B

§ 3 One-round two-prover game for Local Hamiltonian.

Story: Our goal is to prove the following theorem

(by constructing a non-local game for the local Hamiltonian problem)

Theorem 9. ∃ a universal const. Δ s.t. the following holds.

Let $H := \frac{1}{m} \sum_{l \in [m]} \gamma_l H_l$ be an XZ k-local Hamiltonian acting on n-qubits, w/ parameters $\alpha, \beta \in (0,1)$ for $\beta > \alpha$.

Then, ∃ a one-round, two-prover non-local game s.t.

- if $\lambda_0(H) \leq \alpha$, the verifier accepts w.p. $\geq \frac{1}{2} + \Delta$
- if $\lambda_0(H) \geq \beta$, the verifier accepts w.p. $\leq \frac{1}{2} - \Delta$.

Further, each message is of length $\tilde{O}(n/(\beta-\alpha)^{-1})$-bits long.

Story: So we start w/ an XZ Hamiltonian $H = \frac{1}{m} \sum_{l \in [m]} \gamma_l H_l$ (as stated above) &

(1) construct a non-local game, "Hamiltonian test" $G(H)$, based on H

who's max acc prob is upper & lower bounds are tightly related to $\lambda_0(H)$ &

(1.) Based on $G(H)$, we construct another non-local game $\tilde{G}(H)$ s.t. ∃ $\Delta > 0$ s.t.

if $\lambda_0(H) \leq \alpha$, $\omega^*(\tilde{G}(H)) \geq \frac{1}{2} + \Delta$

but if $\lambda_0(H) \geq \beta$, $\omega^*(\tilde{G}(H)) \leq \frac{1}{2} - \Delta$

(just as in the theorem)

We start by describing the Hamiltonian Test $G(H)$
which is based on the Pauli Braiding Test &
(PBT)
the Energy Test (ET)

Informal description of $G(H)$

- The provers share t EPR pairs &
the first prover holds a copy of the groundstate of H.

- for ET, the verifier picks ℓ from $\{1, \dots, m\}$,
$w \sim_R \{X, Z\}^t$ &
$e \sim_R \{0,1\}^t$.
& chooses
$\tau_1 \dots \tau_n \in [t]$ s.t.
$W(e)_{\tau_i}$ matches the i^{th} Pauli observable
of H_ℓ.

Claim: letting $t = O(n \log n)$,
such positions can be chosen for a
random $W(e)$ w/ overwhelming probability.

- The verifier sends $\tau_1 \dots \tau_n$ to Prover 1,
who's supposed to teleport the groundstate
of H through to the EPR pairs in those
positions.

- As in PBT,
the verifier sends $W(e)$ to Prover 2
who's supposed to measure his
EPR halves w/ the corresponding
observables.

- The values of $\tau_1 \dots \tau_n$ were chosen s.t. the first prover

: We start by describing the Hamiltonian test $G(H)$
which is based on the Pauli Braiding test (PBT) &
the Energy test (ET).

Informal description of $G(H)$

- the provers share t EPR pairs &
the first prover holds a copy of the ground state of H.

- In ET, the verifier picks $l \leftarrow \{1, \dots, m\}$,
$w \leftarrow_R \{X, Z\}^t$ &
$e \leftarrow_R \{0,1\}^t$,
& chooses $\tau_1 \dots \tau_n \in [t]$ s.t.
$W(e)_{\tau_i}$ matches the i^{th} Pauli observable of H_l.

Claim: Lefty $t = O(n \log n)$,
such positions can be chosen for a
random $W(e)$ w/ nonnegligible probability.

- The verifier sends $\tau_1 \dots \tau_n$ to Prover 1,
who's supposed to teleport the ground state
of H through the EPR pairs in these
positions.

- As in PBT,
the verifier sends $W(e)$ to Prover 2
who's supposed to measure his
EPR halves w/ the corresponding
observables.

- The values of $\tau_1 \dots \tau_n$ were chosen s.t. the first prover

teleports the groundstate of H
in the exact position of the measurement
according to H_ℓ.

- Using these outcomes from the second phase &
teleportation corrections from the first phase,
the verifier can estimate $\lambda_0(H)$.

└ • See Fig 2.

Figure 2: Hamiltonian Test $G(H)$ for an XZ Hamiltonian H.

The verifier performs each of the following w.p. $1-p$ & p resp.

(A) Pauli-Braiding Test

(B) Energy Test

Verifier

1. $W \leftarrow_R \{X,Z\}^t$

$e \leftarrow_R \{0,1\}^t$ &

$\ell \leftarrow \{1,\dots m\}$

2. $\tau_1 \dots \tau_n$ positions s.t.

