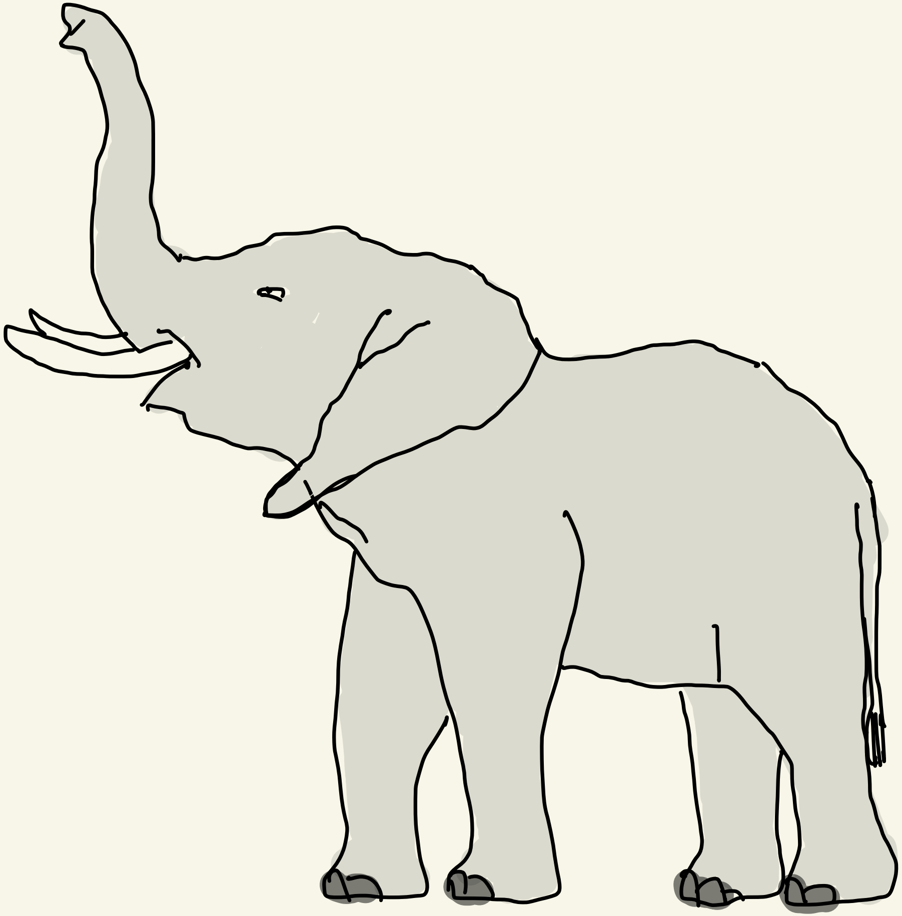
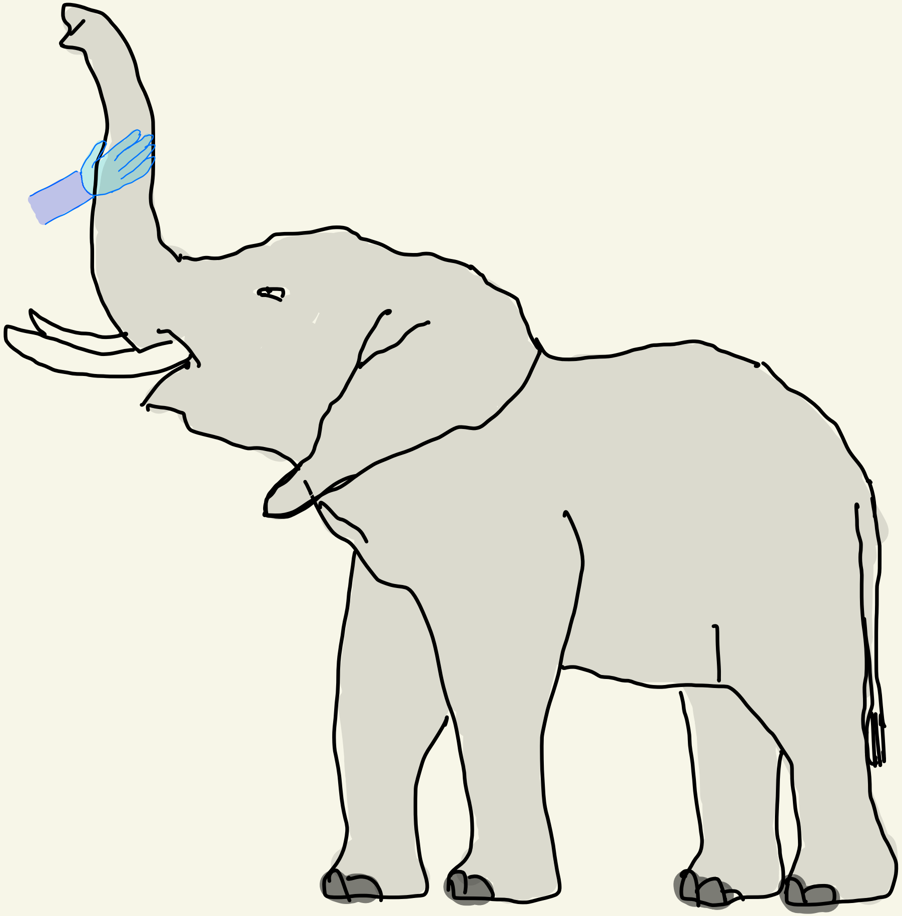
Lower bounds on the complexity of quantum proofs

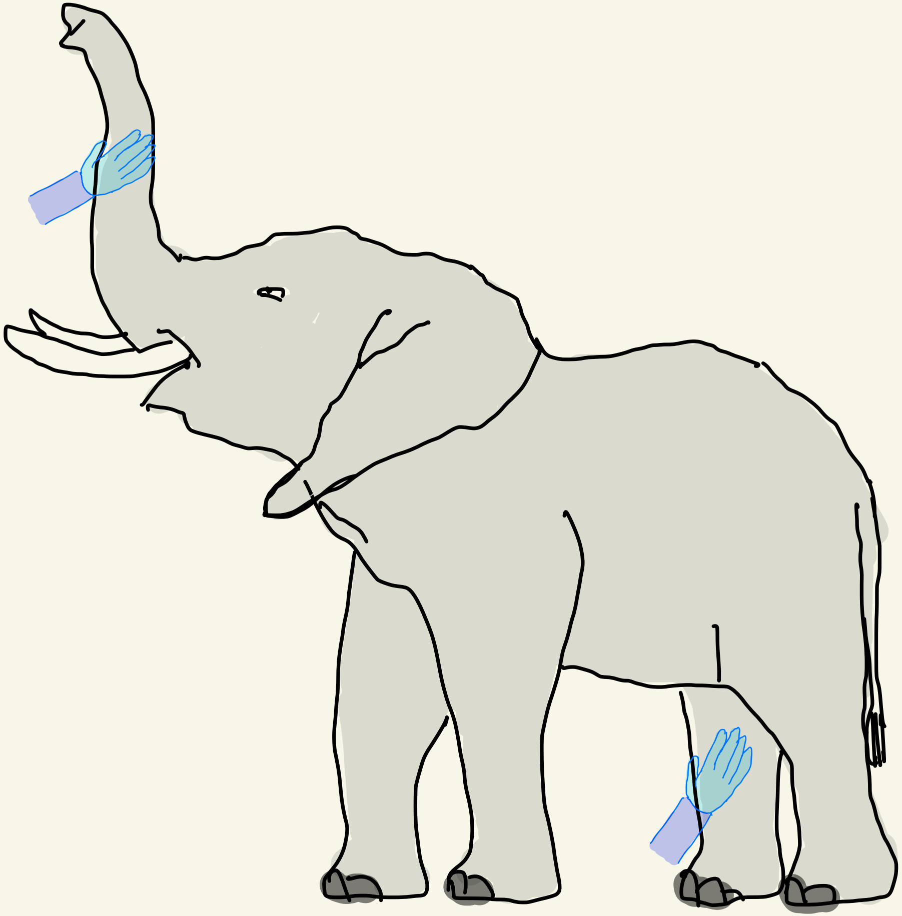
Chinmay Nirkhe

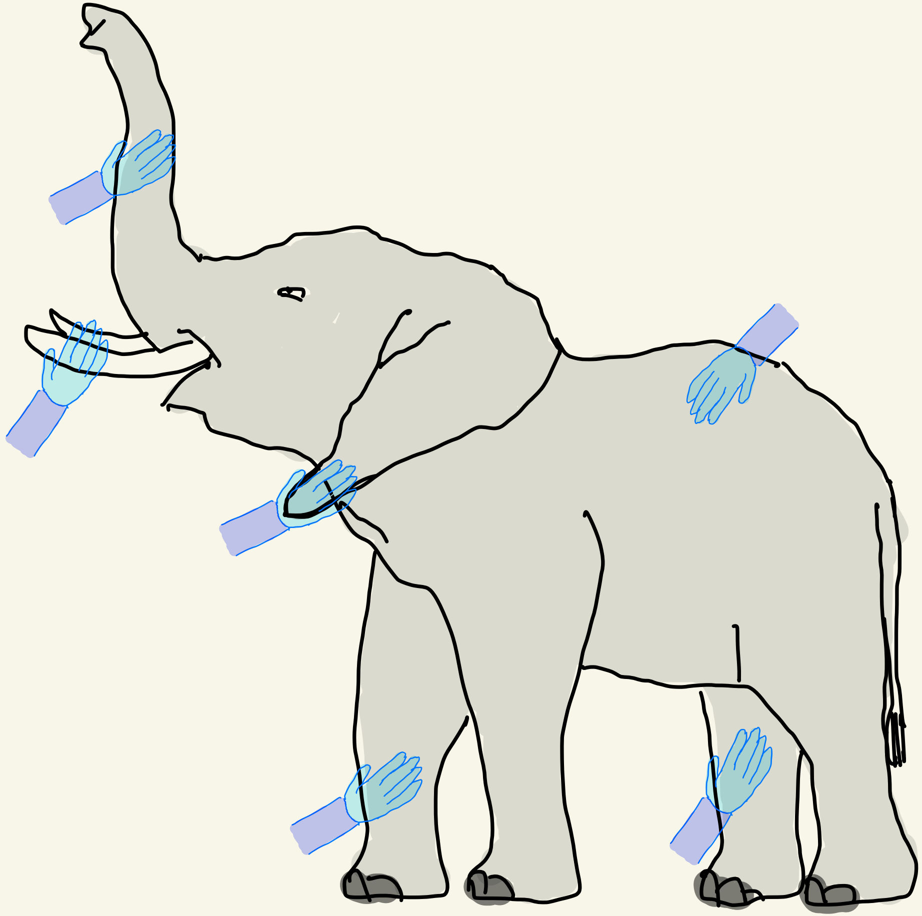
UC Berkeley

August 29th, 2022

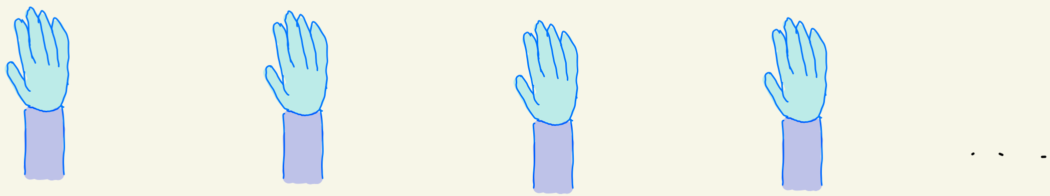


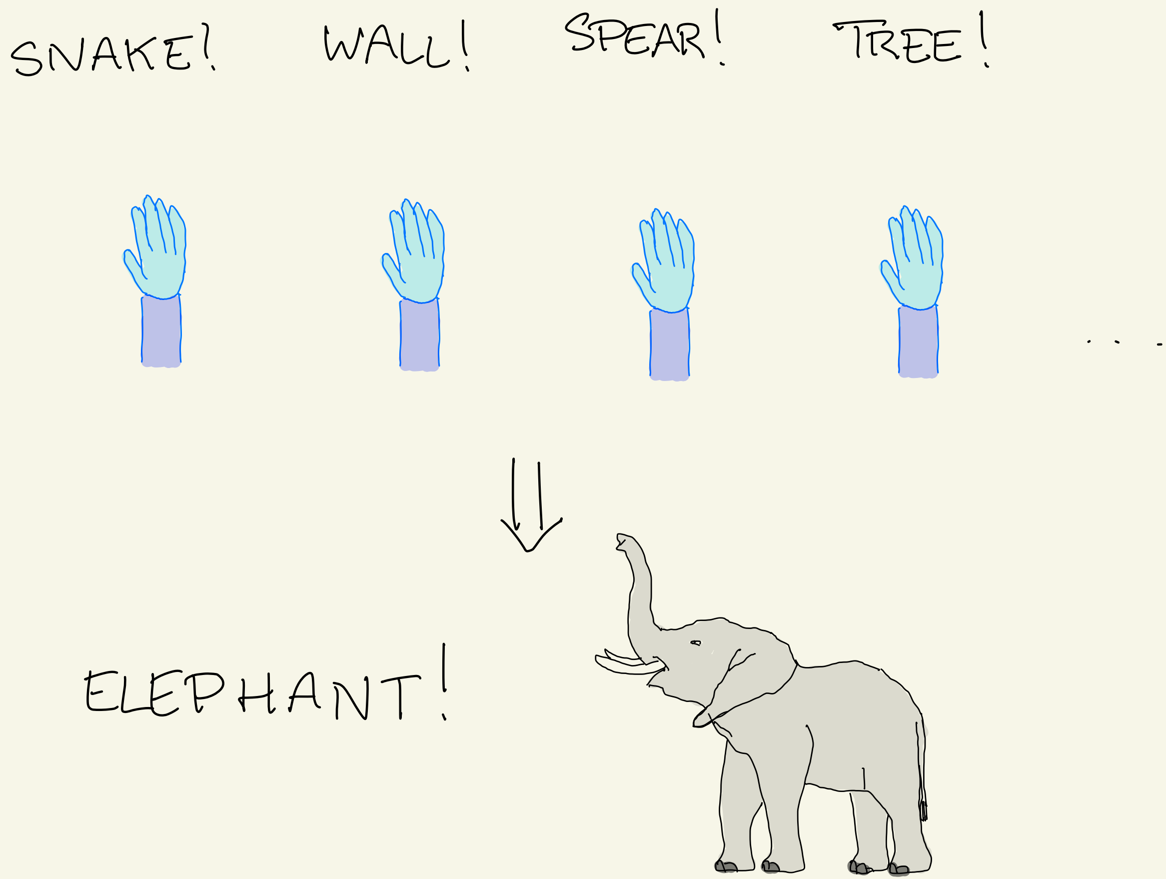


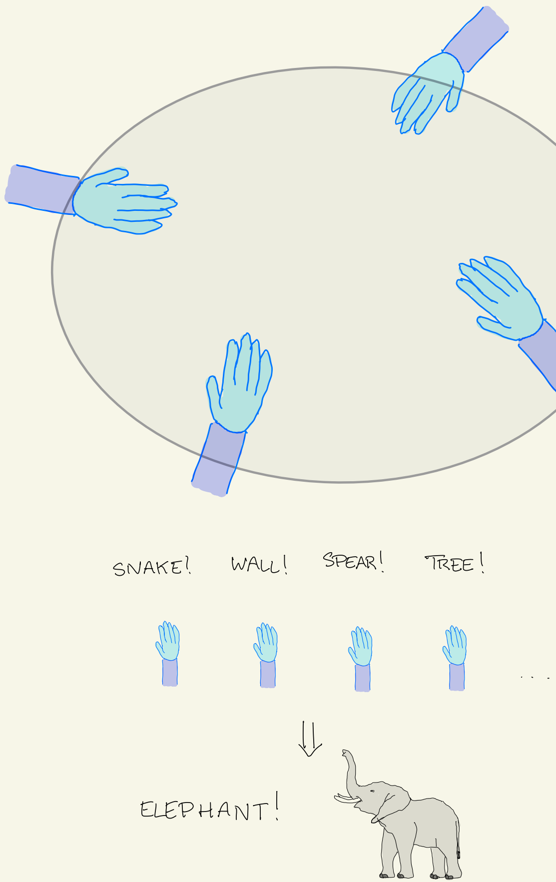


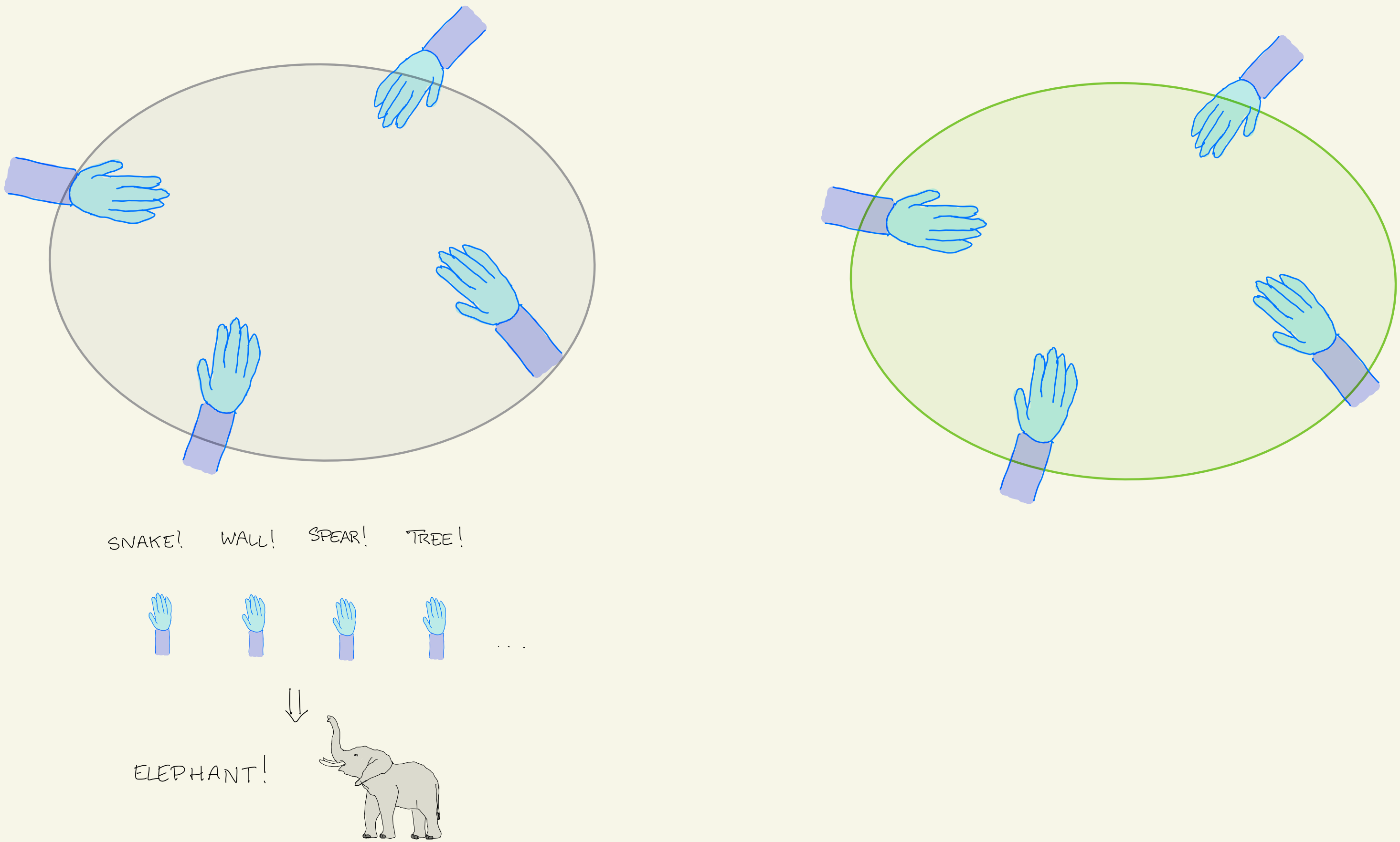


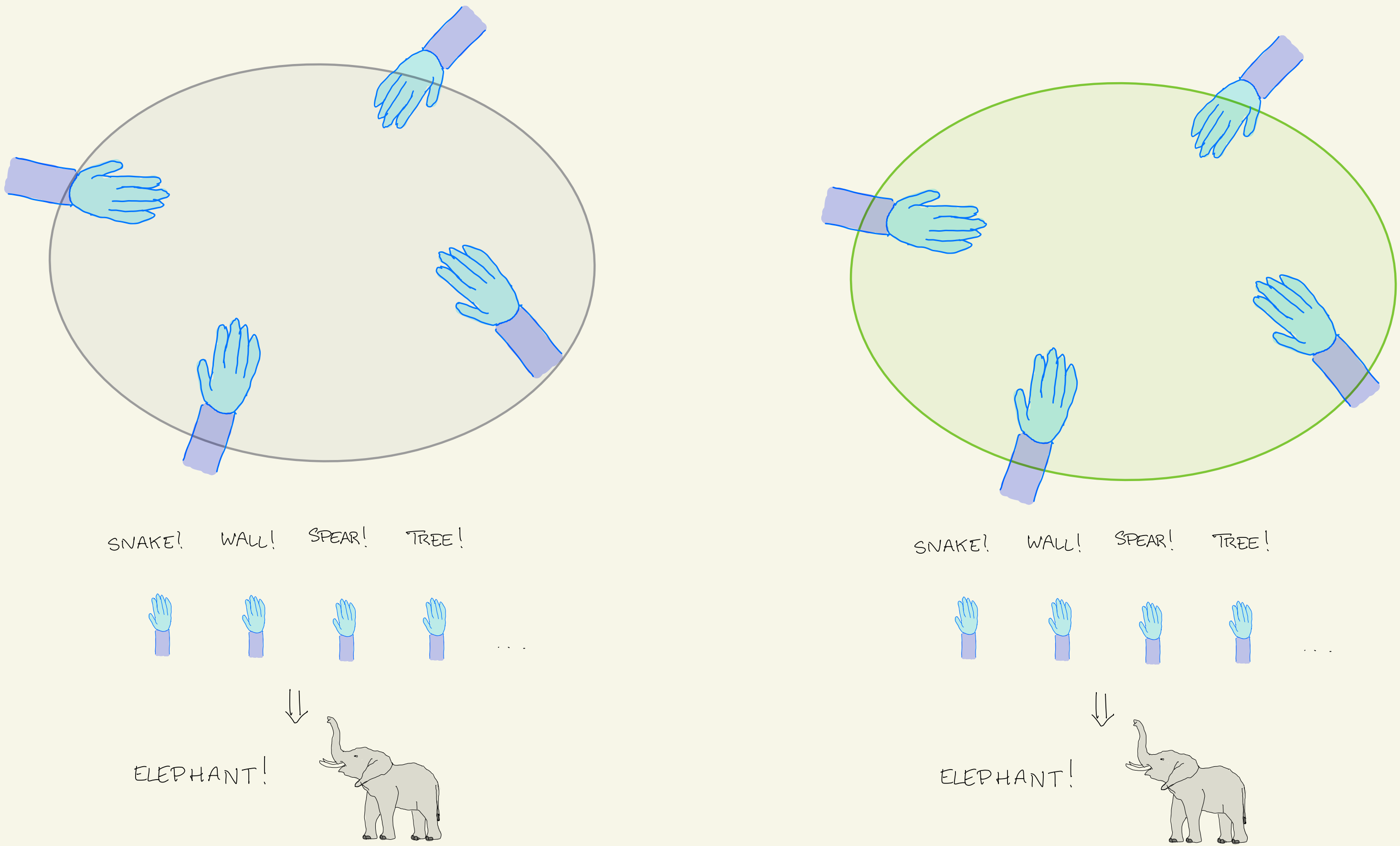
SNAKE! WALL! SPEAR! TREE!

