Withdrawal note for *NLTS Hamiltonians from classical LTCs*

Zhiyang He[1] and Chinmay Nirkhe[2]

[1]Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA, 02139
[2]IBM Quantum, MIT-Watson AI Lab, Cambridge, MA, 02142
szhe@mit.edu,nirkhe@ibm.com

The original incorrect proof is provided below.

Regrettably, we need to withdraw our note arXiv:2210.02999 from the arXiv due to an unrectifiable error. It is always unfortunate when a note needs to be withdrawn, in particular, when it is a *seemingly* elegant proof of an interesting problem. In some sense, we are lucky — our withdrawal only needs to be from the arXiv as this result had not been disseminated to any conference or journal. We thank Anand Natarajan for helping us discover the issue in the proof. We hope, however, that this incorrect proof will prove useful in coming up with a simpler proof of NLTS.

Simplest counterexample The simplest argument that the stated NLTS construction is incorrect is a low-energy trivial state. The n-EPR state

$$|\Phi\rangle \overset{\text{def}}{=} \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{F}_2^n} |x\rangle\, |x\rangle$$

is always stabilized by any term $P \otimes P$ where P is a n-qubit Pauli. The Hamiltonian in our result corresponded to the CSS code with $H_{\mathsf{X}} = H_{\mathsf{Z}} = [H, H]$ for a classical code with check-matrix H. Therefore, $|\Phi\rangle$ is a ground state of such a Hamiltonian but is also a trivial state.

Where the proof goes wrong Since the simple counterexamples proves that the Hamiltonian cannot be NLTS, some line of our short proof must be incorrect. As one might suspect, the reason is because algebra over $\mathbb{F}_2$ does not behave like algebra over $\mathbb{R}$. As the counterexample above holds for a ground state, we can consider $\epsilon = 0$.

Let H be a $[n, k, d]$ classical code. First observe that the classical code with check-matrix $[H, H]$ is the union on 2^k lines in the sense that

$$\ker[H, H] = \bigcup_{v \in \ker H} \ell_v \text{ where } \ell_v \overset{\text{def}}{=} \{(x \oplus v, x) : x \in \mathbb{F}_2^n\} \in \ker[H, H].$$

The first unintuitive fact about these lines is that the Hamming distance between any points $(x \oplus v, x) \in \ell_v$ and $(x' \oplus v', x') \in \ell_{v'}$ on different lines is equal to $|v \oplus v'| \geq d$. If we wanted to apply the fact that well-spread distributions require logarithmic depth circuits to generate, in principal, $\ker[H, H]$ is a good distribution to consider because it is the union of disjoint sets that are far apart. It only remains to show that the induced distribution by measuring the code in the standard or Hadamard basis is not supported on any one line.

This is precisely what happens in the above stated countexample — when $|\Phi\rangle$ is measured in the standard basis or the Hadamard basis, the resulting distribution will always be supported on ℓ_{0^n}. The incorrect statement in our proof is that there is a way to pick anti-commuting logical operators Z^w and X^u such that the lines $\{\ell_v\}$ divide evenly as $+1$ and -1 eigenvalues of the operators Z^w and X^u. This is false and our mistake.

To see why it is impossible to pick such logical operators, notice that in order to not divide any particular line, $w = (v, v)$ in order to be "parallel" to the lines $\{\ell_v\}$. By symmetry, $u = (v', v')$. This is a contradiction as then Z^w and X^u commute. We incorrectly state that picking $w = (v, 0)$ is sufficient but this divides each line into two halves. We incorrectly thought that because $Z^{(v,0)}$ is a logical operator, the distance between the two halves defined by this operator would be large. In fact it is 2, the distance of the code.

Relation to [EH17] Many readers might be familiar with the proof by Eldar and Harrow that QLTCs of linear distance are NLTS Hamiltonians. Our proof attempted to do that by arguing that there exists a single qubit in the exotic QLTC code of [CHN+22] which is constructed by two large anti-commuting Pauli operators while other logical qubits are defined by $O(1)$ anti-commuting Pauli operators. In the same paper, Eldar and Harrow were able to argue the construction of NLETS Hamiltonians by finding a qubit which "locally-manifested" minimal distance. They find such a logical qubit in the hypergraph product code. Our hope was that since the exotic QLTC code had some qubits with locally-manifested minimal distance, we would not need that all the qubits were protected by large distance. When the worst-case distance of the code is large, pick a logical operator Z^w does divide the measurement distribution into two halves with a large distance between them. This is the step that differentiates the proof of [EH17] from ours.

