Approximate low-weight check codes and circuit lower bounds for noisy ground states

Chinmay Nirkhe

nirkhe@cs.berkeley.edu

arXiv:1802.07419

Chinmay Nirkhe

Umesh Vazirani

Henry Yuen

Berkeley
UNIVERSITY OF CALIFORNIA

Robustness of proofs

How much of a classical proof does one need to read to ensure that it is correct?
For 100% confidence, the whole proof.

This notion was however shattered by the
Probabilistically checkable proofs (PCP) theorem [Arora et. al.[98],Dinur[07]].

It states that if one writes the proof down in a special way, then
for 99% confidence, only a constant number of bits need to be read!

Does a quantum version of the PCP theorem hold?

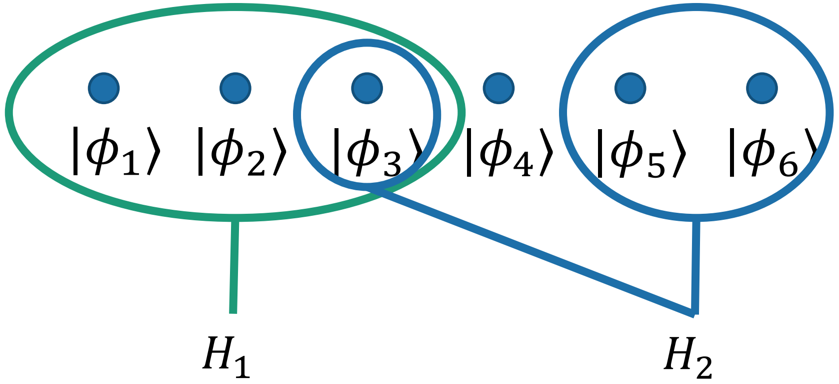
Can quantum computation be done at room- temperature?

Do quantum low-density parity-check codes exist?

These questions may share a common answer!

A quantum perspective on the classical PCP theorem

The Local Hamiltonian Problem



$|\phi_i\rangle \in \mathbb{C}^2$

Each H_j acts non-trivially on only a constant number of terms.

$\|H_j\| \leq 1$

$$H = \sum_{j=1}^{m} H_j$$

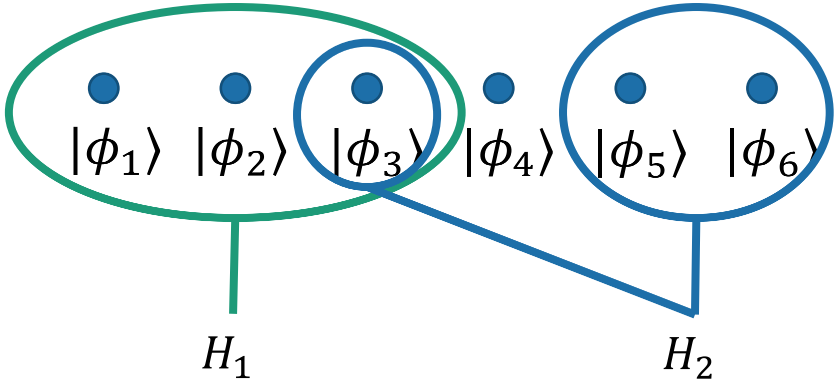
Minimum energy

$$\mathrm{E} = \inf_{|\phi\rangle\in(\mathbb{C}^2)^{\otimes n}} \langle\phi|H|\phi\rangle = \inf_{|\phi\rangle\in(\mathbb{C}^2)^{\otimes n}} \sum_{j=1}^{m} \langle\phi|H_j|\phi\rangle$$

Given a local Hamiltonian H, estimate its minimum energy E.

A quantum perspective on the classical PCP theorem

Constraint Satisfaction Problems (CSPs)



$|\phi_i\rangle \in \mathbb{C}^2$

Each H_j acts non-trivially on only a constant number of terms.

$\|H_j\| \leq 1$

$$H = \sum_{j=1}^{m} H_j$$

Minimum energy

$$\mathrm{E} = \inf_{|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}} \langle \phi | H | \phi \rangle = \inf_{|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}} \sum_{j=1}^{m} \langle \phi | H_j | \phi \rangle$$

H_j can be expressed as a diagonal matrix on the elements is acts non-trivially on.