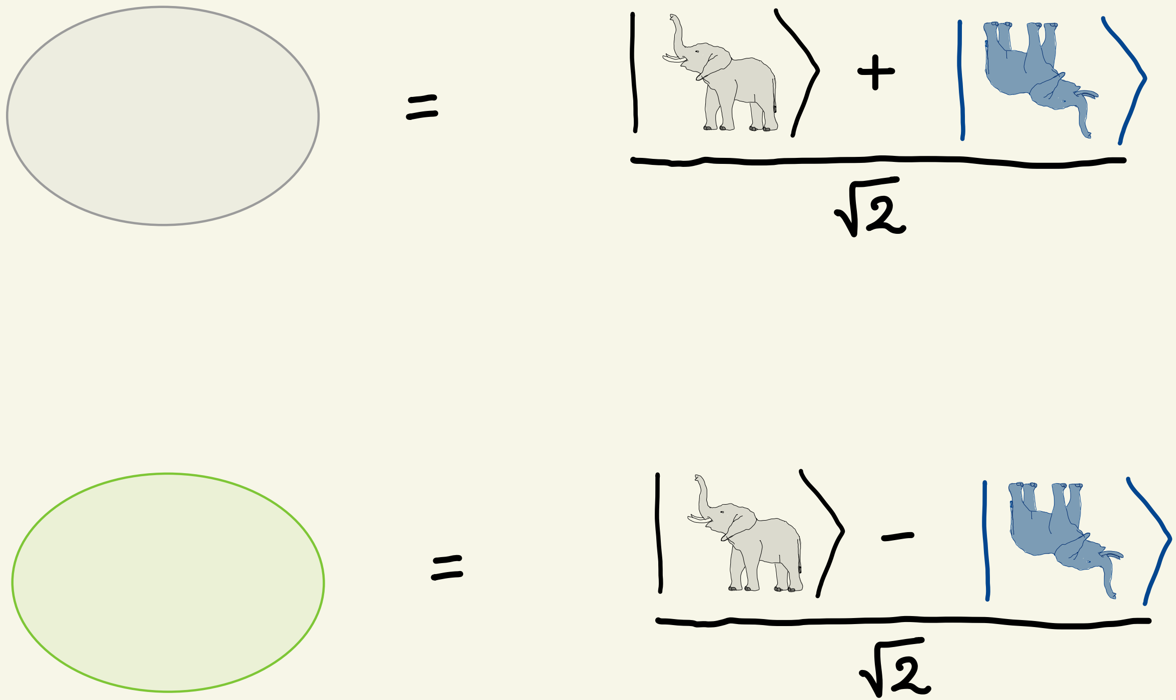


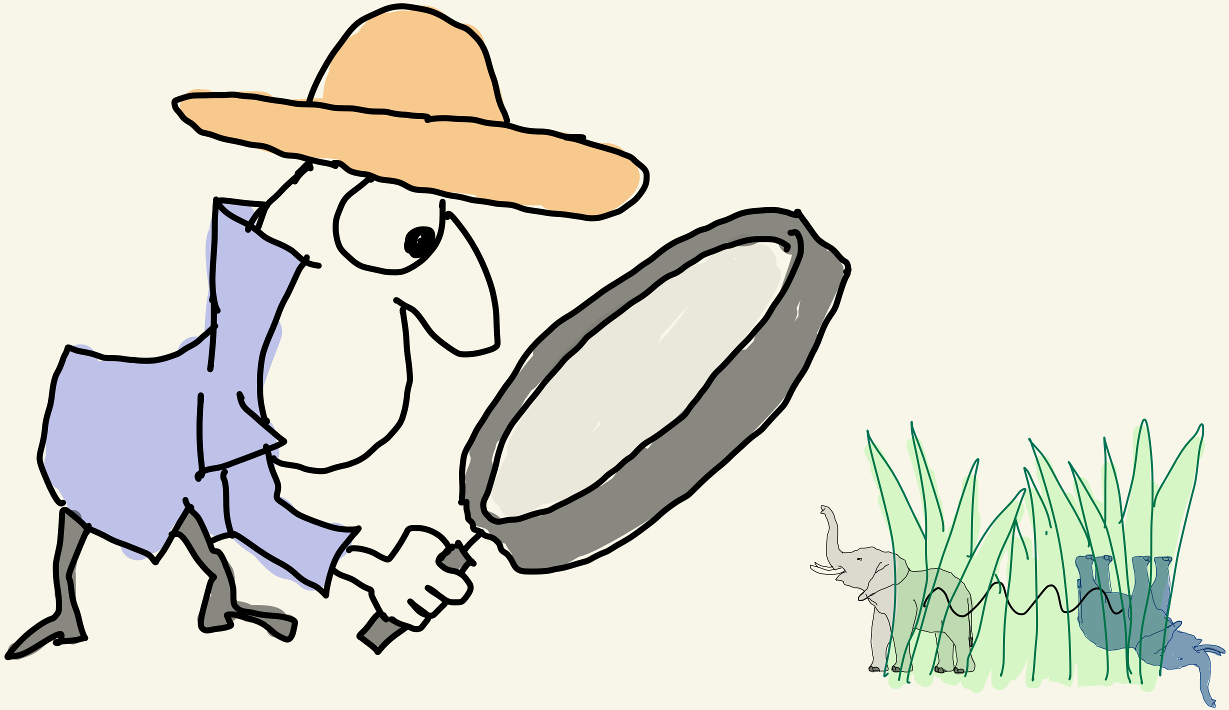

SNAKE!
WALL!
SPEAR!
TREE!
. . .
ELEPHANT!

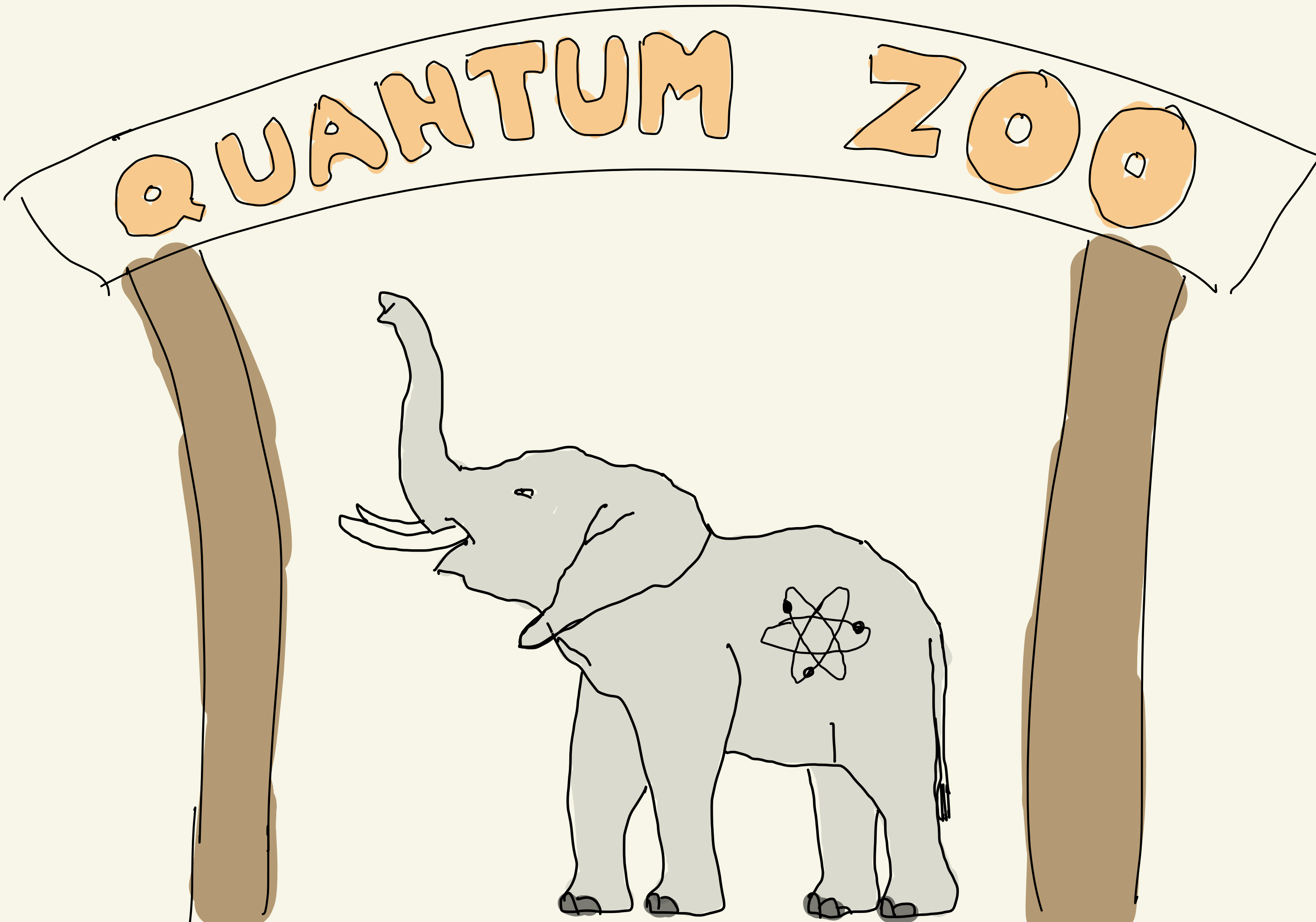

SNAKE!
WALL!
SPEAR!
TREE!
ELEPHANT!

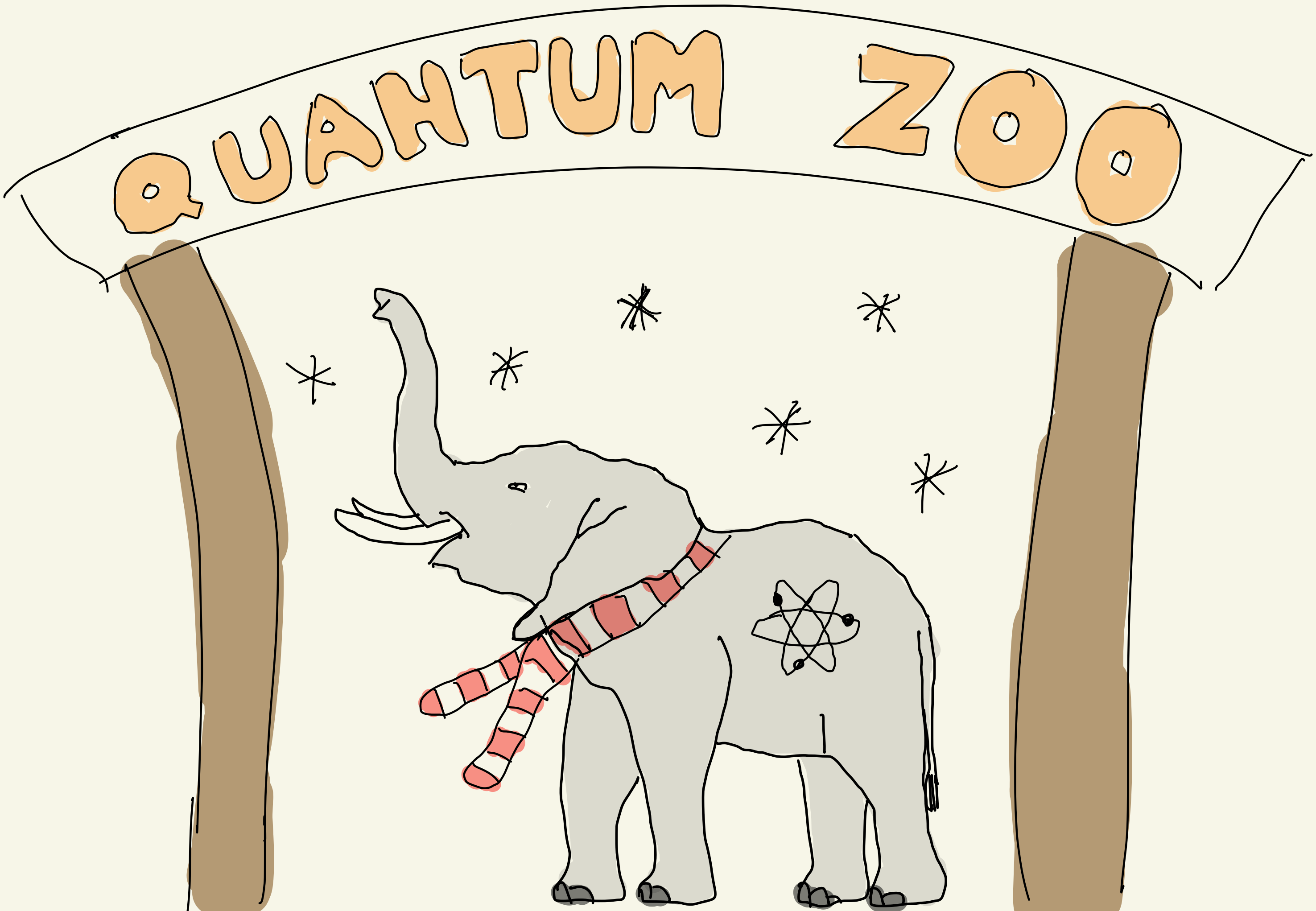

SNAKE!
WALL!
SPEAR!
TREE!
...
ELEPHANT!

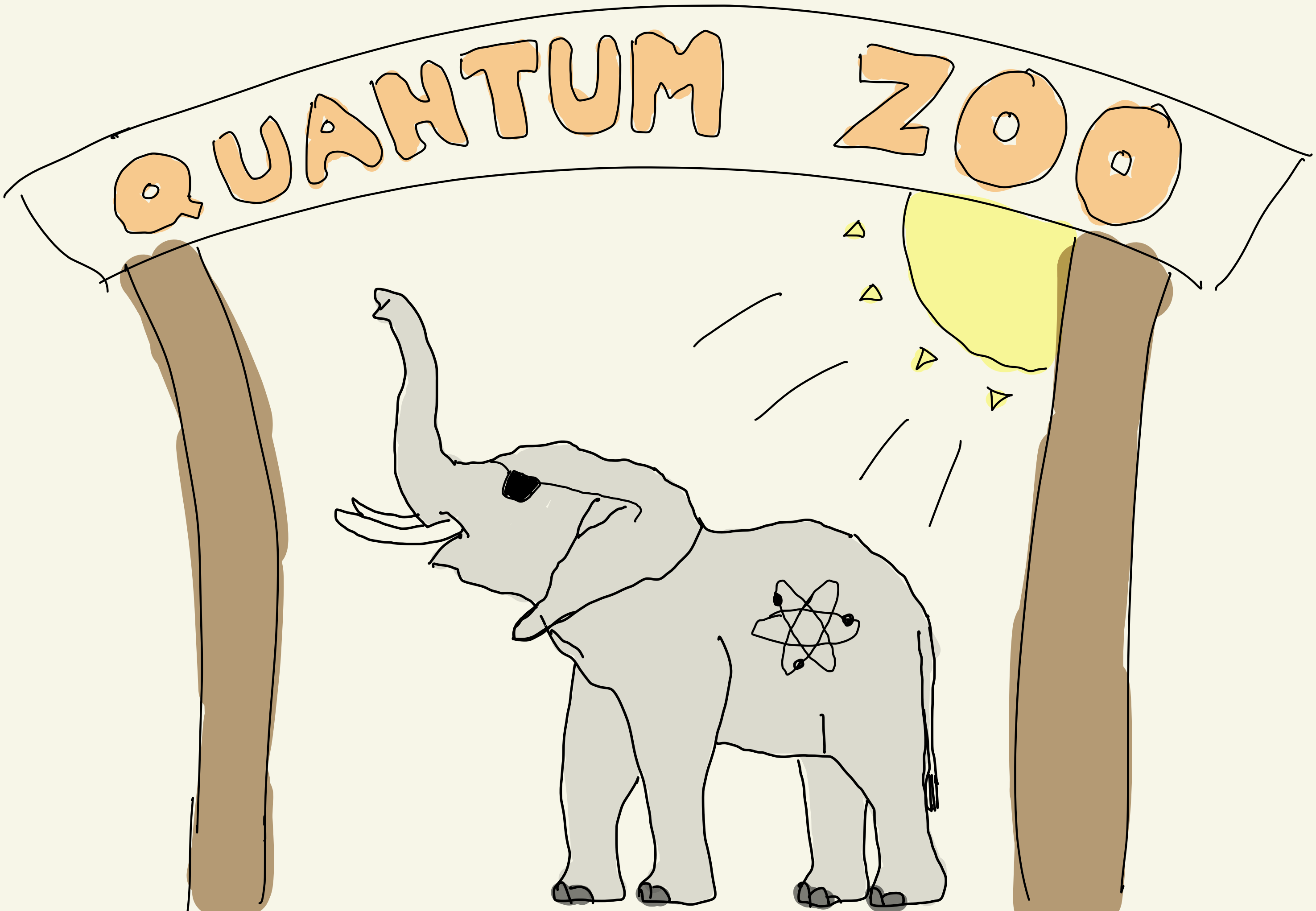

SNAKE!
WALL!
SPEAR!
TREE!
...
ELEPHANT!
SNAKE!
WALL!
SPEAR!
TREE!
...
ELEPHANT!






QUANTUM ZOO


QUANTUM ZOO


QUANTUM ZOO

And now for the actual dissertation...

Lower bounds on the complexity of quantum proofs

Chinmay Nirkhe

UC Berkeley

August 29th, 2022

Understanding classical proofs

Understanding classical proofs

NP = the class of all efficiently (poly(n) time) checkable proofs.

NP has complete problems such as Constraint Satisfaction Problems (CSPs).

Understanding classical proofs

NP = the class of all efficiently (poly(n) time) checkable proofs.

