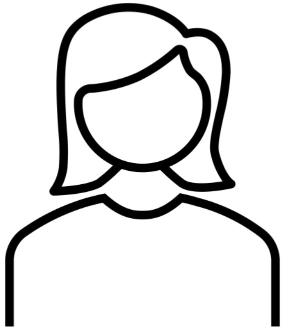
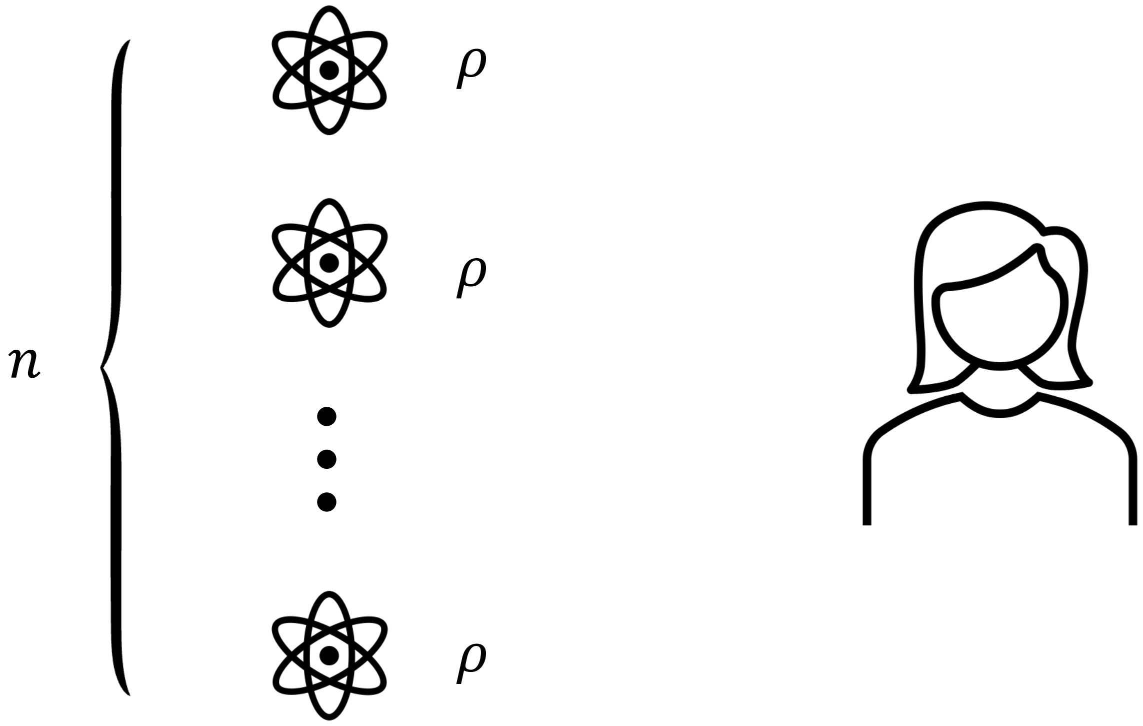
Improved lower bounds for learning quantum states with single-copy measurements

Angus Lowe & Ashwin Nayak

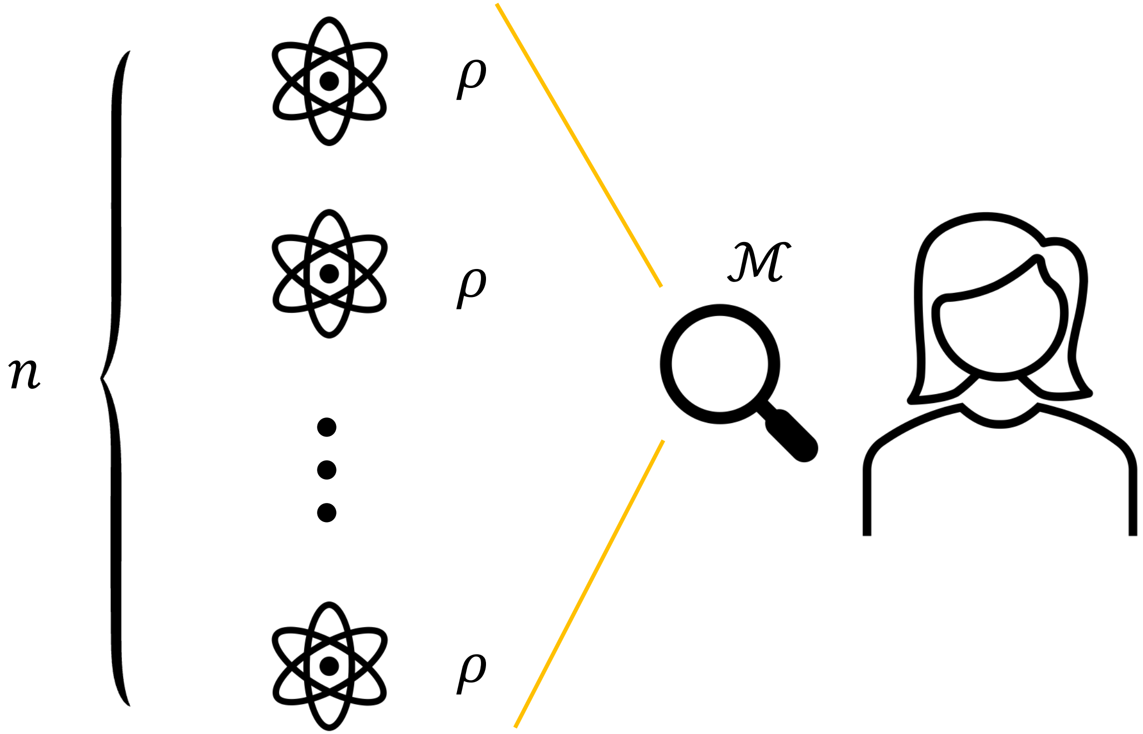
Learning properties of quantum states



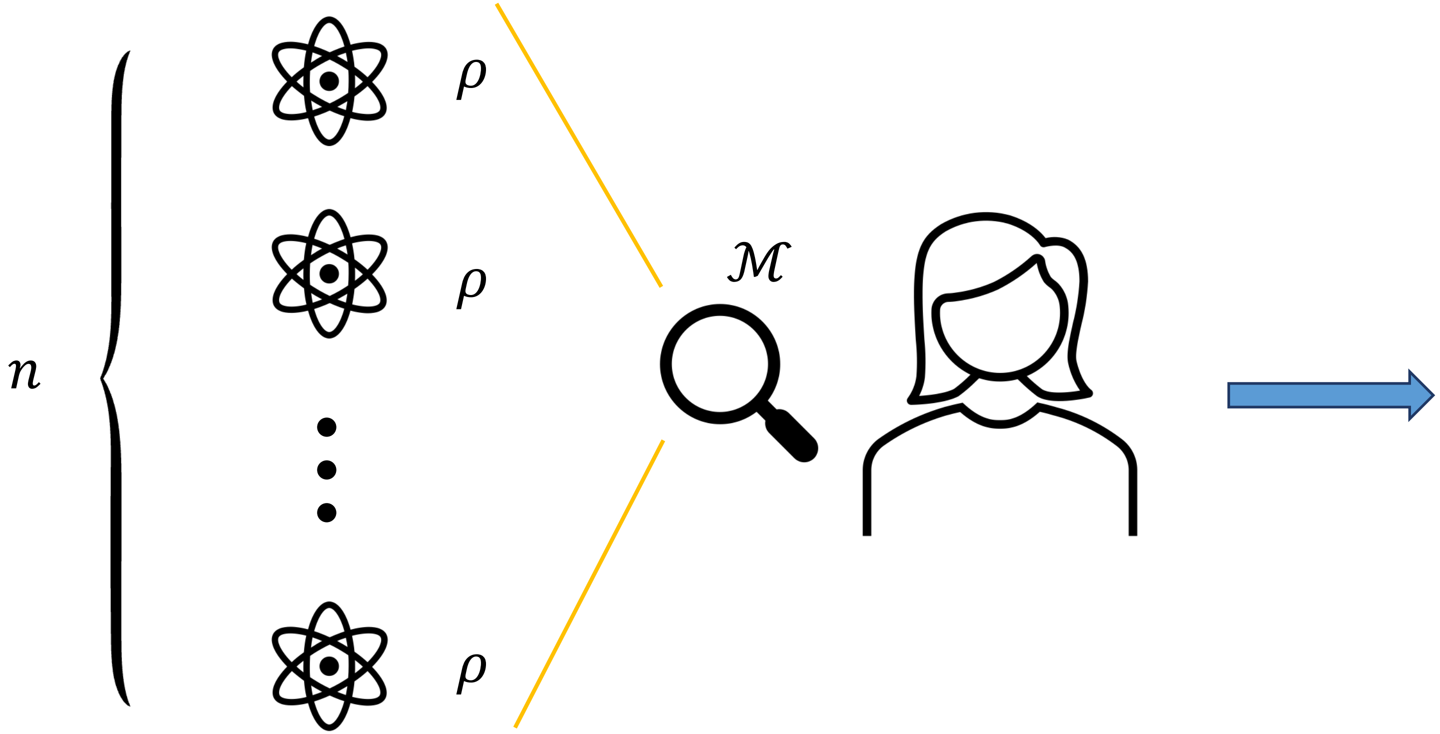
Learning properties of quantum states



Learning properties of quantum states



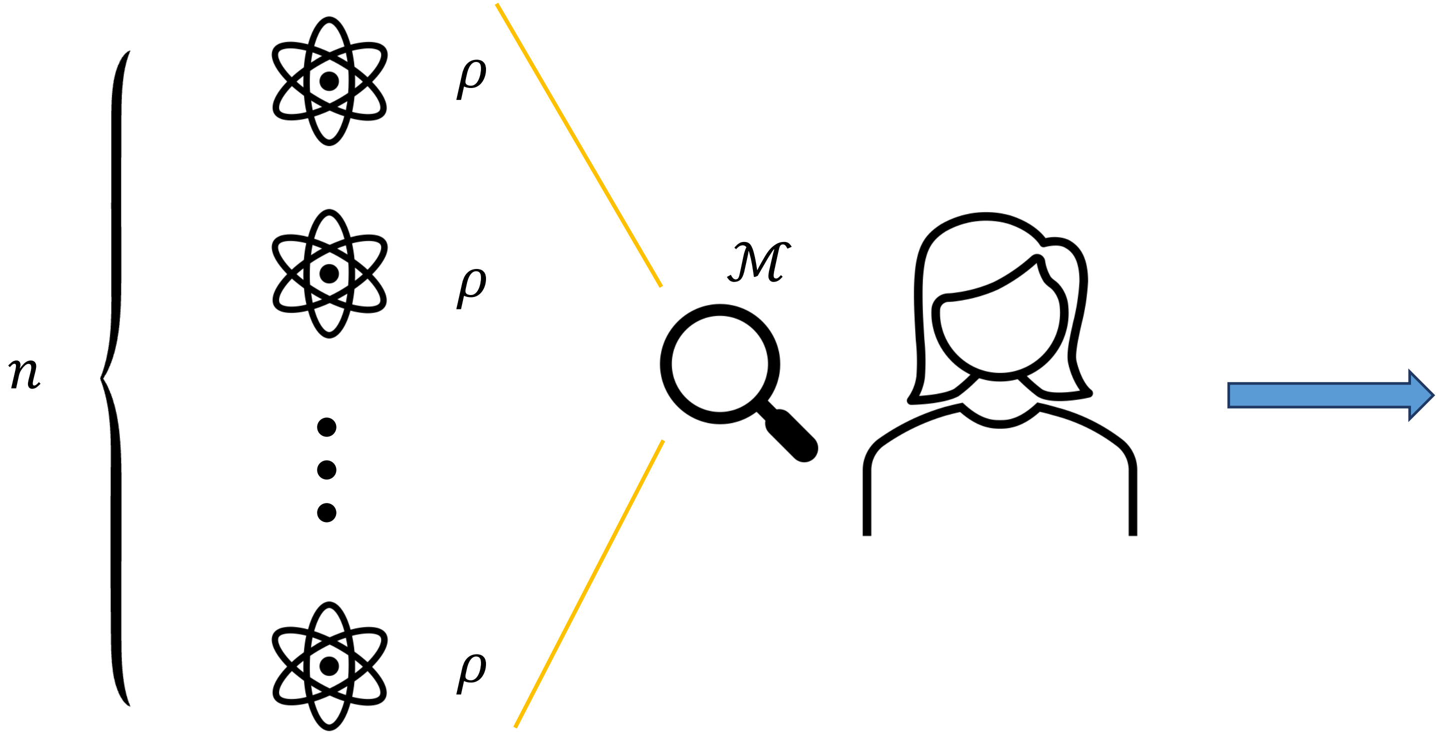
Learning properties of quantum states



Possible questions

- What are the expected values of some observables?
- Is $\rho = \sigma$?
- *What is* ρ*?*

Learning properties of quantum states



Possible questions

- What are the expected values of some observables?
- Is $\rho = \sigma$?
- *What is ρ?*

Quantum tomography

Input: Measurement outcome Y from measurement $\mathcal{M}$ on $\rho^{\otimes n}$, $\rho \in D(\mathbb{C}^d)$.

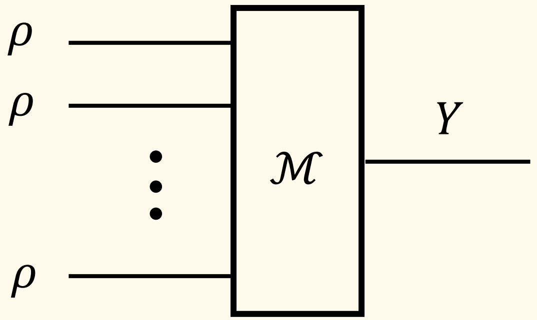
Output: Estimate $\hat{\rho}$ such that $||\hat{\rho} - \rho||_1 \leq \epsilon$ with high probability.

Quantum tomography

Input: Measurement outcome Y from measurement $\mathcal{M}$ on $\rho^{\otimes n}$, $\rho \in D(\mathbb{C}^d)$.

Output: Estimate $\hat{\rho}$ such that $||\hat{\rho} - \rho||_1 \leq \epsilon$ with high probability.

Entangled



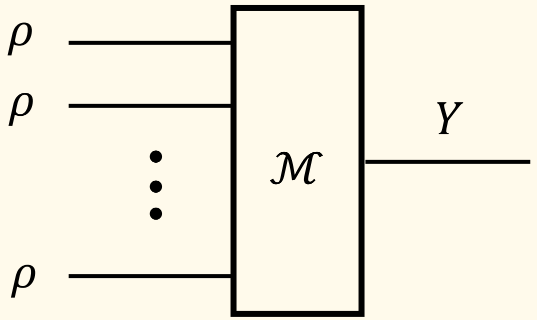
*resolved [O'Donnell, Wright' 16],[Haah, Harrow, Ji, Wu, Yu' 17]

Quantum tomography

Input: Measurement outcome Y from measurement $\mathcal{M}$ on $\rho^{\otimes n}$, $\rho \in D(\mathbb{C}^d)$.