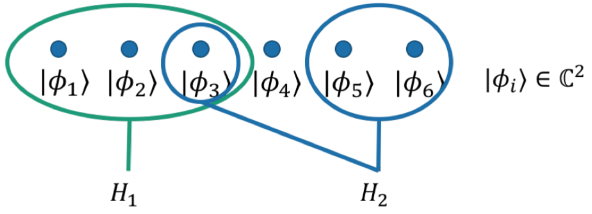
$\Longrightarrow$

The eigenvectors of H are the computational basis.

PCP theorem rephrased

NP-hardness of CSPs [Cook[71],Levin[73]].
It is NP-hard to estimate the energy E of a CSP to $\pm 1/2$.

PCP theorem [Arora et. al.[98],Dinur[07]].
It is NP-hard to estimate the energy E of a CSP to $\pm m/4$.



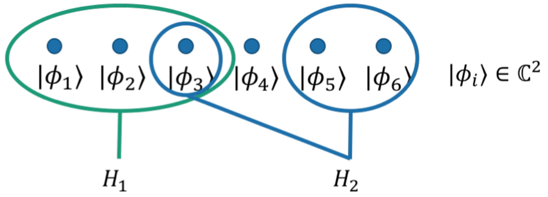
Minimum energy

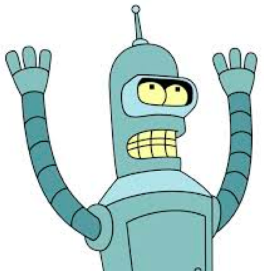
$$E = \inf_{|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}} \sum_{j=1}^{m} \langle \phi | H_j | \phi \rangle$$

Is there an analogous theorem about the hardness of estimating the energy of a local Hamiltonian problem?

QMA: Quantum Merlin-Arthur

Oh no! I don't know how to tell if this LH has energy $E = a \pm 1/2$





Infinitely powerful Quantum Prover

It does. Here is a proof: $|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$

Polynomial time Quantum Verifier

Hmm, nefarious robot… I don't know if I can trust you. But I can *probabilistically check* if your proof is correct.

Pick a LH term H_j at random.
Measure to calculate $\tilde{E} = \langle \phi | H_j | \phi \rangle$. (Only requires measuring local terms).

$$\mathbb{E}(m\tilde{E}) = E.$$

Repeating can give more accurate estimate.

QMA = set of problems for which there exists a *quantum* proof that can be efficiently checkable in *quantum* polynomial time.

Quantum hardness of LH

LH is QMA-hard [Kitaev[99]].

It is QMA-hard to estimate the energy of a local Hamiltonian H to $\pm\Omega(1/\mathrm{poly}(m))$.

qPCP conjecture [Aharanov-Naveh[02],Aaronson[06]].

It is QMA-hard to estimate the energy of a local Hamiltonian H to $\pm\Omega(m)$.

NP $\neq$ QMA

NLTS conjecture [Freedman-Hastings[14]].

There exists a family of local Hamiltonians $H^{(n)}$ acting on n particles and constant $\epsilon > 0$ such that $\forall|\xi\rangle$ with $\mathrm{E} = \langle\xi|H|\xi\rangle \leq \lambda_{\min}(H) + \epsilon m$, $|\xi\rangle$ cannot be generated by a constant-depth circuit.

Complexity of quantum states

Depth of minimum generating circuit

Minimum depth of any circuit C with 2-qubit gates s.t. $|\psi\rangle = C|0\rangle^{\otimes n}$.

Purely quantum notion

Every classical state $x \in \{0,1\}^n$ can be generated by depth 1 circuit: X^x.

If NP $\neq$ QMA,...

Groundstates $|\xi\rangle$ of QMA-hard local Hamiltonians H cannot be generated by constant-depth circuits.

NLTS conjecture [Freedman-Hastings[14]].
There exists a family of local Hamiltonians $H^{(n)}$ acting on n particles and constant $\epsilon > 0$ such that $\forall|\xi\rangle$ with $\mathrm{E} = \langle\xi|H|\xi\rangle \leq \lambda_{\min}(H) + \epsilon m$, $|\xi\rangle$ cannot be generated by a constant-depth circuit.

