Why The Following Doesn't Give Log-Local, Constant Gap Hamiltonian?

David Ponarovsky

September 3, 2023

1 What we would like to have:

Consider the LPS expander on n vertices and denote $t \sim l$ if t is adjacent to l. Let $M_\Delta \in \mathbb{C}^{n \times n}$ be the matrix defined by the product: [**COMMENT**] Such M_Δ dosn't exists.

$$\langle u | M_\Delta | l \rangle^* \langle l+1 | M_\Delta | t-1 \rangle \langle t | M_\Delta | v \rangle = \mathbf{1}_{t \sim l} \mathbf{1}_{u=t} \mathbf{1}_{v=l}$$

Given the Hamiltonian $H_{\text{init}} + m \cdot 2I - H_{\text{prop}} + H_{\text{end}}$, consider the Hamiltonian $\alpha H_{\text{init}} + m \cdot 22\Delta I - H_{\text{prop}} M_\Delta H_{\text{prop}} + \beta H_{\text{end}}$. Denote H_{prop} by $U_1 \otimes |2\rangle \langle 1| + U_2^\dagger \otimes |1\rangle \langle 2| + \cdots$. Now let $\Lambda_{t,l}$ be defined such that:

$$\Lambda_{l,t}^\dagger U_l^\dagger U_t \Lambda_{t,l} = U_l U_{l-1}..U_{t+1} U_t$$

And consider the diagonalization $W^\dagger H_{\text{prop}} M_\Delta H_{\text{prop}} W$. Where:

$$W = \sum \Lambda_{t,l} U_{t-1} U_{t-2}..U_1 \otimes |t\rangle \langle t | M_\Delta | l \rangle \langle t|$$
$$\Rightarrow W^\dagger = \sum U_1^\dagger U_2^\dagger..U_{t-1}^\dagger \Lambda_{t,l}^\dagger \otimes |t\rangle \langle t | M_\Delta | l \rangle^* \langle t|$$

Notice that:

$$W^\dagger U_l^\dagger U_t | l \rangle \langle l+1 | M_\Delta | t-1 \rangle \langle t | W =$$
$$W^\dagger U_l U_t | l+1 \rangle \langle l | M_\Delta | t \rangle \langle t | |t\rangle \langle t | M_\Delta | v \rangle \langle t | \Lambda_{t,v} U_{t-1} U_{t-2}..U_1 =$$
$$U_1^\dagger U_2^\dagger..\Lambda_{l,u}^\dagger U_{l-1}^\dagger U_t \Lambda_{t,l} U_{t-1}..U_1 | l \rangle \langle l | M_\Delta | u \rangle^* \langle l | |l\rangle \langle l+1 | M_\Delta | t-1 \rangle \langle t | |t\rangle \langle t | M_\Delta | v \rangle | l \rangle \langle t|$$
$$U_1^\dagger..U_l^\dagger \Lambda_{l,t}^\dagger U_l^\dagger U_t \Lambda_{t,l} U_{t-1}..U_1 | l \rangle \langle t| = | l \rangle \langle t|$$
$$\Rightarrow W^\dagger H_{\text{prop}} M_\Delta H_{\text{prop}} W = \sum_{i \sim j} | i \rangle \langle j|$$

And the history state will look like:

$$| \eta \rangle = \sum \Lambda_{t,l} U_{t-1} U_{t-2}..U_1 | x_0 \rangle \otimes |t\rangle \langle t | M_\Delta | l \rangle$$

2 Lets change it a little bit.

Mabye we should define Λ to be depands on a single paramter, namely Λ_t and:

$$\Lambda_l^\dagger U_l^\dagger U_t \Lambda_t = U_l U_{l-1}..U_{t+1}$$

That wil allow us to group terms, and if

$$\sum_{v,u} \langle u| D |l\rangle^* \langle l+1| M_\Delta |t-1\rangle \langle t| D |v\rangle = \mathbf{1}_{t\sim l}$$

Then we win. So now we ask wheter there exsits such D, M_Δ and Λ_t's. (Or approximation).