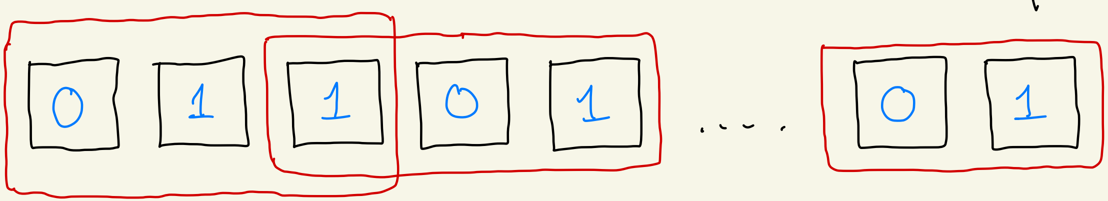
NP has complete problems such as Constraint Satisfaction Problems (CSPs).

$$\boxed{0}\ \boxed{1}\ \boxed{1}\ \boxed{0}\ \boxed{1}\ \cdots\ \boxed{0}\ \boxed{1}$$

Understanding classical proofs

NP = the class of all efficiently (poly(n) time) checkable proofs.

NP has complete problems such as Constraint Satisfaction Problems (CSPs).



[C_i not necessarily geometrically local]

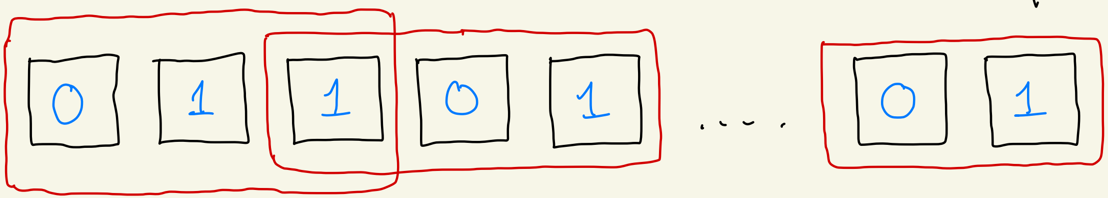
local check $C_i = x_1 \oplus x_2 \oplus x_3 = 0$.

$$C_i : \{0,1\}^3 \longrightarrow [0,1].$$

Understanding classical proofs

NP = the class of all efficiently (poly(n) time) checkable proofs.

NP has complete problems such as Constraint Satisfaction Problems (CSPs).



[C_i not necessarily geometrically local]

local check $C_i = x_1 \oplus x_2 \oplus x_3 = 0$.

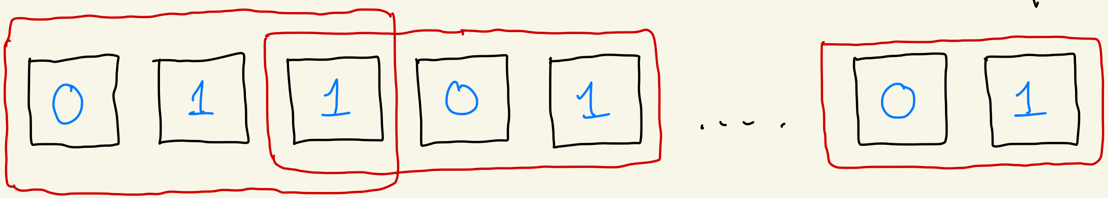
$$C_i : \{0,1\}^3 \longrightarrow [0,1].$$

$$C : \{0,1\}^n \longrightarrow [0,m] \quad \text{by} \quad C(x) = \sum_{i=1}^{m} C_i(x)$$

Understanding classical proofs

NP = the class of all efficiently (poly(n) time) checkable proofs.

NP has complete problems such as Constraint Satisfaction Problems (CSPs).



[C_i not necessarily geometrically local]

local check $C_i = x_1 \oplus x_2 \oplus x_3 = 0$.

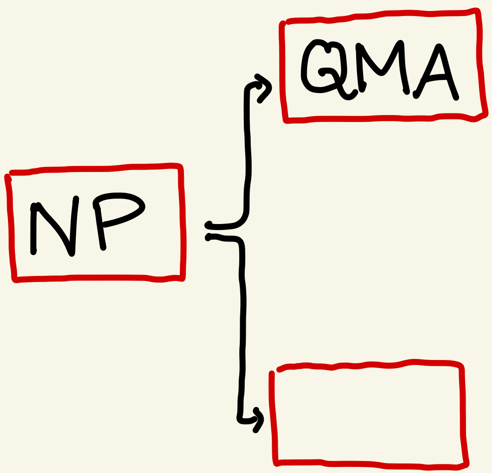
$C_i : \{0,1\}^3 \longrightarrow [0,1]$.

$C : \{0,1\}^n \longrightarrow [0,m]$ by $C(x) = \sum_{i=1}^{m} C_i(x)$

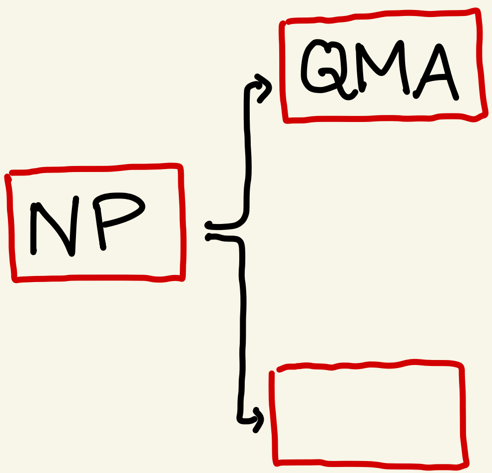
Decide if

1. $\exists\, x,\ C(x) = 0$.
2. $\forall\, x,\ C(x) \geq 1$.

Two extensions of the notion of proofs

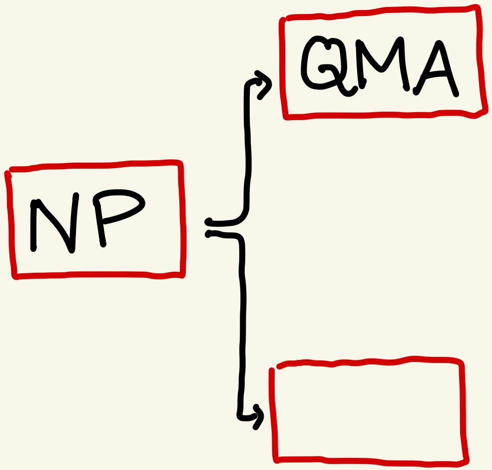


Two extensions of the notion of proofs



q. pfs. so they require a q. verifier (BQP)

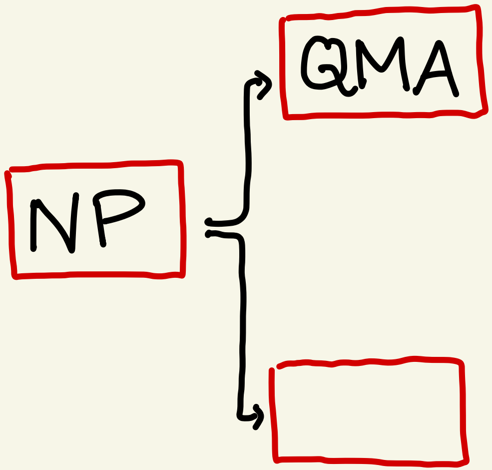
Two extensions of the notion of proofs



q. pfs. so they require a q. verifier (BQP)

Calculating ground energy of local Hamiltonians is a complete problem

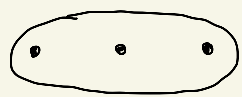
Two extensions of the notion of proofs



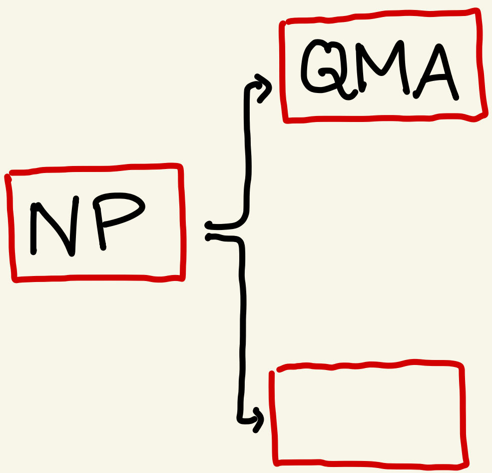
q. pfs. so they require a q. verifier (BQP)

Calculating ground energy of local Hamiltonians is a complete problem

h_i = linear <u>local</u> operator calculating energy

....  ... $h_i = |000\rangle\langle 000| + |111\rangle\langle 111|$

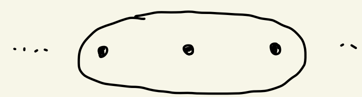
Two extensions of the notion of proofs



q. pfs. so they require a q. verifier (BQP)

Calculating ground energy of local Hamiltonians is a complete problem

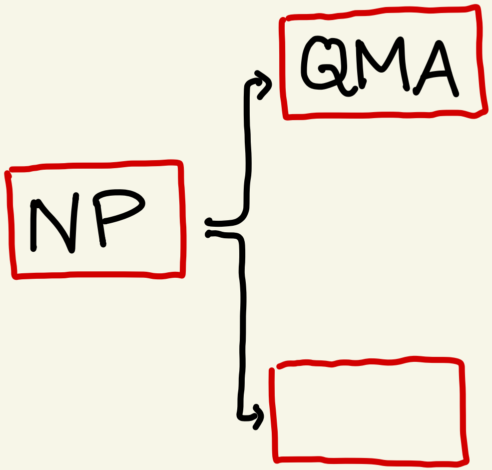
h_i = lineer <u>local</u> operator calculating energy



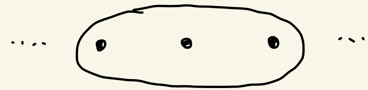
$h_i = |000\rangle\langle 000| + |111\rangle\langle 111|$

$\mathbf{H} = \sum_{i=1}^{m} h_i \qquad |\psi\rangle \longmapsto \langle\psi|\mathbf{H}|\psi\rangle$ (energy)

Two extensions of the notion of proofs



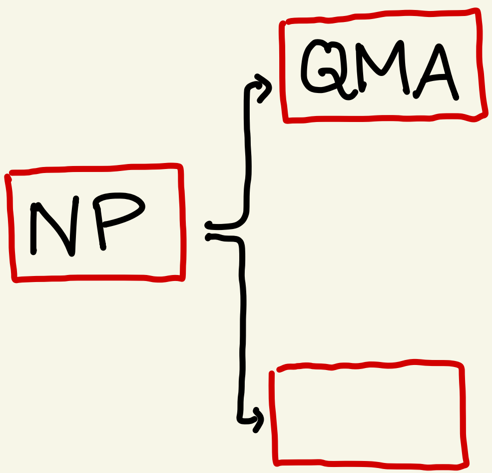
h_i = linear <u>local</u> operator calculating energy



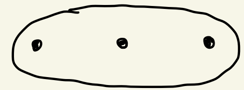
$h_i = |000\rangle\langle 000| + |111\rangle\langle 111|$

$$\mathbf{H} = \sum_{i=1}^{m} h_i \qquad |\psi\rangle \longmapsto \langle \psi | \mathbf{H} | \psi \rangle \text{ (energy)}$$

Two extensions of the notion of proofs



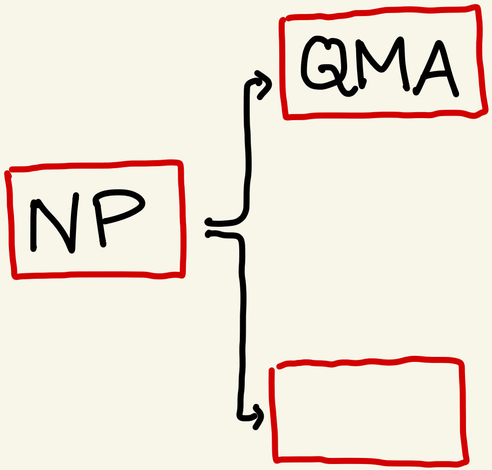
h_i = linear local operator calculating energy

…  … $h_i = |000\rangle\langle 000| + |111\rangle\langle 111|$

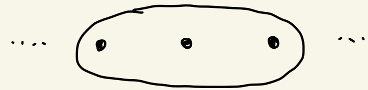
$\mathbf{H} = \sum_{i=1}^{m} h_i$ $\qquad |\psi\rangle \longmapsto \langle\psi|\mathbf{H}|\psi\rangle$ (energy)

ground energy $\quad \lambda_{min}(\mathbf{H}) = \min_{|\psi\rangle} \langle\psi|\mathbf{H}|\psi\rangle$

Two extensions of the notion of proofs



h_i = linear <u>local</u> operator calculating energy



$h_i = |000\rangle\langle 000| + |111\rangle\langle 111|$

$\mathbf{H} = \sum_{i=1}^{m} h_i \qquad |\psi\rangle \longmapsto \langle\psi|\mathbf{H}|\psi\rangle$ (energy)

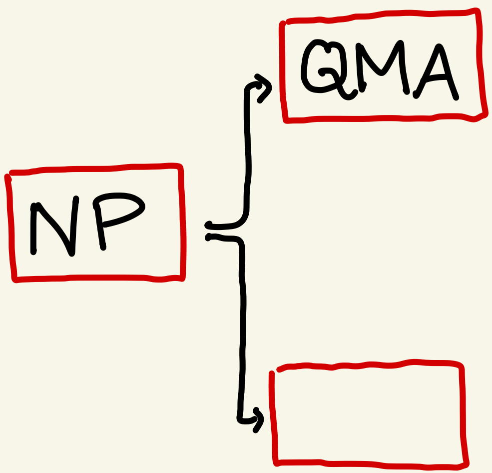
ground energy $\quad \lambda_{min}(\mathbf{H}) = \min_{|\psi\rangle} \langle\psi|\mathbf{H}|\psi\rangle$

QMA-hard to decide for $b - a = 1/\mathrm{poly}(m)$,

① $\lambda_{min}(\mathbf{H}) \leq a \iff \exists |\psi\rangle, \langle\psi|\mathbf{H}|\psi\rangle \leq a$

② $\lambda_{min}(\mathbf{H}) \geq b \iff \forall |\psi\rangle, \langle\psi|\mathbf{H}|\psi\rangle \geq b$

Two extensions of the notion of proofs

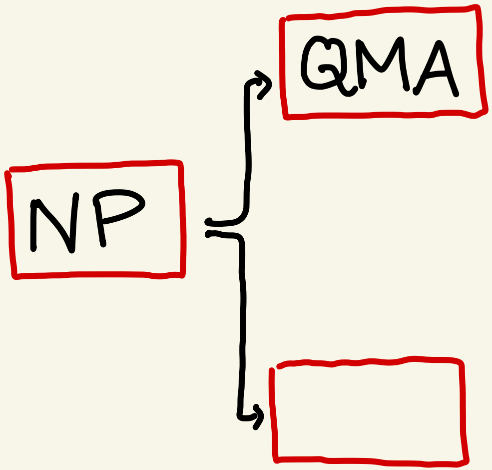


QMA-hard to decide for $b-a = 1/\mathrm{poly}(m)$,

① $\lambda_{min}(\mathbf{H}) \leq a \iff \exists |\psi\rangle, \langle\psi|\mathbf{H}|\psi\rangle \leq a$

② $\lambda_{min}(\mathbf{H}) \geq b \iff \forall |\psi\rangle, \langle\psi|\mathbf{H}|\psi\rangle \geq b$

Two extensions of the notion of proofs



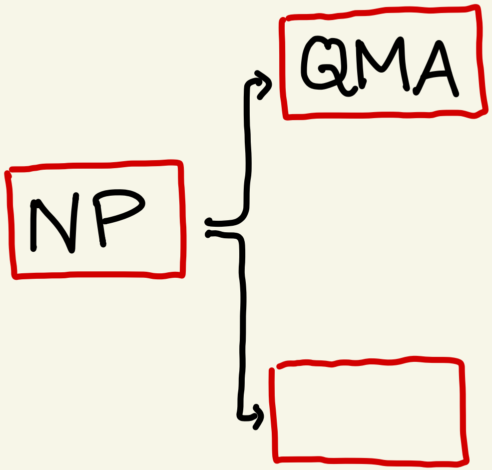
QMA-hard to decide for $b-a = 1/\mathrm{poly}(n)$,

① $\lambda_{min}(\mathbf{H}) \leq a \iff \exists |\psi\rangle, \langle\psi|\mathbf{H}|\psi\rangle \leq a$

② $\lambda_{min}(\mathbf{H}) \geq b \iff \forall |\psi\rangle, \langle\psi|\mathbf{H}|\psi\rangle \geq b$

$\implies$ groundstates of local Hamiltonians are a "canonical" form for all q. pfs.

Two extensions of the notion of proofs



QMA-hard to decide for $b-a = 1/\mathrm{poly}(n)$,

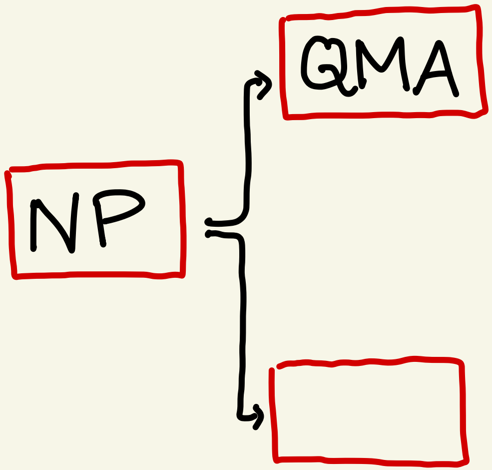
① $\lambda_{min}(\mathbf{H}) \leq a \iff \exists\, |\psi\rangle,\ \langle\psi|\mathbf{H}|\psi\rangle \leq a$

② $\lambda_{min}(\mathbf{H}) \geq b \iff \forall\, |\psi\rangle,\ \langle\psi|\mathbf{H}|\psi\rangle \geq b$

$\Longrightarrow$ groundstates of local Hamiltonians are a "canonical" form for all q. pfs.

It's widely believed that $NP \neq QMA$

Two extensions of the notion of proofs



QMA-hard to decide for $b-a = 1/\mathrm{poly}(m)$,

① $\lambda_{min}(\mathbf{H}) \leq a \iff \exists |\psi\rangle, \langle\psi|\mathbf{H}|\psi\rangle \leq a$

② $\lambda_{min}(\mathbf{H}) \geq b \iff \forall |\psi\rangle, \langle\psi|\mathbf{H}|\psi\rangle \geq b$

$\Longrightarrow$ groundstates of local Hamiltonians are a "canonical" form for all q. pfs.

It's widely believed that $NP \neq QMA$

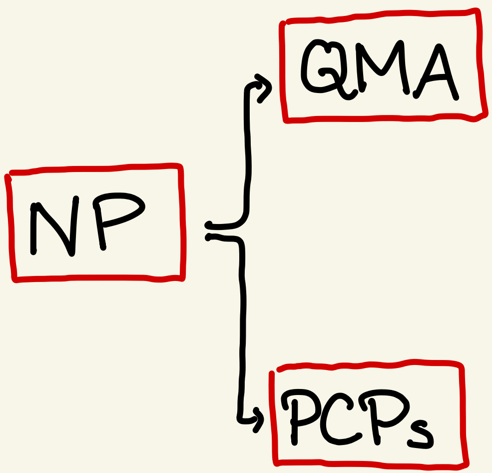
$$\boxed{\text{Therefore, not all groundstates of local Hamiltonians can be \underline{classically} described (in an efficiently verifiable manner)}}$$

Two extensions of the notion of proofs

$$\begin{tikzcd} & \boxed{\text{QMA}} \\ \boxed{\text{NP}} \arrow[ur] \arrow[dr] & \\ & \boxed{\text{PCPs}} \end{tikzcd}$$

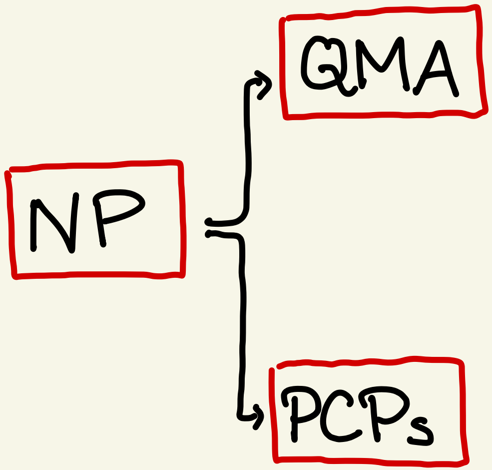
Two extensions of the notion of proofs

we think of pfs as requiring step-by-step checking.