Robustness of entanglement

No low-energy trivial states (NLTS) conjecture [Freedman-Hastings[14]].
There exists a family of local Hamiltonians $H^{(n)}$ acting on n particles and constant $\epsilon > 0$ such that all $|\xi\rangle$ with $E \leq \lambda_{\min}(H) + \epsilon m$, $|\xi\rangle$ cannot be generated by a constant-depth circuit.

qLTCs implies NLTS [Eldar-Harrow[17]].
If one can construct a CSS qLTC, then NLTS follows.

(Classically, LTCs were a part of the proof of the PCP theorem).

No low-error trivial states (NLETS) theorem [Eldar-Harrow[17]].
There exists a family of local Hamiltonians $H^{(n)}$ acting on n particles and constant $\epsilon > 0$ such that for all ϵ-low-error states $|\xi\rangle$, $|\xi\rangle$ cannot be generated by a constant-depth circuit.

The goal today is to understand more about the robustness of highly-complex entanglement.

1. Notions of robustness of entanglement

2. Approximate error correction

Part 1:
Notions of robustness of entanglement

Are these notions the same?

No low-energy trivial states (NLTS) conjecture [Freedman-Hastings[14]].
There exists a family of local Hamiltonians $H^{(n)}$ acting on n particles and constant $\epsilon > 0$ such that $\forall |\xi\rangle$ with $E \leq \lambda_{\min}(H) + \epsilon m$, $|\xi\rangle$ cannot be generated by a constant-depth circuit.

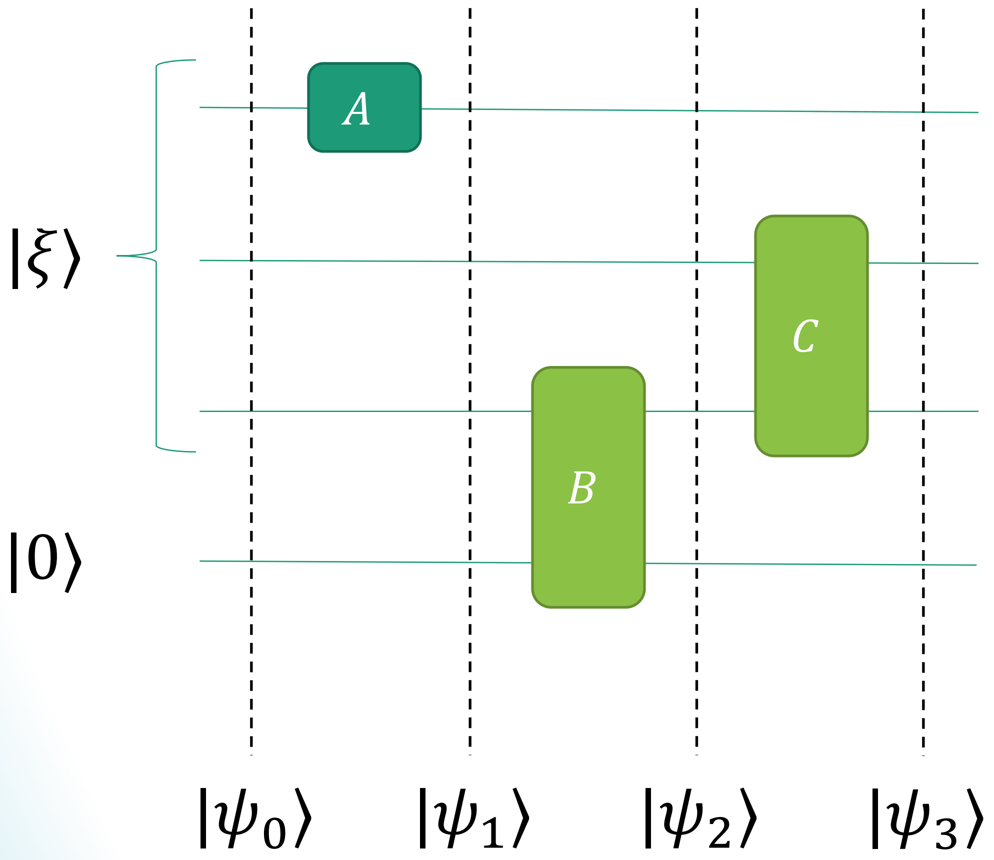
No low-error trivial states (NLETS) theorem [Eldar-Harrow[17]].
There exists a family of local Hamiltonians $H^{(n)}$ acting on n particles and constant $\epsilon > 0$ such that for all ϵ-low-error states $|\xi\rangle$, $|\xi\rangle$ cannot be generated by a constant-depth circuit.

