A simple protocol for Verifiable Delegation of Quantum Computation in one-round.

§ Preliminaries

§2.1 Notation

$\|M\|$ max. singular value (op. on $\mathcal{H}$).

I, X, Z Pauli matrices

§2.2 Non-local games, self-testing & Pauli braiding

G

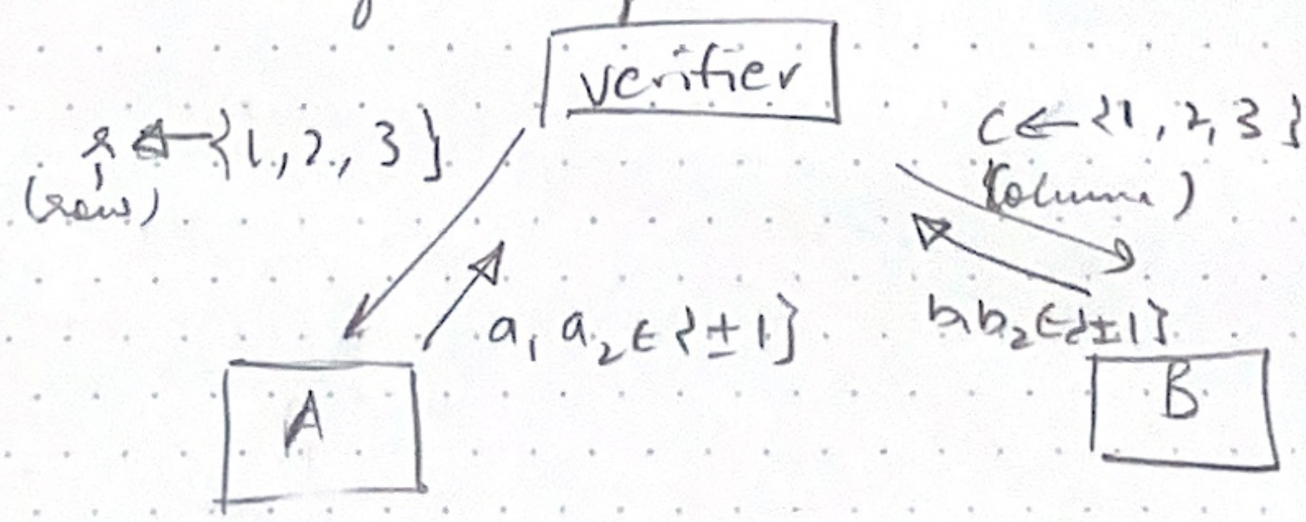
$\omega^*(G) > \omega(G)$ non local games.

close to $\omega^*(G)$ (means strategy) self-testing

the games is ideal, up to isometries.

§2.2.1 Magic Square Game

Def^: G



def^: $a_3 := a_1 \oplus a_2$

$b_3 := b_1 \oplus b_2$

verifier: accepts iff $a_c = b_r$

claim: $\omega(G) = \frac{8}{9}$

$\omega^*(G) = 1$

2 EPR states

On question r (resp. c), perform measurements in first two colums (resp. rows) of row r (resp. col c).

$\mathbb{1}\otimes Z$	$Z\otimes\mathbb{1}$	$Z\otimes Z$
$X\otimes\mathbb{1}$	$\mathbb{1}\otimes X$	$X\otimes X$
		$Y\otimes Y$
$X\otimes Z$	$Z\otimes X$	

NB: Value a_3 & b_3 correspond to measuring the EPR states according to the third column & row resp.

Story: Wu, Bancal & Scarani [46] show if win w.p. close to 1, the provers share two EPR pairs & the measurements are close to the honest Pauli measurements up to local isometries.