Two extensions of the notion of proofs

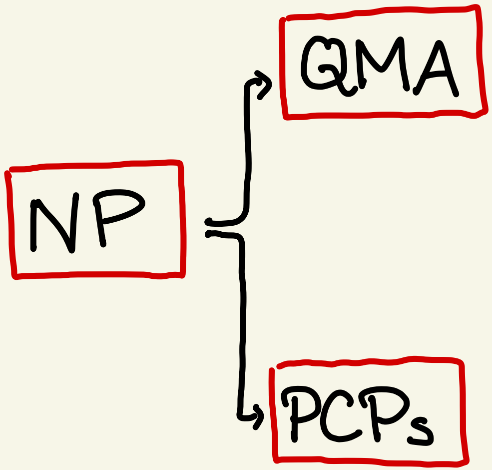
we think of pfs as requiring step-by-step checking.



PCP theorem Every NP problem (i.e. every pf.) can be converted into a form s.t. only $O(1)$ bits need to be read to be 99% confident in validity.

Arora-Safra et.al 98, Dinur

Two extensions of the notion of proofs



we think of pfs as requiring step-by-step checking.

PCP theorem Every NP problem (i.e. every pf.) can be converted into a form s.t. only $O(1)$ bits need to be read to be 99% confident in validity.

Arora-Safra et.al 98, Dinur

NP-hard to decide if

① $\exists x,\ C(x) = 0$

② $\forall x,\ C(x) \geq \frac{m}{2}$ (prev. 1)

[$C(x)$ = analog of $\langle \psi | \mathbf{H} | \psi \rangle$]

Two extensions of the notion of proofs

$$\begin{tikzcd} & \boxed{\text{QMA}} \\ \boxed{\text{NP}} \arrow[ur] \arrow[dr] & \\ & \boxed{\text{PCPs}} \end{tikzcd}$$

we think of pfs as requiring step-by-step checking.

<u>PCP theorem</u> Every NP problem (i.e. every pf.) can be converted into a form s.t. only $O(1)$ bits need to be read to be 99% confident in validity.

Arora-Safra-et.al 98, Dinur

NP-hard to decide if

① $\exists\, x,\ C(x) = 0$

② $\forall\, x,\ C(x) \geq \frac{m}{2}$ (prev. 1)

[$C(x)$ = analog of $\langle \psi | \mathbf{H} | \psi \rangle$]

Important consequence: $\boxed{\text{Noisy pfs suffice!}}$

Two extensions of the notion of proofs

we think of pfs as requiring step-by-step checking.

NP → QMA

NP → PCPs

PCP theorem Every NP problem (i.e. every pf.) can be converted into a form s.t. only $O(1)$ bits need to be read to be 99% confident in validity.

Arora-Safra et al 98, Dinur

NP-hard to decide if

① $\exists x,\ C(x) = 0$

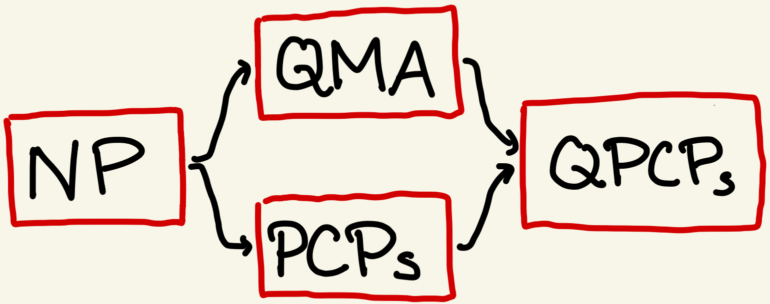
② $\forall x,\ C(x) \geq \frac{m}{2}$ (prev. 1)

[$C(x)$ = analog of $\langle \psi | \mathbf{H} | \psi \rangle$]

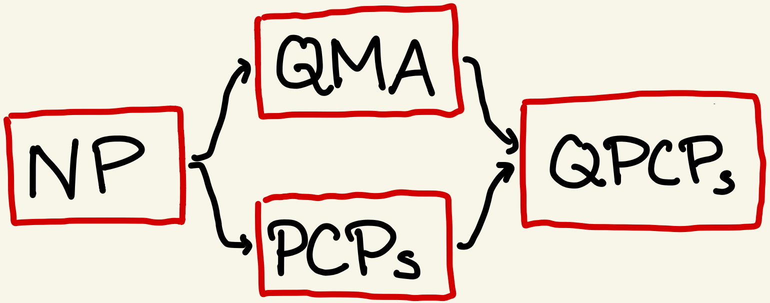
Any x s.t. $C(x) < \frac{m}{4}$ can be prob. verified with $O(1)$ queries.

Important consequence: Noisy pfs suffice!

The Quantum Prob. Checkable Pfs. Conjecture



The Quantum Prob. Checkable Pfs. Conjecture



Conjecture: Every QMA problem (i.e. quantum pf!) can be converted into a form s.t. only $O(1)$ qubits need to be measured

The Quantum Prob. Checkable Pfs. Conjecture

$$\begin{tikzcd}
 & \boxed{\text{QMA}} \arrow[dr] & \\
\boxed{\text{NP}} \arrow[ur] \arrow[dr] & & \boxed{\text{QPCPs}} \\
 & \boxed{\text{PCPs}} \arrow[ur] &
\end{tikzcd}$$

Conjecture: Every QMA problem (i.e. quantum pf!) can be converted into a form s.t. only $O(1)$ qubits need to be measured

Conj. For $\varepsilon > 0$, it's QMA-hard to decide

① $\exists\, |\psi\rangle$ s.t. $\langle\psi|\mathbf{H}|\psi\rangle = 0$ (morally)

② $\forall\, |\psi\rangle$, $\langle\psi|\mathbf{H}|\psi\rangle \gtrsim \varepsilon m$

The Quantum Prob. Checkable Pfs. Conjecture

$$\begin{tikzcd} & \boxed{\text{QMA}} \arrow[dr] & \\ \boxed{\text{NP}} \arrow[ur] \arrow[dr] & & \boxed{\text{QPCPs}} \\ & \boxed{\text{PCPs}} \arrow[ur] & \end{tikzcd}$$

Conjecture: Every QMA problem (i.e. quantum pf!) can be converted into a form s.t. only $O(1)$ qubits need to be measured

Conj. For $\varepsilon > 0$, it's QMA-hard to decide

① $\exists\ |\psi\rangle$ s.t. $\langle \psi | \mathbf{H} | \psi \rangle = 0$ (morally)

② $\forall\ |\psi\rangle$, $\langle \psi | \mathbf{H} | \psi \rangle \geq \varepsilon m$

Similar to PCP theorem, every state of energy $\leq \frac{\varepsilon}{2} m$ is a valid pf. for a QPCP local Hamiltonians.

Set of pfs is much larger!

An important consequence of QPCPs

(A) (if $NP \neq QMA$) quantum pfs. cannot be classically described (in any efficiently checkable manner)

(B) low. energy states of QPCP local Hamiltonians are also valid pfs (since they are noisy pfs.)

An important consequence of QPCPs

Ⓐ (if $NP \neq QMA$) quantum pfs. cannot be classically described (in any efficiently checkable manner)

Ⓑ low. energy states of QPCP local Hamiltonians are also valid pfs (since they are noisy pfs.)

$\Rightarrow$ There exist local Hamiltonians such that <u>every</u> low energy state <u>cannot</u> be classically described

An important consequence of QPCPs

Ⓐ (if NP $\neq$ QMA) quantum pfs. cannot be classically described (in any efficiently checkable manner)

Ⓑ low. energy states of QPCP local Hamiltonians are also valid pfs (since they are noisy pfs.)

$\Rightarrow$ There exist local Hamiltonians such that every low energy state cannot be classically described

Constant depth q. circuit descriptions are classically checkable pfs for output state

An important consequence of QPCPs

(A) (if NP $\neq$ QMA) quantum pfs. cannot be classically described (in any efficiently checkable manner)

(B) low. energy states of QPCP local Hamiltonians are also valid pfs (since they are noisy pfs.)

$\Longrightarrow$ There exist local Hamiltonians such that every low energy state cannot be classically described

Constant depth q. circuit descriptions are classically checkable pfs for output state

No low energy trivial states There exist local Hams. s.t. no low-energy state is the output of a constant depth circuit.

[Freedman-Hastings 14]

$$\boxed{\text{\underline{No low energy} \underline{trivial states}. There exist local Hams. s.t. \underline{no} low-energy state is the output of a constant depth circuit.}}$$

[Freedman-Hastings 14]

$$\boxed{\text{No low energy trivial states: There exist local Hams. s.t. no low-energy state is the output of a constant depth circuit.}}$$

[Freedman-Hastings 14]

- If it was false, then QPCP would have been trivially false.
- Makes a statement about physically realizable robust entanglement.

$\boxed{\text{No low energy trivial states: There exist local Hams. s.t. no low-energy state is the output of a constant depth circuit.}}$

[Freedman-Hastings 14]

- If it was false, then QPCP would have been trivially false.
- Makes a statement about physically realizable robust entanglement.

Theorem [Anurag Anshu, Niko Breuckmann, & C.N. '22]

Local Hamiltonians corresponding to most* linear-rate and -distance QLDPC error-correcting codes are NLTS Hamiltonians.

$\boxed{\text{No low energy trivial states: There exist local Hams. s.t. no low-energy state is the output of a constant depth circuit.}}$

[Freedman-Hastings 14]

- If it was false, then QPCP would have been trivially false.
- Makes a statement about physically realizable robust entanglement.

Theorem [Anurag Anshu, Niko Breuckmann, & C.N. '22]

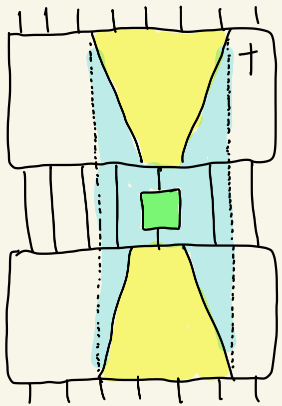
Local Hamiltonians corresponding to most* linear-rate and -distance QLDPC error-correcting codes are NLTS Hamiltonians.

$\exists\, \varepsilon > 0$, and Hamiltonian family $\mathbf{H}$ s.t. every state ψ of energy $\le \varepsilon n$, the minimum depth circuit to generate ψ is $\Omega(\log n)$.

Proof sketch of the NLTS theorem

① Trivial states ⇒ Local Hamiltonians

⇒ Circuit depth lower bounds

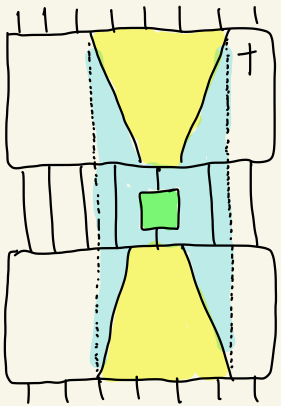


Lightcones for low depth circuits

Proof sketch of the NLTS theorem

① Trivial states ⟹ Local Hamiltonians

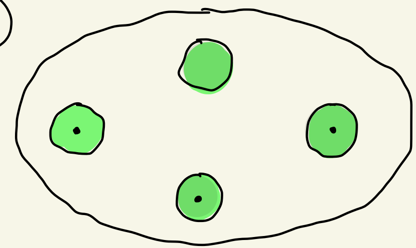
⟹ Circuit depth lower bounds



Lightcones for low depth circuits

Error Correction Codes (ECC)

②

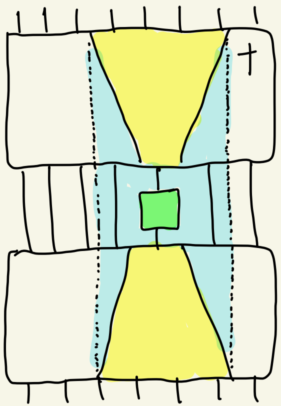


low energy subspace of expanding codes.

Proof sketch of the NLTS theorem

① Trivial states ⇒ Local Hamiltonians

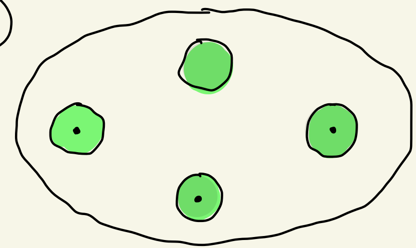
⇒ Circuit depth lower bounds



Lightcones for low depth circuits

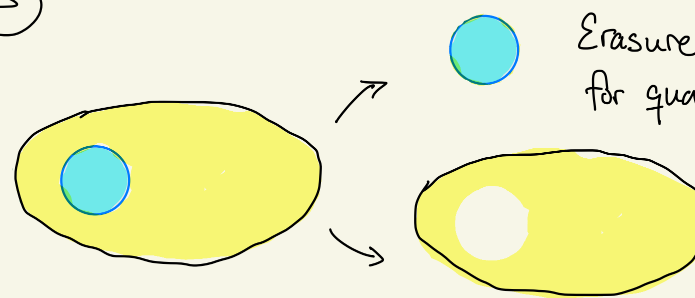
Error Correction Codes (ECC)

②



low energy subspace of expanding codes.

③



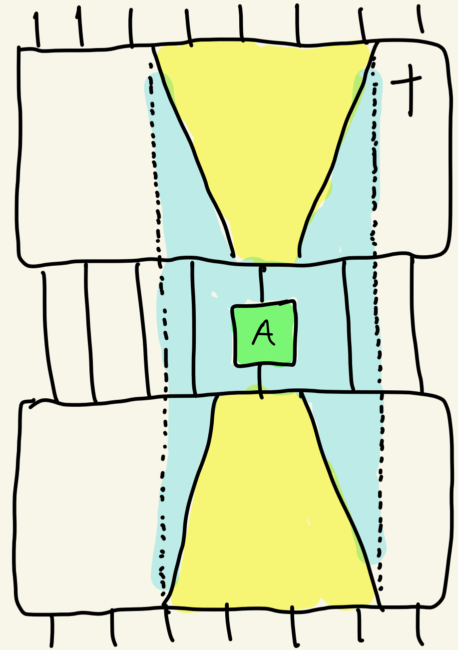
Erasure errors for quantum codes

Lightcones and quantum circuits

If A is a local operator and $\mathcal{U}$ is a q. circuit of depth t, then $\mathcal{U}^\dagger A \mathcal{U}$ is a $\leq 2^t \cdot |A|$ local operator.

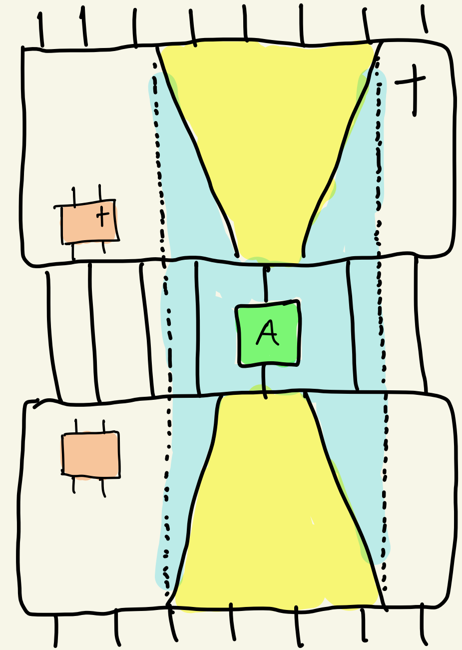
Lightcones and quantum circuits

If A is a local operator and $\mathcal{U}$ is a q. circuit of depth t, then $\mathcal{U}^\dagger A \mathcal{U}$ is a $\leq 2^t \cdot |A|$ local operator.



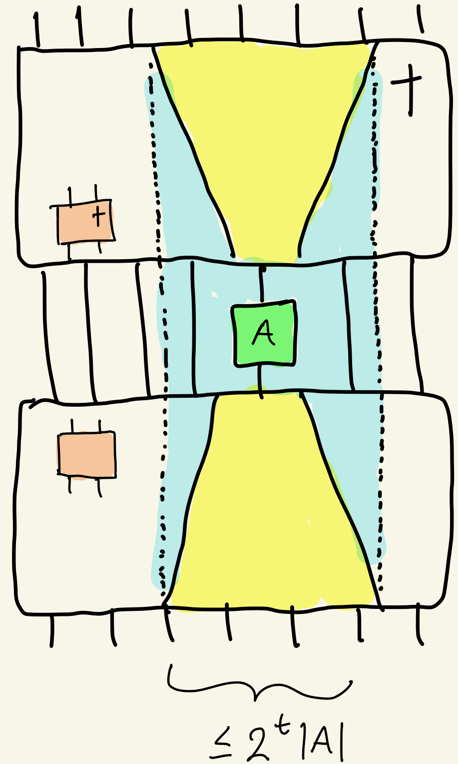
Lightcones and quantum circuits

If A is a local operator and $\mathcal{U}$ is a q. circuit of depth t, then $\mathcal{U}^\dagger A \mathcal{U}$ is a $\leq 2^t \cdot |A|$ local operator.



Lightcones and quantum circuits

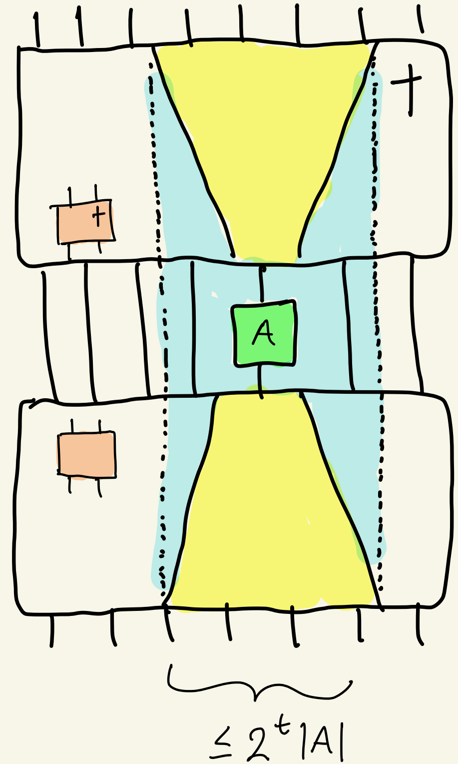
If A is a local operator and $\mathcal{U}$ is a q. circuit of depth t, then $\mathcal{U}^\dagger A \mathcal{U}$ is a $\leq 2^t \cdot |A|$ local operator.



Lightcones and quantum circuits

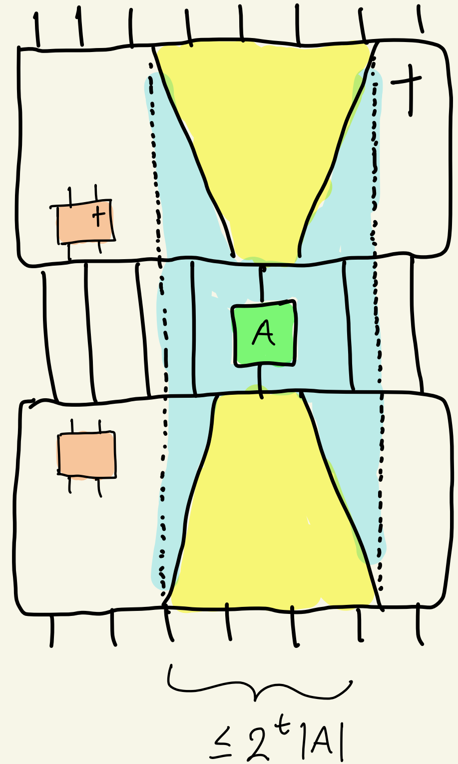
If A is a local operator and $\mathcal{U}$ is a q. circuit of depth t, then $\mathcal{U}^\dagger A \mathcal{U}$ is a $\leq 2^t \cdot |A|$ local operator.

Given a local Hamiltonian $\mathbf{H} = \sum_i^m h_i$ and a state $|\psi\rangle = \mathcal{U}|0^n\rangle$, we can evaluate $\langle\psi|\mathbf{H}|\psi\rangle$ in classical time $2^{2^t} \cdot \mathrm{poly}(n) = \mathrm{poly}(n)$ when $t = O(1)$.



Lightcones and quantum circuits

If A is a local operator and $\mathcal{U}$ is a q. circuit of depth t, then $\mathcal{U}^\dagger A \mathcal{U}$ is a $\leq 2^t \cdot |A|$ local operator.