Low-error state
A state $|\xi\rangle$ is a ϵ-low-error state for a local Hamiltonian H, if there exists a subset S of size $\leq \epsilon n$ of the particles and a groundstate $|\phi\rangle \in \mathcal{G}$ such that $\mathrm{Tr}_S\left(|\xi\rangle\langle\xi|\right) = \mathrm{Tr}_S\left(|\phi\rangle\langle\phi|\right)$.

Our contribution

A simpler construction of NLETS Hamiltonian that shows low-error is not the same as low-energy.

Circuit-to-Hamiltonian construction



$$|\psi_0\rangle = |\xi\rangle|0\rangle$$
$$|\psi_1\rangle = A|\psi_0\rangle$$
$$|\psi_2\rangle = B|\psi_1\rangle$$
$$|\psi_3\rangle = C|\psi_2\rangle$$

Together, $\{|\psi_t\rangle\}$ are a "proof" that the circuit was executed correctly.

But, $|\widetilde{\Psi}\rangle = |\psi_0\rangle|\psi_1\rangle \dots |\psi_T\rangle$ is not locally-checkable.

Instead, the following "clock" state* is:

$$|\Psi\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle|\psi_t\rangle$$

*Quantum analog of Cook[71]-Levin[73] Tableau.

Feynman-Kitaev Clock Hamiltonian

Express a computation as the groundstate of a 5-local Hamiltonian [Kitaev99]

Let $C = C_T C_{T-1} \dots C_1$ be a circuit with gates $\{C_i\}$ and let $|\psi_0\rangle = |\xi\rangle|0\rangle^{\otimes n-k}$ be an initial state for $|\xi\rangle \in (\mathbb{C}^2)^{\otimes k}$.

There is a local Hamiltonian with ground space of:

$$\mathcal{G} = \left\{ |\Psi_\xi\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |\mathrm{unary}(t)\rangle \otimes |\psi_t\rangle : \begin{array}{c} |\psi_t\rangle = C_t|\psi_{t-1}\rangle, \\ |\psi_0\rangle = |\xi\rangle|0\rangle^{\otimes(n-k)} \end{array} \right\}.$$

Used to prove that Local Hamiltonians is QMA-hard [Kitaev99].

Approximate |cat⟩ state

$$|\text{cat}_n\rangle = \frac{|0\rangle^{\otimes n} + |1\rangle^{\otimes n}}{\sqrt{2}}$$

Error states of cat states have $\Omega(\log n)$ circuit complexity

Let S be a subset of particles of size ϵn. Then,

$$\text{Tr}_S(|\text{cat}\rangle\langle\text{cat}|) = \frac{|0 \ldots 0\rangle\langle 0 \ldots 0| + |1 \ldots 1\rangle\langle 1 \ldots 1|}{2}.$$

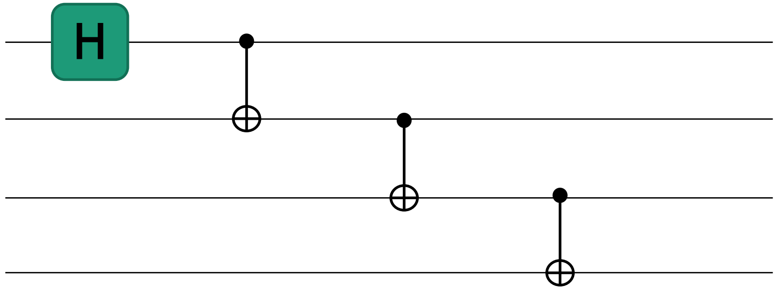
Information theoretic argument shows this state has $\Omega(\log n)$ circuit complexity.

But, cat states are not unique groundstates of local Hamiltonians...

Create a Hamiltonian whose groundspace is almost a cat state. This will preserve the low-error property.