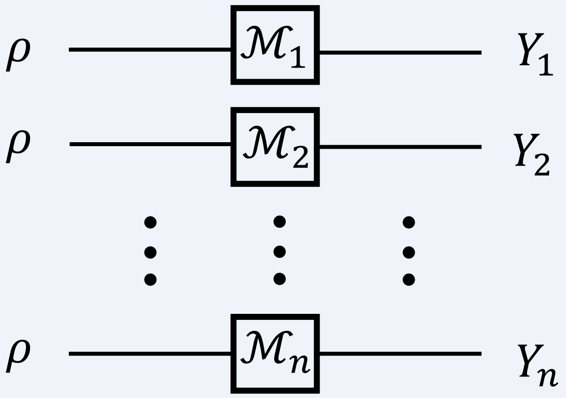
Output: Estimate $\hat{\rho}$ such that $\|\hat{\rho} - \rho\|_1 \leq \epsilon$ with high probability.

Entangled

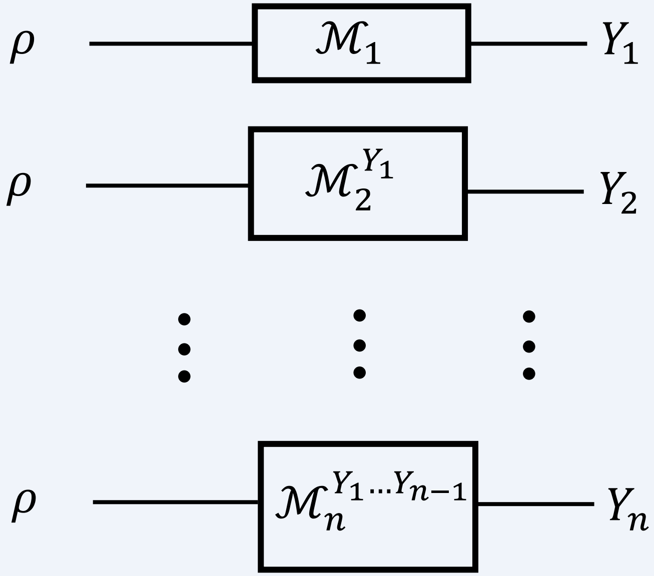


*resolved [O'Donnell, Wright' 16],[Haah, Harrow, Ji, Wu, Yu' 17]

Single-copy



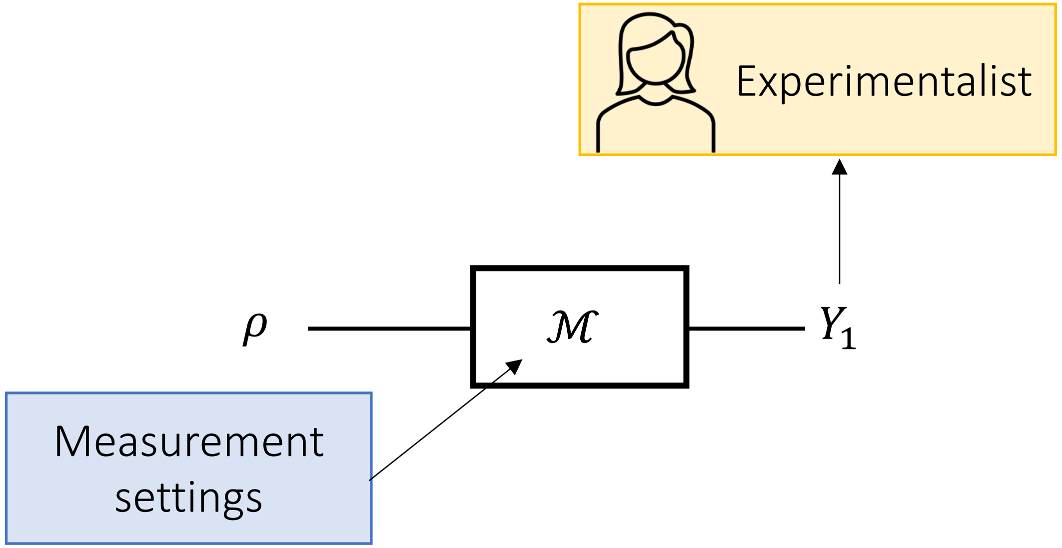
Nonadaptive



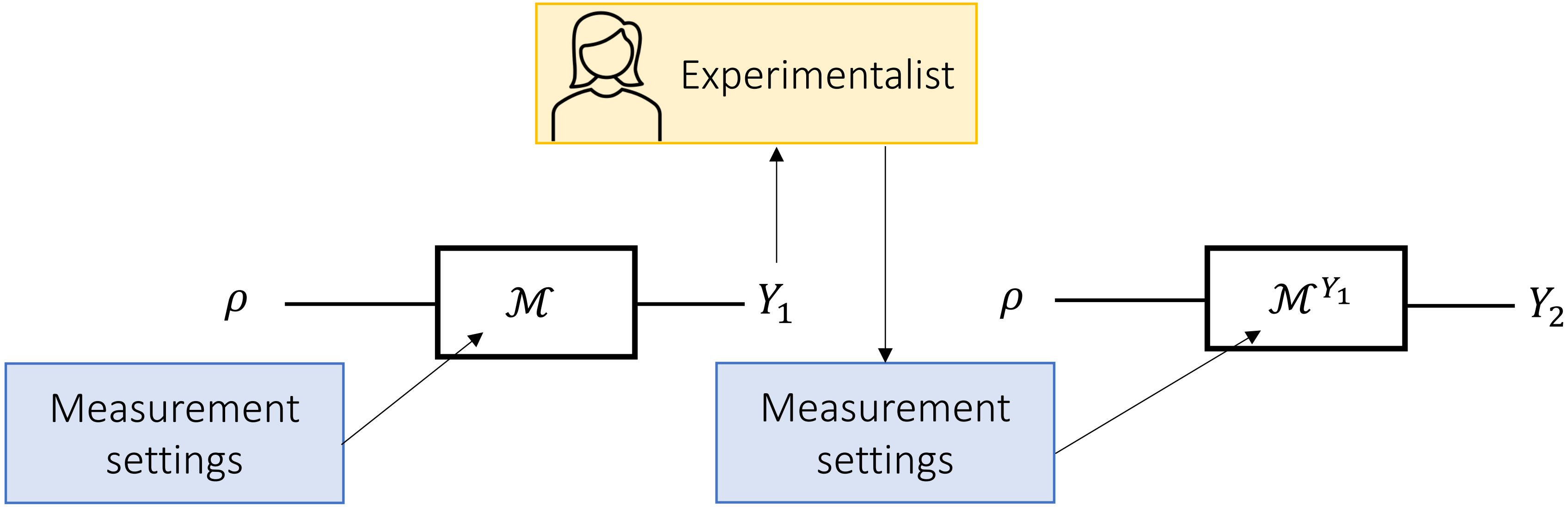
Adaptive

Single-copy quantum tomography

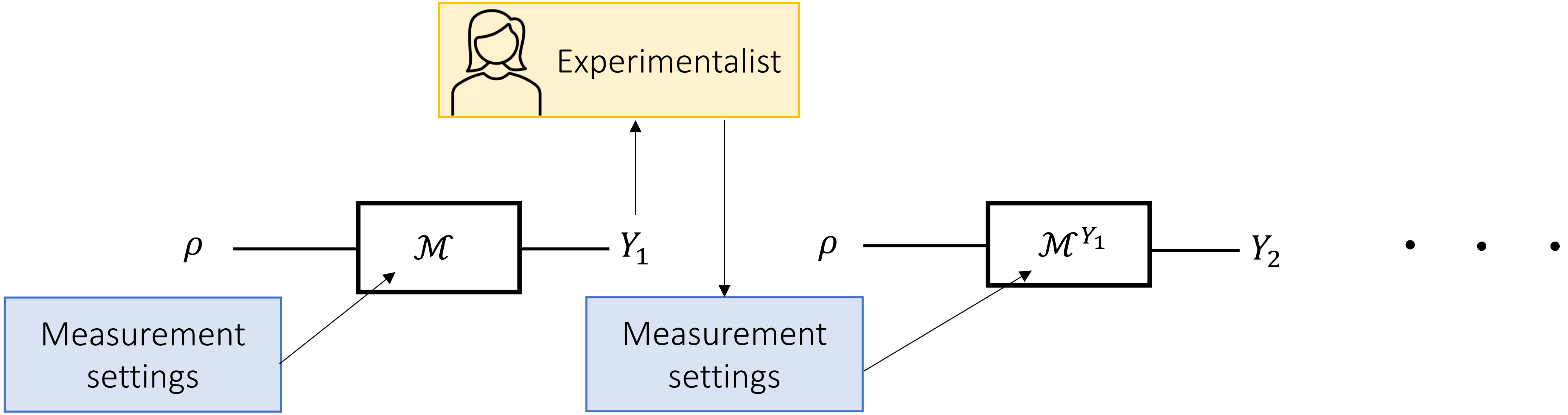
Single-copy quantum tomography



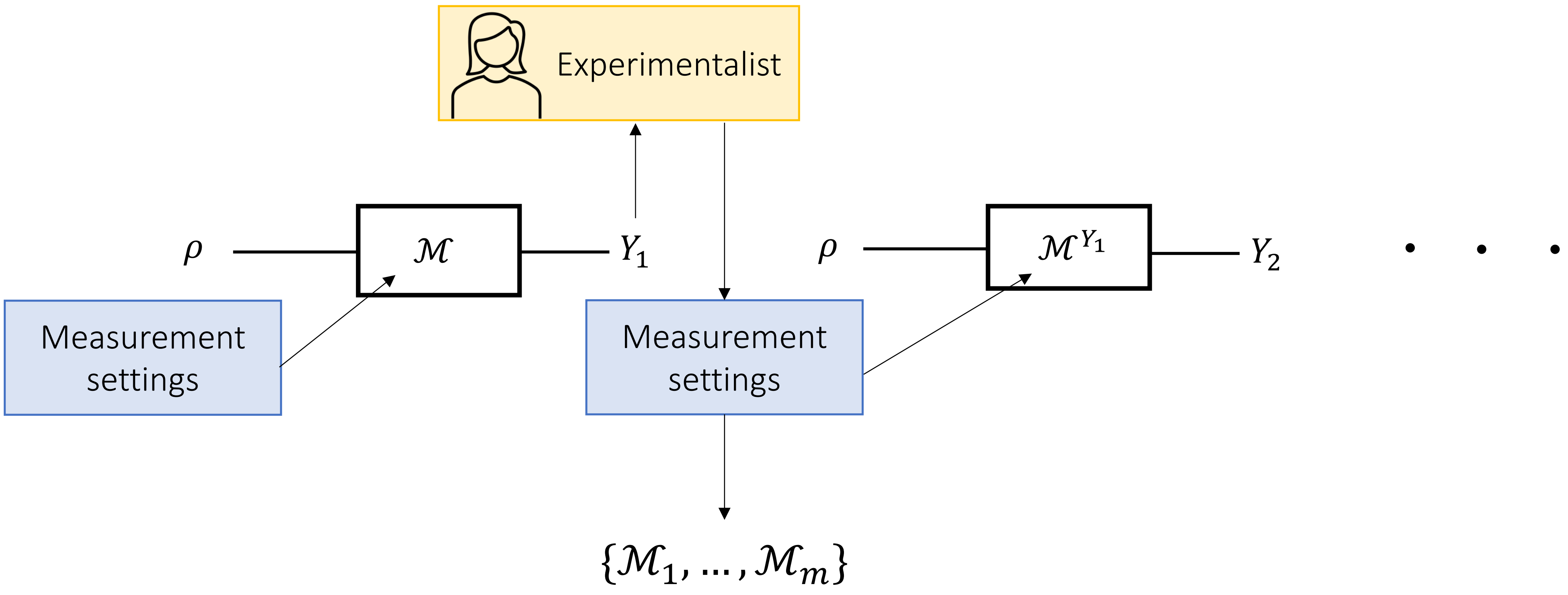
Single-copy quantum tomography



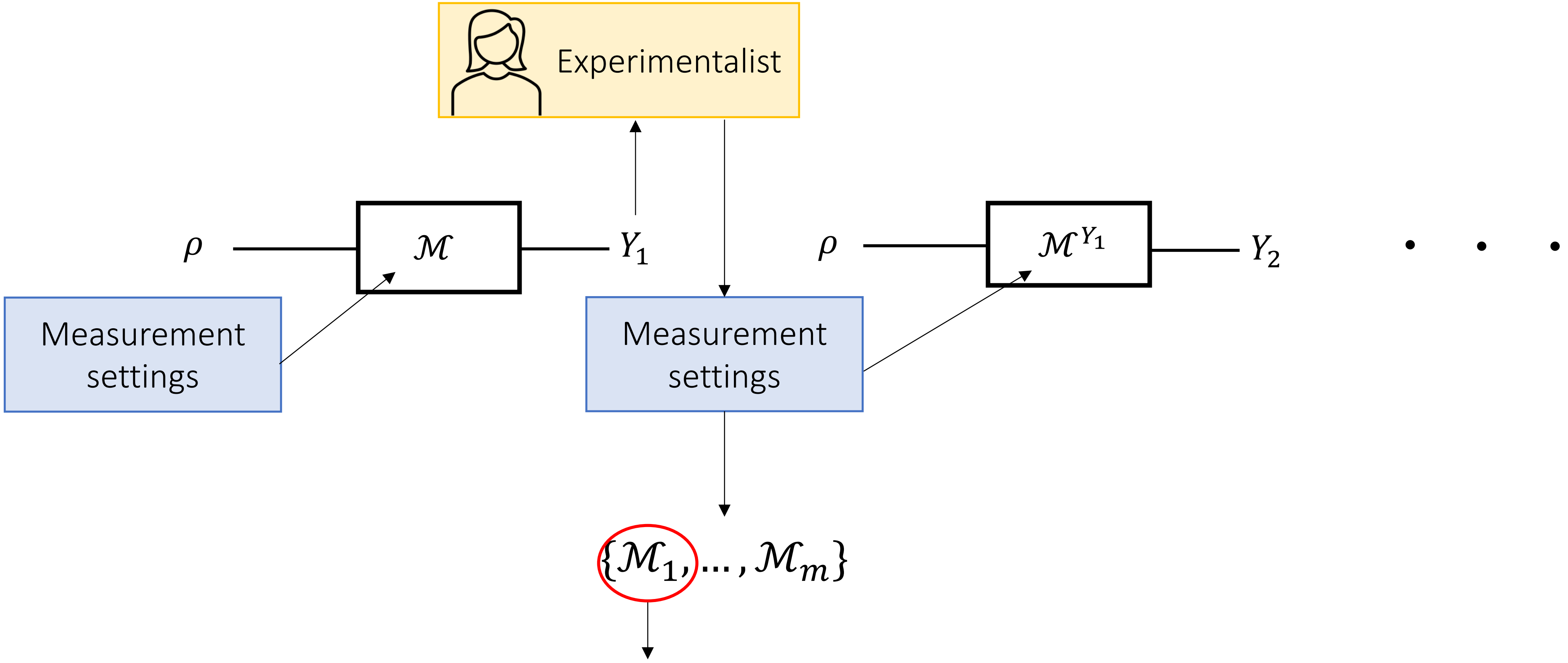
Single-copy quantum tomography



Single-copy quantum tomography



Single-copy quantum tomography



$\{E_1^{(1)}, \ldots, E_L^{(1)}\}$ is a POVM

Results and prior work

Upper bounds

Strategy	Number of Copies
Nonadaptive, 2-outcome Pauli	$O(d^4/\epsilon^2)$ [Folklore]
Nonadaptive, random (2-design) basis	$O(d^3/\epsilon^2)$ [Kueng, Rauhut, Terstiege' 14]