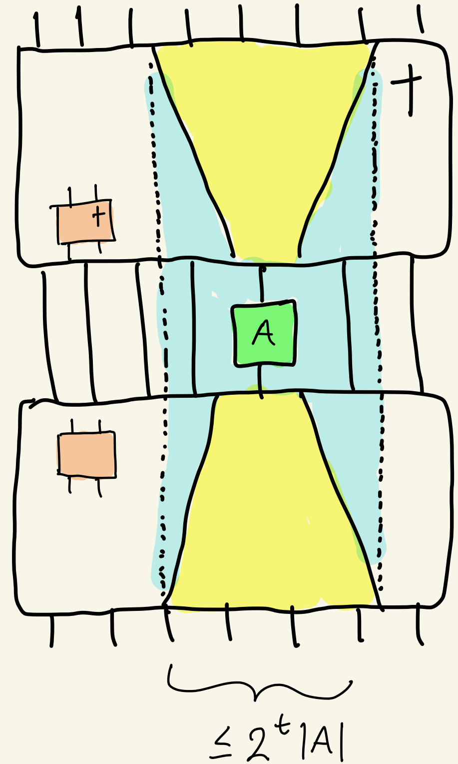
Given a local Hamiltonian $\mathbf{H} = \sum_i^m h_i$ and a state $|\psi\rangle = \mathcal{U}|0^n\rangle$, we can evaluate $\langle\psi|\mathbf{H}|\psi\rangle$ in classical time $2^{2^t} \cdot \text{poly}(n) = \text{poly}(n)$ when $t = O(1)$.

$$\langle\psi|\mathbf{H}|\psi\rangle = \sum_i^m \langle\psi|h_i|\psi\rangle$$

$$= \sum_i^m \langle 0^n|\mathcal{U}^\dagger h_i \mathcal{U}|0^n\rangle$$

Lightcones and quantum circuits

If A is a local operator and $\mathcal{U}$ is a q. circuit of depth t, then $\mathcal{U}^\dagger A \mathcal{U}$ is a $\leq 2^t \cdot |A|$ local operator.



Given a local Hamiltonian $\mathbf{H} = \sum_i^m h_i$ and a state $|\psi\rangle = \mathcal{U}|0^n\rangle$, we can evaluate $\langle\psi|\mathbf{H}|\psi\rangle$ in classical time $2^{2^t} \cdot \mathrm{poly}(n) = \mathrm{poly}(n)$ when $t = O(1)$.

$$\langle\psi|\mathbf{H}|\psi\rangle = \sum_i^m \langle\psi|h_i|\psi\rangle$$

$$= \sum_i^m \underbrace{\langle 0^n|\mathcal{U}^\dagger h_i \mathcal{U}|0^n\rangle}_{\text{computation on } O(2^t) \text{ qubits}}$$

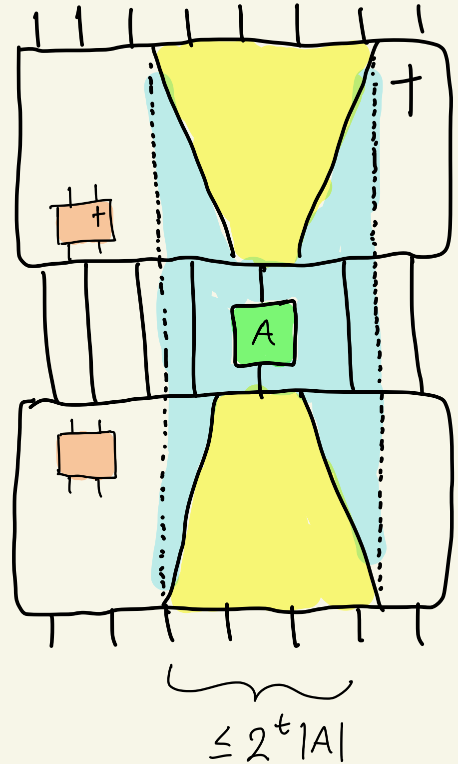
Lightcones and quantum circuits

If A is a local operator and $\mathcal{U}$ is a q. circuit of depth t, then $\mathcal{U}^\dagger A \mathcal{U}$ is a $\leq 2^t \cdot |A|$ local operator.

Given a local Hamiltonian $\mathbf{H} = \sum_i^m h_i$ and a state $|\psi\rangle = \mathcal{U}|0^n\rangle$, we can evaluate $\langle\psi|\mathbf{H}|\psi\rangle$ in classical time $2^{2^t} \cdot \mathrm{poly}(n) = \mathrm{poly}(n)$ when $t = O(1)$.

$$\langle\psi|\mathbf{H}|\psi\rangle = \sum_i^m \langle\psi|h_i|\psi\rangle$$

$$= \sum_i^m \underbrace{\langle 0^n|\mathcal{U}^\dagger h_i \mathcal{U}|0^n\rangle}_{\text{computation on } O(2^t) \text{ qubits}}$$



Low-depth states are classical witnesses for energy

Trivial states ⇒ Local Hamiltonians

The state $|0^n\rangle$ is the <u>unique</u> solution to a very simple local Hamiltonian.

Trivial states ⇒ Local Hamiltonians

The state $|0^{n'}\rangle$ is the unique solution to a very simple local Hamiltonian.

$$H_0 = \sum_{i=1}^{n'} |1\rangle\langle 1|_i \leftarrow \text{qubit-wise projectors enforcing qubits equal } |0\rangle.$$

Trivial states $\Rightarrow$ Local Hamiltonians

The state $|0^{n'}\rangle$ is the unique solution to a very simple local Hamiltonian.

$$\mathbf{H}_0 = \sum_{i=1}^{n'} |1\rangle\langle 1|_i \leftarrow \text{qubit-wise projectors enforcing qubits equal } |0\rangle.$$

$\mathbf{H}_0$ is commuting and has a spectrum of $0, 1, 2, \dots, n'$, with eigenvectors $|x\rangle$ of eigenvalue $|x|$.

Trivial states $\Rightarrow$ Local Hamiltonians

The state $|0^{n'}\rangle$ is the unique solution to a very simple local Hamiltonian.

$$\mathbf{H}_0 = \sum_{i=1}^{n'} |1\rangle\langle 1|_i \leftarrow \text{qubit-wise projectors enforcing qubits equal } |0\rangle.$$

$\mathbf{H}_0$ is commuting and has a spectrum of $0, 1, 2, \dots, n'$, with eigenvectors $|x\rangle$ of eigenvalue $|x|$.

Let $\mathbf{H}_U = U^\dagger \mathbf{H} U$ for depth t circuit U.

Trivial states ⇒ Local Hamiltonians

The state $|0^{n'}\rangle$ is the unique solution to a very simple local Hamiltonian.

$$\mathbf{H}_0 = \sum_{i=1}^{n'} |1\rangle\langle 1|_i$$ ← qubit-wise projectors enforcing qubits equal $|0\rangle$.

$\mathbf{H}_0$ is commuting and has a spectrum of $0, 1, 2, \dots, n'$, with eigenvectors $|x\rangle$ of eigenvalue $|x|$.

Let $\mathbf{H}_{\mathcal{U}} = \mathcal{U}^\dagger \mathbf{H} \, \mathcal{U}$ for depth t circuit $\mathcal{U}$.

$\mathbf{H}_{\mathcal{U}}$ is commuting and has a spectrum of $0, 1, 2, \dots, n'$, with eigenvectors $\mathcal{U}|x\rangle$ of eigenvalue $|x|$.

And $\mathbf{H}_{\mathcal{U}}$ is a 2^t-local Hamiltonian.

Local indistinguishability

Two states $|\psi\rangle$ and $|\psi'\rangle$ are d-locally indistinguishable if for every region S of size $\leq d$,

$$\boxed{\psi_{-S} = \psi'_{-S}}.$$

Local indistinguishability

Two states $|\psi\rangle$ and $|\psi'\rangle$ are d-locally indistinguishable if for every region S of size $\leq d$,

$$\boxed{\psi_{-S} = \psi'_{-S}}.$$

Ex. The states
$$|🐱_{\pm}\rangle = \frac{|0^n\rangle \pm |1^n\rangle}{\sqrt{2}}$$
are $(n-1)$ locally indistinguishable.

Local indistinguishability

Two states $|\psi\rangle$ and $|\psi'\rangle$ are d-locally indistinguishable if for every region S of size $\leq d$,

$$\boxed{\psi_{-S} = \psi'_{-S}}.$$

Ex. The states $$|\mathrm{cat}_\pm\rangle = \frac{|0^n\rangle \pm |1^n\rangle}{\sqrt{2}}$$

are $(n-1)$ locally indistinguishable.

Any strict reduced density matrix equals

$$(\mathrm{cat}_\pm)_{-S} = \frac{|0\rangle\langle 0|^{n-|S|} + |1\rangle\langle 1|^{n-|S|}}{2}.$$

Local indistinguishability

Two states $|\Psi\rangle$ and $|\Psi'\rangle$ are d-locally indistinguishable if for every region S of size $\leq d$,

$$\boxed{\Psi_{-S} = \Psi'_{-S}}.$$

Local indistinguishability

Two states $|\psi\rangle$ and $|\psi'\rangle$ are d-locally indistinguishable if for every region S of size $\leq d$,

$$\boxed{\psi_{-S} = \psi'_{-S}}.$$

Lemma If $|\psi\rangle$ and $|\psi'\rangle$ are d-locally indistinguishable, then if $|\psi\rangle = \mathcal{U}|0^n\rangle$ for $\mathcal{U}$ of depth t, then $2^t \geq d$. $\Rightarrow$ $\boxed{t \geq \log d.}$

Local indistinguishability

Two states $|\psi\rangle$ and $|\psi'\rangle$ are d-locally indistinguishable if for every region S of size $\leq d$, $\boxed{\psi_{-S} = \psi'_{-S}}$.

Lemma If $|\psi\rangle$ and $|\psi'\rangle$ are d-locally indistinguishable, then if $|\psi\rangle = \mathcal{U}|0^n\rangle$ for $\mathcal{U}$ of depth t, then $2^t \geq d$. $\Rightarrow$ $\boxed{t \geq \log d.}$

Pf. $\langle\psi'|\mathbf{H}_{\mathcal{U}}|\psi'\rangle = \sum_i \langle\psi'|h_i|\psi'\rangle$

$= \sum_i \langle\psi|h_i|\psi\rangle$

since $\mathbf{H}_{\mathcal{U}}$ is 2^t-local and are $d > 2^t$ locally indistinguishable

Local indistinguishability

Two states $|\psi\rangle$ and $|\psi'\rangle$ are d-locally indistinguishable if for every region S of size $\leq d$,

$$\boxed{\psi_{-S} = \psi'_{-S}}.$$

Lemma If $|\psi\rangle$ and $|\psi'\rangle$ are d-locally indistinguishable, then if $|\psi\rangle = \mathcal{U}|0^n\rangle$ for $\mathcal{U}$ of depth t, then $2^t \geq d$. $\Rightarrow$ $\boxed{t \geq \log d.}$

Pf. $\langle \psi' | \mathbf{H}_{\mathcal{U}} | \psi' \rangle = \sum_i \langle \psi' | h_i | \psi' \rangle$

since $\mathbf{H}_{\mathcal{U}}$ is 2^t-local and are $d > 2^t$ locally indistinguishable

$$= \sum_i \langle \psi | h_i | \psi \rangle = \langle \psi | \mathbf{H} | \psi \rangle = 0$$

Local indistinguishability

Two states $|\psi\rangle$ and $|\psi'\rangle$ are d-locally indistinguishable if for every region S of size $\leq d$,

$$\boxed{\psi_{-S} = \psi'_{-S}}.$$

Lemma If $|\psi\rangle$ and $|\psi'\rangle$ are d-locally indistinguishable, then if $|\psi\rangle = \mathcal{U}|0^n\rangle$ for $\mathcal{U}$ of depth t, then $2^t \geq d$. $\Rightarrow$ $\boxed{t \geq \log d.}$

Pf. $\langle\psi'|\mathbf{H}_{\mathcal{U}}|\psi'\rangle = \sum_i \langle\psi'|h_i|\psi'\rangle$ since $\mathbf{H}_{\mathcal{U}}$ is 2^t-local and are $d > 2^t$ locally indistinguishable

$$= \sum_i \langle\psi|h_i|\psi\rangle = \langle\psi|\mathbf{H}|\psi\rangle = 0$$

But groundstate $|\psi\rangle$ is unique! $\Rightarrow$ $|\psi\rangle = |\psi'\rangle$, a contradiction!

Local indistinguishability

Lemma If $|\psi\rangle$ and $|\psi'\rangle$ are d-locally indistinguishable, then if $|\psi\rangle = U|0^n\rangle$ for U of depth t, then $2^t \geq d$. $\Rightarrow$ $\boxed{t \geq \log d.}$

Local indistinguishability

Lemma If $|\psi\rangle$ and $|\psi'\rangle$ are d-locally indistinguishable, then if $|\psi\rangle = U|0^n\rangle$ for U of depth t, then $2^t \geq d$. $\Rightarrow$ $\boxed{t \geq \log d.}$

Since, spectral gap of $\mathbf{H}_U$ is 1, this argument is only robust to perturbations of $O(\frac{1}{n})$.

Local indistinguishability

Lemma If $|\psi\rangle$ and $|\psi'\rangle$ are d-locally indistinguishable, then if $|\psi\rangle = \mathcal{U}|0^n\rangle$ for $\mathcal{U}$ of depth t, then $2^t \geq d$. $\Rightarrow$ $\boxed{t \geq \log d.}$

Since, spectral gap of $\mathbf{H}_{\mathcal{U}}$ is 1, this argument is only robust to perturbations of $O(\frac{1}{n})$.

Using mathematics from Chebyshev polynomials, we can make l.b. robust.

Local indistinguishability

Lemma If $|\psi\rangle$ and $|\psi'\rangle$ are d-locally indistinguishable, then if $|\psi\rangle = \mathcal{U}|0^n\rangle$ for $\mathcal{U}$ of depth t, then $2^t \geq d$. $\Rightarrow$ $\boxed{t \geq \log d.}$

Since, spectral gap of $\mathbf{H}_\mathcal{U}$ is 1, this argument is only robust to perturbations of $O(\frac{1}{n})$.

Using mathematics from Chebyshev polynomials, we can make l.b. robust.

Theorem Let $S_1, S_2 \subset \{0,1\}^n$ be sets and $p(\ )$ a prob. dist. on $\{0,1\}^n$. If $p(S_1), p(S_2) \geq \mu$, then minimum q. ckt. depth to generate p is $\Omega\left(\log\left(\frac{\text{dist}(S_1,S_2)^2 \cdot \mu}{n}\right)\right)$.

Local indistinguishability

<u>Theorem</u> Let $S_1, S_2 \subset \{0,1\}^n$ be sets and $p(\ )$ a prob. dist. on $\{0,1\}^n$.

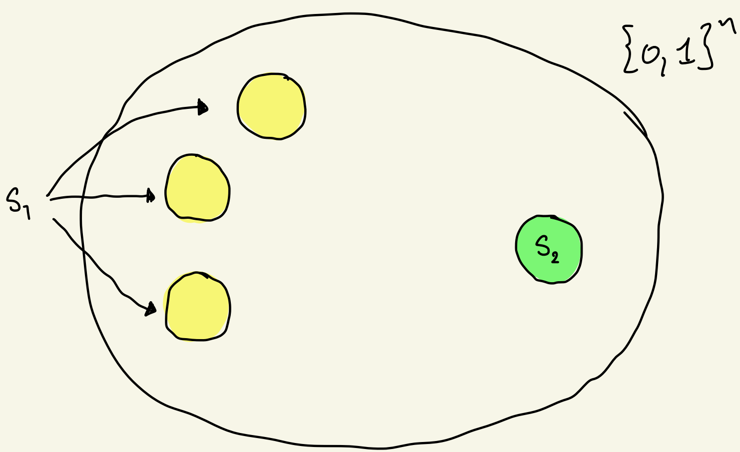
If $p(S_1), p(S_2) \geq \mu$, then minimum q. ckt. depth to generate p

is $$\Omega\left(\log\left(\frac{\mathrm{dist}(S_1, S_2)^2 \cdot \mu}{n}\right)\right).$$

Local indistinguishability

Theorem Let $S_1, S_2 \subset \{0,1\}^n$ be sets and $p(\ )$ a prob. dist. on $\{0,1\}^n$.
If $p(S_1), p(S_2) \geq \mu$, then minimum q. ckt. depth to generate p is

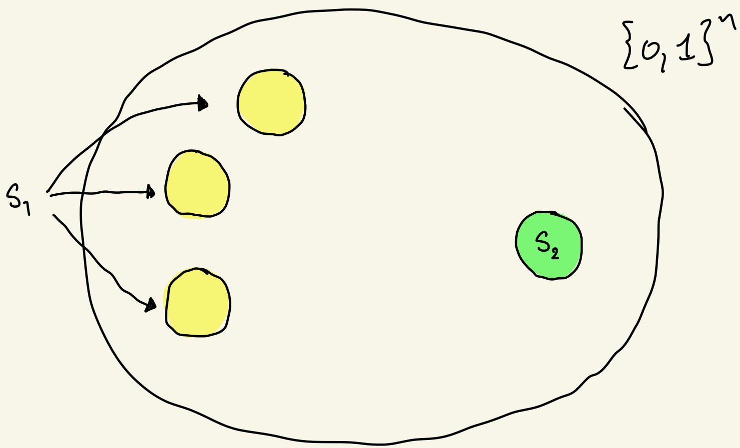
$$\Omega\left(\log\left(\frac{\text{dist}(S_1, S_2)^2 \cdot \mu}{n}\right)\right).$$



Local indistinguishability

Theorem Let $S_1, S_2 \subset \{0,1\}^n$ be sets and $p(\ )$ a prob. dist. on $\{0,1\}^n$. If $p(S_1), p(S_2) \geq \mu$, then minimum q. ckt. depth to generate p is

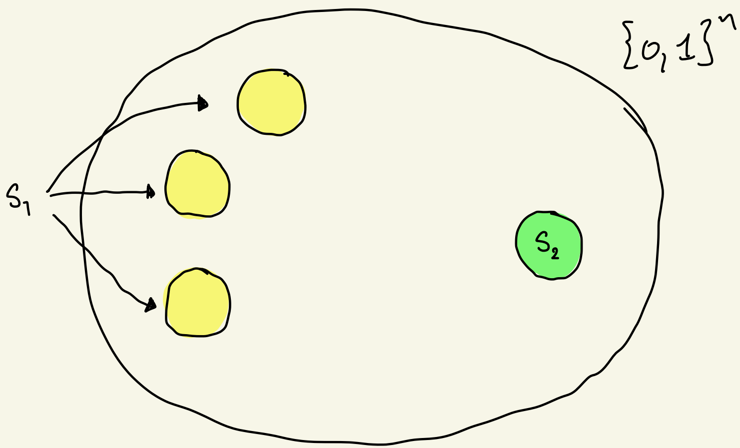
$$\Omega\left(\log\left(\frac{\operatorname{dist}(S_1,S_2)^2 \cdot \mu}{n}\right)\right).$$



Pf sketch. Let $|\psi\rangle$ generate p.

Local indistinguishability

Theorem Let $S_1, S_2 \subset \{0,1\}^n$ be sets and $p(\ )$ a prob. dist. on $\{0,1\}^n$. If $p(S_1), p(S_2) \geq \mu$, then minimum q. ckt. depth to generate p is
$$\Omega\left(\log\left(\frac{\mathrm{dist}(S_1,S_2)^2 \cdot \mu}{n}\right)\right).$$

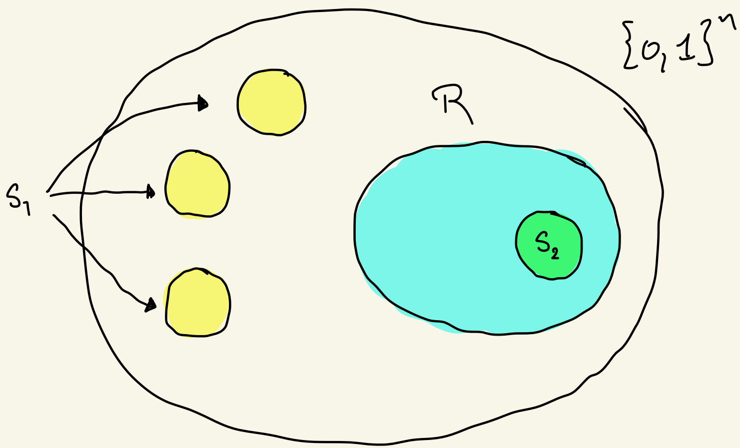


Pf sketch. Let $|\Psi\rangle$ generate p.

Then $\exists$ region R s.t.

Local indistinguishability

Theorem Let $S_1, S_2 \subset \{0,1\}^n$ be sets and $p(\ )$ a prob. dist. on $\{0,1\}^n$.
If $p(S_1), p(S_2) \geq \mu$, then minimum q. ckt. depth to generate p
is $\Omega\left(\log\left(\frac{\mathrm{dist}(S_1,S_2)^2 \cdot \mu}{n}\right)\right)$.



