2$.
2. *Simplification:*
   $\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 = \frac{32\varepsilon}{rd}\left\|XY^\dagger\right\|_1$, where
   1. $X = [U^{(1)}\delta^{(1)} \ \cdots \ U^{(r)}\delta^{(r)}]$,
   2. $Y = [U^{(1)}\mathbb{1} \ \cdots \ U^{(r)}\mathbb{1}]$,
   3. $\delta^{(j)} = (-1)^{b^{(j)}} - (-1)^{\widetilde{b}^{(j)}}$.

Lower bound – proximity probability analysis

Remains to prove: $\exists c \in (0,1)$ s.t.
$\mathbb{P}\left[\left\|\rho_b - \rho_{\tilde{b}}\right\|_1 \leq 2\varepsilon\right] \leq 2^{-cdr}$.

Approximation: $\sqrt{\frac{1}{2} \pm 128\varepsilon} \approx \frac{1}{\sqrt{2}}(1 \pm 128\varepsilon)$.

1. *Total error:* $2(256\varepsilon)^2$.
2. *Simplification:*
   $\left\|\rho_b - \rho_{\tilde{b}}\right\|_1 = \frac{32\varepsilon}{rd}\left\|XY^\dagger\right\|_1$, where
   1. $X = [U^{(1)}\delta^{(1)} \ \cdots \ U^{(r)}\delta^{(r)}]$,
   2. $Y = [U^{(1)}\mathbb{1} \ \cdots \ U^{(r)}\mathbb{1}]$,
   3. $\delta^{(j)} = (-1)^{b^{(j)}} - (-1)^{\tilde{b}^{(j)}}$.
3. *Interpretation:* overlaying point clouds.

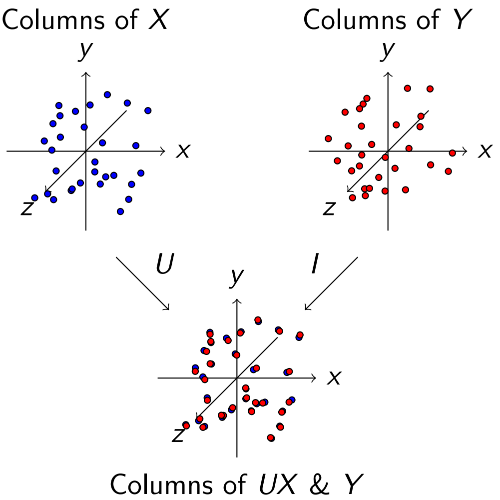
$$\left\|XY^\dagger\right\|_1 = \max_{U \text{ unitary}} \left|\mathrm{Tr}[Y^\dagger UX]\right| = \max_{U \text{ unitary}} \sum_{j=1}^r |y_j^\dagger U x_j|.$$

Lower bound – proximity probability analysis

Remains to prove: $\exists c \in (0,1)$ s.t.
$\mathbb{P}\left[\left\|\rho_b - \rho_{\tilde{b}}\right\|_1 \leq 2\varepsilon\right] \leq 2^{-cdr}$.

Approximation: $\sqrt{\frac{1}{2} \pm 128\varepsilon} \approx \frac{1}{\sqrt{2}}(1 \pm 128\varepsilon)$.

1. *Total error:* $2(256\varepsilon)^2$.
2. *Simplification:*
   $\left\|\rho_b - \rho_{\tilde{b}}\right\|_1 = \frac{32\varepsilon}{rd}\left\|XY^\dagger\right\|_1$, where
   1. $X = [U^{(1)}\delta^{(1)} \ \cdots \ U^{(r)}\delta^{(r)}]$,
   2. $Y = [U^{(1)}\mathbb{1} \ \cdots \ U^{(r)}\mathbb{1}]$,
   3. $\delta^{(j)} = (-1)^{b^{(j)}} - (-1)^{\tilde{b}^{(j)}}$.
3. *Interpretation:* overlaying point clouds.
   $$\left\|XY^\dagger\right\|_1 = \max_{U \text{ unitary}} \left|\mathrm{Tr}[Y^\dagger UX]\right| = \max_{U \text{ unitary}} \sum_{j=1}^r |y_j^\dagger U x_j|.$$



Lower bound – proximity probability analysis II

Recall: $Y = \begin{bmatrix} U^{(1)}\mathbb{1} & \cdots U^{(r)}\mathbb{1} \end{bmatrix}$.