Claim 2.1. *There are such Λ's and they given by:*

$$\Lambda_l^\dagger = U_l \Lambda_{l-1}^\dagger U_{l-1}^\dagger U_l$$

Proof. By induction, assume existness for any $l, t \leq l-1$, namely $\Lambda_{l-1} = U_{l-1}^\dagger U_{l-2} \Lambda_{l-2} U_{l-1}^\dagger$. Then:

$$\Lambda_l^\dagger U_l^\dagger U_t \Lambda_t = \Lambda_l^\dagger U_l^\dagger U_{l-1} U_{l-1}^\dagger U_t \Lambda_t$$
$$\Lambda_l^\dagger U_l^\dagger U_{l-1} \Lambda_{l-1} \Lambda_{l-1}^\dagger U_{l-1}^\dagger U_t \Lambda_t = \Lambda_l^\dagger U_l^\dagger U_{l-1} \Lambda_{l-1} \cdot \ U_{l-1}..U_{t+1} =$$
$$U_l U_{l-1}..U_{t+1} =$$
$$\Rightarrow \Lambda_l^\dagger = U_l \Lambda_{l-1}^\dagger U_{l-1}^\dagger U_l$$

$\square$

What about defining $\tilde{D} = \langle t| \mathbf{1}_{t\sim l} |l\rangle$, $D = \tilde{D}/det(D)$ and $\langle l+1| M_\Delta |t-1\rangle = \mathbf{1}_{t\sim l} 1/\Delta^2$?

3 Ideas.

1. M_Δ has to be unitar (and not just hermitan).

2. H_{init} and H_{end} are the critical terms and deserve more gentle treatment.

4 Constant Clock.

We can encode the time by unarity encoding. namely $|t\rangle = |1^t 000..\rangle$. Then the check $|l\rangle \langle t|$ replaced by the check $|1_l 0\rangle \langle 1_t 0|$. And we also add checks for the validity of the input $|*10*1\rangle \langle *10*1|$ that add a quaderic number of checks.

5 Using the classical LTC as hmiltonian

The idea of looking for a quantum LTC code through a construction of CSS code just committed to failure as approximating the ground state of local commute Hamiltonian sets on the expanders is in NP. Yet that fact also gives hope that using the classical LTC codes, as non-commute Hamiltonian on expanders, as they are as quantum Hamiltonian might yield a Hamiltonian which approximates it is in QMA. Let $H_X = J_0 I - \mathcal{T}(V^+, C_A \otimes C_B) H_Z = J_0 I - \mathcal{T}(V^+, C_A^\perp \otimes C_B^\perp)$. Here the notation H_X is used to describe Hamiltona and not a parity check matrix. Denote $H = H_X + H_Z$.

Definition 5.1. *Consider the Hamitonain above, over $\frac{1}{4}\Delta^2 n$ qubits, the decion problem q-c-LTC[a, b] is to answer wheter there exsits state $|\psi\rangle$ such that $\langle \psi| H |\psi\rangle \leq a$ or that for any state the $\langle \psi| H |\psi\rangle \geq b$.*

Claim 5.1. *q-c-LTC[a, b] in QMA.*

Proof. By definition the problem is Local Hamiltonain with polynomail gap. □

Claim 5.2. *q-c-LTC[a, b] in quantum PCP.*

$$\langle \psi | H_X + H_Z | \psi \rangle \geq \kappa d\left(\psi, C_X\right) + \kappa d\left(\psi, C_Z\right)$$

$$\frac{1}{\sqrt{2}}\left(\langle \varphi | + \langle \psi |\right) H \frac{1}{\sqrt{2}}\left(|\varphi\rangle + |\psi\rangle\right)$$

$$\frac{1}{2}\langle \varphi | H_X | \varphi \rangle + \frac{1}{2}\langle \psi | H_Z | \psi \rangle - \frac{1}{2}\langle \varphi | H_X | \psi \rangle - \frac{1}{2}\langle \varphi | H_Z | \psi \rangle +$$

$$+ \frac{1}{2}\langle \psi | H_X | \psi \rangle + \frac{1}{2}\langle \varphi | H_Z | \varphi \rangle$$

$$= a + \frac{1}{2}\langle \varphi | H_X | \psi \rangle - \frac{1}{2}\langle \varphi | H_Z | \psi \rangle$$

$$+ \frac{1}{2}\langle \psi | H_X | \psi \rangle + \frac{1}{2}\langle \varphi | H_Z | \varphi \rangle$$

$$\geq a + \frac{1}{2}\langle \varphi | H_X | \psi \rangle - \frac{1}{2}\langle \varphi | H_Z | \psi \rangle$$