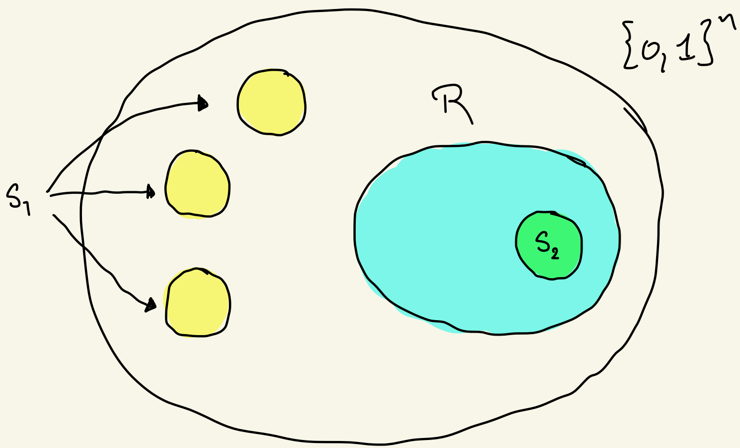
Pf sketch. Let $|\Psi\rangle$ generate p.

Then $\exists$ region R s.t.

Local indistinguishability

Theorem Let $S_1, S_2 \subset \{0,1\}^n$ be sets and $p(\ )$ a prob. dist. on $\{0,1\}^n$.
If $p(S_1), p(S_2) \geq \mu$, then minimum q. ckt. depth to generate p is

$$\Omega\left(\log\left(\frac{\mathrm{dist}(S_1,S_2)^2 \cdot \mu}{n}\right)\right).$$



Pf sketch. Let $|\psi\rangle$ generate p.

Then $\exists$ region R s.t.

$|\psi'\rangle$ = "flip sign of $|\psi\rangle$ on R"

and $|\psi\rangle$ and $|\psi'\rangle$ are approx. locally indistinguishable.

Local indistinguishability

<u>Theorem</u> Let $S_1, S_2 \subset \{0,1\}^n$ be sets and $p(\ )$ a prob. dist. on $\{0,1\}^n$.
If $p(S_1), p(S_2) \geq \mu$, then minimum q. ckt. depth to generate p

is $$\Omega\left(\log\left(\frac{\mathrm{dist}(S_1, S_2)^2 \cdot \mu}{n}\right)\right).$$

Local indistinguishability

Theorem Let $S_1, S_2 \subset \{0,1\}^n$ be sets and $p(\ )$ a prob. dist. on $\{0,1\}^n$.

If $p(S_1), p(S_2) \geq \mu$, then minimum q. ckt. depth to generate p

is $$\Omega\left(\log\left(\frac{\mathrm{dist}(S_1,S_2)^2 \cdot \mu}{n}\right)\right).$$

When $\mathrm{dist}(S_1,S_2) \geq \omega(\sqrt{n})$ and $\mu = \Omega(1)$,

we call such distributions well spread. To prove NLTS, we need to show $\exists$ a local Hamiltonians whose entire low-energy subspace induces well-spread distributions.

Expanding codes & Tanner codes

A linear code $\subseteq \{0,1\}^n$ can be expressed as $\ker H$ for $H \in \mathbb{F}_2^{m \times n}$

Expanding codes & Tanner codes

$$\begin{pmatrix} & H & \end{pmatrix} \begin{pmatrix} \\ x \\ \\ \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}$$

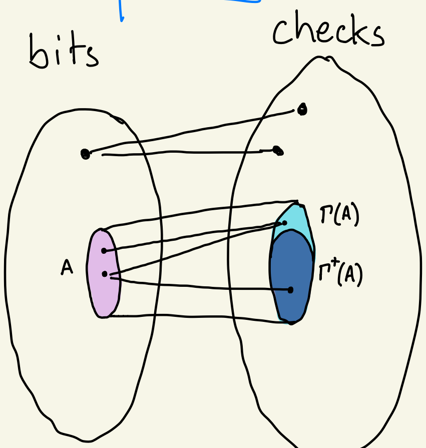
A linear code $\subseteq \{0,1\}^n$ can be expressed as $\ker H$ for $H \in \mathbb{F}_2^{m \times n}$

Expanding codes & Tanner codes

$$\begin{pmatrix} & H & \end{pmatrix}\begin{pmatrix} x \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}$$

A linear code $\subseteq \{0,1\}^n$ can be expressed as $\ker H$ for $H \in \mathbb{F}_2^{m \times n}$

We can draw the adjacency graph corresponding to H.

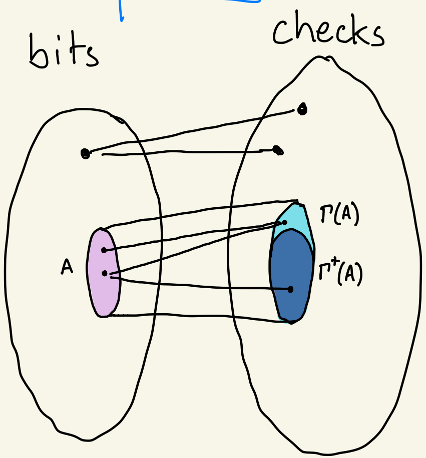


Expanding codes & Tanner codes

$$\begin{pmatrix} & H & \end{pmatrix}\begin{pmatrix} x \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}$$

A linear code $\subseteq \{0,1\}^n$ can be expressed as $\ker H$ for $H \in \mathbb{F}_2^{m \times n}$

We can draw the adjacency graph corresponding to H.



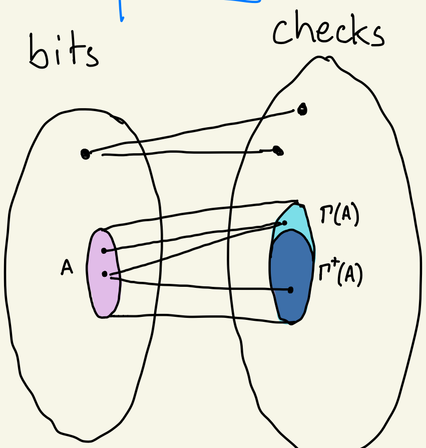
If the graph is small-set expanding, $\Gamma(A) \geq (1-\gamma) d |A|$ for all $|A| \leq c_2 n$, then the low-energy subspace of the code clusters into far-apart regions.

Expanding codes & Tanner codes

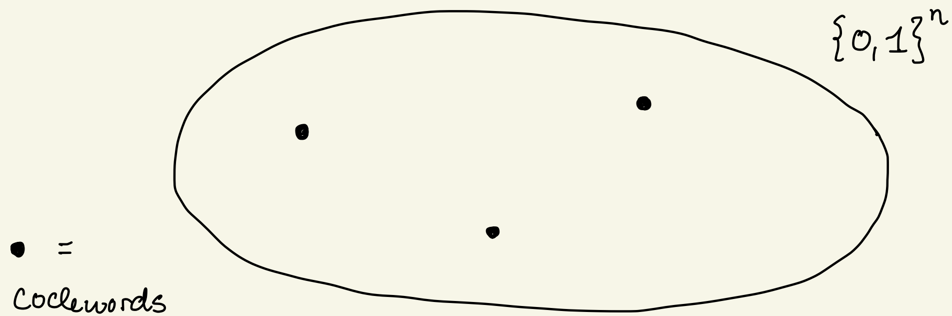
$$\begin{pmatrix} & H & \end{pmatrix}\begin{pmatrix} x \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}$$

A linear code $\subseteq \{0,1\}^n$ can be expressed as $\ker H$ for $H \in \mathbb{F}_2^{m \times n}$

We can draw the adjacency graph corresponding to H.



If the graph is small-set expanding, $\Gamma(A) \geq (1-\gamma) d |A|$ for all $|A| \leq c_2 n$, then the low-energy subspace of the code clusters into far-apart regions.

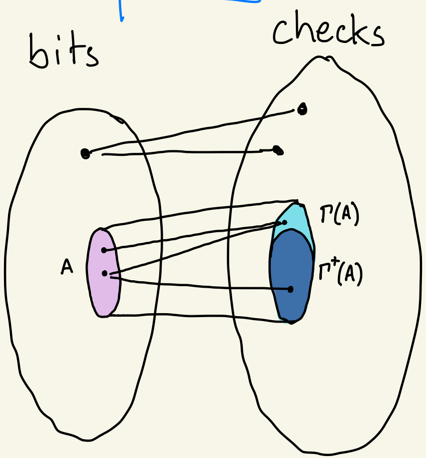


Expanding codes & Tanner codes

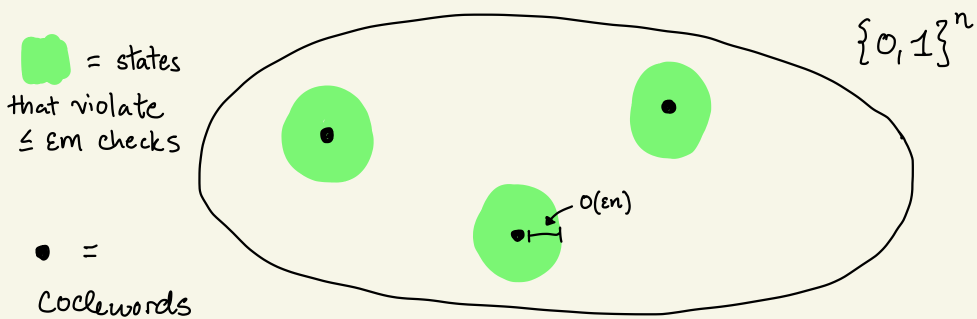
$$\begin{pmatrix} & H & \end{pmatrix}\begin{pmatrix} x \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}$$

A linear code $\subseteq \{0,1\}^n$ can be expressed as $\ker H$ for $H \in \mathbb{F}_2^{m \times n}$

We can draw the adjacency graph corresponding to H.



If the graph is small-set expanding, $|\Gamma(A)| \geq (1-\gamma) d |A|$ for all $|A| \leq c_2 n$, then the low-energy subspace of the code clusters into far-apart regions.

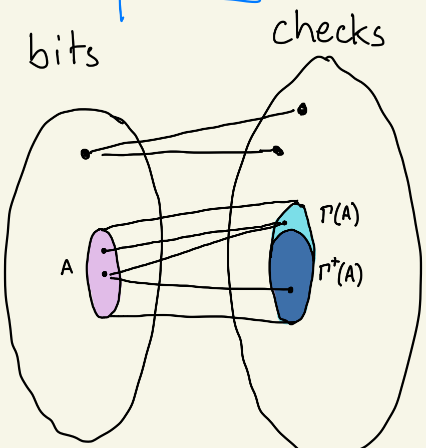


Expanding codes & Tanner codes

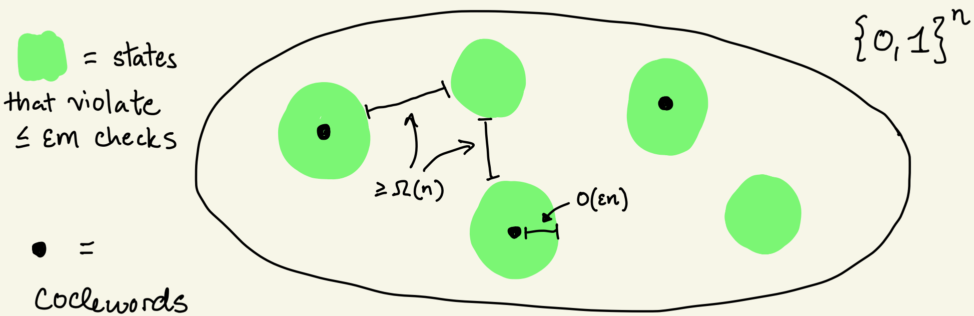
$$\begin{pmatrix} & H & \end{pmatrix}\begin{pmatrix} x \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}$$

A linear code $\subseteq \{0,1\}^n$ can be expressed as $\ker H$ for $H \in \mathbb{F}_2^{m \times n}$

We can draw the adjacency graph corresponding to H.



If the graph is small-set expanding, $\Gamma(A) \geq (1-\gamma)d|A|$ for all $|A| \leq c_2 n$, then the low-energy subspace of the code clusters into far-apart regions.

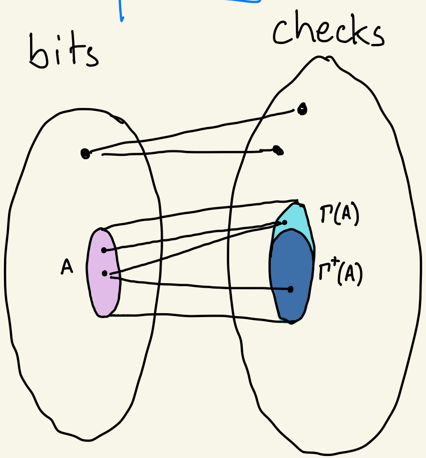


Expanding codes & Tanner codes

$$\begin{pmatrix} & H & \end{pmatrix}\begin{pmatrix} x \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}$$

A linear code $\subseteq \{0,1\}^n$ can be expressed as $\ker H$ for $H \in \mathbb{F}_2^{m \times n}$

We can draw the adjacency graph corresponding to H.



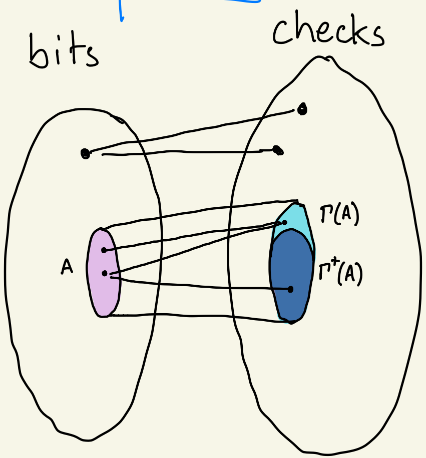
If the graph is small-set expanding, $\Gamma(A) \geq (1-\gamma) d|A|$ for all $|A| \leq c_2 n$, then the low-energy subspace of the code clusters into far-apart regions.

Expanding codes & Tanner codes

$$\begin{pmatrix} & H & \end{pmatrix}\begin{pmatrix} x \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}$$

A linear code $\subseteq \{0,1\}^n$ can be expressed as $\ker H$ for $H \in \mathbb{F}_2^{m\times n}$

We can draw the adjacency graph corresponding to H.



If the graph is small-set expanding, $\Gamma(A) \geq (1-\gamma)d|A|$ for all $|A| \leq c_2 n$, then the low-energy subspace of the code clusters into far-apart regions.

For all $y \in \{0,1\}^n$ s.t. $|Hy| \leq \varepsilon m$, then either

(1) $|y| \leq c_1 \cdot \varepsilon n$ or (2) $|y| \geq c_2 n$

Expanding codes & Tanner codes

$$\begin{pmatrix} & H & \end{pmatrix}\begin{pmatrix} x \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}$$

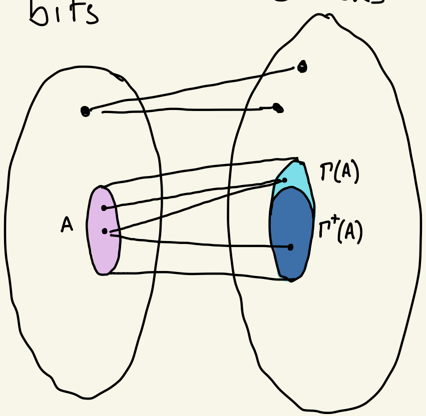
A linear code $\subseteq \{0,1\}^n$ can be expressed as $\ker H$ for $H \in \mathbb{F}_2^{m \times n}$

We can draw the adjacency graph corresponding to H.

For all $y \in \{0,1\}^n$ s.t. $|Hy| \leq \varepsilon m$, then either

① $|y| \leq c_1 \cdot \varepsilon n$ or ② $|y| \geq c_2 n$

bits checks



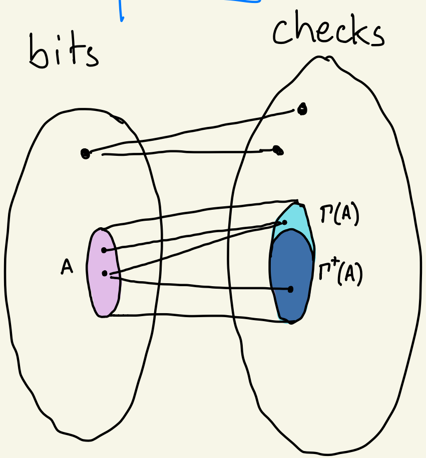
γ- expanding

Expanding codes & Tanner codes

$$\begin{pmatrix} & H & \end{pmatrix}\begin{pmatrix} x \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}$$

A linear code $\subseteq \{0,1\}^n$ can be expressed as $\ker H$ for $H \in \mathbb{F}_2^{m \times n}$

We can draw the adjacency graph corresponding to H.



γ- expanding

For all $y \in \{0,1\}^n$ s.t. $|Hy| \leq \varepsilon m$, then either

① $|y| \leq c_1 \cdot \varepsilon n$ or ② $|y| \geq c_2 n$

Pf sketch: $A = \mathrm{supp}(y)$. $\Gamma^+(A)$ = unique neighbors of $|A|$.
$|\Gamma^+(A)| \geq (1-2\gamma) d |A|$. Every check in $\Gamma^+(A)$ will flag. So $|Hy| \geq (1-2\gamma) d |y|$ unless $|y| \geq c_2 n$.

Expanding codes & Tanner codes

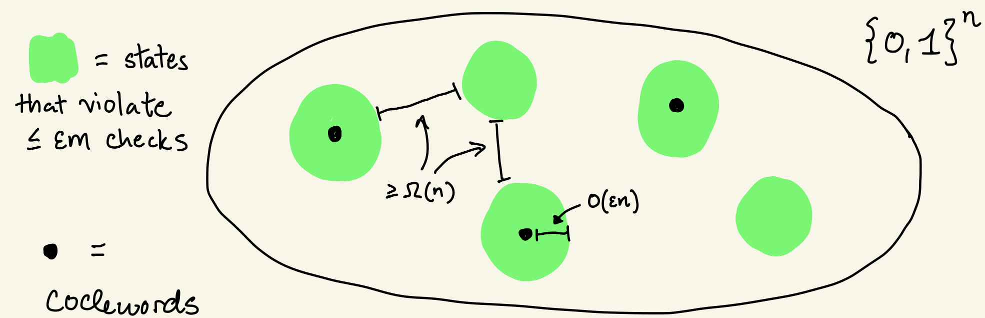
$$\begin{pmatrix} & H & \end{pmatrix} \begin{pmatrix} \\ x \\ \\ \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}$$

A linear code $\subseteq \{0,1\}^n$ can be expressed as $\ker H$ for $H \in \mathbb{F}_2^{m \times n}$

Expanding codes & Tanner codes

$$\begin{pmatrix} & H & \end{pmatrix}\begin{pmatrix} x \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}$$

A linear code $\subseteq \{0,1\}^n$ can be expressed as $\ker H$ for $H \in \mathbb{F}_2^{m \times n}$

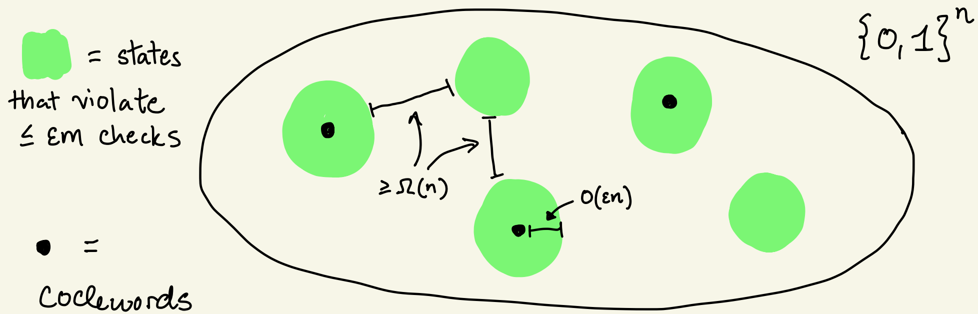


Expanding codes & Tanner codes

$$\begin{pmatrix} & H & \end{pmatrix}\begin{pmatrix} x \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}$$

A linear code $\subseteq \{0,1\}^n$ can be expressed as $\ker H$ for $H \in \mathbb{F}_2^{m \times n}$

The low-energy space of a code is a great support for a distribution that we hope to prove is well-spread.