Results and prior work

Upper bounds

Strategy	Number of Copies
Nonadaptive, 2-outcome Pauli	$O(d^4/\epsilon^2)$ [Folklore]
Nonadaptive, random (2-design) basis	$O(d^3/\epsilon^2)$ [Kueng, Rauhut, Terstiege' 14]

$$\rho \longrightarrow \boxed{\mathcal{M}_i} \longrightarrow Y_i$$

$$\left\{\frac{1}{2}(1 \pm P_i)\right\},\ P_i \in \{\mathbb{I}, \sigma_x, \sigma_y, \sigma_z\}^{\otimes \log(d)}$$

Results and prior work

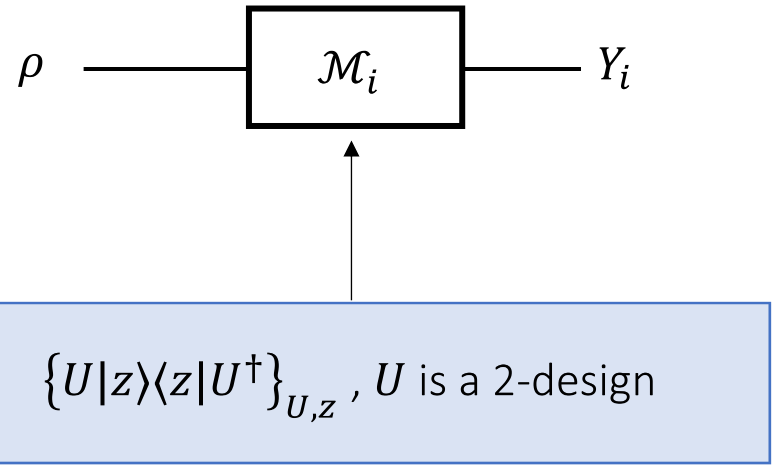
Upper bounds

Strategy	Number of Copies
Nonadaptive, 2-outcome Pauli	$O(d^4/\epsilon^2)$ [Folklore]
Nonadaptive, random (2-design) basis	$O(d^3/\epsilon^2)$ [Kueng, Rauhut, Terstiege' 14]

Results and prior work

Upper bounds

Strategy	Number of Copies
Nonadaptive, 2-outcome Pauli	$O(d^4/\epsilon^2)$ [Folklore]
Nonadaptive, random (2-design) basis	$O(d^3/\epsilon^2)$ [Kueng, Rauhut, Terstiege' 14]



Results and prior work

Upper bounds

Strategy	Number of Copies
Nonadaptive, 2-outcome Pauli	$O(d^4/\epsilon^2)$ [Folklore]
Nonadaptive, random (2-design) basis	$O(d^3/\epsilon^2)$ [Kueng, Rauhut, Terstiege' 14]

ρ —— $\boxed{\mathcal{M}_i}$ —— Y_i

$\{U|z\rangle\langle z|U^\dagger\}_{U,z}$, U is a 2-design

e.g., U a random Clifford circuit

Results and prior work

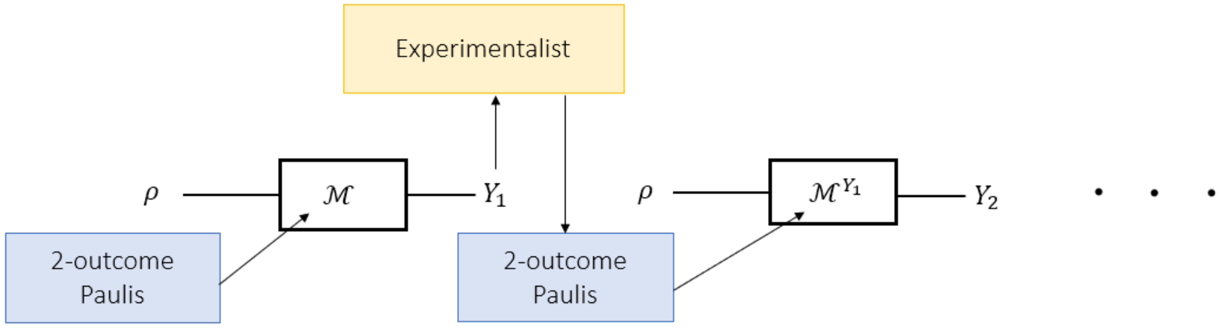
Lower bounds

Measurements	Adaptivity?	Number of Copies
2-outcome Pauli	✓	$\Omega(d^4/\log(d))$ [Flammia, Gross, Liu, Eisert' 12]
Any	✗	$\Omega(d^3/\epsilon^2)$ [Haah+17]

Results and prior work

Lower bounds

Measurements	Adaptivity?	Number of Copies
2-outcome Pauli	✓	$\Omega(d^4/\log(d))$ [Flammia, Gross, Liu, Eisert' 12]
Any	✗	$\Omega(d^3/\epsilon^2)$ [Haah+17]



Results and prior work

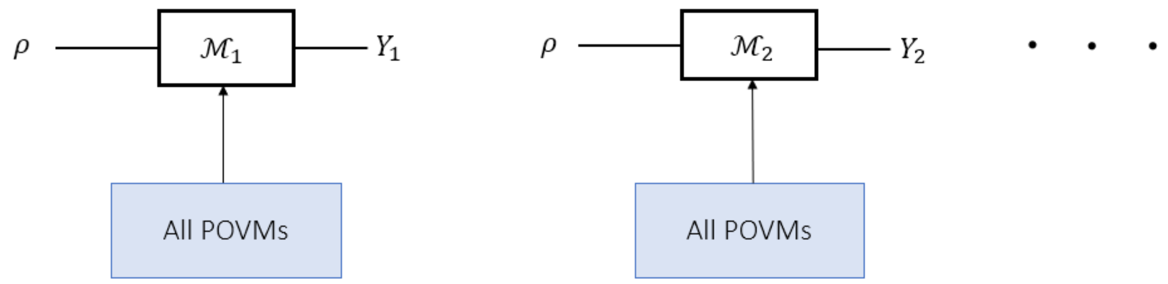
Lower bounds

Measurements	Adaptivity?	Number of Copies
2-outcome Pauli	✓	$\Omega(d^4/\log(d))$ [Flammia, Gross, Liu, Eisert' 12]
Any	✗	$\Omega(d^3/\epsilon^2)$ [Haah+17]

Results and prior work

Lower bounds

Measurements	Adaptivity?	Number of Copies
2-outcome Pauli	✓	$\Omega(d^4/\log(d))$ [Flammia, Gross, Liu, Eisert' 12]
Any	✗	$\Omega(d^3/\epsilon^2)$ [Haah+17]



Results and prior work

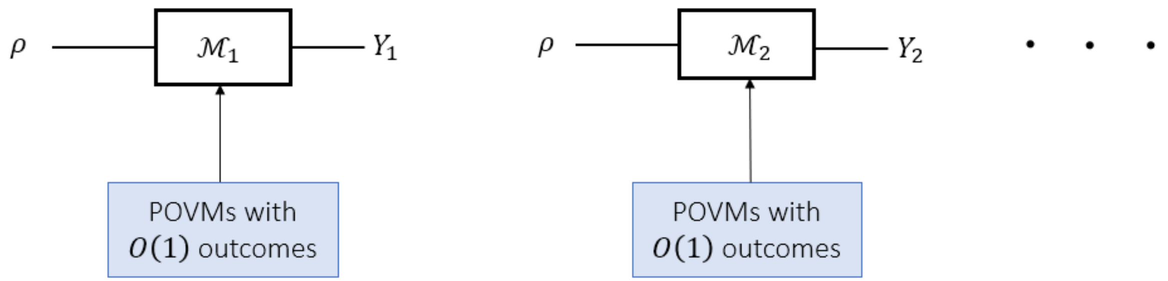
Lower bounds

Measurements	Adaptivity?	Number of Copies
2-outcome Pauli	✓	$\Omega(d^4/\log(d))$ [Flammia, Gross, Liu, Eisert' 12]
Any	✗	$\Omega(d^3/\epsilon^2)$ [Haah+17]
$O(1)$-outcomes	✗	$\Omega(d^4/\epsilon^2)$ [this work]

Results and prior work

Lower bounds

Measurements	Adaptivity?	Number of Copies
2-outcome Pauli	✓	$\Omega(d^4/\log(d))$ [Flammia, Gross, Liu, Eisert' 12]
Any	✗	$\Omega(d^3/\epsilon^2)$ [Haah+17]
$O(1)$-outcomes	✗	$\Omega(d^4/\epsilon^2)$ [this work]



Results and prior work

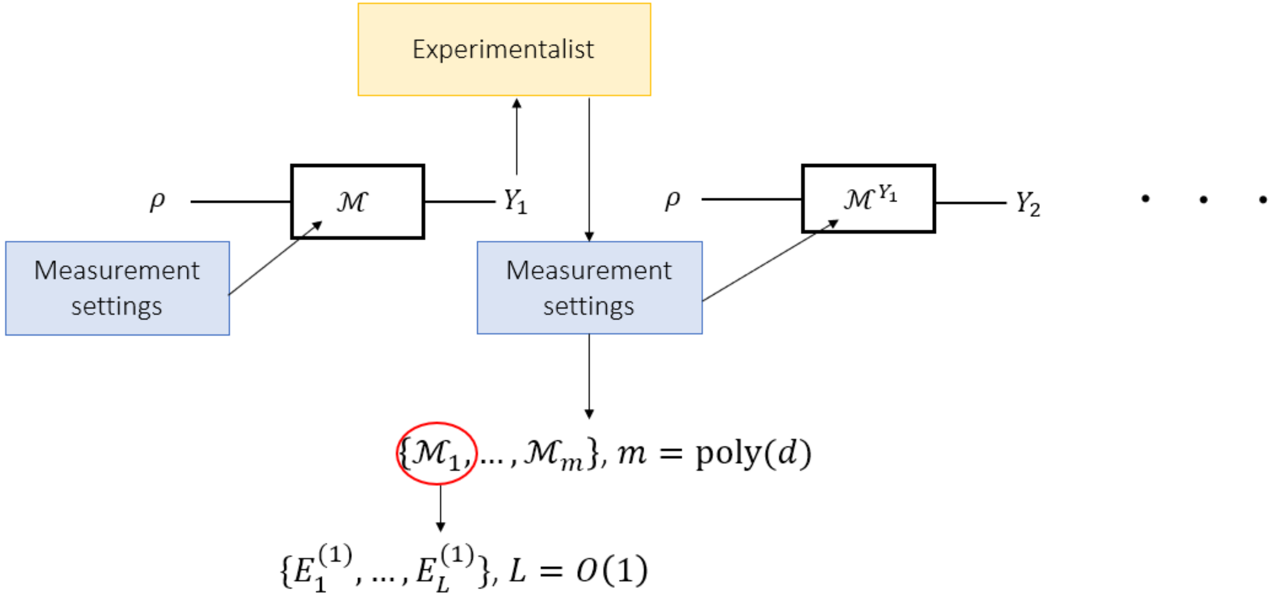
Lower bounds

Measurements	Adaptivity?	Number of Copies
2-outcome Pauli	✓	$\Omega(d^4/\log(d))$ [Flammia, Gross, Liu, Eisert' 12]
Any	✗	$\Omega(d^3/\epsilon^2)$ [Haah+17]
$O(1)$-outcomes	✗	$\Omega(d^4/\epsilon^2)$ [this work]
$\mathrm{poly}(d)$ settings $+O(1)$-outcomes	✓	$\Omega(d^4/\epsilon^2\log(d))$ [this work]

Results and prior work

Lower bounds

Measurements	Adaptivity?	Number of Copies
2-outcome Pauli	✓	$\Omega(d^4/\log(d))$ [Flammia, Gross, Liu, Eisert' 12]
Any	✗	$\Omega(d^3/\epsilon^2)$ [Haah+17]
$O(1)$-outcomes	✗	$\Omega(d^4/\epsilon^2)$ [this work]
$\mathrm{poly}(d)$ settings $+O(1)$-outcomes	✓	$\Omega(d^4/\epsilon^2\log(d))$ [this work]



Results and prior work

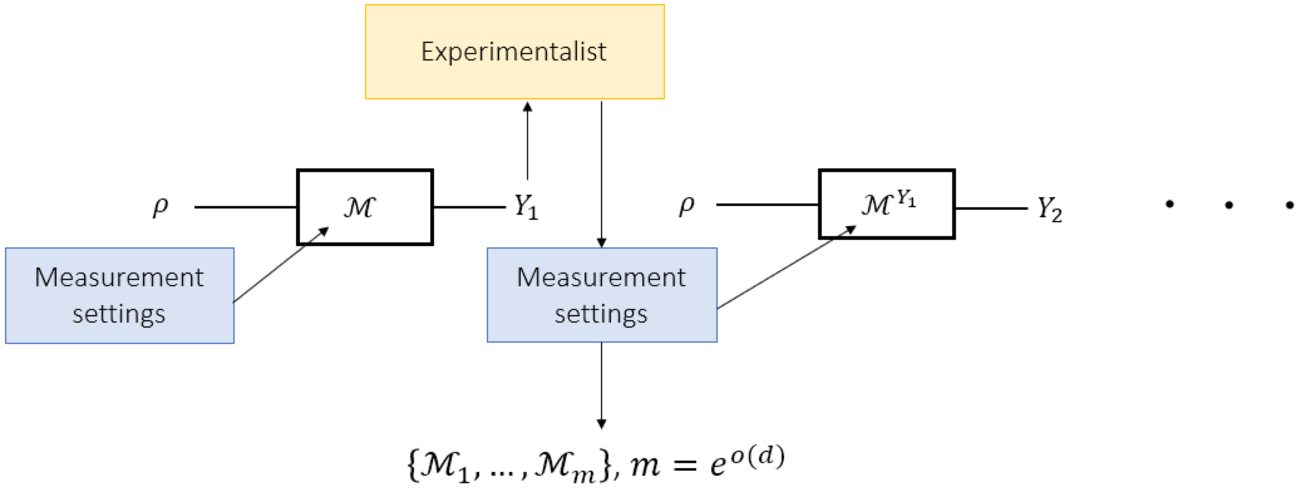
Lower bounds

Measurements	Adaptivity?	Number of Copies
2-outcome Pauli	✓	$\Omega(d^4/\log(d))$ [Flammia, Gross, Liu, Eisert' 12]
Any	✗	$\Omega(d^3/\epsilon^2)$ [Haah+17]
$O(1)$-outcomes	✗	$\Omega(d^4/\epsilon^2)$ [this work]
$\mathrm{poly}(d)$ settings $+O(1)$-outcomes	✓	$\Omega(d^4/\epsilon^2 \log(d))$ [this work]
$e^{o(d)}$ settings	✓	$\Omega(d^3/\epsilon^2)$ [this work]