Personal notes Thomas Vidick [Vid20] and Scott Aaronson [Aar16] have wonderful blog posts on their prior retractions and this gave us some solace in the fact that errors (and subsequent retractions) can happen to anyone. While we are somewhat frustrated that we didn't discover this issue before putting the note online — especially when the counterexample is so ridiculously simple — we are glad that our research community has a tolerance for mistakes.

Original (incorrect) proof

In this short note, we provide a completely self-contained construction of a family of NLTS Hamiltonians [FH14] based on ideas from [ABN22], [CHN+22] and [EH17]; all omitted facts are proven in the appendix. Crucially, it does not require optimal-parameter quantum LDPC codes and can be built from simple classical LTCs such as the repetition code on an expander graph. Furthermore, it removes the constant-rate requirement from the construction of [ABN22]. We recommend [Nir22] for an introduction to the NLTS problem and a proof of the result of [ABN22].

Theorem 1. *There exists a fixed constant $\epsilon > 0$ and an explicit family of $O(1)$-local frustration-free commuting Hamiltonians $\{\mathbf{H}^{(n)}\}_{n=1}^{\infty}$ where $\mathbf{H}^{(n)} = \sum_{i=1}^{m} h_i^{(n)}$ acts on n particles and consists of $m = \Theta(n)$ local terms such that for any family of states $\{\psi_n\}$ satisfying $\mathrm{tr}\big(\mathbf{H}^{(n)}\psi\big) < \epsilon n$, the circuit complexity of the state ψ_n is at least $\Omega(\log n)$.*

Like [ABN22], we will prove that the local Hamiltonians corresponding to a family of quantum CSS codes are NLTS. Proving an NLTS result amounts to proving circuit lower bounds for *all* low energy states of a Hamiltonian $\mathbf{H}$. A simple way of proving logarithmic circuit lower bounds is to show that every low-energy state induces a *well-spread* distribution when measured in either the standard or Hadamard basis.

Fact 1 (Fact 4 of [ABN22])**.** *Let D be a probability distribution on n bits generated by measuring the output of a quantum circuit in the standard basis. If two sets $S^0, S^1 \subset \{0,1\}^n$ satisfy $D(S^0), D(S^1) \geq \mu$, and $\operatorname{dist}(S^0, S^1)$ is the minimum Hamming distance between elements of the sets, then the depth of the circuit is at least*

$$\frac{1}{3} \log \left(\frac{\operatorname{dist}(S^0, S^1)^2}{400n \cdot \log \frac{1}{\mu}} \right). \tag{1}$$

A fruitful technique (used in [EH17, Theorem 45] and [ABN22, Theorem 1]) for showing that a distribution is well-spread is to show that the distribution is (1) mostly supported on $S^0 \cup S^1$ and second (2) using an uncertainty principle prove that the distribution must have constant mass on both S^0 and S^1.

In the context of quantum CSS codes, this idea manifests very easily. Let us consider a CSS code on $2n$ qubits. The code is constructed by taking two classical codes C_{x} and C_{z} such that $C_{\mathsf{z}} \supset C_{\mathsf{x}}^{\perp}$. The code C_{z} is the kernel of a row- and column-sparse matrix $H_{\mathsf{z}} \in \mathbb{F}_2^{m_{\mathsf{z}} \times 2n}$; the same for C_{x} and $H_{\mathsf{x}} \in \mathbb{F}_2^{m_{\mathsf{x}} \times n}$. The following fact due to Markov's inequality proves large support.