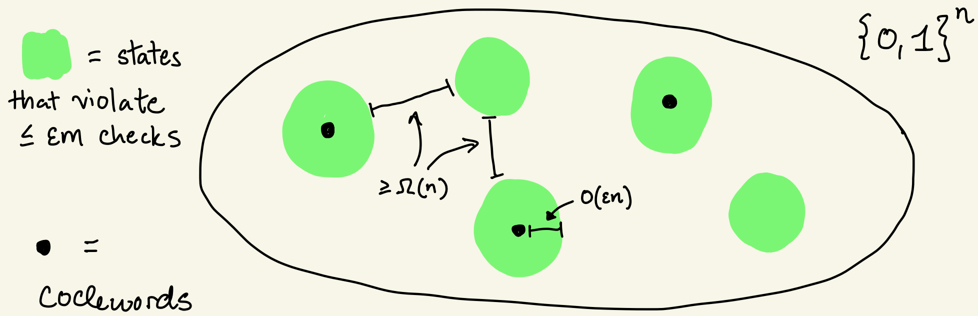


Expanding codes & Tanner codes

$$\begin{pmatrix} & H & \end{pmatrix} \begin{pmatrix} x \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}$$

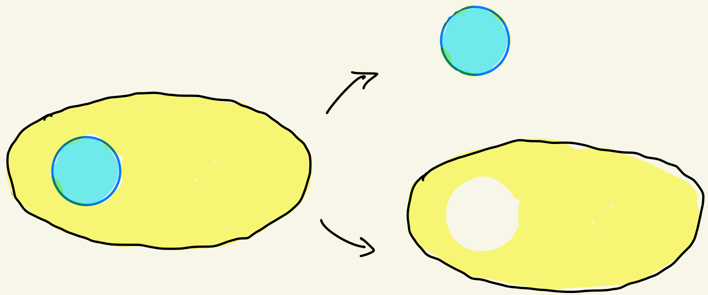
A linear code $\subseteq \{0,1\}^n$ can be expressed as $\ker H$ for $H \in \mathbb{F}_2^{m \times n}$

The low-energy space of a code is a *great* support for a distribution that we hope to prove is well-spread.



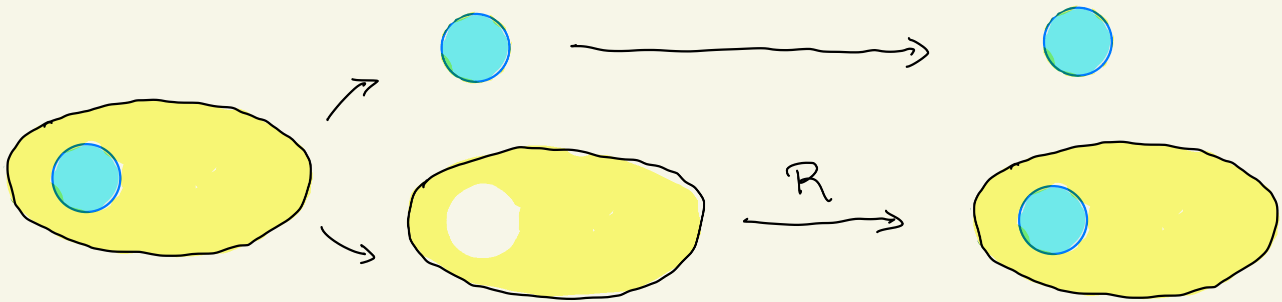
Only question is how to construct Hamiltonian with such property?

Quantum error correcting codes



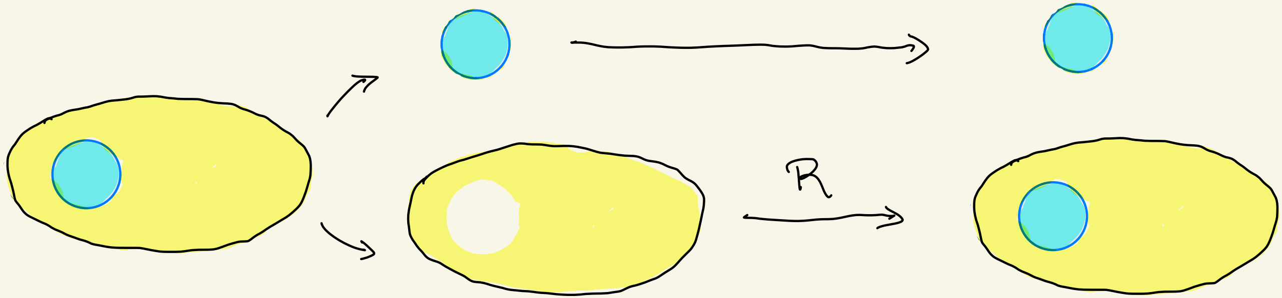
Consider a state subject to an erasure error.

Quantum error correcting codes

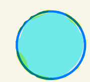


Consider a state subject to
an erasure error.

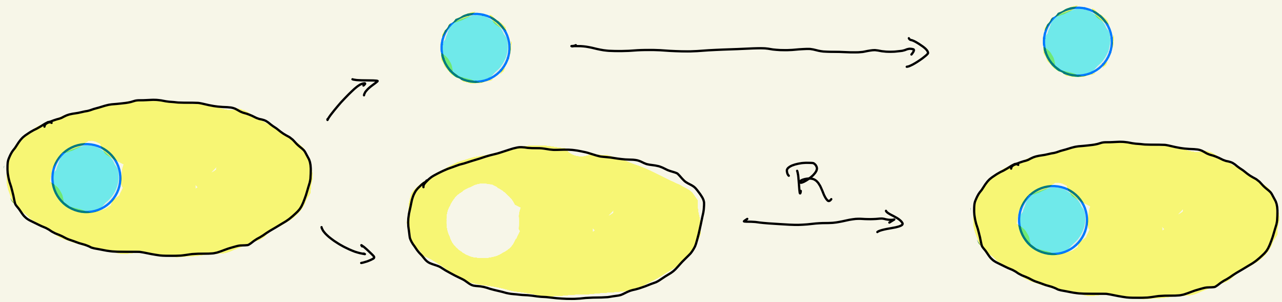
Quantum error correcting codes



Consider a state subject to an erasure error.

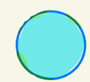
If we could recover the original state then unless  contains no information about the original state, this violates the no-cloning theorem.

Quantum error correcting codes



Consider a state subject to an erasure error.

> Erasure error-correction implies local indistinguishability for codes.

If we could recover the original state then unless  contains no information about the original state, this violates the no-cloning theorem.

Quantum error correcting codes

$$\boxed{\text{Erasure error-correction implies local indistinguishability for codes.}}$$

Quantum error correcting codes

$\boxed{\text{Erasure error-correction implies local indistinguishability for codes.}}$

Exact codewords of codes of distance d require circuits of depth $\geq \Omega(\log d)$ to generate.

Quantum error correcting codes

$\boxed{\text{Erasure error-correction implies local indistinguishability for codes.}}$

Exact codewords of codes of distance d require circuits of depth $\geq \Omega(\log d)$ to generate.

Error-correcting codes that are LDPC naturally have a local Hamiltonian, one that applies every local check.

Quantum error correcting codes

Erasure error-correction implies local indistinguishability for codes.

Exact codewords of codes of distance d require circuits of depth $\geq \Omega(\log d)$ to generate.

Error-correcting codes that are LDPC naturally have a local Hamiltonian, one that applies every local check.

How do we prove circuit depth lower bounds for the low-energy subspace of these code Hamiltonians?

Optimal-parameter CSS codes

There is a class of q. codes called Calderbank-Shor-Steane codes that correct for X-type (bit-flip) and Z-type (phase-flip) errors separately.

Optimal-parameter CSS codes

There is a class of q. codes called Calderbank-Shor-Steane codes that correct for X-type (bit-flip) and Z-type (phase-flip) errors separately.

They are constructed from two classical codes C_X, C_Z (w. check-matrix H_X, H_Z) s.t. $C_X^\perp \subseteq C_Z$ (equiv. $C_Z^\perp \subseteq C_X$).

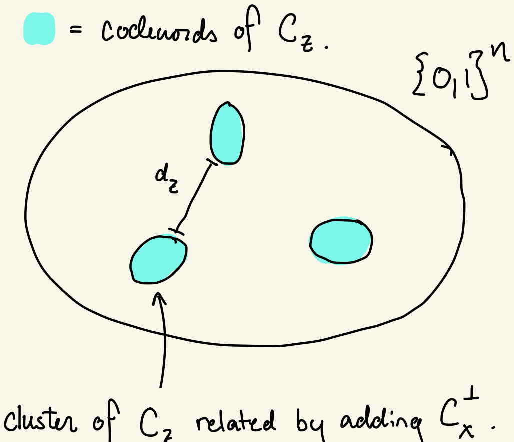
Optimal-parameter CSS codes

There is a class of q. codes called Calderbank-Shor-Steane codes that correct for X-type (bit-flip) and Z-type (phase-flip) errors separately.

They are constructed from two classical codes C_X, C_Z (w. check-matrix H_X, H_Z) s.t. $C_X^\perp \subseteq C_Z$ (equiv. $C_Z^\perp \subseteq C_X$).

$$d_Z = \min_{w \in C_Z} |w|_{C_X^\perp}, \quad d_X = \min_{w \in C_X} |w|_{C_Z^\perp}$$

where $|w|_S = \min_{w' \in S} |w + w'|$.



Optimal-parameter CSS codes

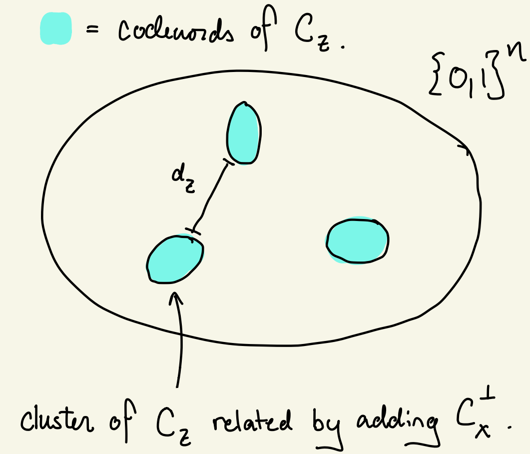
There is a class of q. codes called Calderbank-Shor-Steane codes that correct for X-type (bit-flip) and Z-type (phase-flip) errors separately.

They are constructed from two classical codes C_X, C_Z (w. check-matrix H_X, H_Z) s.t. $C_X^\perp \subseteq C_Z$ (equiv. $C_Z^\perp \subseteq C_X$).

$$d_Z = \min_{w \in C_Z} |w|_{C_X^\perp} \quad , \quad d_X = \min_{w \in C_X} |w|_{C_Z^\perp}$$

where $|w|_S = \min_{w' \in S} |w + w'|$.

$$d = \min \{ d_X, d_Z \}.$$

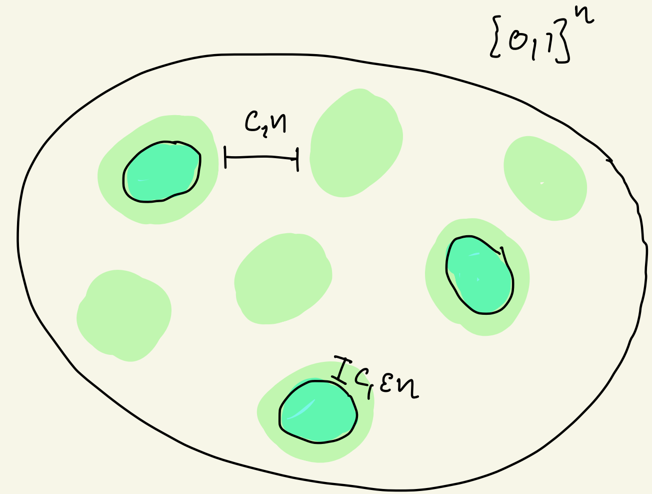


Expanding CSS codes

Similar to classical example, we consider codes that have the property that if $|H_z y| \leq \varepsilon m$ then either

① $|y|_{C_x^\perp} \leq c_1 \varepsilon n$ or

② $|y|_{C_x^\perp} \geq c_2 n$.

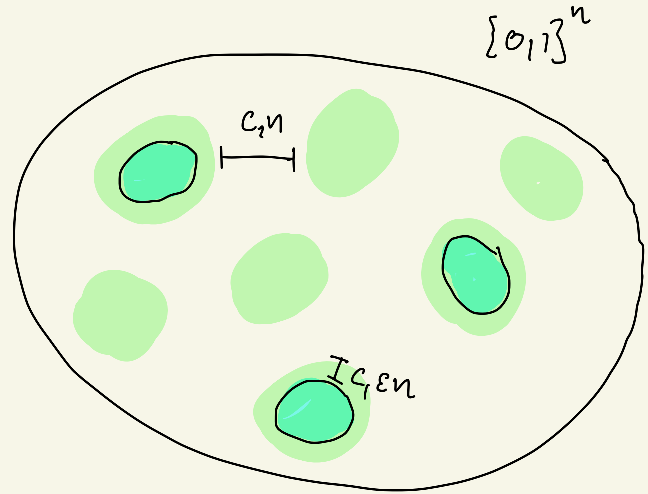


Expanding CSS codes

Similar to classical example, we consider codes that have the property that if $|H_z y| \leq \varepsilon m$ then either

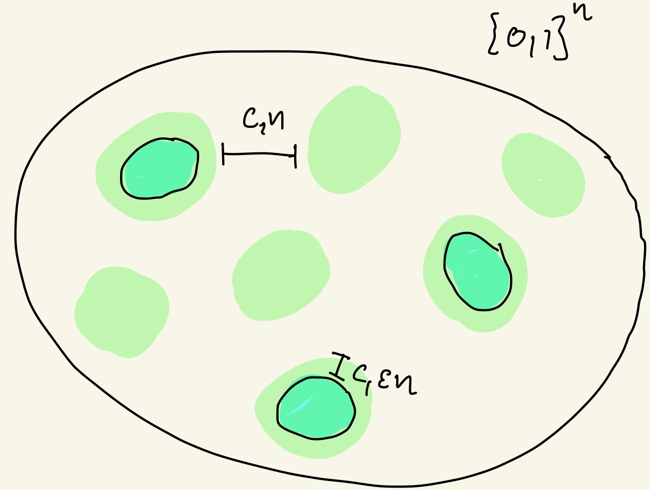
① $|y|_{C_x^\perp} \leq c_1 \varepsilon n$ or

② $|y|_{C_x^\perp} \geq c_2 n$.

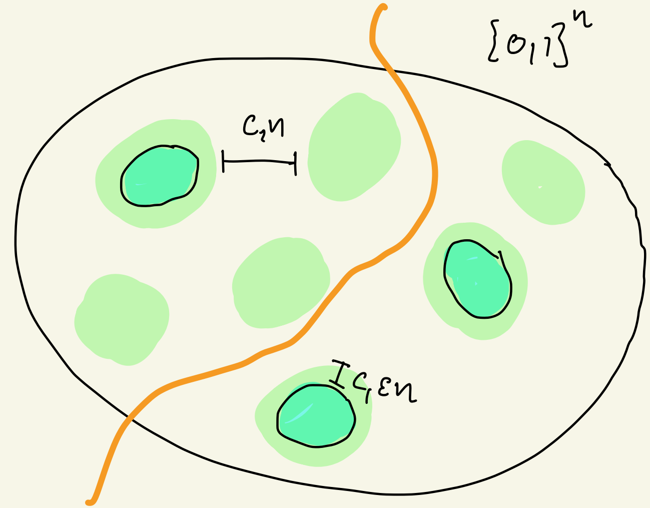


And, if we consider a $\frac{\varepsilon}{200}$-low-energy state of the code's local Hamiltonian, measuring in the Z-basis yields a dist. 99.5% supported on .

The uncertainty principle

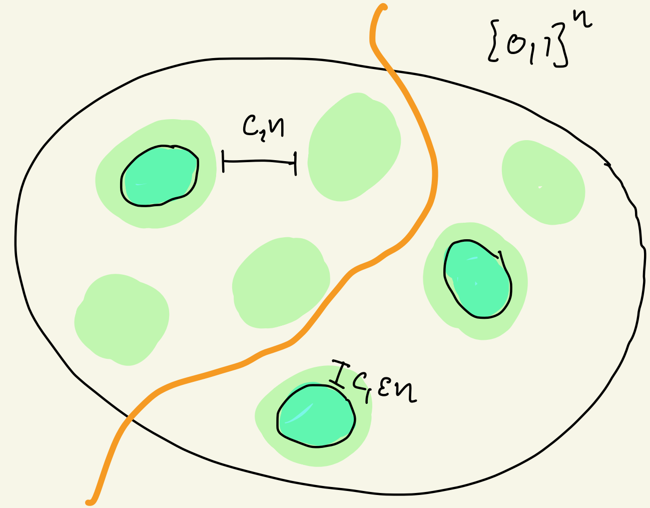


The uncertainty principle



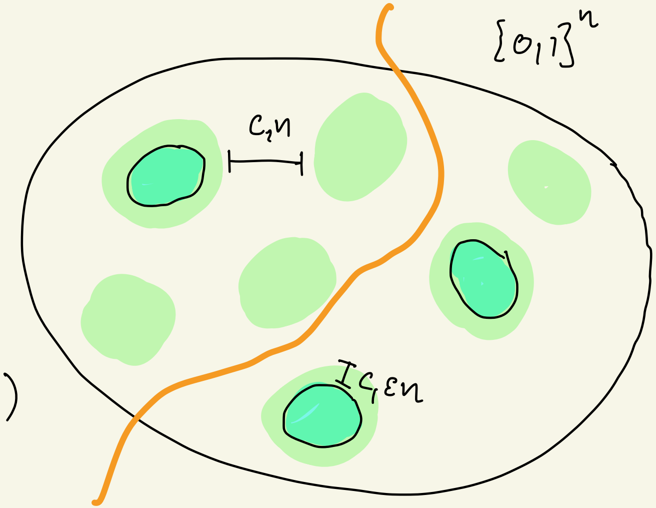
The uncertainty principle

All that remains to show is that the distribution is not 99% concentrated on any 1 cluster.



The uncertainty principle

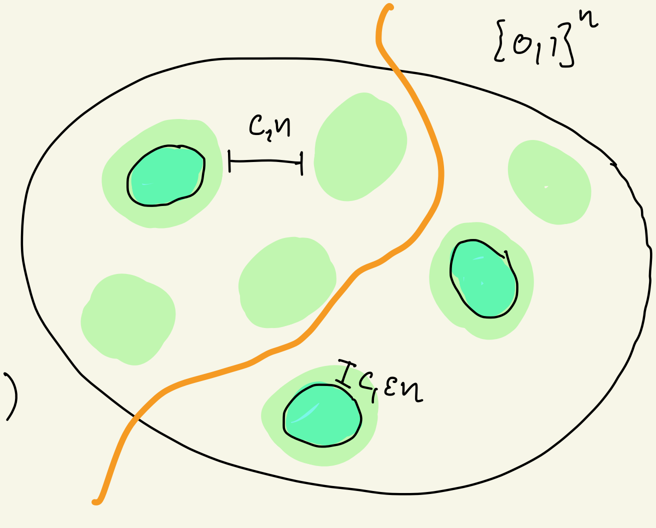
All that remains to show is that the distribution is not 99% concentrated on any 1 cluster. $\Rightarrow$ dist. is well-spread ($\mu = \frac{1}{400}$)



The uncertainty principle

All that remains to show is that the distribution is not 99% concentrated on any 1 cluster. $\Rightarrow$ dist. is well-spread ($\mu = \frac{1}{400}$)

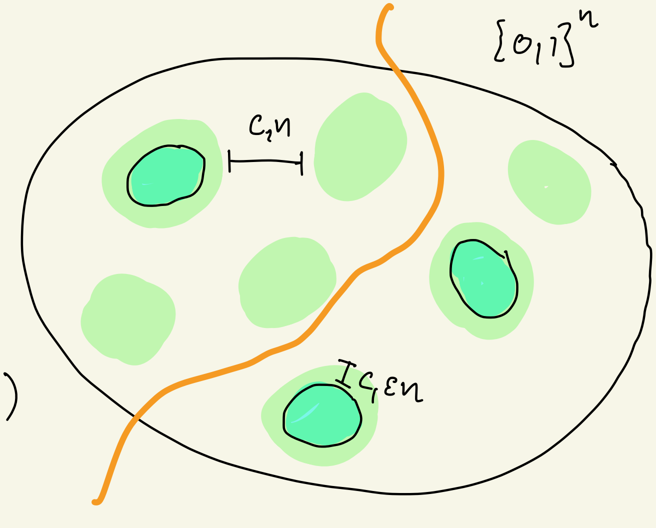
$\Rightarrow$ circuit depth lower bound.