$$+ \frac{1}{2}\kappa d\left(C_X, \psi\right) + \frac{1}{2}\kappa d\left(C_Z, \varphi\right)$$

$$\geq a + \frac{1}{2}\langle \varphi | H_X | \psi \rangle - \frac{1}{2}\langle \varphi | H_Z | \psi \rangle$$

$$+ \frac{1}{2}\kappa d\left(C_X, \psi\right) + \frac{1}{2}\kappa d\left(C_Z, \varphi\right)$$

$$\mathbf{Pr}\left[\langle \psi | H | \psi \rangle \geq b\right] \leq \delta$$

Suppose that $\mathbf{Pr}\left[\langle \psi | H | \psi \rangle \geq b\right] \leq \delta$, So at most δ of the vertices has energy greater than b and at least $1 - \delta$ ofthe vertices has energy less than a. We will say that good vertex is a negative vertex that sibiling only to one positive vertex which doesn't pass the test. We will say that a normal vertex is a positive non-passing vertex that adjoint only to good vertices. What can we say about the normal vertices?

Claim 5.3. *Let $x \in \mathbb{F}_2^{\Delta}$ and denote by H_x the Hamiltonain which on the ith coordinate applay X if $x_i = 1$ and identty otherwise.And let $c(x) \in [\Delta, \rho\Delta, \delta\Delta]$ be the codeword obtained by encoding x. Then $H_x \leq H_{c(x)}$.*

$$\sum H_{x_i} \to \sum_{|I|=m} \prod_{x^i \in I} H_{x_i} \to \sum_{|I|=m} H_{\sum_{x_i \in I} x_i}$$

$$\to \sum_{|I|=m} H_{c\left(\sum_{x_i \in I} x_i\right)} \to \sum_{|I|=m} H_{\sum_{z_i} z_i}$$

6 Exersices.

Exercise 6.1 (Beasd on Free Games)**.** *Consider the following protocol, First we measure k arbitrary qubits in the Fourier base, then we take only the bits measrued zero.. [COMMENT] somthing here is wrong.*

Definition 6.1. *BellQMA protocol is a QMA varition when the Arthur is restricted to perform only non adaptive and untangled measurments and classical computation.*

Claim 6.1. *There is a BellQMA protocol which, given a 3-SAT instance with m clauses, uses $\Theta\left(\sqrt{m}\right)$ Merlines, each of them sends $Q(\log m)$ quabits. The protocol has a completeness $1 - exp(-\Omega(\sqrt{m}))$ and soundness $1 - \Omega(1)$.*

Bottom line, They shown that the entangled measurment is not necessary.

Definition 6.2. *Given state $|\psi\rangle$ over n qubits. Let $|\psi^{(i)}\rangle$ be one qubit state defined as $|\psi^{(i)}\rangle = (\langle 0|\psi\rangle)\,|0\rangle + (\langle 1|\psi\rangle)\,|1\rangle$. In addition, define the state $|\psi\rangle^{-i}$ to be the state over $n-1$ qubits, obtained by tracing out the ith qubit. We will abuse the notation and denote by $|\psi^{-i}\rangle \otimes |\psi^{(i)}\rangle$ the results by stacking in the qubit of $|\psi^{(i)}\rangle$ in the ith position.*

Claim 6.2. *Denote by H_f the k-local Hamiltonian obtained by applying Kitaev reduction on a fault tolerant circuit, with gap $b - a \geq 1/poly(n)$. And suppose there is a state $|\psi\rangle$ over n qubits with energy lower than a. Than for any $i \in [n]$ it holds that*

$$\langle |\psi^{-i}\rangle \otimes |\psi^{(i)}\rangle |H_f| |\psi^{-i}\rangle \otimes |\psi^{(i)}\rangle\rangle < a$$

Definition 6.3. *Given H_f Consider the Hamiltonian H_f' over $2n$ qubits defined by summing local terms H_j such that either H_j is a local term of H_f or that there exist H_i in H_f such that H_i equavilance to H_j on $k-1$ nontrival coordinates, and in addition, let $l \in [n]$ be the kth nontrivial qubit been act by H_i and denote the by U the corresponding opereation applplied by it, namely $H_i^{(l)} = U$. Then $H_j^{(l+n)} = U$.*