Lemma 1. Suppose the provers use $|\psi\rangle$ & observables W & succeed w/ prob. $\geq 1-\epsilon$ in G (Magic Square). Then, $\exists$ isometries $V_D : \mathcal{H}_D \to (\mathbb{C}^2\otimes\mathbb{C}^2)_D \otimes \mathcal{H}_{D'}$ for $D\in\{A,B\}$ & a state $|AUX\rangle_{\hat{A}\hat{B}} \in \mathcal{H}_{\hat{A}}\otimes\mathcal{H}_{\hat{B}}$ s.t.

$$\left\| (V_A\otimes V_B)|\psi\rangle_{AB} - |\Phi_{00}\rangle^{\otimes 2}_{A'B'} |AUX\rangle_{\hat{A}\hat{B}} \right\|^2 = O(\sqrt{\epsilon})$$

& for $W\in\{\mathbb{1},X,Z\}\times\{\mathbb{1},W,Z\}$

$$\left\| (W - V_A^\dagger \sigma_W V_A)\otimes \mathbb{1}_B |\psi\rangle \right\|^2 = O(\sqrt{\epsilon}).$$

(used to index

§2.2.2 Pauli Braiding Test (PBT)

Story: PBT is a non-local game that
allows the verifier to certify that
two provers share t EPR pairs &
perform the indicated measurements
consisting of Pauli observables.

: We define PBT in detail later,
& state the main properties that will be used:

(i) "Syntax" / Question/Answers: Each prover is asked $W \in \{X, Z, \mathbb{1}\}^t$,
& each answers w/ $b \in \{-1, +1\}^t$.

Not": For $W \in \{X, Z\}^t$, & $a \in \{0,1\}^t$

$$W(a)_i = W_i \quad \text{if } a_i = 1$$
$$W(a)_i = \mathbb{1} \quad \text{if } a_i = 0$$

(basically, $W(a)_i = (W_i)^{a_i}$)

(ii) Honest strategy: Provers share t EPR states &
measure $\sigma_W := \bigotimes_{i \in [1:t]} \tau_{W_i}$ on
question W.

(self-testing: even if provers use an arbitary state $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$
& make projective measurements
τ_W^A τ_W^B for each W,
if the pass PBT w.p. $\geq 1-\epsilon$,
$|\psi\rangle$ is $O(\sqrt{\epsilon})$ close to k EPR &
$\tau_W^A \tau_W^B$ is σ_W (upto local isometries)

Story: We now describe PBT.

- Divided into three parts B
  each happens w/ equal prob.

(i) Consistency Test — checks if the measurement performed by both provers on W are equivalent,

i.e. $\tau^{A}_{W} \otimes \mathbb{I}\,|\psi\rangle_{AB} \approx \mathbb{1} \otimes \tau^{\dagger}_{W}\,|\psi\rangle_{AB}$.

(ii) Linearity test — checks if

$$\tau^{\hat{A}}_{W(a)}\,\tau^{\hat{A}}_{W(a')} \otimes \mathbb{I}_B\,|\psi\rangle_{AB} \approx$$

$$\tau^{\hat{A}}_{W(a+a')} \otimes \mathbb{I}_B\,|\psi\rangle_{AB}.$$

(iii) Anti-commutation — checks if provers measuring follow commut^/anti-commutation rules, consistent w/ honest measurements

i.e. $\tau^{A}_{W(a)}\,\tau^{A}_{W(a')} \otimes \mathbb{I}_B\,|\psi\rangle_{AB} \approx$

$$(-1)^{\left|\{W_i \neq W_i' \;\&\; a_i = a_i' = 1\}\right|}\,\tau^{A}_{W'(a')}\,\tau^{*}_{W(a)} \otimes \mathbb{1}_B\,|\psi\rangle_{AB}$$

(parity of the set of locations where (non-I) diffs. were measured)

- Linearity & Consistency tests are very simple & described in Fig 1.