Lower bound – proximity probability analysis II

Recall: $Y = \begin{bmatrix} U^{(1)}\mathbb{1} & \cdots U^{(r)}\mathbb{1} \end{bmatrix}$.

Idea: Let

$$U^{(1)} = \frac{1}{\sqrt{d}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_d & \omega_d^2 & \cdots & \omega_d^{d-1} \\ 1 & \omega_d^2 & \omega_d^4 & \cdots & \omega_d^{2(d-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_d^{d-1} & \omega_d^{2(d-1)} & \cdots & \omega_d^{(d-1)^2} \end{bmatrix}$$

$$U^{(2)} = \frac{1}{\sqrt{d}} \begin{bmatrix} 1 & \omega_d^{d-1} & \omega_d^{2(d-1)} & \cdots & \omega_d^{(d-1)^2} \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_d & \omega_d^2 & \cdots & \omega_d^{d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_d^{d-2} & \omega_d^{2(d-2)} & \cdots & \omega_d^{(d-2)(d-1)} \end{bmatrix}$$

Then $Y = \sqrt{d}I$.

Lower bound – proximity probability analysis II

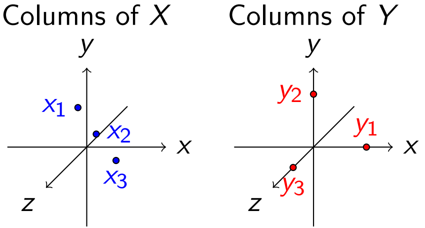
Recall: $Y = \begin{bmatrix} U^{(1)}\mathbb{1} & \cdots U^{(r)}\mathbb{1} \end{bmatrix}$.

Idea: Let

$$U^{(1)} = \frac{1}{\sqrt{d}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_d & \omega_d^2 & \cdots & \omega_d^{d-1} \\ 1 & \omega_d^2 & \omega_d^4 & \cdots & \omega_d^{2(d-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_d^{d-1} & \omega_d^{2(d-1)} & \cdots & \omega_d^{(d-1)^2} \end{bmatrix}$$

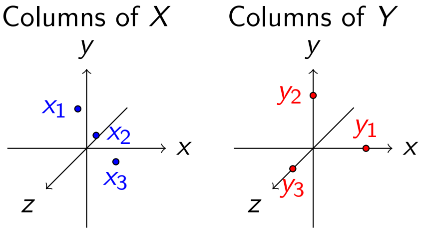
$$U^{(2)} = \frac{1}{\sqrt{d}} \begin{bmatrix} 1 & \omega_d^{d-1} & \omega_d^{2(d-1)} & \cdots & \omega_d^{(d-1)^2} \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_d & \omega_d^2 & \cdots & \omega_d^{d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_d^{d-2} & \omega_d^{2(d-2)} & \cdots & \omega_d^{(d-2)(d-1)} \end{bmatrix}$$

Then $Y = \sqrt{d} I$.



Lower bound – proximity probability analysis II

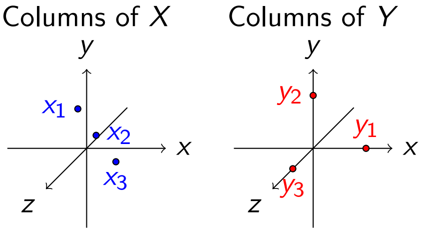
Recall $X = \begin{bmatrix} U^{(1)}\delta^{(1)} & \cdots & U^{(r)}\delta^{(r)} \end{bmatrix}$.



Lower bound – proximity probability analysis II

Recall $X = \begin{bmatrix} U^{(1)}\delta^{(1)} & \cdots & U^{(r)}\delta^{(r)} \end{bmatrix}$.

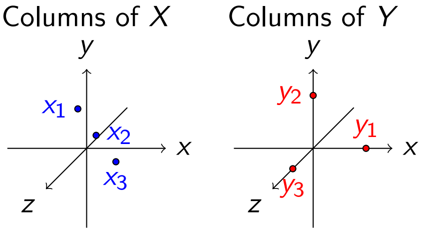
1. For any unitary U:
   $\left\|\rho_b - \rho_{\tilde{b}}\right\|_1 \geq \frac{32\varepsilon}{r\sqrt{d}} \sum_{j=1}^r |e_j^\dagger U x_j|$.



Lower bound – proximity probability analysis II

Recall $X = \begin{bmatrix} U^{(1)}\delta^{(1)} & \cdots & U^{(r)}\delta^{(r)} \end{bmatrix}$.