Fact 2 (From Theorem 1 of ABN22)**.** *We define G_{z}^{δ} as the set of vectors which violate at most a δ-fraction of checks from C_{z}, i.e. $G_{\mathsf{z}}^{\delta} = \{y : |H_{\mathsf{z}} y| \leq \delta m_{\mathsf{z}}\}$. We similarly define G_{x}^{δ}. Consider a state ψ on n qubits such that $\operatorname{tr}(\mathbf{H}\psi) \leq \epsilon n$. Let D_{x} and D_{z} be the distributions generated by measuring the ψ in the (Hadamard) $X-$ and (standard) $Z-$ bases, respectively. Then, with the choice $\epsilon_1 = \frac{200n}{\min\{m_{\mathsf{x}}, m_{\mathsf{z}}\}} \cdot \epsilon$,*

$$D_{\mathsf{z}}(G_{\mathsf{z}}^{\epsilon_1}), D_{\mathsf{x}}(G_{\mathsf{x}}^{\epsilon_1}) \geq \frac{99}{100}. \tag{2}$$

Next, we see that $G_{\mathsf{z}}^{\epsilon_1}$ (and, likewise, $G_{\mathsf{x}}^{\epsilon_1}$) can be expressed as $S_v^0 \cup S_v^1$ for two sets that are far apart. To see this, we need to consider a specific code. For this, we consider the "exotic" quantum locally testable code from [CHN+22]. To define the code of [CHN+22], choose a classical LTC C with check-matrix $H \in \mathbb{F}_2^{m \times n}$ of non-zero dimension, distance d and soundness ρ. Consider, the quantum CSS code Q defined by $H_{\mathsf{x}} = H_{\mathsf{z}} = [H, H] \in \mathbb{F}_2^{m \times 2n}$.

Fact 3 (Part of Theorem 1.1 of [CHN+22])**.** *$C_{\mathsf{x}} = C_{\mathsf{z}}$ are LTCs with soundness 2ρ.*

Since C has non-zero dimension, for any non-zero $v \in C$ and $x \in \mathbb{F}_2^n$, it is easy to see that $w \overset{\mathsf{def}}{=} (x \oplus v, x) \in C_{\mathsf{z}}$. Pick a linearly independent basis $\{v = v_1, \ldots, v_k\} \subset \mathbb{F}_2^n$ for C. Define the sets

$$C_v^0 \overset{\mathsf{def}}{=} \left\{ \left(y \oplus \left(\textstyle\sum_{j>1}^k a_j v_j \right), y \right) \ : \ a_2, \cdots, a_k \in \mathbb{F}_2, y \in \mathbb{F}_2^n \right\}, \tag{3a}$$

$$C_v^1 \overset{\mathsf{def}}{=} C_v^0 \oplus (v, 0) = C_v^0 \oplus (0, v) = \left\{ w \oplus \left(z \oplus \left(\textstyle\sum_{j>1}^k b_j v_j \right), z \right) \mid b_2, \cdots, b_k \in \mathbb{F}_2, z \in \mathbb{F}_2^n \right\}. \tag{3b}$$

Then $C_{\mathsf{z}} = C_v^0 \cup C_v^1$. Since the field is $\mathbb{F}_2$, the distance between any two points $c_0 \in C_v^0$ and $c_1 \in C_v^1$ is

$$\left| v \oplus \textstyle\sum_{j>1}^k (a_j + b_j) v_j \right|. \tag{4}$$

Since the basis is linearly independent, this is a non-zero vector $\in C$ and therefore has weight at least d. Therefore, the Hamming distance between sets C_v^0 and C_v^1 is $\geq d$. Since C_z is a LTC with soundness 2ρ, by the definition of local testability, we know that $G_z^{\epsilon_1}$ is contained in $B_r(C_\mathsf{z})$, the ball of radius $r \overset{\text{def}}{=} \frac{\epsilon_1 n}{2\rho}$ about C_z. Then,

$$G_z^{\epsilon_1} \subset S_v^0 \cup S_v^1 \text{ where } S_v^0 \overset{\text{def}}{=} B_r(C_v^0) \text{ and } S_v^1 \overset{\text{def}}{=} B_r(C_v^1). \tag{5}$$

Whenever, $r < d/4$, then the distance between S_v^0 and S_v^1 is $> d/2$. A similar statement can be made for C_x. Now it only remains to use an uncertainty principle.