Results and prior work

Lower bounds

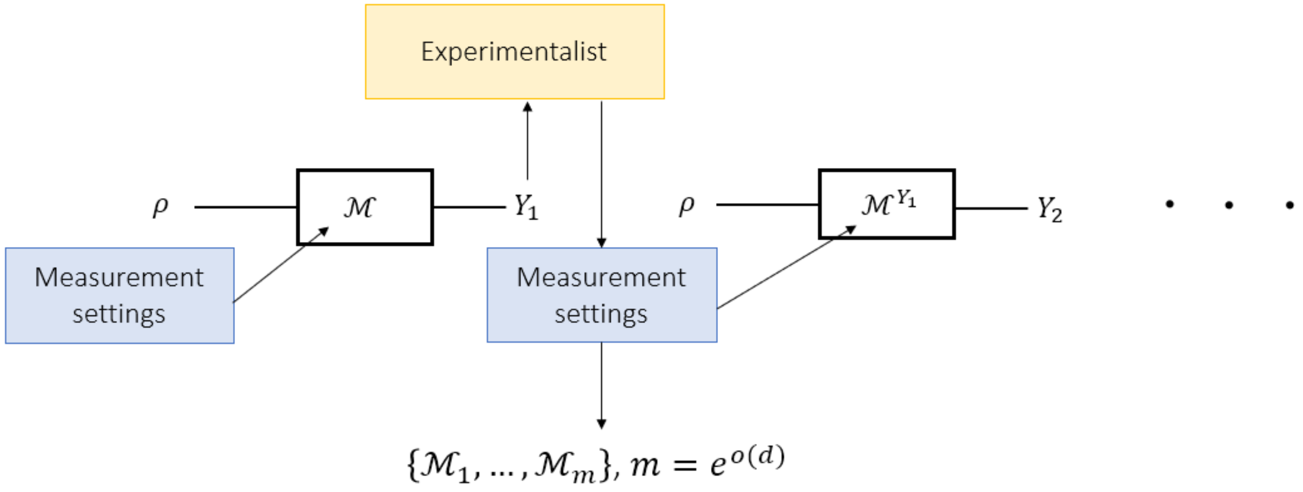
Measurements	Adaptivity?	Number of Copies
2-outcome Pauli	✓	$\Omega(d^4/\log(d))$ [Flammia, Gross, Liu, Eisert' 12]
Any	✗	$\Omega(d^3/\epsilon^2)$ [Haah+17]
$O(1)$-outcomes	✗	$\Omega(d^4/\epsilon^2)$ [this work]
$\mathrm{poly}(d)$ settings $+O(1)$-outcomes	✓	$\Omega(d^4/\epsilon^2 \log(d))$ [this work]
$e^{o(d)}$ settings	✓	$\Omega(d^3/\epsilon^2)$ [this work]



Results and prior work

Lower bounds

Measurements	Adaptivity?	Number of Copies
2-outcome Pauli	✓	$\Omega(d^4/\log(d))$ [Flammia, Gross, Liu, Eisert' 12]
Any	✗	$\Omega(d^3/\epsilon^2)$ [Haah+17]
$O(1)$-outcomes	✗	$\Omega(d^4/\epsilon^2)$ [this work]
$\mathrm{poly}(d)$ settings $+O(1)$-outcomes	✓	$\Omega(d^4/\epsilon^2\log(d))$ [this work]
$e^{o(d)}$ settings	✓	$\Omega(d^3/\epsilon^2)$ [this work]

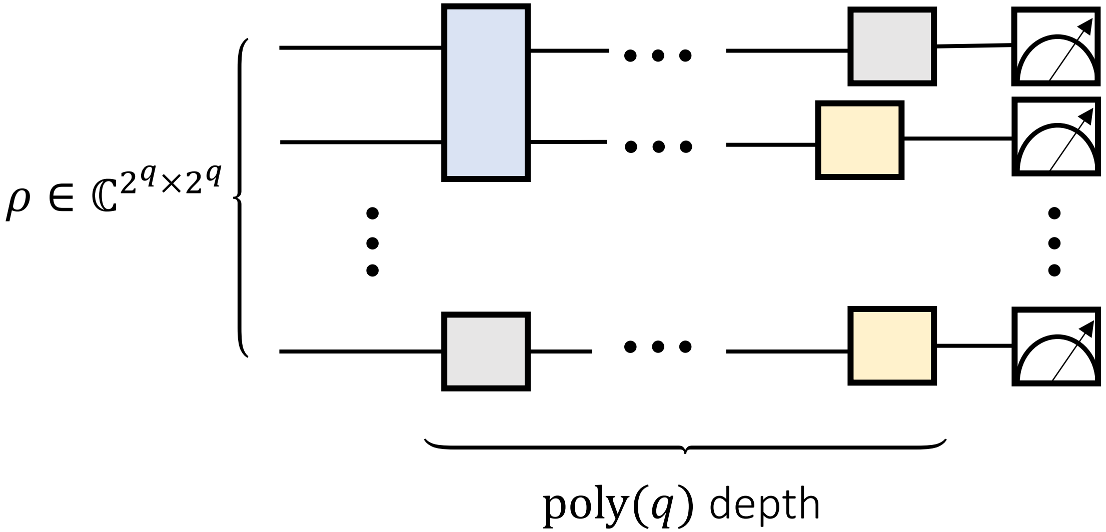


A lower bound for low-depth circuits

$\Rightarrow$ adaptivity makes no difference without $\sim \exp(2^q)$ distinct measurement settings on a system comprised of q qubits.

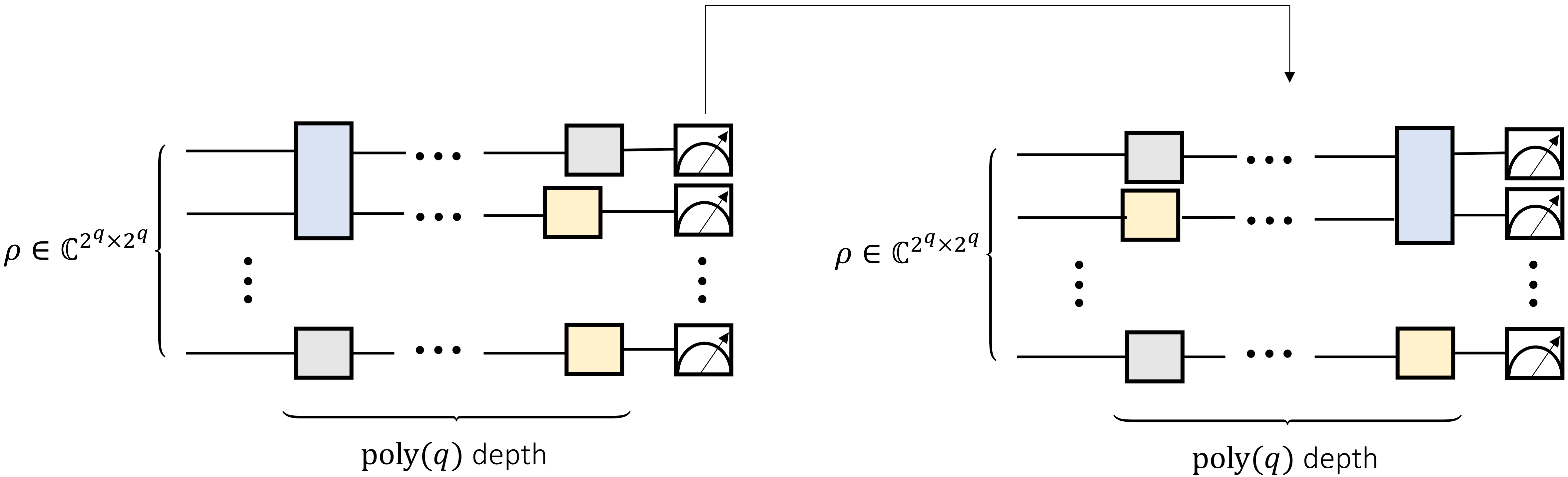
A lower bound for low-depth circuits

$\Rightarrow$ adaptivity makes no difference without $\sim \exp(2^q)$ distinct measurement settings on a system comprised of q qubits.

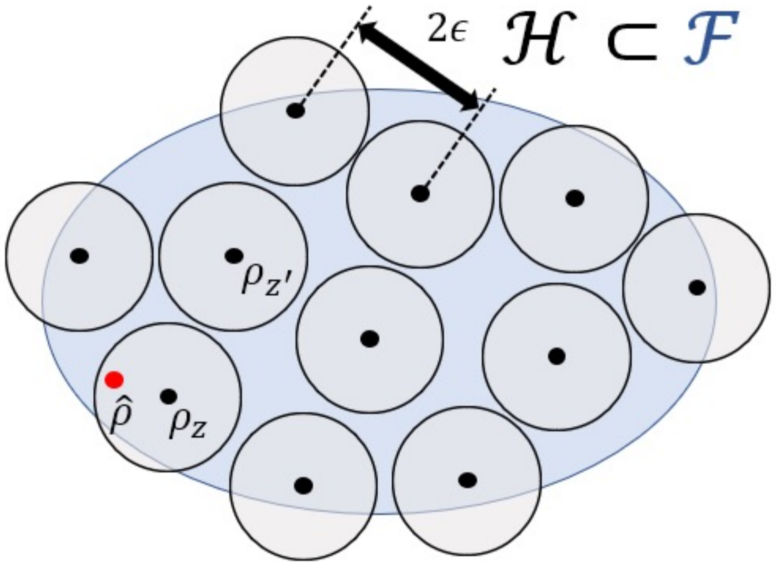


A lower bound for low-depth circuits

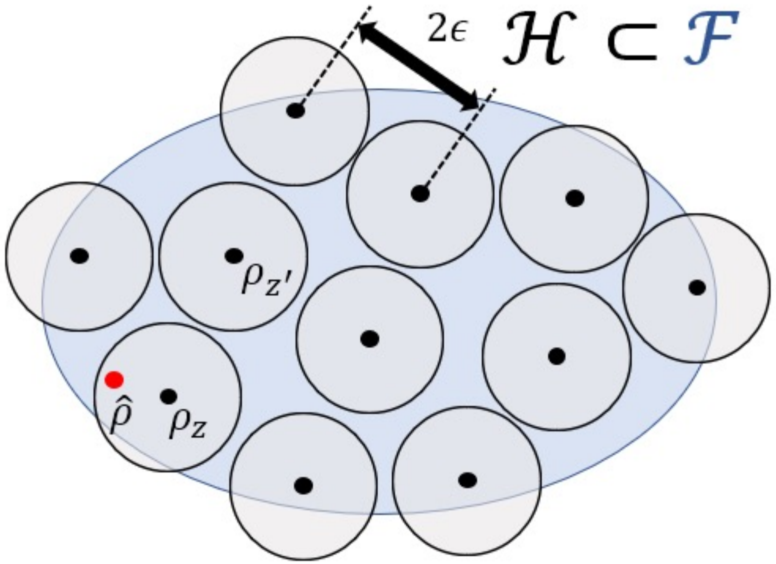
⇒ adaptivity makes no difference without $\sim \exp(2^q)$ distinct measurement settings on a system comprised of q qubits.



Recipe for a lower bound

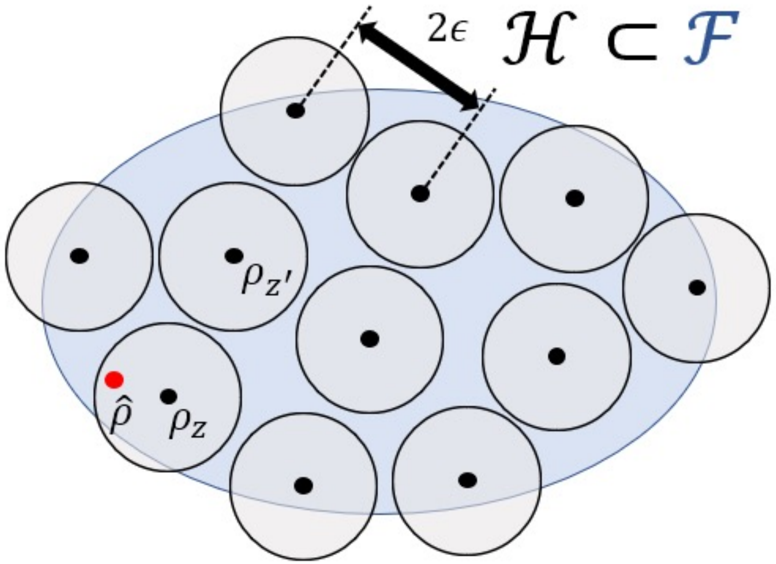


Recipe for a lower bound



Quantum state discrimination of $\mathcal{H}$ $\leq$ Tomography

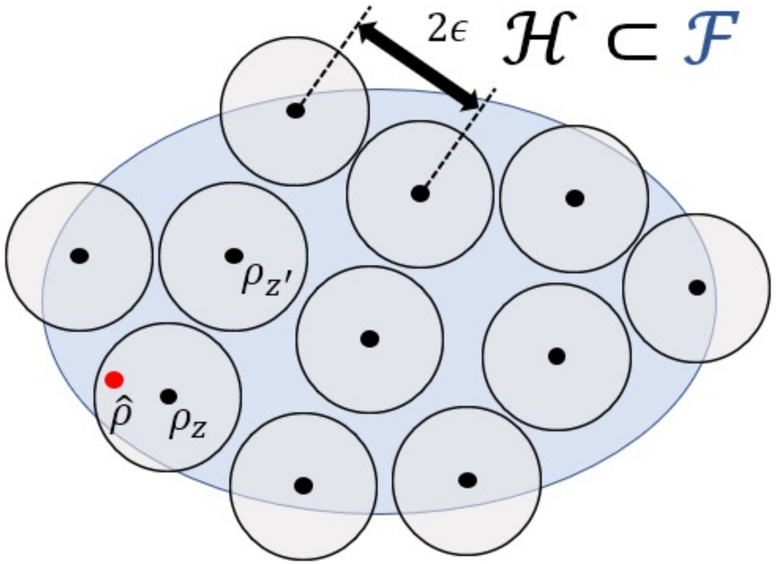
Recipe for a lower bound



Quantum state discrimination of $\mathcal{H}$ $\leq$ Tomography

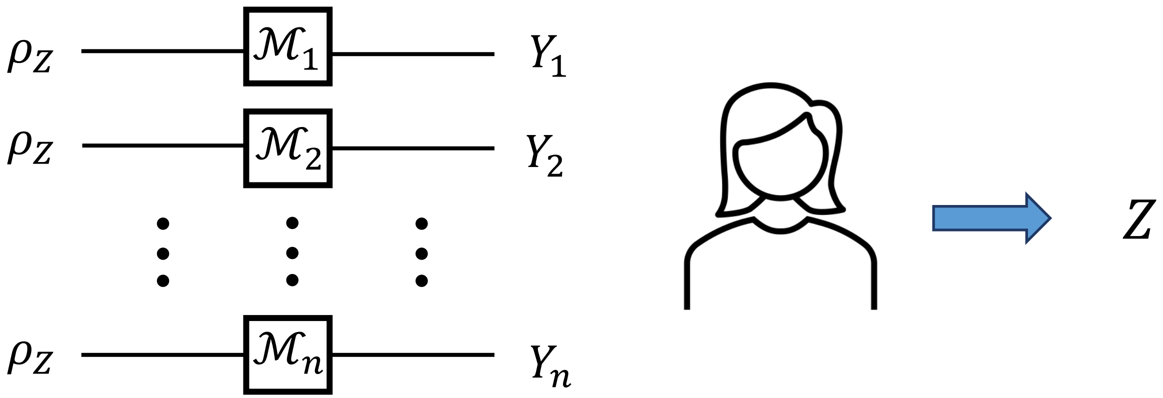
$Z \sim \text{Unif}(\{1, \dots, |\mathcal{H}|\})$