1. For any unitary U:
   $\left\|\rho_b - \rho_{\tilde{b}}\right\|_1 \geq \frac{32\varepsilon}{r\sqrt{d}} \sum_{j=1}^r |e_j^\dagger U x_j|$.
2. Greedy strategy to build U.

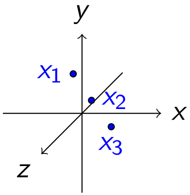


Lower bound – proximity probability analysis II

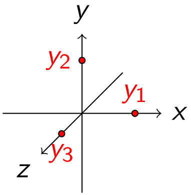
Recall $X = \begin{bmatrix} U^{(1)}\delta^{(1)} & \cdots & U^{(r)}\delta^{(r)} \end{bmatrix}$.

1. For any unitary U:
   $\left\|\rho_b - \rho_{\tilde{b}}\right\|_1 \geq \frac{32\varepsilon}{r\sqrt{d}} \sum_{j=1}^r |e_j^\dagger U x_j|$.
2. Greedy strategy to build U.
3. Let $S_j = \mathrm{Span}\{x_1, \dots, x_{j-1}\}$. Then:
   1. $\dim(S_j) = j - 1$.
   2. $|e_j^\dagger U x_j| = \left\|\Pi_{S_j^\perp} x_j\right\|$.
   3. S_j is independent from x_j.

Columns of X



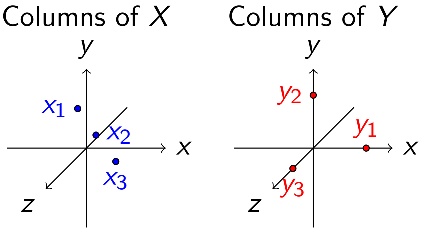
Columns of Y



Lower bound – proximity probability analysis II

Recall $X = \begin{bmatrix} U^{(1)}\delta^{(1)} & \cdots & U^{(r)}\delta^{(r)} \end{bmatrix}$.

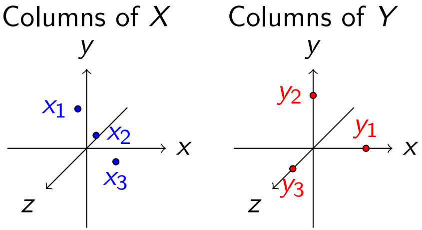
1. For any unitary U:
   $\left\|\rho_b - \rho_{\tilde{b}}\right\|_1 \geq \frac{32\varepsilon}{r\sqrt{d}} \sum_{j=1}^r |e_j^\dagger U x_j|$.
2. Greedy strategy to build U.
3. Let $S_j = \mathrm{Span}\{x_1, \dots, x_{j-1}\}$. Then:
   1. $\dim(S_j) = j - 1$.
   2. $|e_j^\dagger U x_j| = \left\|\Pi_{S_j^\perp} x_j\right\|$.
   3. S_j is independent from x_j.
4. Since $\delta^{(j)}$ has independent entries, $\exists c \in (0,1)$ s.t.
   $\mathbb{P}\left[\left|\left\|\Pi_{S_j^\perp} x_j\right\| - \sqrt{d-j+1}\right| \geq \frac{1}{4}\sqrt{d}\right] \leq 2^{-cd}$.[RV'13]



Lower bound – proximity probability analysis II

Recall $X = \begin{bmatrix} U^{(1)}\delta^{(1)} & \cdots & U^{(r)}\delta^{(r)} \end{bmatrix}$.

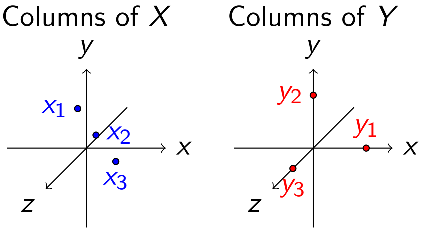
1. For any unitary U:
   $\left\|\rho_b - \rho_{\tilde{b}}\right\|_1 \geq \frac{32\varepsilon}{r\sqrt{d}} \sum_{j=1}^r |e_j^\dagger U x_j|$.
2. Greedy strategy to build U.
3. Let $S_j = \mathrm{Span}\{x_1, \dots, x_{j-1}\}$. Then:
   1. $\dim(S_j) = j - 1$.
   2. $|e_j^\dagger U x_j| = \left\|\Pi_{S_j^\perp} x_j\right\|$.
   3. S_j is independent from x_j.
4. Since $\delta^{(j)}$ has independent entries, $\exists c \in (0,1)$ s.t.
   $\mathbb{P}\left[\left|\left\|\Pi_{S_j^\perp} x_j\right\| - \sqrt{d-j+1}\right| \geq \frac{1}{4}\sqrt{d}\right] \leq 2^{-cd}$.[RV'13]
5. If $\left\|\rho_b - \rho_{\tilde{b}}\right\|_1 \leq 2\varepsilon$, then the above must hold for at least $r/4$ terms.