The uncertainty principle

All that remains to show is that the distribution is not 99% concentrated on any 1 cluster. $\Rightarrow$ dist. is well-spread ($\mu = \frac{1}{400}$)

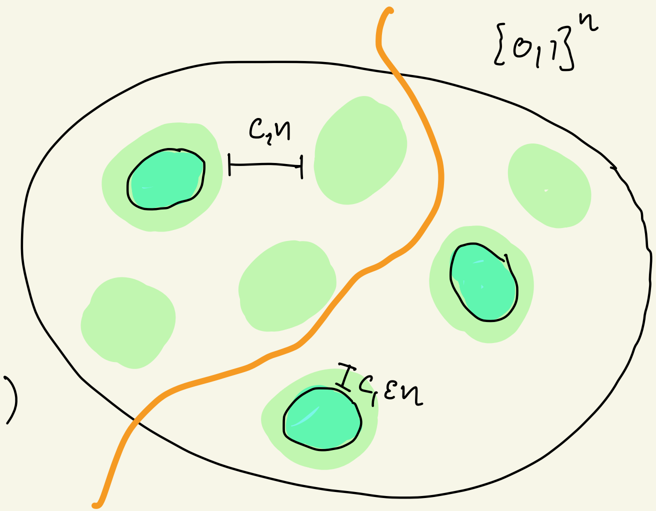
$\Rightarrow$ circuit depth lower bound.



Uncertainty principle: For sets $S, T \subseteq \{0,1\}^n$, any state Ψ with dists. D_x, D_z

$$D_x(T) \leq 2\sqrt{1 - D_z(S)} + \sqrt{\frac{|S| \cdot |T|}{2^n}}$$

The uncertainty principle



All that remains to show is that the distribution is not 99% concentrated on any 1 cluster. $\Rightarrow$ dist. is well-spread $\left(\mu = \frac{1}{400}\right)$

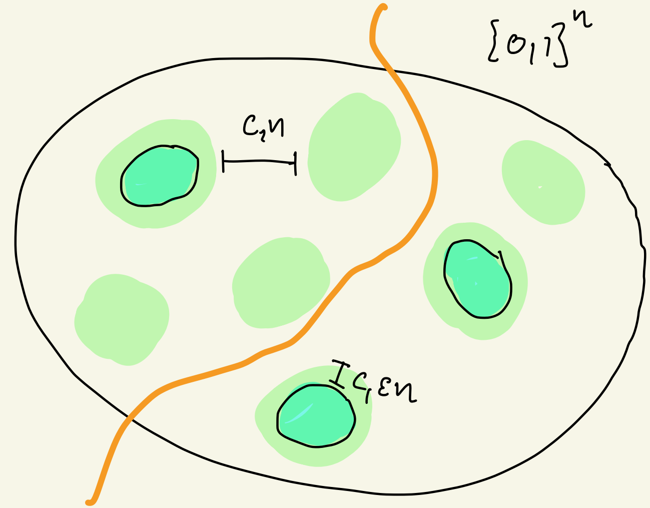
$\Rightarrow$ circuit depth lower bound.

Uncertainty principle: For sets $S, T \subseteq \{0,1\}^n$, any state Ψ with dists. D_x, D_z

$$D_x(T) \leq 2\sqrt{1 - D_z(S)} + \sqrt{\frac{|S| \cdot |T|}{2^n}}$$

Assume D_z is $\geq 99\%$ concentrated on some Z-cluster S. Then for any X-cluster T, $D_x(T) < 0.99$ $\Rightarrow$ Either D_x or D_z is well-spread.

The uncertainty principle



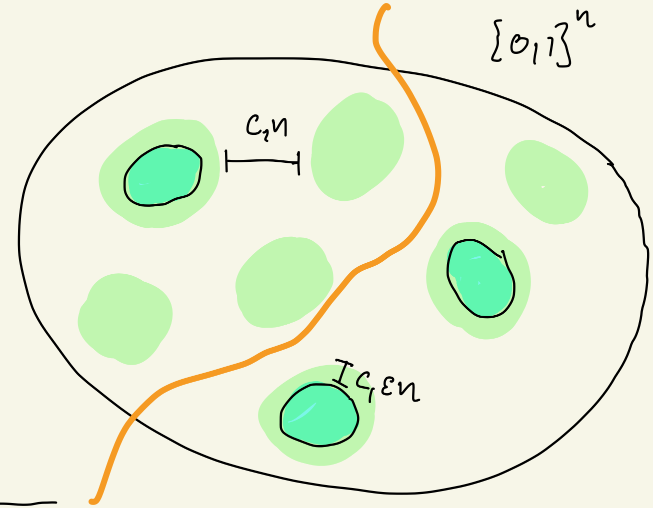
Uncertainty principle: For sets $S, T \subseteq \{0,1\}^n$, any state Ψ with dists. D_X, D_Z

$$D_X(T) \leq 2\sqrt{1 - D_Z(S)} + \sqrt{\frac{|S| \cdot |T|}{2^n}}$$

Assume D_Z is $\geq 99\%$ concentrated on some Z-cluster S. Then for any X-cluster T, $D_X(T) < 0.99$ $\Rightarrow$ Either D_X or D_Z is well-spread.

The uncertainty principle

$$|S| \le \underbrace{\binom{n}{O(\varepsilon n)}}_{\text{violate check}} \cdot \underbrace{2^{r_x}}_{C_x^{\perp}\text{ def!}}$$



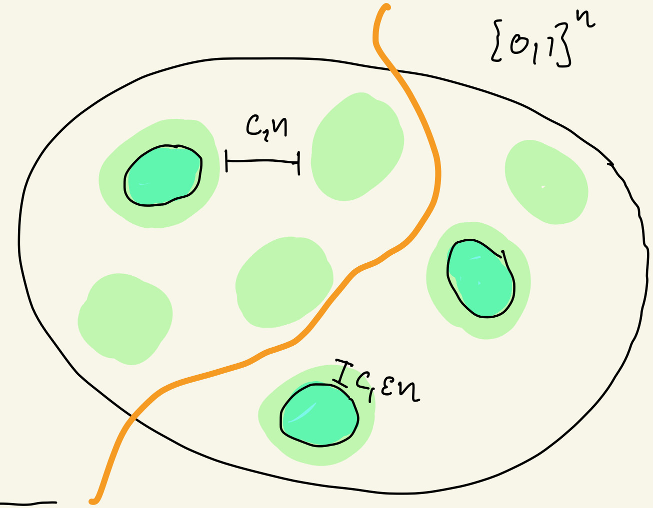
Uncertainty principle: For sets $S, T \subseteq \{0,1\}^n$, any state Ψ with dists. D_x, D_z

$$D_x(T) \le 2\sqrt{1 - D_z(S)} + \sqrt{\frac{|S|\cdot|T|}{2^n}}$$

Assume D_z is $\geq 99\%$ concentrated on some Z-cluster S. Then for any X-cluster T, $D_x(T) < 0.99$ $\Rightarrow$ Either D_x or D_z is well-spread.

The uncertainty principle

$$|S| \leq \underbrace{\binom{n}{O(\varepsilon n)}}_{\text{violate check}} \cdot \underbrace{2^{r_x}}_{C_x^\perp \text{ def!}} \leq 2^{r_x + O(\sqrt{\varepsilon}\, n)}$$



Uncertainty principle: For sets $S, T \subseteq \{0,1\}^n$, any state Ψ with dists. D_x, D_z

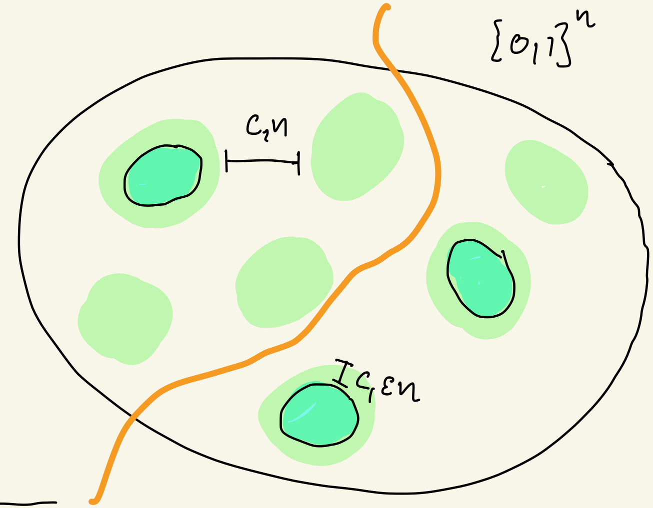
$$D_x(T) \leq 2\sqrt{1 - D_z(S)} + \sqrt{\frac{|S| \cdot |T|}{2^n}}$$

Assume D_z is $\geq 99\%$ concentrated on some Z-cluster S. Then for any X-cluster T, $D_x(T) < 0.99$ $\Rightarrow$ Either D_x or D_z is well-spread.

The uncertainty principle

$$|S| \le \underbrace{\binom{n}{O(\varepsilon n)}}_{\text{violate check}} \cdot \underbrace{2^{r_x}}_{C_x^\perp \text{ def!}} \le 2^{r_x + O(\sqrt{\varepsilon}\, n)}$$

$$|T| \le 2^{r_z + O(\sqrt{\varepsilon}\, n)}$$



Uncertainty principle: For sets $S, T \subseteq \{0,1\}^n$, any state ψ with dists. D_x, D_z

$$D_x(T) \le 2\sqrt{1 - D_z(S)} + \sqrt{\frac{|S| \cdot |T|}{2^n}}$$

Assume D_z is $\ge 99\%$ concentrated on some Z-cluster S. Then for any X-cluster T, $D_x(T) < 0.99$ $\Rightarrow$ Either D_x or D_z is well-spread.

The uncertainty principle

$$|S| \le \underbrace{\binom{n}{O(\varepsilon n)}}_{\text{violate check}} \cdot \underbrace{2^{r_X}}_{C_X^\perp \text{ def!}} \lesssim 2^{r_X + O(\sqrt{\varepsilon}\, n)}$$

$$|T| \le 2^{r_Z + O(\sqrt{\varepsilon}\, n)}$$

Uncertainty principle: For sets $S, T \subseteq \{0,1\}^n$, any state ψ with dists. D_X, D_Z

$$D_X(T) \le 2\sqrt{1 - D_Z(S)} + \sqrt{\frac{|S| \cdot |T|}{2^n}}$$

Assume D_Z is $\geq 99\%$ concentrated on some Z-cluster S. Then for any X-cluster T, $D_X(T) < 0.99 \implies$ Either D_X or D_Z is well-spread.

The uncertainty principle

$$|S| \le \underbrace{\binom{n}{O(\varepsilon n)}}_{\text{violate check}} \cdot \underbrace{2^{r_x}}_{C_x^\perp \text{ def!}} \le 2^{r_x + O(\sqrt{\varepsilon}\, n)}$$

$$|T| \le 2^{r_z + O(\sqrt{\varepsilon}\, n)}$$

$$D_x(T) \le 2\sqrt{\frac{1}{100}} + 2^{r_x + r_z + O(\sqrt{\varepsilon}\, n) - n}$$

Uncertainty principle: For sets $S, T \subseteq \{0,1\}^n$, any state Ψ with dists. D_x, D_z

$$D_x(T) \le 2\sqrt{1 - D_z(S)} + \sqrt{\frac{|S| \cdot |T|}{2^n}}$$

Assume D_z is $\ge 99\%$ concentrated on some Z-cluster S. Then for any X-cluster T, $D_x(T) < 0.99$ $\Rightarrow$ Either D_x or D_z is well-spread.

The uncertainty principle

$$|S| \le \underbrace{\binom{n}{O(\varepsilon n)}}_{\text{violate check}} \cdot \underbrace{2^{r_x}}_{C_x^\perp \text{ def!}} \le 2^{r_x + O(\sqrt{\varepsilon}\, n)}$$

$$|T| \le 2^{r_z + O(\sqrt{\varepsilon}\, n)}$$

$$D_x(T) \le 2\sqrt{\frac{1}{100}} + 2^{r_x + r_z + O(\sqrt{\varepsilon}\, n) - n}$$

$$= \frac{1}{5} + 2^{\overset{\uparrow}{\underset{\text{code rate}}{-k}} + O(\sqrt{\varepsilon}\, n)}$$

Uncertainty principle: For sets $S, T \subseteq \{0,1\}^n$, any state ψ with dists. D_x, D_z

$$D_x(T) \le 2\sqrt{1 - D_z(S)} + \sqrt{\frac{|S| \cdot |T|}{2^n}}$$

Assume D_z is $\ge 99\%$ concentrated on some Z-cluster S. Then for <u>any</u> X-cluster T, $D_x(T) < 0.99$ $\Rightarrow$ Either D_x or D_z is well-spread.

The uncertainty principle

$$|S| \leq \underbrace{\binom{n}{O(\varepsilon n)}}_{\text{violate check}} \cdot \underbrace{2^{r_x}}_{C_x^\perp \text{ def!}} \leq 2^{r_x + O(\sqrt{\varepsilon}\, n)}$$

$$|T| \leq 2^{r_z + O(\sqrt{\varepsilon}\, n)}$$

$$D_x(T) \leq 2\sqrt{\frac{1}{100}} + 2^{r_x + r_z + O(\sqrt{\varepsilon}\, n) - n}$$

$$= \frac{1}{5} + 2^{-k + O(\sqrt{\varepsilon}\, n)}$$

Code rate

So if $\varepsilon < O\left(\frac{k^2}{n^2}\right)$, then $D_x(T) < 0.99$.

Uncertainty principle: For sets $S, T \subseteq \{0,1\}^n$, any state Ψ with dists. D_x, D_z

$$D_x(T) \leq 2\sqrt{1 - D_z(S)} + \sqrt{\frac{|S| \cdot |T|}{2^n}}$$

Assume D_z is $\geq 99\%$ concentrated on some Z-cluster S. Then for any X-cluster T, $D_x(T) < 0.99$ $\Rightarrow$ Either D_x or D_z is well-spread.

Conclusion of the proof

CSS code of linear-rate and linear-distance which are expanding are NLTS.

any state violating ϵn checks cannot be the output of a constant depth ckt.

Conclusion of the proof

CSS code of linear-rate and linear-distance which are expanding are NLTS.

any state violating εn checks cannot be the output of a constant depth ckt.

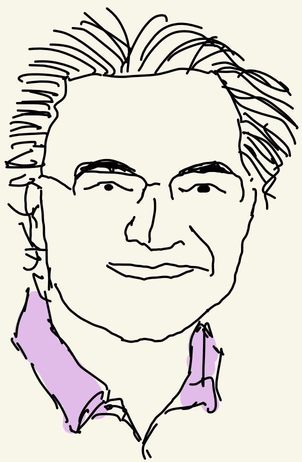
QPCP conjecture implications

1. Much harder to disprove QPCP now!

2. We need a stronger classical ansatz for classical proofs of local Hamiltonians.

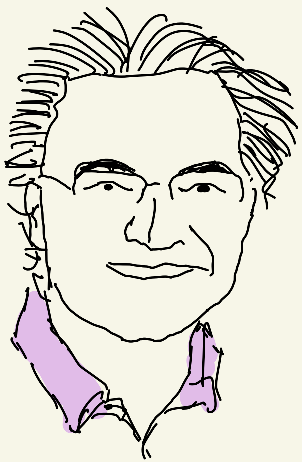
Acknowledgments

Acknowledgments: Incredible Advisors



Umesh Vazirani

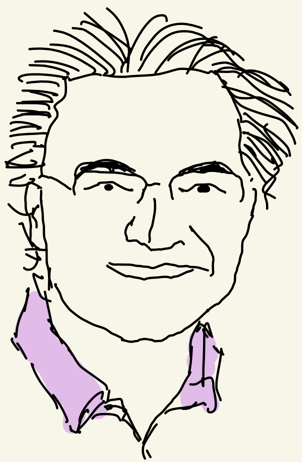
Acknowledgments: Incredible Advisors



Umesh Vazirani

Zeph Landau

Acknowledgments: Incredible Advisors

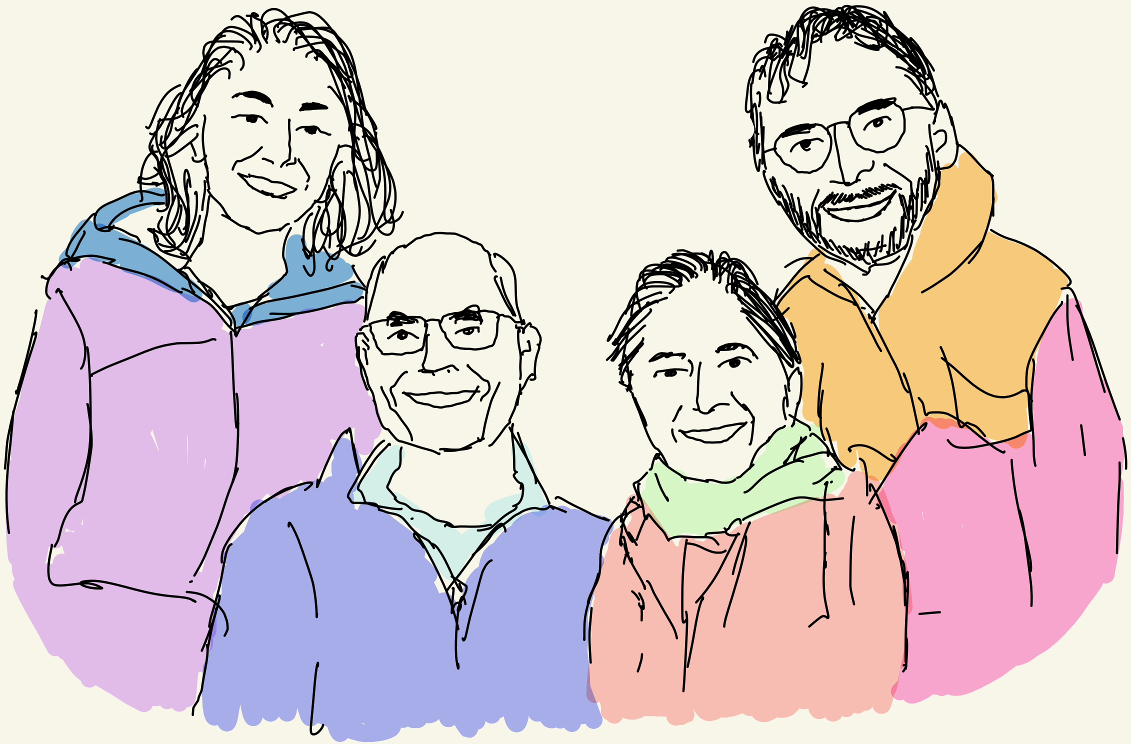


Umesh Vazirani

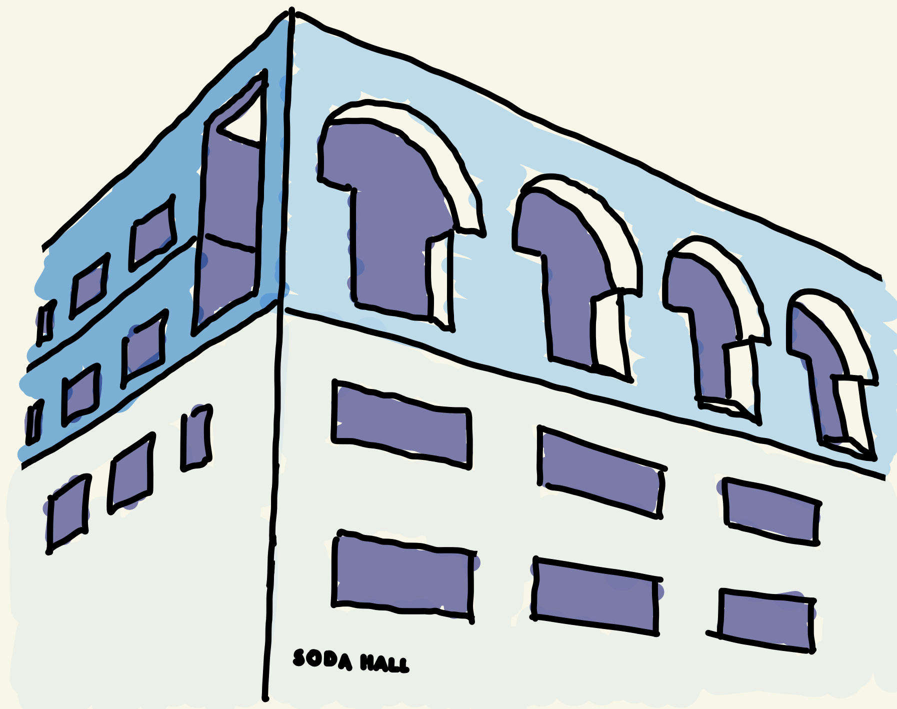
Zeph Landau

Anurag Anshu

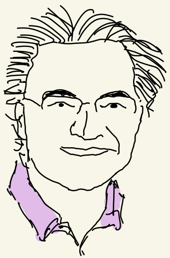
Acknowledgments: My wonderful family



Acknowledgments: The best research environment

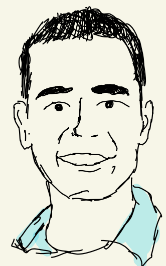


Acknowledgments



Umesh Vazirani

Zeph Landau



Anurag Anshu