Recipe for a lower bound

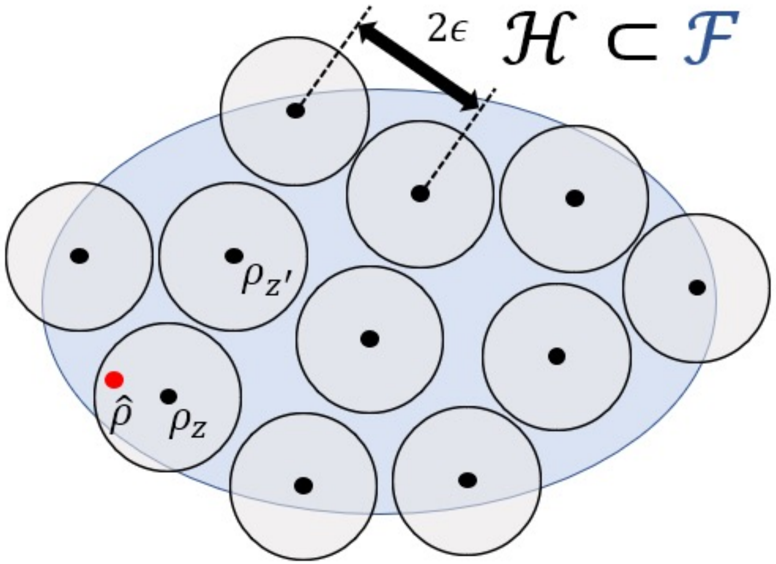


Quantum state discrimination of $\mathcal{H}$ $\leq$ Tomography

$Z \sim \mathrm{Unif}(\{1, \dots, |\mathcal{H}|\})$

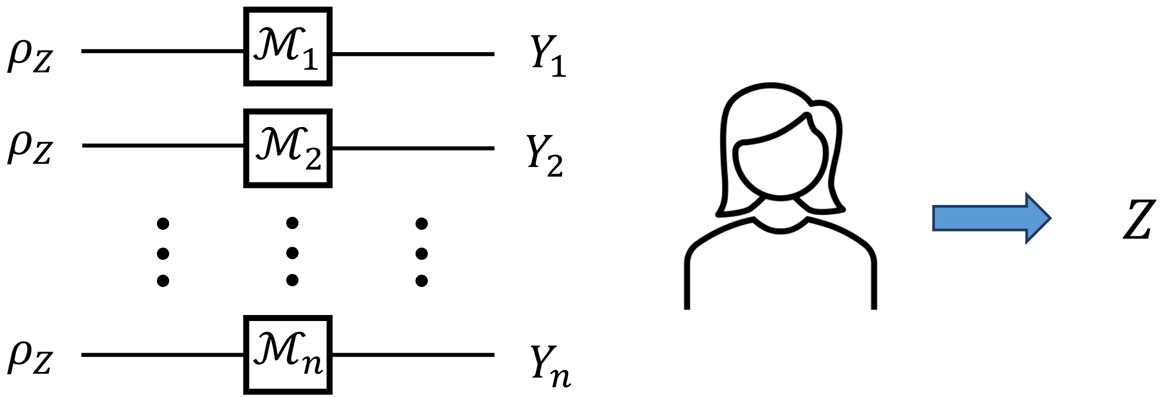


Recipe for a lower bound



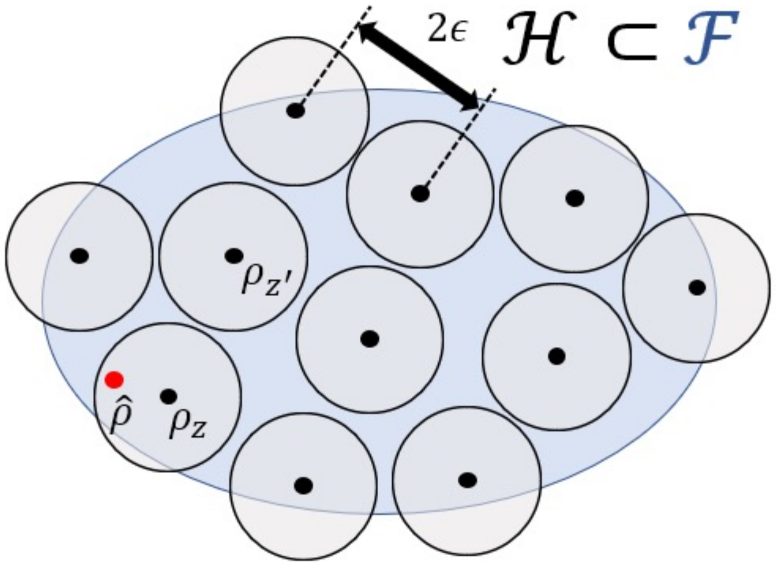
Quantum state discrimination of $\mathcal{H}$ $\leq$ Tomography

$$Z \sim \mathrm{Unif}(\{1, \dots, |\mathcal{H}|\})$$



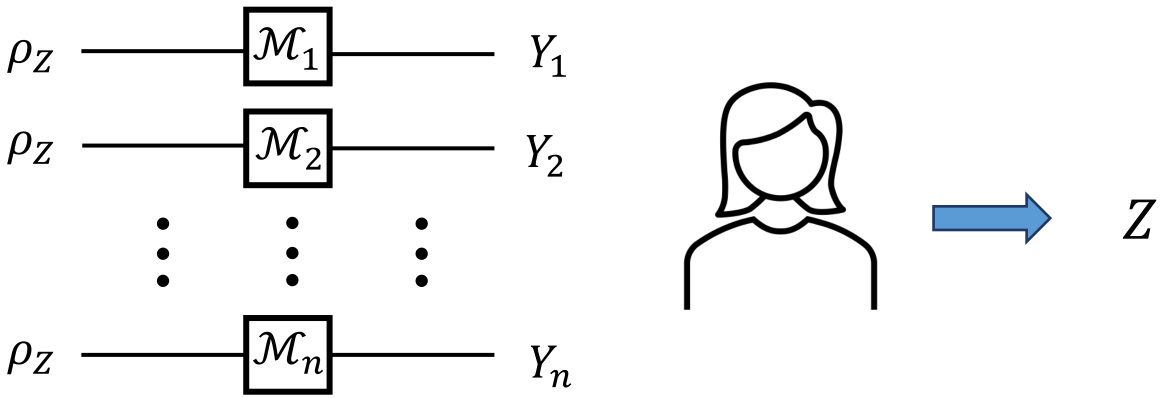
$$I(Z : Y_1, \dots, Y_n) \gtrsim \log(|\mathcal{H}|)$$ *(Fano's inequality)*

Recipe for a lower bound



Quantum state discrimination of $\mathcal{H}$ $\leq$ Tomography

$$Z \sim \mathrm{Unif}(\{1, \ldots, |\mathcal{H}|\})$$

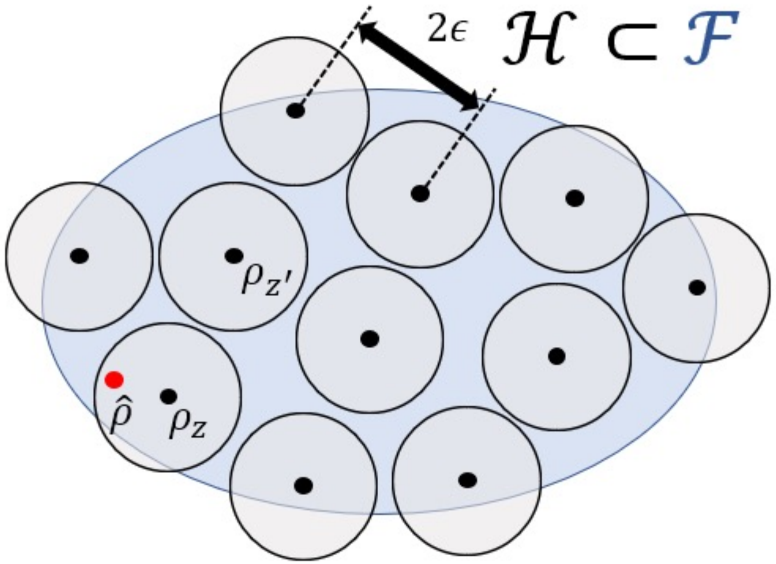


$$I(Z\!:Y_1, \ldots, Y_n) \gtrsim \log(|\mathcal{H}|)$$ *(Fano's inequality)*

Choose $\mathcal{F}$ and $\mathcal{H} \subset \mathcal{F}$ so that

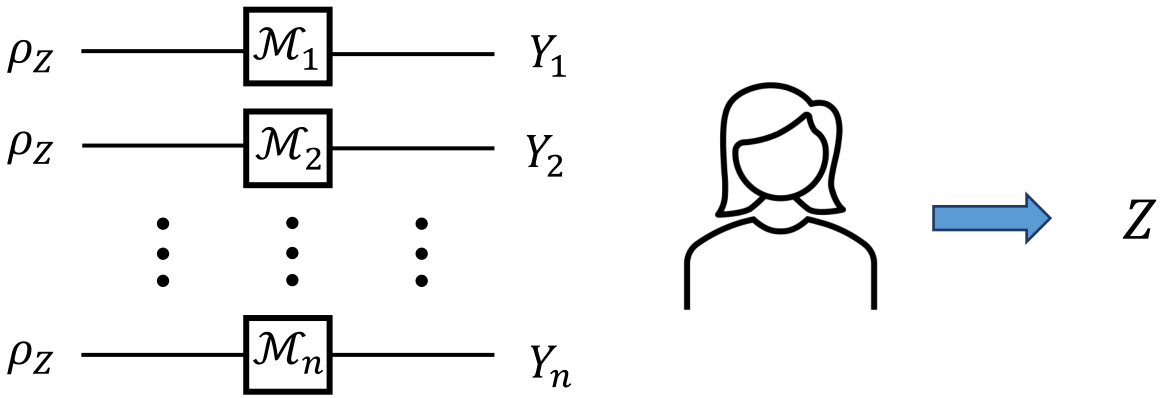
$$n\delta \geq I(Z\!:Y_1, \ldots, Y_n) \geq \Omega(d^2)$$

Recipe for a lower bound



Quantum state discrimination of $\mathcal{H}$ $\leq$ Tomography

$Z \sim \mathrm{Unif}(\{1, \dots, |\mathcal{H}|\})$



$I(Z\!:Y_1, \dots, Y_n) \gtrsim \log(|\mathcal{H}|)$ *(Fano's inequality)*

Choose $\mathcal{F}$ and $\mathcal{H} \subset \mathcal{F}$ so that

$$\boxed{n\delta \geq I(Z\!:Y_1, \dots, Y_n) \geq \Omega(d^2)}$$

Large packing

Large packing

$$\rho_U \coloneqq \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d} \qquad \mathcal{F} \coloneqq \{\rho_U : U \in \mathbb{U}(d)\}$$

Large packing

$$\rho_U \coloneqq \frac{2\epsilon}{d} U\Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d} \qquad \mathcal{F} \coloneqq \{\rho_U : U \in \mathbb{U}(d)\}$$

Lemma [Haah+17 via Hayden, Leung, Winter' 04]: Let $\epsilon \in (0, 1/2)$, $U \in \mathbb{U}(d)$ be a Haar-random unitary operator, and $\zeta \in \mathcal{F}$ be an arbitrary state in the family. It holds that

$$\mathbb{P}(\|\rho_U - \zeta\|_1 \le \epsilon) \le e^{-cd^2}$$

for some universal constant c.

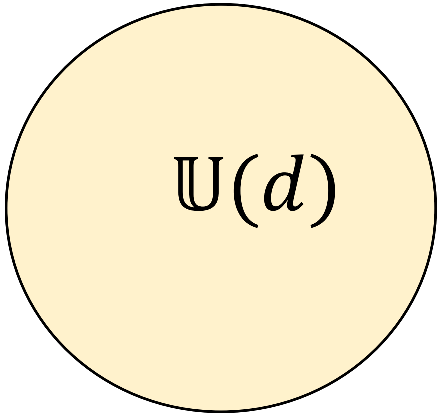
Large packing

$$\rho_U := \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d} \qquad \mathcal{F} := \{\rho_U : U \in \mathbb{U}(d)\}$$

Lemma [Haah+17 via Hayden, Leung, Winter' 04]: Let $\epsilon \in (0, 1/2)$, $U \in \mathbb{U}(d)$ be a Haar-random unitary operator, and $\zeta \in \mathcal{F}$ be an arbitrary state in the family. It holds that

$$\mathbb{P}(\|\rho_U - \zeta\|_1 \leq \epsilon) \leq e^{-cd^2}$$

for some universal constant c.



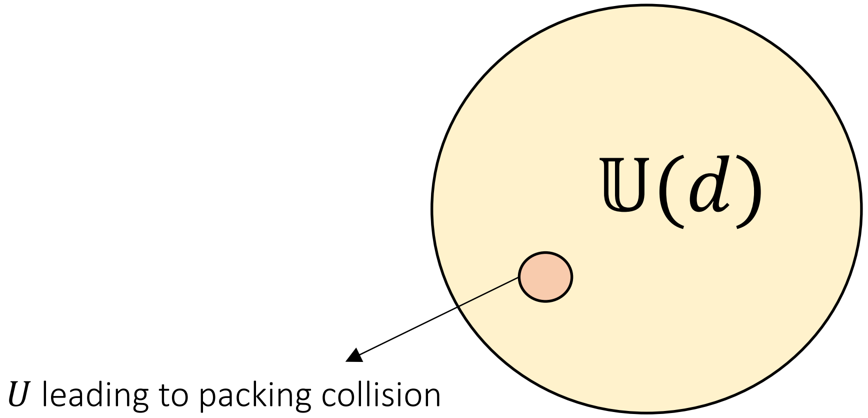
Large packing

$$\rho_U := \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d} \qquad \mathcal{F} := \{\rho_U : U \in \mathbb{U}(d)\}$$

Lemma [Haah+17 via Hayden, Leung, Winter' 04]: Let $\epsilon \in (0, 1/2)$, $U \in \mathbb{U}(d)$ be a Haar-random unitary operator, and $\zeta \in \mathcal{F}$ be an arbitrary state in the family. It holds that

$$\mathbb{P}(\|\rho_U - \zeta\|_1 \leq \epsilon) \leq e^{-cd^2}$$

for some universal constant c.