$H_\ell = \bigotimes \sigma_{W(e)_{\tau_i}}$

$\tau_1 \dots \tau_n$ ← 3. → $W(e)$

$a,b \in \{0,1\}^n$ → 4. ← $c \in \{+1,-1\}^t$

5. Let $d \in \{-1,+1\}^n$ be s.t

$$\begin{cases} d_i = (-1)^{a_i} c_{\tau_i} & \text{if } W_{\tau_i} = X \\ d_i = (-1)^{b_i} c_{\tau_i} & \text{if } W_{\tau_i} = Z \end{cases}$$

6. If $\prod_{i\in[n]} d_i \neq \mathrm{sgn}(\gamma_\ell)$, accept

7. Else, reject w.p. $|\gamma_\ell|$.

└

Story: Before we start the proof of the main Theorem,
we state two auxiliary Lemmas that
upper & lower bound the acceptance prob. of $G(H)$.
The proofs of these are deferred to §3.1

Lemma 7. Let $H = \sum_{l\in[m]} \gamma_l H_l$ be an XZ Hamiltonian
$G(H)$ be the game in Fig 2 & let

$$w_h(H) := 1 - p\left(\frac{1}{2m}\sum_{l\in[m]}|\gamma_l| - \frac{1}{2}\lambda_0(H)\right).$$

If the provers use the honest strategy in PBT,
the max. acceptance prob. in $G(H)$ is $w_h(H)$
& it can be achieved if the first prover behaves honestly,
in the energy test (ET).

Lemma 8. Let H, $G(H)$ & $w_h(H)$ be as above (Lemma 7).
For each $\eta>0$, $\exists$ some $p = O(\sqrt{\eta})$ s.t.

$$w^*(G(H)) \le w_h(H) + \eta.$$

Story: Using these, we prove theorem 9.

Proof: Lemma 5 states that from H one can construct H' s.t.

$$\begin{cases} \lambda_0(H) \le \alpha \Rightarrow \lambda_0(H') \le \frac{1}{2} & \text{&} \\ \lambda_0(H') \ge \beta \Rightarrow \lambda_0(H') \ge 1 \end{cases}$$

where $H' = \sum_{l\in m'} \gamma'_l H'_l$ is an XZ local Hamiltonian.

upcoming: We bound the max. acceptance prob. of the Hamiltonian test on H', relating it to the groundstate energy of H.

NB: (From Lemma 7)

$$\lambda_0(H) \leq \alpha \Rightarrow \omega^*(G(H')) \geq 1 - p\left(\frac{1}{2m}\sum_{l\in[m]}|\gamma_l| - \frac{1}{4}\right)$$

$=: c$

NB2: (From Lemma 8', for any $\eta > 0$ & some $p \leq G'\sqrt{\eta}$

$$\lambda_0(H) \geq \beta \Rightarrow \omega^*(G(H')) \leq 1 - p\left(\frac{1}{2m}\sum_{l\in[m]}|\gamma'_l| - \frac{1}{2}\right) + \eta$$

$$= c - \frac{G\sqrt{\eta}}{4} + \eta$$

(using $\lambda_0(H') \geq 1$ when $\lambda_0(H) \geq \beta$).

Convention: Choose η to be s.t. $\eta' := \frac{G\sqrt{\eta}}{4} - \eta > 0$.

NB: $\lambda_0(H) \leq \alpha \Rightarrow \omega^*(G(H')) \geq c$ &

$\lambda_0(H) \geq \beta \Rightarrow \omega^*(G(H')) \leq c - \eta'$.

Upcoming: We define $\tilde{G}(H)$ that achieves soundness & completeness as in the theorem statement.

Def^n: $\tilde{G}$: accept w/p: $\frac{1}{2} - \frac{2c-\eta'}{4}$

reject w/p. $\frac{2c-\eta'}{4}$

play G w/p $\frac{1}{2}$.

NB: If $\lambda_0(H) \leq \alpha$ $\quad w^*(\tilde{G}(H')) \geq \frac{1}{2} - \frac{2c-\eta'}{4} + \frac{1}{2} w^*(G(H'))$

$$\geq \frac{1}{2} + \frac{\eta'}{4}$$

If $\lambda_0(H) \geq \beta$ $\quad w^*(\tilde{G}(H')) \leq \frac{1}{2} - \frac{2c-\eta'}{4} + \frac{1}{2} w^*(G(H'))$

$$= \frac{1}{2} - \frac{2c-\eta'}{4} + \frac{1}{2}(c-\eta')$$

$$= \frac{1}{2} - \frac{\eta'}{4}.$$

□

Corollary 10. ∃ a protocol for verifiable deleg^n of quantum comput^n where a classical client communicates w/ 2 provers in one round of (classical) communication.

[Via the circuit to Hamiltonian construction

§3.1 Proof of Lemmas 7 & 8.

Upcoming: We start w/ the proof of Lemma 7 that gives an upper bound on the acceptance prob of the provers are honest in PBT.

[Proof of Lemma 7.

NB 1: ∵ PBT & ET are indistinguishable to the second prover, he also follows the honest strategy in ET (by assump^n, they follow the honest strategy for PBT)

& therefore, the acceptance prob. in $G(H)$
depends uniquely in the strategy of the first prover in E^T.

Let: $a, b \in \{0,1\}^n$ be the answers of the first prover in E^T &
τ be the reduced state held by the
second prover on positions $\tau_1 \dots \tau_n$ of
his EPR halves,
after teleportation.