Lower bound – proximity probability analysis II

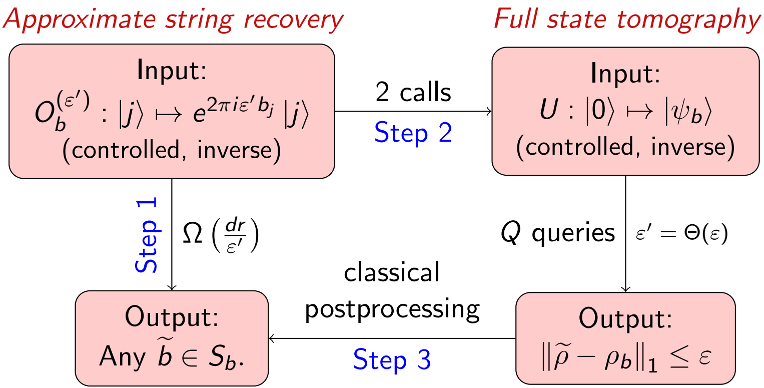
Recall $X = \begin{bmatrix} U^{(1)}\delta^{(1)} & \cdots & U^{(r)}\delta^{(r)} \end{bmatrix}$.

1. For any unitary U:
   $\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \geq \frac{32\varepsilon}{r\sqrt{d}} \sum_{j=1}^r |e_j^\dagger U x_j|$.
2. Greedy strategy to build U.
3. Let $S_j = \mathrm{Span}\{x_1, \dots, x_{j-1}\}$. Then:
   1. $\dim(S_j) = j - 1$.
   2. $|e_j^\dagger U x_j| = \left\|\Pi_{S_j^\perp} x_j\right\|$.
   3. S_j is independent from x_j.
4. Since $\delta^{(j)}$ has independent entries, $\exists c \in (0,1)$ s.t.
   $\mathbb{P}\left[\left|\left\|\Pi_{S_j^\perp} x_j\right\| - \sqrt{d-j+1}\right| \geq \frac{1}{4}\sqrt{d}\right] \leq 2^{-cd}$. [RV'13]
5. If $\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon$, then the above must hold for at least $r/4$ terms.
6. Thus $\mathbb{P}\left[\left\|\rho_b - \rho_{\widetilde{b}}\right\|_1 \leq 2\varepsilon\right] \leq 2^{-cdr/4}$.



Lower bound – proof overview

Idea: "Embed the approximate string recovery problem into the full state-tomography problem."



References I

[vA'21] van Apeldoorn. *Quantum probability oracles & multidimensional amplitude estimation.*

[Bel'15] Belovs. *Variations on quantum adversary.* arXiv:1504.06943

[CHL+'22] Chen, Huang, Li, Liu, Sellke. *Tight bounds for state tomography with incoherent measurments.* arXiv:2206.05265

[CJ'21] Cornelissen, Jerbi. *Quantum algorithms for multivariate Monte Carlo estimation.* arXiv:2107.03410

[FGGS'99] Farhi, Goldstone, Gutmann, Sipser. *How many functions can be distinguished with k quantum queries?* arXiv:quant-ph/9901012

[HHJ+'17] Haah, Harrow, Ji, Wu, Yu. *Sample-optimal tomography of quantum states.* arXiv:1508.01797

[HKP'20] Huang, Kueng, Preskill. *Predicting many properties of a quantum system from very few measurements.* arXiv:2002.08953

References II

[HWM+'21] Huggins, Wan, McClean, O'Brien, Wiebe, Babbush. *Nearly optimal quantum algorithm for estimating multiple expectation values*. `arXiv:2111.09283`

[KP'20] Kerenidis, Prakash. *A quantum interior point method for LPs and SDPs*. `arXiv:1808.09266`

[LMRŠS'11] Lee, Mittal, Reichardt, Špalek, Szegedy. *Quantum query complexity of state conversion*. `arXiv:1011.3020`

[RV'13] Rudelson, Vershynin. *Hanson-Wright inequality and sub-gaussian concentration*. `arXiv:1306.2872`

[Yue'22] Yuen. *An improved sample complexity lower bound for quantum state tomography*. `arXiv:2206.11185`