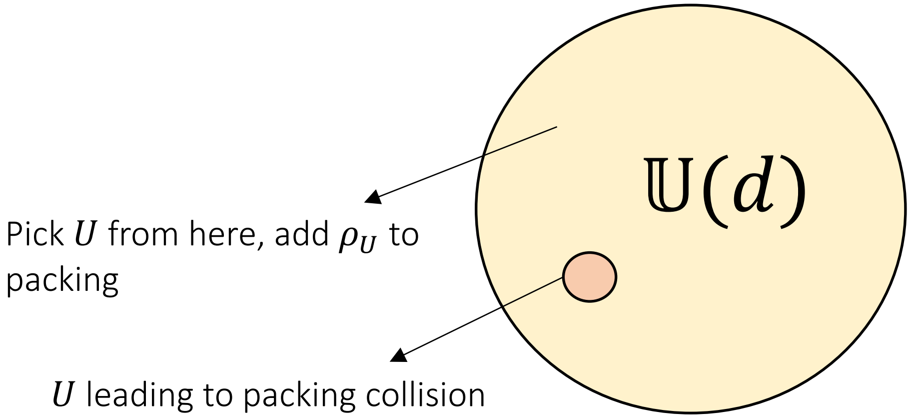
Large packing

$$\rho_U := \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d} \qquad \mathcal{F} := \{\rho_U : U \in \mathbb{U}(d)\}$$

Lemma [Haah+17 via Hayden, Leung, Winter' 04]: Let $\epsilon \in (0, 1/2)$, $U \in \mathbb{U}(d)$ be a Haar-random unitary operator, and $\zeta \in \mathcal{F}$ be an arbitrary state in the family. It holds that

$$\mathbb{P}(\|\rho_U - \zeta\|_1 \leq \epsilon) \leq e^{-cd^2}$$

for some universal constant c.



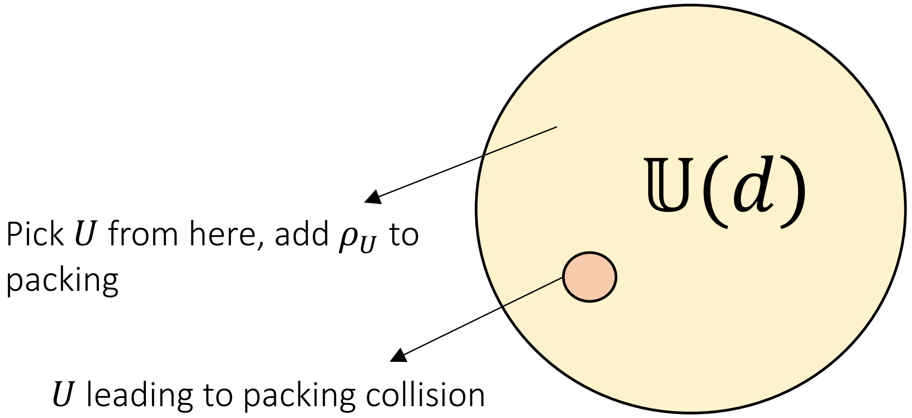
Large packing

$$\rho_U \coloneqq \frac{2\epsilon}{d} U\Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d} \qquad \mathcal{F} \coloneqq \{\rho_U : U \in \mathbb{U}(d)\}$$

Lemma [Haah+17 via Hayden, Leung, Winter' 04]: Let $\epsilon \in (0, 1/2)$, $U \in \mathbb{U}(d)$ be a Haar-random unitary operator, and $\zeta \in \mathcal{F}$ be an arbitrary state in the family. It holds that

$$\mathbb{P}(\|\rho_U - \zeta\|_1 \leq \epsilon) \leq e^{-cd^2}$$

for some universal constant c.



There is a large packing $\mathcal{H}$, $|\mathcal{H}| \sim e^{\Omega(d^2)}$

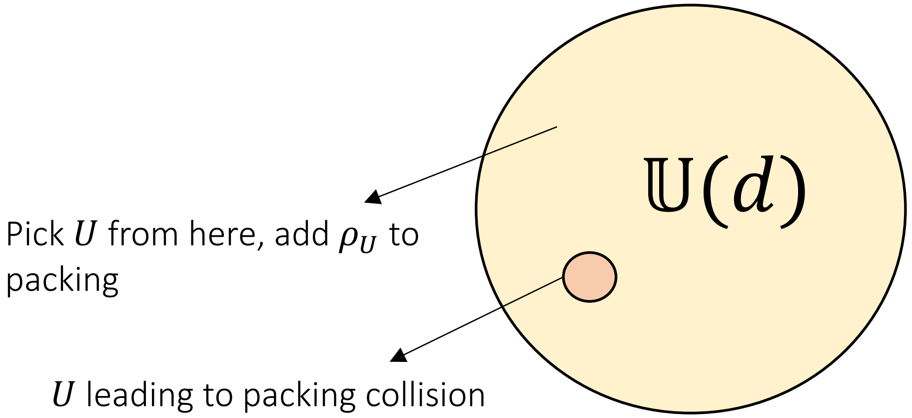
Large packing

$$\rho_U := \frac{2\epsilon}{d} U\Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d} \qquad \mathcal{F} := \{\rho_U : U \in \mathbb{U}(d)\}$$

Lemma [Haah+17 via Hayden, Leung, Winter' 04]: Let $\epsilon \in (0, 1/2)$, $U \in \mathbb{U}(d)$ be a Haar-random unitary operator, and $\zeta \in \mathcal{F}$ be an arbitrary state in the family. It holds that

$$\mathbb{P}(\|\rho_U - \zeta\|_1 \leq \epsilon) \leq e^{-cd^2}$$

for some universal constant c.



There is a large packing $\mathcal{H}$, $|\mathcal{H}| \sim e^{\Omega(d^2)}$

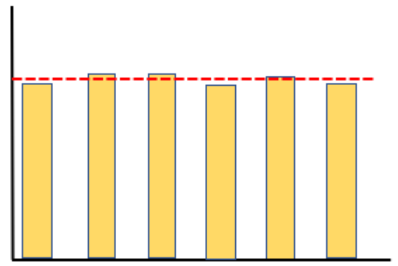
$\Longrightarrow I(Z:Y_1, \ldots, Y_n) \geq \Omega(d^2)$

Bounding the information in a measurement

$$\rho_U \coloneqq \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d}$$

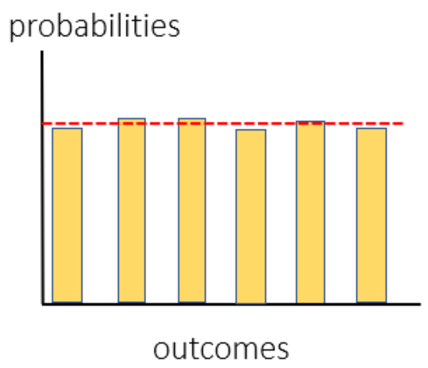
Bounding the information in a measurement

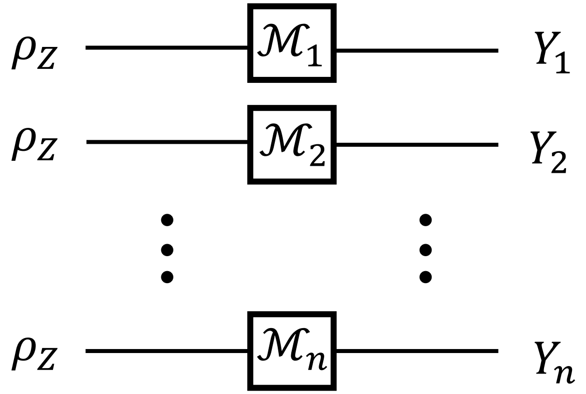
$$\rho_U \coloneqq \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d} \longrightarrow$$



Bounding the information in a measurement

$$\rho_U \coloneqq \frac{2\epsilon}{d} U\Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d} \longrightarrow$$

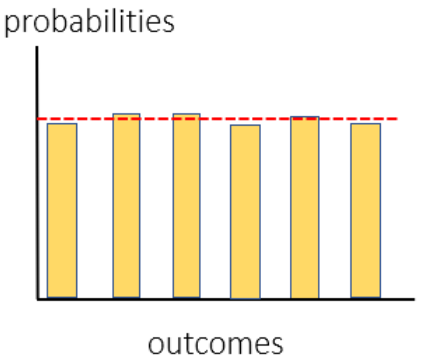


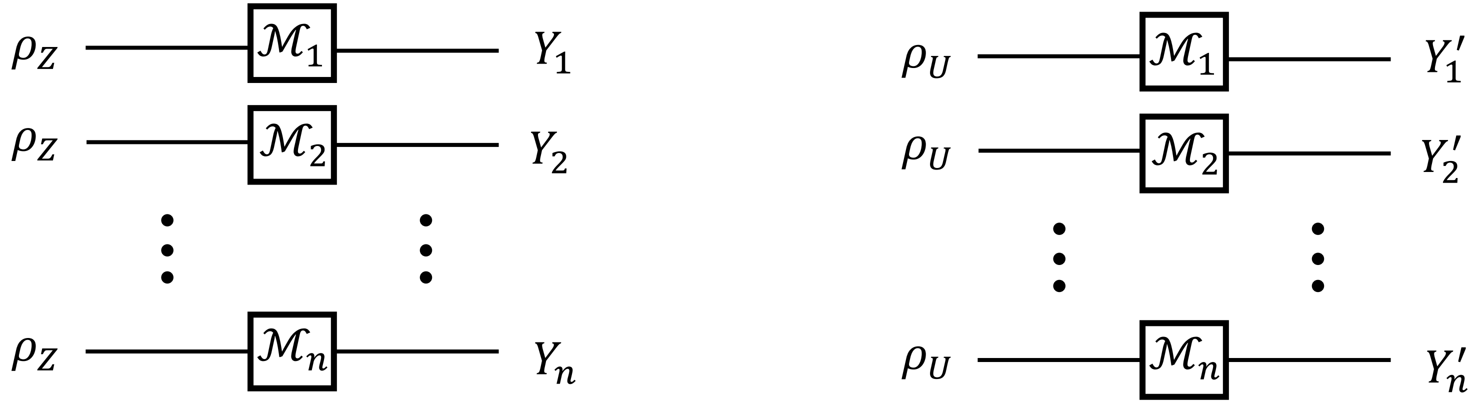


$$I(Z : Y_1, \ldots, Y_n)$$

Bounding the information in a measurement

$$\rho_U := \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d}$$

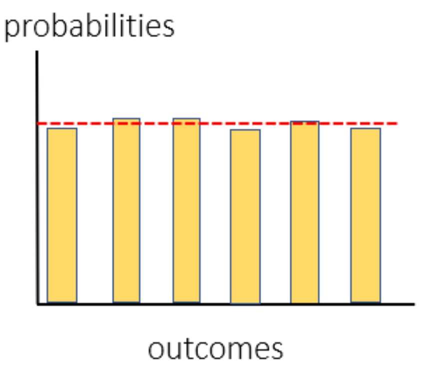


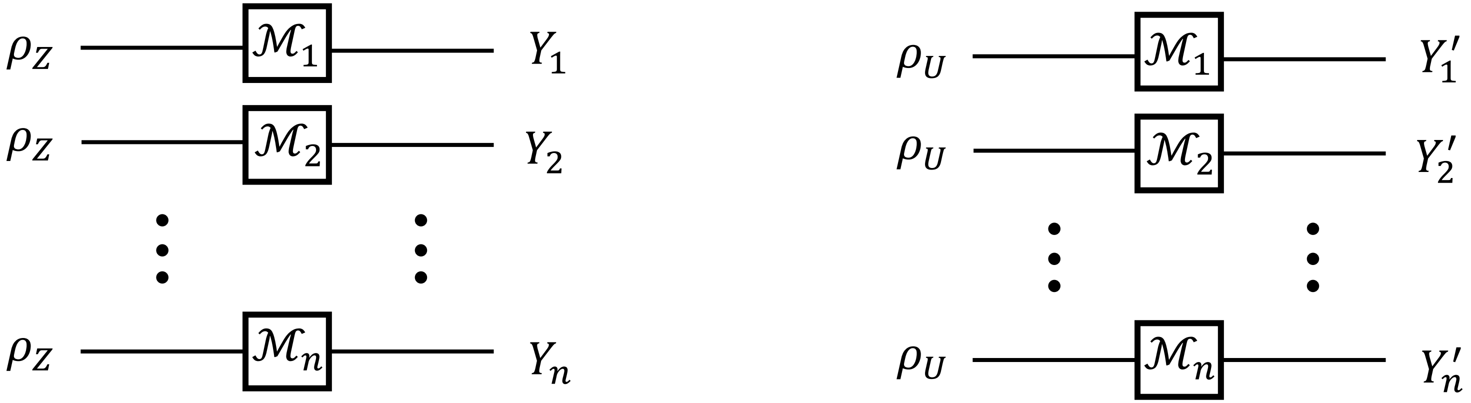


$$I(Z : Y_1, \ldots, Y_n) \quad \leq \quad I(U : Y_1', \ldots, Y_n')$$

Bounding the information in a measurement

$$\rho_U := \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d}$$



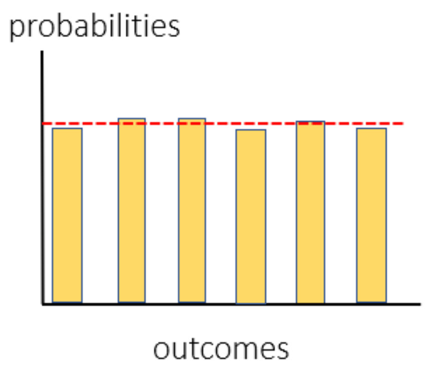


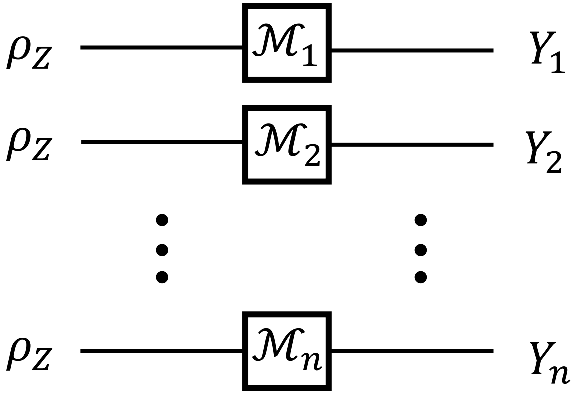
$$I(Z:Y_1,\dots,Y_n) \quad \leq \quad I(U:Y_1',\dots,Y_n')$$

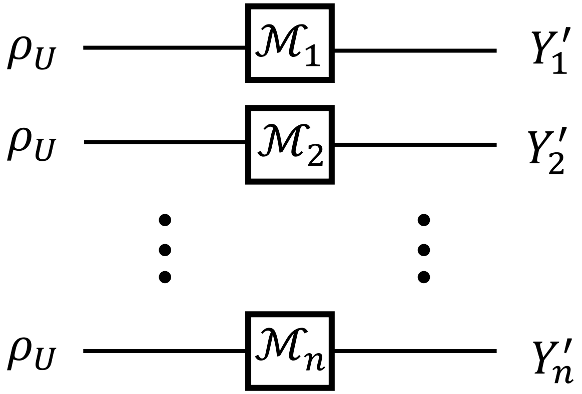
Haar-random

Bounding the information in a measurement

$$\rho_U \coloneqq \frac{2\epsilon}{d} U\Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d} \longrightarrow$$