Approximate $|\text{cat}\rangle$ state

$$|\text{cat}_n\rangle = \frac{|0\rangle^{\otimes n} + |1\rangle^{\otimes n}}{\sqrt{2}}$$



Generate the FK clock Hamiltonian for the circuit generating $|\text{cat}\rangle$. Has unique ground state if we restrict input to $|0\rangle^{\otimes n}$.

$$|\Psi\rangle = \frac{1}{\sqrt{n+1}} \sum_{t=0}^{n} |t\rangle \otimes |\text{cat}_t\rangle |0\rangle^{\otimes(n-t)}$$

Intuition: For $t \geq \frac{n}{3}$, the first $\frac{n}{3}$ qubits form a cat state. Enough to prove that error states have $\Omega(\log n)$ circuit complexity.

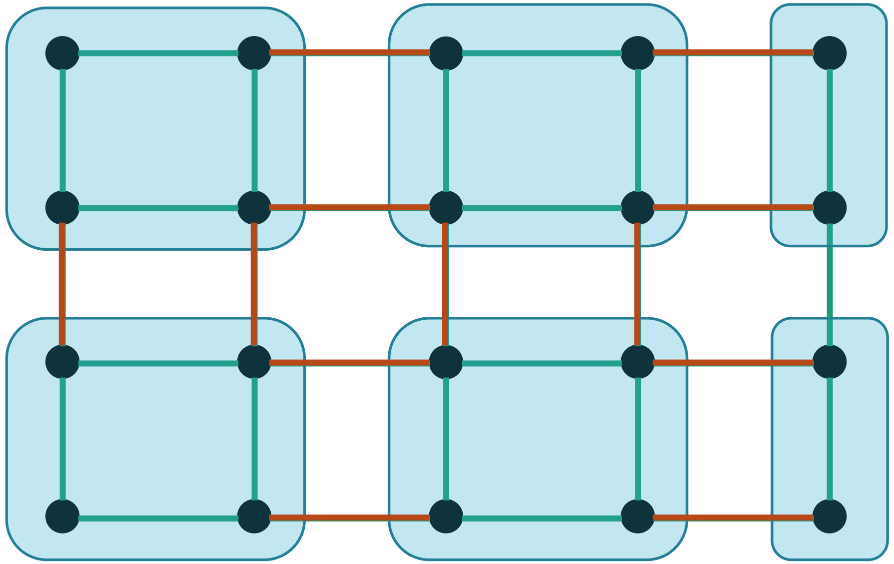
NLETS but not NLTS

With some additional technical details, can make construction 1-D geometrically local.

NLTS cannot be geometrically local.

Proof:

Smaller than constant fraction of terms will be violated. Can produce constant-depth states for subsection.



Low-energy vs low-error

Low-energy

Correct definition for qPCP
Robustness of entanglement at room-temperature

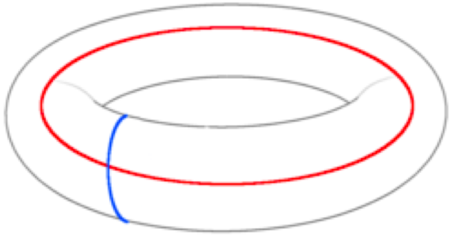
Low-error

Errors attack specific particles
Reasonable model for physical processes, quantum fault-tolerance, noisy channels, noisy adiabatic quantum computation, etc.

$$\mathcal{M}(\rho) = \left((1-\epsilon)\mathcal{I} + \epsilon\mathcal{N}\right)^{\otimes n}(\rho) \approx \sum_{S:|S|\leq 2\epsilon n} (1-\epsilon)^{n-|S|}\epsilon^{|S|}\mathcal{N}^{S}(\rho)$$