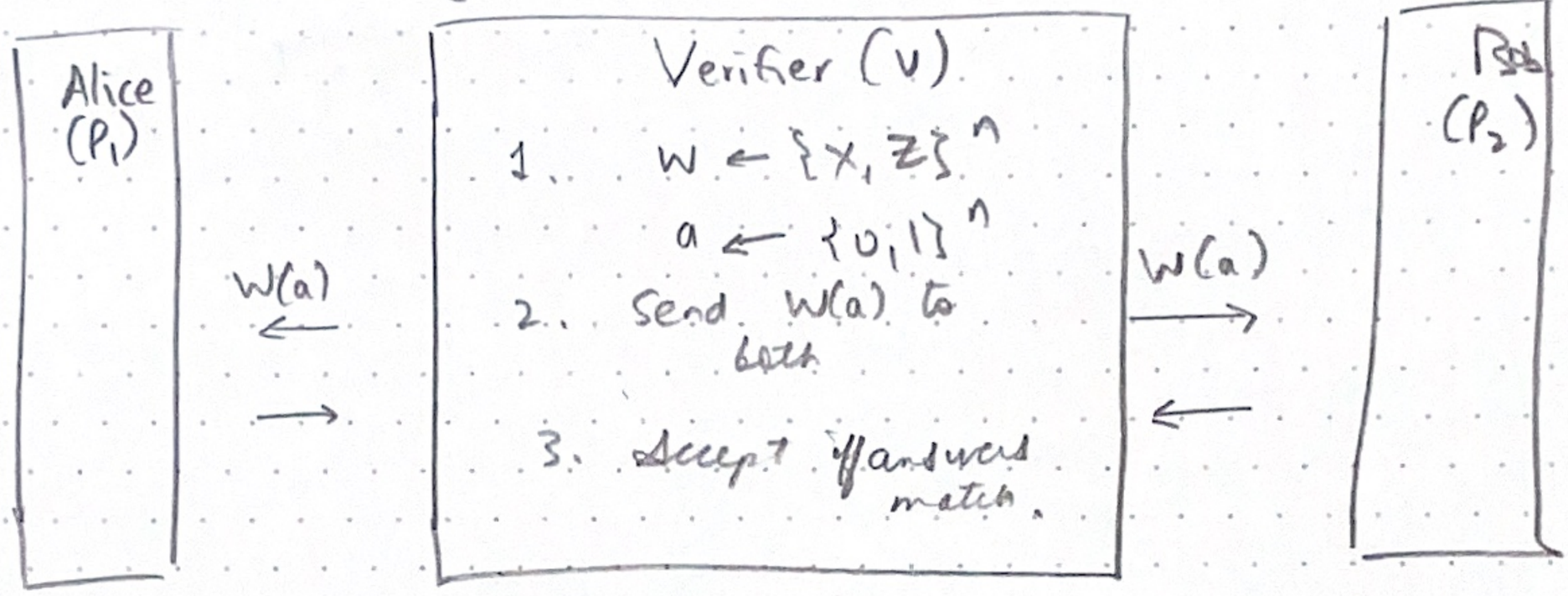
- The anti-commutation test — uses the Magic Square game (one can potentially use other games as well).

  allows the verifier to check that the provers share a const. # of EPR pairs & perform Pauli measurements on them.