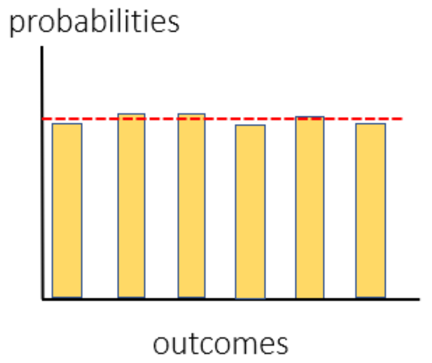


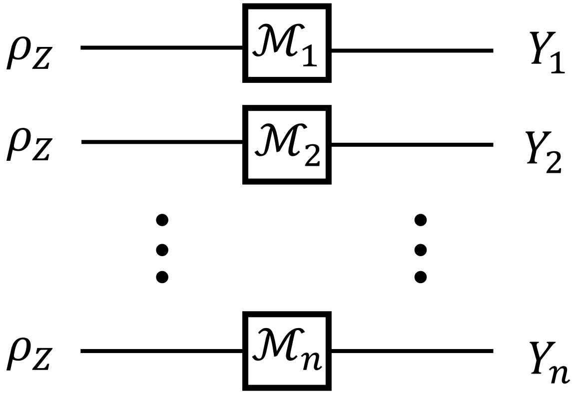


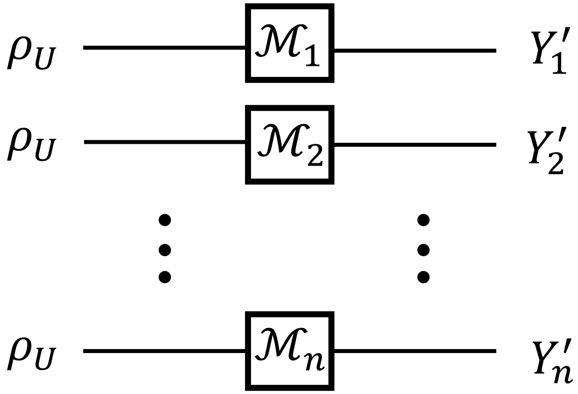
$$I(Z:Y_1,\dots,Y_n) \leq I(\underset{\substack{\downarrow \\ \text{Haar-random}}}{U}:Y'_1,\dots,Y'_n) \leq \sum_{i=1}^{n} I(U:Y'_i)$$

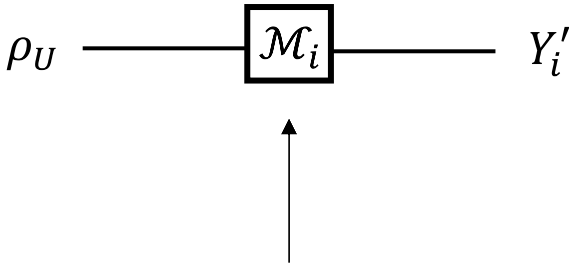
Bounding the information in a measurement

$$\rho_U \coloneqq \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d} \longrightarrow$$







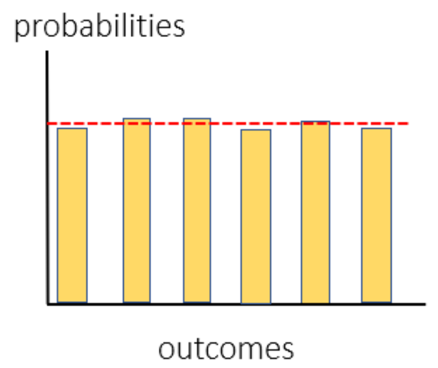


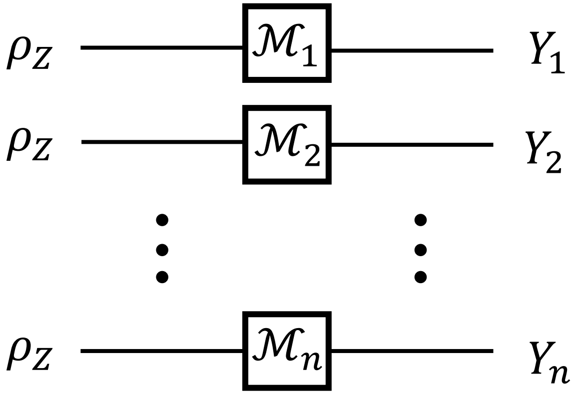
$$I(Z:Y_1,\dots,Y_n) \quad \leq \quad I(U:Y_1',\dots,Y_n') \quad \leq \quad \sum_{i=1}^{n} I(U:Y_i')$$

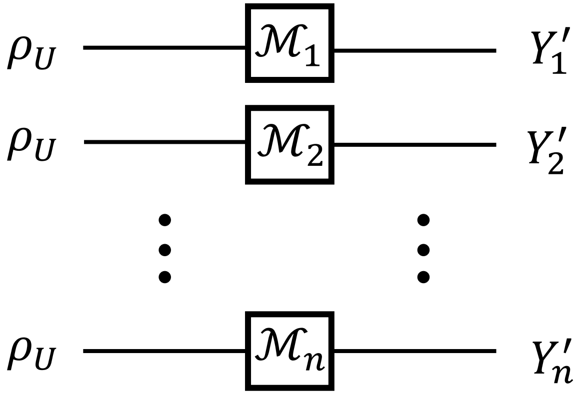
Haar-random

Bounding the information in a measurement

$$\rho_U := \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d} \longrightarrow$$







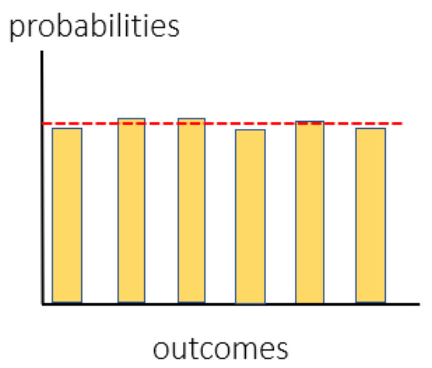
Compute using Haar integration

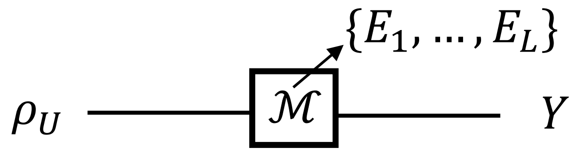
$$I(Z:Y_1,\dots,Y_n) \leq I(U:Y_1',\dots,Y_n') \leq \sum_{i=1}^{n} I(U:Y_i')$$

Haar-random

Bounding the information in a measurement

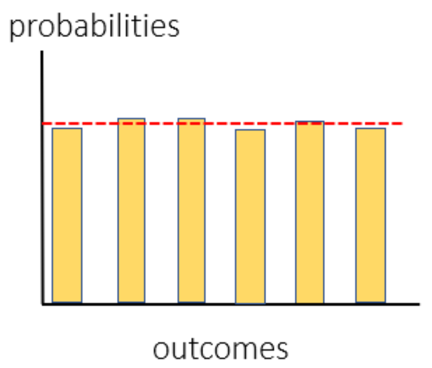
$$\rho_U \coloneqq \frac{2\epsilon}{d} U\Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d} \longrightarrow$$

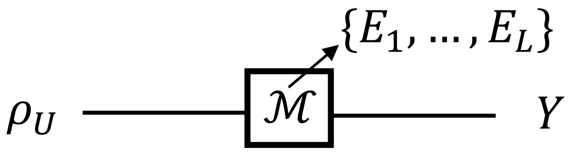




Bounding the information in a measurement

$$\rho_U := \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d} \longrightarrow$$



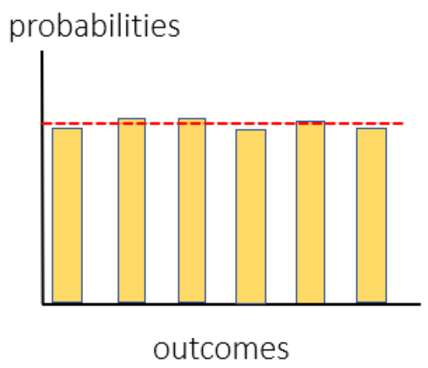


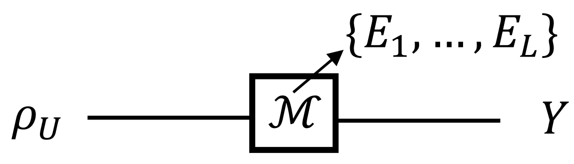
$$p_V(y) := \mathbb{P}(Y = y | U = V) = \mathrm{Tr}\left(E_y \rho_V\right)$$

$$w(y) := \mathbb{E}_{V \sim Haar} \mathbb{P}(Y = y | U = V) = \mathrm{Tr}(E_y)/d$$

Bounding the information in a measurement

$$\rho_U := \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d} \longrightarrow$$





$$p_V(y) := \mathbb{P}(Y = y | U = V) = \mathrm{Tr}\big(E_y \rho_V\big)$$

$$w(y) := \mathbb{E}_{V \sim Haar} \mathbb{P}(Y = y | U = V) = \mathrm{Tr}(E_y)/d$$

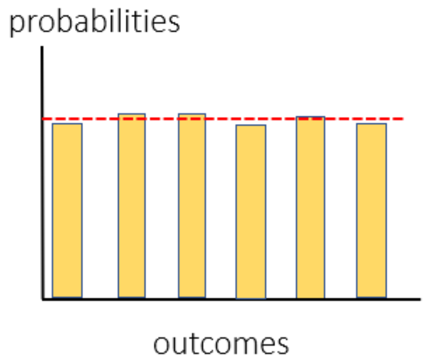
Proposition: It holds that

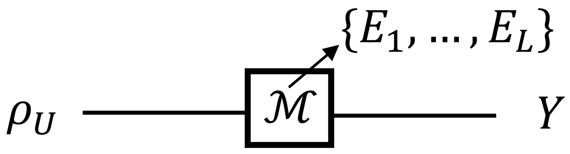
$$I(U:Y) \leq \mathbb{E}_{V \sim Haar}\, \chi^2(p_V \,\|\, w)$$

$$\chi^2(p \,\|\, q) := \textstyle\sum_x q(x) \left(\frac{p(x)}{q(x)} - 1\right)^2.$$

Bounding the information in a measurement

$$\rho_U := \frac{2\epsilon}{d} U\Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d} \longrightarrow$$





$$p_V(y) := \mathbb{P}(Y = y | U = V) = \mathrm{Tr}(E_y \rho_V)$$

$$w(y) := \mathbb{E}_{V\sim Haar}\mathbb{P}(Y = y | U = V) = \mathrm{Tr}(E_y)/d$$

Proposition: It holds that

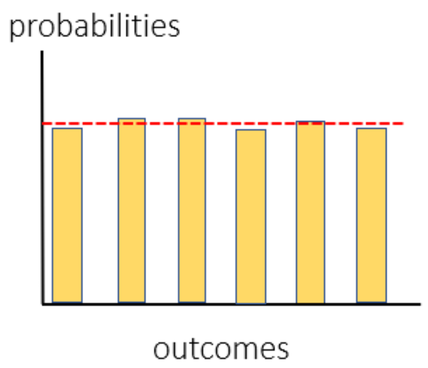
$$I(U{:}Y) \leq \mathbb{E}_{V\sim Haar}\, \chi^2(p_V \parallel w)$$

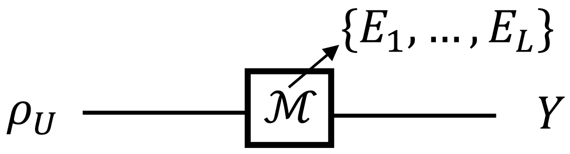
$$\chi^2(p \parallel q) := \sum_x q(x)\left(\frac{p(x)}{q(x)} - 1\right)^2.$$

$$\mathbb{E}_{V\sim Haar}\, \chi^2(p_V \parallel w) \approx \mathbb{E}_{y\sim w}\left[\frac{\epsilon^2 \mathrm{Tr}(E_y^2)}{d^3 w(y)^2}\right]$$

Bounding the information in a measurement

$$\rho_U := \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d}$$





$$p_V(y) := \mathbb{P}(Y = y | U = V) = \mathrm{Tr}\big(E_y \rho_V\big)$$

$$w(y) := \mathbb{E}_{V\sim Haar} \mathbb{P}(Y = y | U = V) = \mathrm{Tr}(E_y)/d$$

Proposition: It holds that

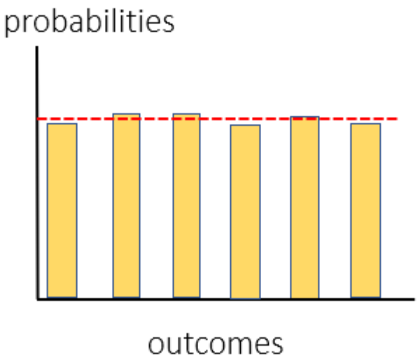
$$I(U\!:Y) \leq \mathbb{E}_{V\sim Haar}\, \chi^2(p_V \parallel w)$$

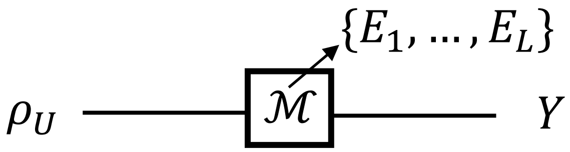
$$\chi^2(p \parallel q) := \textstyle\sum_x q(x) \left(\frac{p(x)}{q(x)} - 1\right)^2.$$

$$\mathbb{E}_{V\sim Haar}\, \chi^2(p_V \parallel w) \approx \mathbb{E}_{y\sim w}\left[\frac{\epsilon^2 \mathrm{Tr}\big(E_y^2\big)}{d^3 w(y)^2}\right] \leq \min\left\{\frac{\epsilon^2}{d}, \sum_y \frac{\epsilon^2}{d^2}\right\}$$

Bounding the information in a measurement

$$\rho_U := \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d} \longrightarrow$$





$$p_V(y) := \mathbb{P}(Y = y | U = V) = \mathrm{Tr}\big(E_y \rho_V\big)$$

$$w(y) := \mathbb{E}_{V\sim Haar} \mathbb{P}(Y = y | U = V) = \mathrm{Tr}(E_y)/d$$

Proposition: It holds that

$$I(U:Y) \leq \mathbb{E}_{V\sim Haar}\, \chi^2(p_V \parallel w)$$

$$\chi^2(p \parallel q) := \textstyle\sum_x q(x)\left(\frac{p(x)}{q(x)} - 1\right)^2.$$

$$\mathbb{E}_{V\sim Haar}\, \chi^2(p_V \parallel w) \approx \mathbb{E}_{y\sim w}\left[\frac{\epsilon^2 \mathrm{Tr}\big(E_y^2\big)}{d^3 w(y)^2}\right] \leq \min\left\{\frac{\epsilon^2}{d}, \sum_y \frac{\epsilon^2}{d^2}\right\}$$