Part 2:
Approximate low-weight check codes

The quest for good qLDPC codes

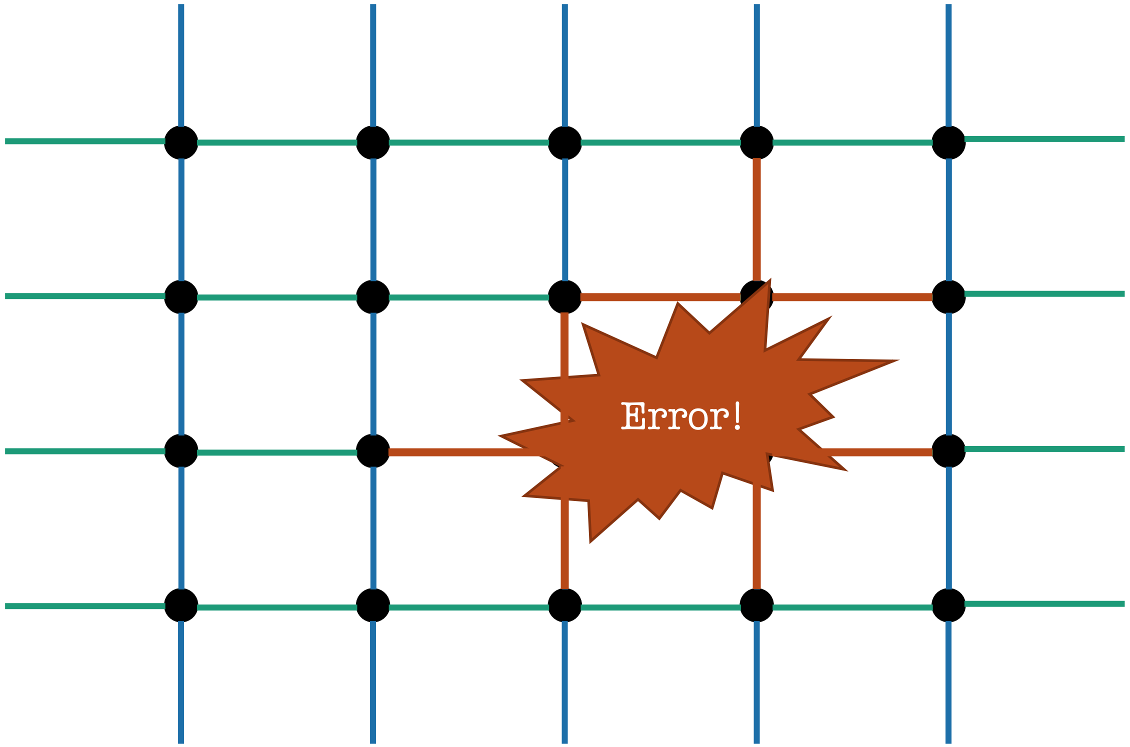


Example: Toric Code [Kitaev[97]]

Checks involve $O(1)$ particles.

Each particle is involved in $O(1)$ checks.

Good LDPC codes yield fault-tolerant computation [Gottesman[14]].



Currently…

Code	Rate	Distance	Locality	Approximation Factor
CSS [Folklore]	$\Omega(n)$	$\Omega(n)$	$\Omega(n)$	0
qLDPC [Tillich-Zémor[13]]	$\Omega(n)$	$O(\sqrt{n})$	$O(1)$	0
Subsystem [Bacon-Flammia-Harrow-Shi[17]]	$\Omega(n)$	$O(n^{1-\epsilon})$	$O(1)$	0
Approx. qLWC [N-Vazirani-Yuen[18]]	$\Omega(n)$	$\Omega(n)$	$O(1)$	$1/\text{poly}(n)$

Approximate Error Correcting Codes

A w-local Hamiltonian $H = H_1 + H_2 + \ldots + H_m$ acting on n qubits is a $[[n, k, d]]$ code with error δ if

1. each term H_i acts on at most w qubits

2. Maps $\mathrm{Enc}, \mathrm{Dec}$ s.t. $\langle\Psi|H|\Psi\rangle = 0$ iff $|\Psi\rangle\langle\Psi| = \mathrm{Enc}(|\xi\rangle\langle\xi|)$ for some $|\xi\rangle \in (\mathbb{C}^2)^{\otimes k}$

3. For all $|\phi\rangle \in (\mathbb{C}^2)^{\otimes k} \otimes \mathcal{R}$ for purify register $\mathcal{R}$, and CPTP error map $\mathcal{E}$ acting on $(d-1)/2$ qubits