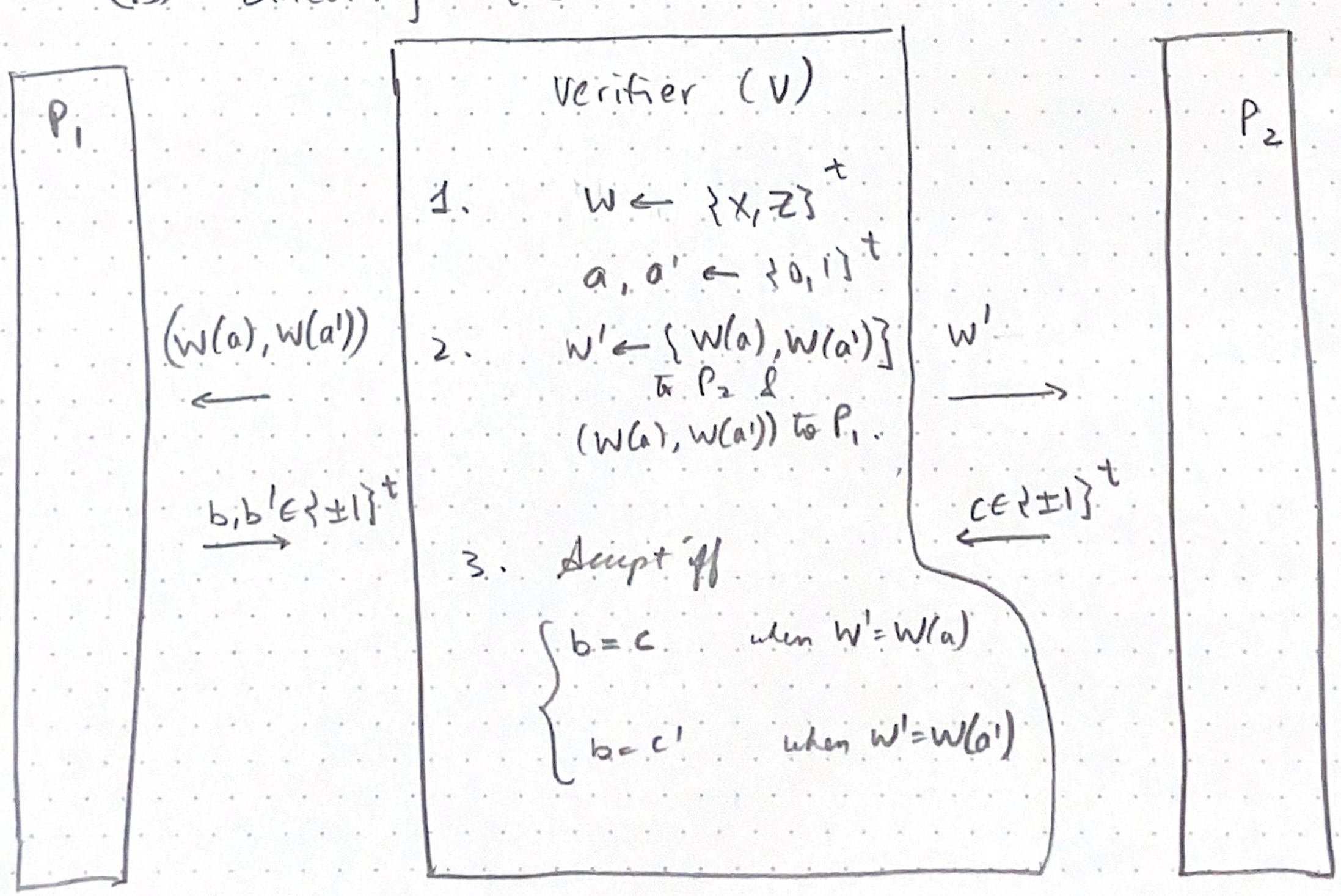
Figure 1: Pauli Braiding test

The verifier performs the following steps w/p. $\frac{1}{3}$ each.

(A) Consistency test



(B) Linearity test



(C) Anti-commutation Test

Play Magic Square w/ t EPR pairs in parallel.

Theorem 2 (Theorem 14 of [40]). ~ Natarajan & Vidick (STOC'17)

Suppose $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ &

$W(a) \in \text{Observables}(\mathcal{H}_A)$ for $W \in \{X, Z\}^t$

$a \in \{0,1\}^t$

specify the provers strategy, that

wins BLT w.p. $\geq 1-\epsilon$

Then, $\exists$ isometries

$$V_D : \mathcal{H}_D \to \left((\mathbb{C}^2)^{\otimes t}\right)_{D'} \otimes \hat{\mathcal{H}}_D$$

for $D \in \{A, B\}$ s.t.

$$\| (V_A \otimes V_B) |\psi\rangle_{AB} - |\Phi_{00}\rangle^{\otimes t}_{A'B'} |AUX\rangle_{AB} \|^2 = O(\sqrt{\epsilon}),$$

& on expectation over $W \in \{X, Z\}^t$,

$$\mathop{\mathbb{E}}_{a \in \{0,1\}^t} \| (W(a) - V_A^\dagger (\sigma_W(a) \otimes \mathbb{I}) V_A) \otimes \mathbb{I}_B |\psi\rangle \|^2 = O(\epsilon)$$

Moreover, if the provers share $|\Phi_{00}\rangle^{\otimes t}_{A'B'}$ &

measure w/ observables $\otimes \sigma_{W_i}$ on W,

they pass the BLT w.p. 1.