$Tr\big(E_y^2\big) \leq Tr\big(E_y\big)^2$

$Tr\big(E_y^2\big) \leq Tr\big(E_y\big)$

Summary of nonadaptive lower bounds

$$\Omega(d^2) \le I(Z{:}Y) \le I(U{:}Y') \le \sum_{i=1}^{n} I(U{:}Y_i') \le \begin{cases} \frac{n\epsilon^2}{d}, & \text{Arbitrary POVMs} \\ \frac{n\epsilon^2}{d^2}, & \text{Measurements with O(1) outcomes} \end{cases}$$

Summary of nonadaptive lower bounds

χ^2-divergence bound

$$\Omega(d^2) \leq I(Z:Y) \leq I(U:Y') \leq \sum_{i=1}^{n} I(U:Y_i') \leq \begin{cases} \frac{n\epsilon^2}{d}, & \text{Arbitrary POVMs} \\ \frac{n\epsilon^2}{d^2}, & \text{Measurements with O(1) outcomes} \end{cases}$$

Fano

Conditional independence of Y_i'

Summary of nonadaptive lower bounds

χ^2-divergence bound

$$\Omega(d^2) \leq I(Z{:}Y) \leq I(U{:}Y') \leq \sum_{i=1}^{n} I(U{:}Y_i') \leq \begin{cases} \dfrac{n\epsilon^2}{d}, & \text{Arbitrary POVMs} \\ \dfrac{n\epsilon^2}{d^2}, & \text{Measurements with O(1) outcomes} \end{cases}$$

Fano

$\boxed{\text{Conditional independence of } Y_i'}$

Information from adaptive measurements

$$I(Z:Y_1,\dots,Y_n) \quad \leq \quad \sum_{i=1}^{n} I(Z:Y_i)$$

Information from adaptive measurements

$$I(Z:Y_1,\ldots,Y_n) \quad \leq \quad \sum_{i=1}^{n} I(Z:Y_i) \quad ✗$$

Information from adaptive measurements

$$I(Z{:}Y_1,\ldots,Y_n) \quad \leq \quad \sum_{i=1}^{n} I(Z{:}Y_i) \quad ✗$$

Use **chain rule** for mutual information instead:

$$I(Z{:}Y_1,\ldots,Y_n) = I(Z{:}Y_1) + I(Z{:}Y_2|Y_1) + \cdots + I(Z{:}Y_n|Y_{n-1},\ldots,Y_1) \quad ✓$$

Information from adaptive measurements

$$I(Z:Y_1, \ldots, Y_n) \quad \leq \quad \sum_{i=1}^{n} I(Z:Y_i) \quad ✗$$

Use **chain rule** for mutual information instead:

$$I(Z:Y_1, \ldots, Y_n) = I(Z:Y_1) + I(Z:Y_2|Y_1) + \cdots + I(Z:Y_n|Y_{n-1}, \ldots, Y_1) \quad ✓$$

$$\leq \mathbb{E}_Z\, \chi^2\left(p_{Y_1|Z} \| p_{Y_1}\right) + \mathbb{E}_{Y_1} \mathbb{E}_{Z|Y_1} \chi^2\left(p_{Y_2|Y_1,Z} \| p_{Y_2|Y_1}\right) + \cdots$$

Information from adaptive measurements

$$I(Z : Y_1, \dots, Y_n) \quad \leq \quad \sum_{i=1}^{n} I(Z : Y_i)$$

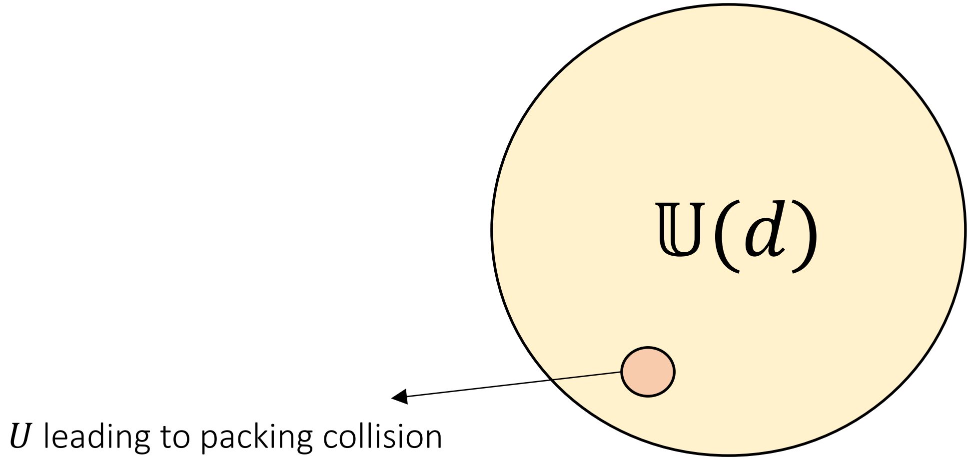
Use **chain rule** for mutual information instead:

$$\begin{aligned} I(Z : Y_1, \dots, Y_n) &= I(Z : Y_1) + I(Z : Y_2 | Y_1) + \cdots + I(Z : Y_n | Y_{n-1}, \dots, Y_1) \\ &\leq \mathbb{E}_Z\, \chi^2\left(p_{Y_1|Z} \| p_{Y_1}\right) + \mathbb{E}_{Y_1} \mathbb{E}_{Z|Y_1} \chi^2\left(p_{Y_2|Y_1,Z} \| p_{Y_2|Y_1}\right) + \cdots \end{aligned}$$

Can we pick $\{\rho_z\}_z$ such that χ^2-divergence terms are small?

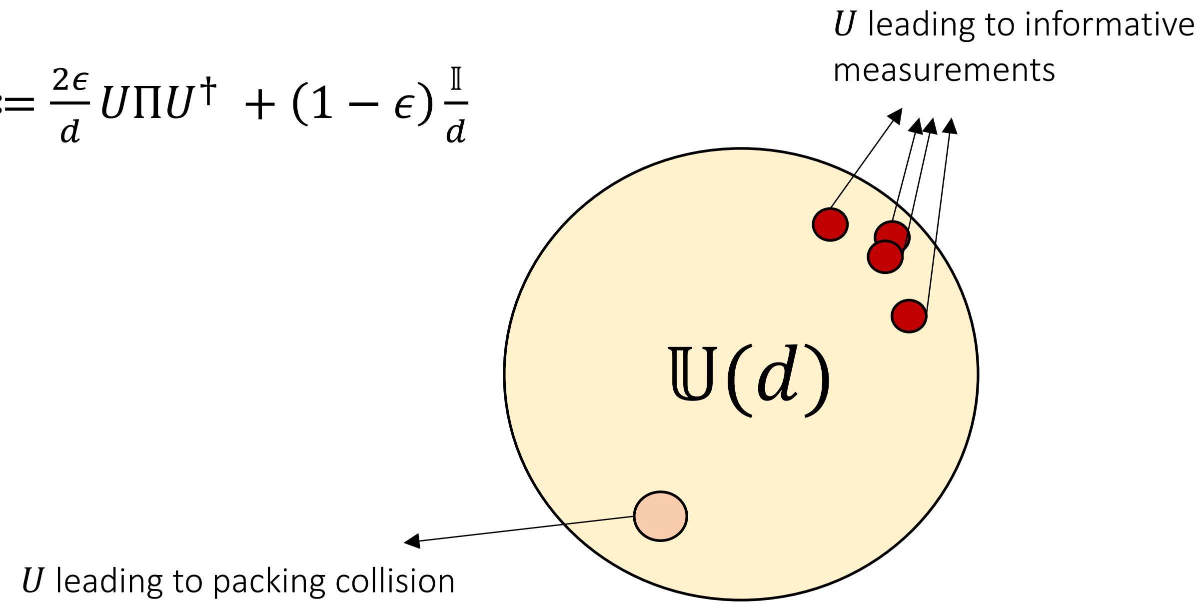
Constructing the hard case

$$\mathcal{F} \coloneqq \{\rho_U : U \in \mathbb{U}(d)\}, \quad \rho_U \coloneqq \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d}$$



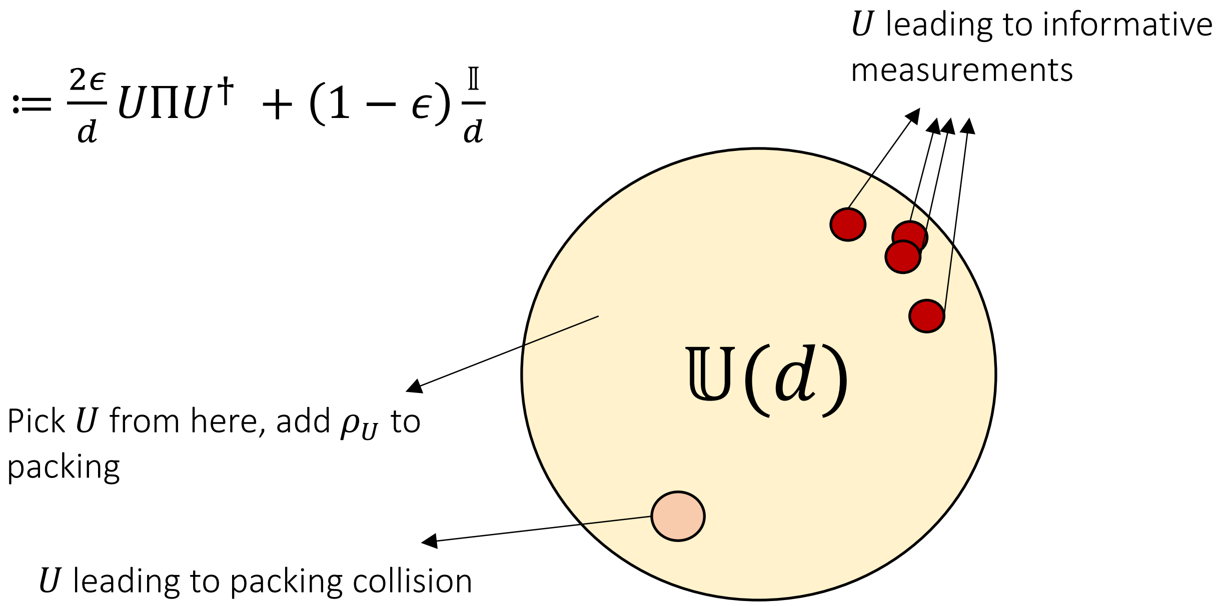
Constructing the hard case

$$\mathcal{F} \coloneqq \{\rho_U : U \in \mathbb{U}(d)\}, \quad \rho_U \coloneqq \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d}$$



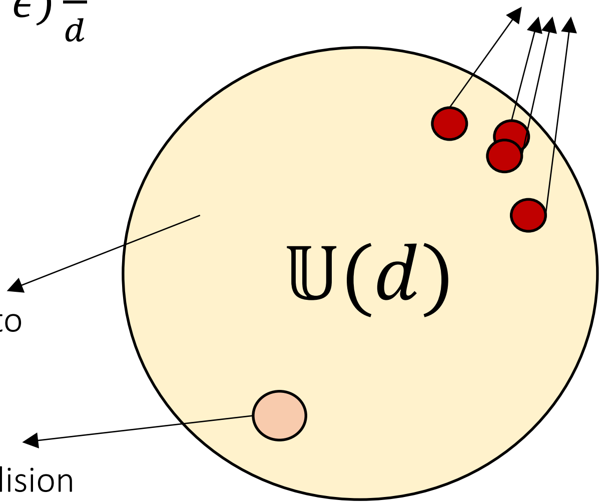
Constructing the hard case

$$\mathcal{F} \coloneqq \{\rho_U : U \in \mathbb{U}(d)\}, \quad \rho_U \coloneqq \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d}$$



Constructing the hard case

$$\mathcal{F} := \{\rho_U : U \in \mathbb{U}(d)\}, \quad \rho_U := \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d}$$

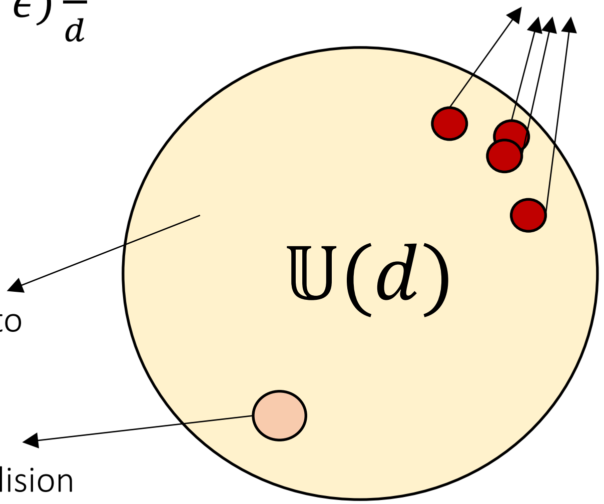


Lemma (χ^2-concentration): For a fixed measurement $\mathcal{M}$, let p_U be the distribution over outcomes from measuring ρ_U and $w := \mathbb{E}_{U\sim Haar}\, p_U$. It holds that

$$\mathbb{P}_{U\sim Haar}\left(\chi^2(p_U \,\|\, w) \geq O\left(\frac{\epsilon^2}{d}\right)\right) \leq e^{-\Omega(d)}.$$

Constructing the hard case

$$\mathcal{F} \coloneqq \{\rho_U : U \in \mathbb{U}(d)\}, \quad \rho_U \coloneqq \frac{2\epsilon}{d} U \Pi U^\dagger + (1-\epsilon)\frac{\mathbb{I}}{d}$$



Lemma (χ^2-concentration): For a fixed measurement $\mathcal{M}$, let p_U be the distribution over outcomes from measuring ρ_U and $w \coloneqq \mathbb{E}_{U \sim Haar}\, p_U$. It holds that

$$\mathbb{P}_{U\sim Haar}\left(\overbrace{\chi^2(p_U \,\|\, w) \geq O\left(\frac{\epsilon^2}{d}\right)}^{\text{“Informative measurement statistics”}} \right) \leq e^{-\Omega(d)}.$$

Lower bound for adaptive tomography with limited settings

$$I(Z\colon Y_1, \dots, Y_n) = I(Z\colon Y_1) + I(Z\colon Y_2|Y_1) + \cdots + I(Z\colon Y_n|Y_{n-1}, \dots, Y_1)$$

$$\leq n\left(\frac{\epsilon^2}{d} + \frac{\epsilon^2 \log(m)}{d^2}\right)$$

Theorem: Any procedure for quantum tomography using single-copy (possibly adaptive) measurements chosen from a fixed set of m possible measurements requires

$$n = \Omega\left(\frac{d^3}{\epsilon^2\left(1 + \frac{\log(m)}{d}\right)}\right)$$

copies of ρ.

Open problems

- Unconditional, non-trivial bounds for adaptive tomography?
- Rank-dependent bounds with finite measurement settings?
- Testing (e.g., quantum state certification) using single-copy measurements and finite measurement settings?
- Using these techniques, can we get "circuit lower bounds" for optimal, entangled quantum tomography?
  - Related conjecture: optimal, entangled tomography can be implemented using depth $\mathrm{poly}(n, d, \log 1/\epsilon)$ [Haah+17].