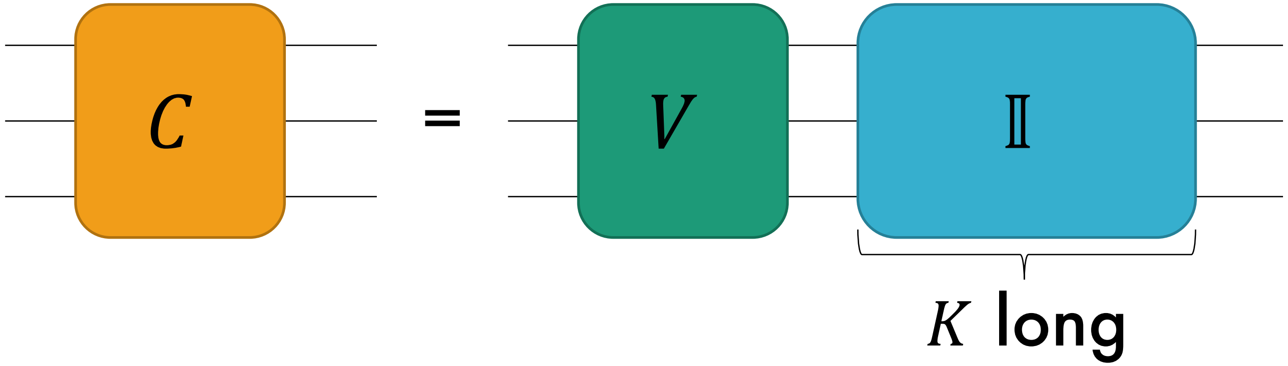
$$\|\mathrm{Dec} \circ \mathcal{E} \circ \mathrm{Enc}(|\phi\rangle\langle\phi|) - |\phi\rangle\langle\phi|\,\| \leq \delta$$

Approximate qLWC codes

CSS Codes have good distance and rate but lack locality.

Create a Hamiltonian whose groundspace is almost exactly that of a CSS code but is locally checkable.

Let V be the encoding circuit for a good CSS Code.



Choose $K = O(T_V\, \delta^{-2})$.

Construct the clock Hamiltonian for this “padded” circuit C.

Approximate qLWC codes

The groundspace of H is $\approx$ the groundspace of a CSS code tensored with junk.

$$\mathcal{G}_C = \left\{ \frac{1}{\sqrt{T_C + 1}} \sum_{t=0}^{T} |t\rangle|\psi_t\rangle \; : \; \begin{array}{c} |\psi_t\rangle = C_t C_{t-1} \dots C_1 |\psi_0\rangle, \\ |\psi_0\rangle = |\xi\rangle|0\rangle^{\otimes(n-k)} \end{array} \right\}$$

But for $t \geq T_V$, $|\psi_t\rangle = V|\psi_0\rangle$. Thus, $1 - O(\delta^2)$ fraction of $|\psi_t\rangle = V|\psi_0\rangle$.

$$\mathcal{G}_C \approx \frac{1}{\sqrt{T_C + 1}} \sum_{t=0}^{T} |t\rangle \otimes \left\{ V|\psi_0\rangle : |\psi_0\rangle = |\xi\rangle|0\rangle^{\otimes(n-k)} \right\}.$$

Plus, $\mathcal{G}_C$ is the groundspace of a 5-local Hamiltonian!

Remains to define encoding and decoding functions and check that distance and rate of code is preserved.

Encoding and decoding circuits

Encoding circuit.

$\mathrm{Enc}(\rho) = W(\rho \otimes |0\rangle\langle 0|^{\otimes(n-k)})W^\dagger$ for

$|\xi\rangle \mapsto_W \frac{1}{\sqrt{T_C+1}} \sum_{t=0}^{T_C} |t\rangle \otimes C_t C_{t-1} \dots C_1 |\xi\rangle$

W can be implemented efficiently by first generating superposition over $|t\rangle$ and the apply $C_t C_{t-1} \dots C_1$ conditionally.

Approximate decoding circuit.

$\mathrm{Dec}(\sigma) = \mathrm{Tr}_{\mathrm{ancilla}}\left(V^\dagger \mathrm{Tr}_{\mathrm{time}}(\sigma) V\right)$.

time is the collection of qubits holding the time register and $\mathrm{ancilla}$ are the last $n-k$ qubits of the main register.

V is the encoding circuit of the CSS code. Then $V^\dagger$ is a decoding circuit.

Distance of code

Encoding circuit.

$\mathrm{Enc}(\rho) = W(\rho \otimes |0\rangle\langle 0|^{\otimes(n-k)}W^\dagger$ for

$$|\xi\rangle \mapsto_W \frac{1}{\sqrt{T_C+1}} \sum_{t=0}^{T_C} |t\rangle \otimes C_t C_{t-1} \dots C_1 |\xi\rangle$$

Approximate decoding circuit.