§2.3 Local Hamiltonian Problem:

Story: • LH Problem — quantum analogue of MAX-SAT problem

• The problem:

$$H := \frac{1}{m} \sum_{i \in [1, m]} H_i$$

(action at most k qubits.

Which is the case: (i) $\exists$ a state w/ energy $\leq \alpha$ or

(ii) $\forall$ state, energy $\geq \beta$.

• LH Problem QMA complete for $k=5$ & $\beta - \alpha \geq \frac{1}{\text{poly}}$.

- Here, we consider the variant of LH where all terms are tensor products of σ_x, σ_z (and σ_I).

Def^3 (XZ Local Hamiltonian).

Parameters: $k \in \mathbb{Z}^+$
$\alpha, \beta \in [0,1]$
$\alpha < \beta$

XZ k-local Hamiltonian is the following promise problem:

Let: n be the # qubits in a quantum system.

Input: $m(n)$ values $r_1 \dots r_{m(n)} \in [-1,1]$
$m(n)$ Hamiltonians $H_1 \dots H_{m(n)}$ each has the form
poly in n

$$\bigotimes_{j \in n} \sigma_{w_j} \in \{\sigma_x, \sigma_z, \sigma_I\}^{\otimes n}$$

with at most k non-identity terms,
i.e. $|\{j \mid j \in [n] \ \& \ \sigma_{w_j} \neq \sigma_I\}| \leq k$.

for $H := \frac{1}{m(n)} \sum_{j \in [m(n)]} r_j H_j$ one of the following two conditions hold:

Yes. $\exists$ a state $|\psi\rangle \in \mathbb{C}^{2^n}$ s.t. $\langle\psi|H|\psi\rangle \leq \alpha(n)$

No. $\forall$ $|\psi\rangle \in \mathbb{C}^{2^n}$ it holds that $\langle\psi|H|\psi\rangle \geq \beta(n)$.

Remark: This problem is also known to be QMA complete.

Lemma 4 (Lemma 22 of [23], & [16]).

$\exists$ $\alpha, \beta \in [0,1]$ satisfying $\beta - \alpha \geq \frac{1}{\text{poly}}$ s.t.

XZ k-local Hamiltonian is QMA-complete for some constant k.

Story: open whether, QMA-complete for $\beta - \alpha = O(1)$ while k-LH is const.

: can achieve this gap, by "diversify" the locality of the Hamiltonian

Lemma 5 (Lemma 26 of [40]) Let : H be an n-qubit Hamiltonian w/ min energy $\lambda_0(H) \geq 0$ &

s.t. $\|H\| \leq 1$ (i.e. max singular value)

: $\alpha, \beta \geq \frac{1}{poly}$, $\alpha < \beta$ $\forall$ n

: H' be the following Hamiltonian on $(\beta-\alpha)^{-1}$ qubits

$$H' := \sigma_I^{\otimes na} - \left(\sigma_I^{\otimes n} - \left(H - a^{-1}\sigma_I^{\otimes n}\right)\right)^{\otimes a}$$

where $a = (\beta-\alpha)^{-1}$.

Then,

if $\lambda_0(H) \leq \alpha$ then $\lambda_0(H') \leq \frac{1}{2}$

while if $\lambda_0(H) \geq \beta$ then $\lambda_0(H') \geq 1$.

Moreover, if H is an XZ-Hamiltonian,

then so is H'.

Story: It'll be useful to define "non-local" games for Local Hamiltonian problems.

Def^n 6 (Non-local games for Hamiltonians).

Given: local Hamiltonian H acting on n qudits

Output: A non-local game $G(H)$ w/ (unique & s provers,

(parameters: $\alpha, \beta, c, s \in [0,1]$, $\alpha < \beta$, $c > s$)

satisfying the following:

completeness: If $\lambda_0(H) \leq \alpha$, $\omega^*(G(H)) \geq c$

soundness: If $\lambda_0(H) \geq \beta$, $\omega^*(G(H)) \leq s$.