(sorry, these were Ts in the paper; now τ conflicts w/ $\tau_1 \dots \tau_n$ a bit)

Claim: For a fixed H_ℓ,
the verifier rejects w.p.

$$\frac{|\gamma_\ell| + \gamma_\ell \, E\left[\prod_{i\in[n]} d_i\right]}{2} \qquad (1)$$

idea:
(when the sign matches,
rejected w.p. $\frac{2|\gamma_\ell|}{\chi}$
when it doesn't,
$\frac{2|\gamma_\ell|}{\chi}\left(1 + \Pr(\text{sign match})\right)$
$|\gamma_\ell|$ sign match. $\Pr(\text{sign match})$

NB: Measuring a qubit $|\phi\rangle$ in
the Z-basis w/ outcome $f \in \{\pm 1\}$
$\Leftrightarrow$
outcome $(-1)^g f$ when measuring
$X^g Z^h |\phi\rangle$
in the same basis.

The analogue also holds for X-basis.

NB2: Given the answers of the first prover,
the following behaviours of the second prover are equivalent:
(i) measure τ w.r.t. H_ℓ w/ outcome c,
(ii) measure $\rho = Z^b X^a \tau X^a Z^b$ w.r.t H_ℓ
w/ outcome d

NB3: Using (ii), taking $\prod_{i\in n} d_i$ as the outcome of H_ℓ on ρ,
averaging over all $\ell \in [m]$

from Eq (1) it follows that the verifier rejects in ET w.p.

$$\frac{1}{m} \sum_{l \in [m]} \frac{|\gamma_l| + \gamma_l \, tr[\rho H_l]}{2}$$

$$= \frac{1}{2m} \sum_{l \in [m]} |\gamma_l| + \frac{1}{2} tr(\rho H).$$

NB4: This value is minimised when ρ is the ground state of H.

NB5: The overall acceptance prob. in $G(H)$ is at most (in this case)

$$1 - p\left(\frac{1}{2m} \sum_{l \in [m]} |\gamma_l| - \frac{1}{2} \lambda_0(H) \right) = w_\Lambda(H).$$

NB6: This acceptance prob. is achieved if the first prover teleports the ground state $|\psi\rangle$ of H & reports the honest outcomes from the teleportation i.e. $\tau = X^a Z^b |\psi\rangle\langle\psi| Z^b X^a$ & $\rho = |\psi\rangle\langle\psi|$.

□

Upcoming: We now use the self testing of PBT to certify the measurements of the second prover in ET.

⌈Proof of Lemma 8.

Let: S be the strategy of the provers that leads to

acc. prob. $1-\epsilon$ in PBT &

" " $1 - \frac{1}{2m} \sum_{l \in [m]} |\gamma_l| - \frac{1}{2} \lambda_0(H) + \delta$ in ET

for some ϵ & δ.

NB: (By Thm 2)
their strategy in PBT is $O(\sqrt{\varepsilon})$-close to the
honest strategy, up to local isometries
V_A & V_B.

⟵ Let: S_h be the strategy where the provers
follow the honest strategy in PBT &
for ET, the first prover performs the
same op^ of S but
considering the isometry V_A from Thm 2.

NB: ∴ the measurements performed by the provers in S & S_h
are $O(\sqrt{\varepsilon})$-close, (considering isometries),
the distr^n of the corresponding transcripts have
statistical distance at most $O(\sqrt{\varepsilon})$.

NB2: Thus, the provers following S_h are
accepted in ET w.p. ≥
$$1 - \frac{1}{2m} \sum_{\ell \in [m]} |\gamma_\ell| - \frac{1}{2}\lambda_0(H) + \delta - O(\sqrt{\varepsilon})$$

NB3: Since S_h follows the honest strategy in PBT,
it follows from Lemma 7 that
$$1 - \frac{1}{2m} \sum_{\ell \in [m]} |\gamma_\ell| - \frac{1}{2}\lambda_0(H) + \delta - O(\sqrt{\varepsilon}) \leq 1 - \frac{1}{2m} \sum_{\ell \in [m]}^{+} |\gamma_\ell| - \frac{1}{2}\lambda_0(H)$$

$\Rightarrow \quad \delta \leq C\sqrt{\varepsilon}$ for some const C.

NB4: The original strategy S leads to
acceptance prob. at most

$$(1-\rho)(1-\epsilon) + \rho\left(1 - \frac{1}{2m}\sum_{\ell\in[m]}|\gamma_\ell| - \frac{\lambda_0(H)}{2} + C\sqrt{\epsilon}\right)$$

$$= \omega_h(H) - (1-\rho)\epsilon + \rho C\sqrt{\epsilon}.$$

NB 5: For any η, one can pick $\rho = \min\left\{\frac{\sqrt{\eta}}{15}, 1\right\}$ where $\Delta \geq 1 \geq 2C$, & deduce

$$\rho C\sqrt{\epsilon} - (1-\rho)\epsilon \leq \frac{2C\sqrt{\eta}\sqrt{\epsilon}}{\Delta} - \epsilon$$

$$\leq \sqrt{\eta}\sqrt{\epsilon} - \epsilon \leq \eta$$

& thus, the max. acceptance prob is $\leq \omega_H(H) + \eta$.

□