Claim 6.3. *If H_f has a, b-gap, So is H_f'. Furthmore H_f' has the same locality.*

Definition 6.4. *Let H be a local Hamiltonian and consider the a qunbit q. Denote by $H(q)$ the set of the local terms in H act nontrivially on q. Now we will define the q, ζ-majority-term relative to H, $M[H, q, \zeta]$, to be the k^2 Hamiltonian defined by:*

$$\langle\psi|M[H, q, \zeta]|\psi\rangle = \begin{cases} 1 & \mathbf{Pr}_{H_i \sim H(q)}\left[\langle\psi|H_i|\psi\rangle \geq 1\right] \geq \zeta \\ 0 & \mathbf{Pr}_{H_i \sim H(q)}\left[\langle\psi|H_i|\psi\rangle \geq 1\right] < \zeta \end{cases}$$

Claim 6.4. *There is a $f(k)$-time algorithm that compute $M[H, q, \zeta]$ where $f(k)$ is a function of k, namely doesn't depeand on n.*

Definition 6.5. *Let H be a k-local, Denote by $M[H, \zeta]$ the ζ-majority Hamiltonian relative to H to be:*

$$M[H, \zeta] = \frac{1}{n}\sum_{q \in [n]} M[H, q, \zeta]$$

Claim 6.5. *There exist ζ such that $M[H, \zeta]$ is k^2 local Hamiltonian with $1\frac{1}{2}$ gap.*

Proof. Suppose that H has a state $|\psi\rangle$ with energy below a. Then:

$$\langle\psi|M[H, q, \zeta]|\psi\rangle = \mathbf{E}_{\sim q}\left[\langle\psi|M[H, q, \zeta]|\psi\rangle\right]$$

$$= \mathbf{E}_{\sim q}\left[\mathbf{Pr}_{H_i \sim H(q)}\left[\langle\psi|H_i|\psi\rangle \geq 1\right] \geq \zeta\right]$$

$$\leq \frac{\mathbf{E}_{\sim q}\left[\mathbf{E}_{H_i \sim H(q)}\left[\langle\psi|H_i|\psi\rangle\,|q\rangle\right]\right]}{\zeta}$$

$$\leq \frac{\mathbf{E}_{H_i \sim H}\left[\langle\psi|H_i|\psi\rangle\right]}{\zeta} \leq \frac{a}{\zeta}$$

Frathmore consider the case in which for every state it holds that $\langle\psi|H|\psi\rangle \geq b$, and denote by α the portion of the qubits which see lass than ζk energy around them, then:

$$\langle\psi|H|\psi\rangle = \frac{1}{m} \sum_{H_i \in H} \langle\psi|H_i|\psi\rangle$$

$$= \frac{1}{m \cdot k} \sum_{q \in [n]} \sum_{H_i \in H(q)} \langle\psi|H_i|\psi\rangle$$

$$= \frac{1}{n \cdot k_2} \sum_{q \in [n]} \sum_{H_i \in H(q)} \langle\psi|H_i|\psi\rangle$$

$$\leq \frac{1}{n \cdot k_2} n \cdot k_2 \left(\alpha\zeta + (1-\alpha)\right)$$

$$\Rightarrow \alpha \leq \frac{1-b}{1-\zeta}$$

$$\langle\psi|M[H,q,\zeta]|\psi\rangle = \mathbf{E}_{\sim q}\left[\langle\psi|M[H,q,\zeta]|\psi\rangle\right]$$
$$y$$

$\square$

Definition 6.6. *Let C a qaumtum circuit, and let $P : \mathcal{C} \times s \to \mathcal{C}$ be a function which given a quantum circuit C and a seed s maps the circuit into another circuits. We will think about P as a mapping ideal circuits to those which might run in the end. We will say that C_f is a P-fault tolerece verision of C if for any state such that $C |\psi\rangle$ measure 1 with high probability, it holds that $P(C_f, s) |\psi\rangle$ measure string $\bar{1}$ (on which we think as logical 1) with high probability.*

Claim 6.6. *Let $C_f = U_T U_{T-1}..U_0$ be a P-fault tolereance circuit verision of circuit C. Than for any $t < T$ it holds that:*

$$|| P\left(U_1^\dagger U_2^\dagger .. U_t^\dagger, s' \right) P\left(U_t .. U_2 U_1, s \right) || < 1/poly(T)$$