$\mathrm{Dec}(\sigma) = \mathrm{Tr}_{\mathrm{ancilla}}\left(V^\dagger \mathrm{Tr}_{\mathrm{time}}(\sigma) V\right)$.

time is the collection of qubits holding the time register and $\mathrm{ancilla}$ are the last $n-k$ qubits of the main register.

Distance of code (sketch).

Tracing out time qubits, yields a mixed state over t of main register.

W.h.p. $t \geq T_V$ so we are decoding $\mathcal{E}(V\rho V^\dagger)$ for encoded state ρ.

Thus, distance is the same as that of CSS code. Or $\Omega(n)$.

Rate of code

Uses more qubits than CSS code.

Requires more qubits to store time register. CSS circuits have $O(n^2)$ gates.

Storing $|t\rangle$ in unary would require additional $O(T_C) = O(n^2\delta^{-2})$ qubits! Destroys rate (and distance).

Store register in different base.

Express time in base $O(r)$ where r is the solution to $T_C = n^r$.

Increases locality of Hamiltonian by $2r$. If $\delta = 1/\mathrm{poly}(n)$ then still a local Hamiltonian.

And rate and distance of $\Omega(n)$.

The error-correcting zoo

Quantum low-density parity-check codes (qLDPC) [Folklore]

Linear rate and distance codes with $O(1)$ row- and column-spare parity check matrices exist.

Quantum locally testable codes (qLTC) [Aharanov-Eldar[13]]

A local Hamiltonian $H = \sum H_j$ is a qLTC with soundness $R(\delta)$ if a state $|\psi\rangle$ distance δn from the groundspace $\mathcal{G}$ has energy $E = \langle\psi|H|\psi\rangle \geq R(\delta)\, m$.

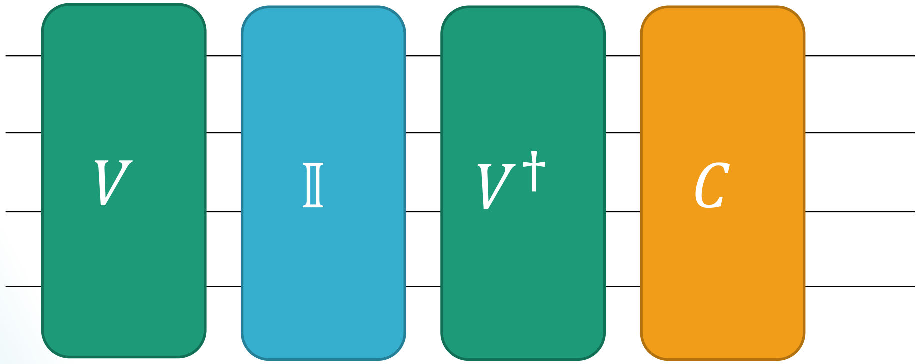
Quantum low-weight check (qLWC) codes [N-Vazirani-Yuen[18]]

A local Hamiltonian $H = \sum H_j$ is a qLWC if the groundspace $\mathcal{G}$ forms a linear rate and distance code and each Hamiltonian term acts on $O(1)$ particles.

Aside: Strong NLETS result

Theorem: Assuming QCMA≠QMA, there is a family of local Hamiltonians $H^{(n)}$ acting on n particles such that all ϵ-low-error states of $H^{(n)}$ have super-polynomial circuit complexity,

Proof idea: $L \in \mathrm{QMAcomp} - \mathrm{QCMA}$ of witness-checking circuits C. For $C \in L$, construct FK clock Hamiltonian H of following circuit.



ϵ-error-states of H can be error-corrected and then used as witnesses for $C \in L$. But, if they have polynomial circuit complexity, then the generating circuit is a classical witness. Then QMA = QCMA. $\perp$.

The computational perspective seems to be immensely useful for understanding robustness of entanglement as well as constructing novel error-correcting codes.

Open Questions

- Can approximate qLWC codes be made geometrically local?
- Do super-positions of low-error states requires large circuit complexity? (vs convex combination)
- How do qLWC codes compare to qLTCs, qLDPCs? Do they offer progress towards the qPCP conjecture?
- Combinatorial NLTS vs standard NLTS

Thanks!