Fact 4 (Lemma 37 of [EH17])**.** *Let A and B be two anti-commuting Hermitian operators such that $A^2 = B^2 = \mathbb{I}$. For any state $|\psi\rangle$, $\frac{1}{2} \geq \min(\mathrm{tr}(A\psi)^2, \mathrm{tr}(B\psi)^2)$.*

To apply this uncertainly lemma, pick $w = (v, 0)$ and $u = (e_i, e_i \oplus v)$ for $v \in C$ and $e_i^\top v = 1$. Then the operators $A = Z^w$ and $B = X^u$ anti-commute. If $\frac{1}{2} \geq \mathrm{tr}(A\psi)^2$, then using Fact 2, we have that

$$D_\mathsf{z}(S_v^0), D_\mathsf{z}(S_v^1) \geq \frac{1}{2} - \frac{1}{2\sqrt{2}} - 2 \cdot \frac{1}{100} > \frac{1}{10}. \tag{6}$$

Therefore, the distribution is well-spread. Likewise, if $\frac{1}{2} \geq \mathrm{tr}(B\psi)^2$, then a similar well-spread distribution must occur (but in the Hadamard basis). By Fact 1,

Theorem 1 (Formal statement)**.** *Consider the CSS code Q on $2n$ qubits built from $H_\mathsf{x} = H_\mathsf{z} = [H, H]$ where $H \in \mathbb{F}_2^{m \times n}$ is the check-matrix of a classical LTC with non-zero dimension, distance d and soundness ρ. Let $\mathbf{H}$ be the corresponding local Hamiltonian consisting of $2m$ terms and $2n$ qubits. Then for*

$$\epsilon < \frac{dm\rho}{400n^2} \tag{7}$$

and every state ψ such that $\mathrm{tr}(\mathbf{H}\psi) \leq \epsilon n$, the circuit depth of ψ is at least $\frac{1}{3}\log\left(\frac{d^2}{6400n}\right)$.

Many n- bit classical LDPC code with linear-distance and positive soundness exist. One simple example is the repetition code with check matrix equal to the edge-vertex incidence matrix of a Ramanujan graph (or any expander).

Appendix[a]

Proof of Fact 1: Let $|\rho\rangle = U|0\rangle^{\otimes n'}$ on $n' \geq n$ qubits, where U is a depth t quantum circuit such that when $|\rho\rangle$ is measured in the standard basis, the resulting distribution is D. Note that $n' \leq 2^t n$ without loss of generality (see [Nir22, Section 3.1] for a justification based on the light cone argument). The Hamiltonian

$$\mathbf{H}_U = \mathop{\mathbf{E}}_{i=1}^{n'} U|1\rangle\langle 1|_i U^\dagger \tag{8}$$

has $|\rho\rangle$ as its unique ground-state, is commuting, has locality 2^t, and has eigenvalues $0, 1/n', 2/n', \ldots 1$. There exists a polynomial P of degree f, built from Chebyshev polynomials, such that

$$P(0) = 1, \qquad |P(i/n')| \leq \exp\left(-\frac{f^2}{100n'}\right) \leq \exp\left(-\frac{f^2}{100 \cdot 2^t n}\right) \text{ for } i = 1, 2, \ldots, n'. \tag{9}$$

See [AAG22, Theorem 3.1] for details on the construction of P. Applying the polynomial P to the Hamiltonian G results in an *approximate ground-state projector*, $P(\mathbf{H}_U)$, such that

$$\| \, |\rho\rangle\langle\rho| - P(\mathbf{H}_U)\|_\infty \leq \exp\left(-\frac{f^2}{100 \cdot 2^t n}\right) \tag{10}$$

Furthermore, $P(\mathbf{H}_U)$ is a $f \cdot 2^t$ local operator. Setting $u \overset{\mathsf{def}}{=} \mathrm{dist}(S^0, S^1)$ and choosing $f \overset{\mathsf{def}}{=} \frac{u}{2^{t+1}}$, we obtain

$$\| \, |\rho\rangle\langle\rho| - P(\mathbf{H}_U)\|_\infty \leq \exp\left(-\frac{u^2}{400 \cdot 2^{3t} n}\right). \tag{11}$$

Let Π_{S^0}, Π_{S^1} be projections onto the strings in sets S^0, S^1 respectively. Note that $\Pi_{S^0} P(\mathbf{H}_U) \Pi_{S^1} = 0$, which implies

$$\|\Pi_{S^0} \, |\rho\rangle\langle\rho| \, \Pi_{S_1}\|_\infty \leq \exp\left(-\frac{u^2}{400 \cdot 2^{3t} \cdot n}\right). \tag{12}$$

However,

$$\|\Pi_{S^0} \, |\rho\rangle\langle\rho| \, \Pi_{S^1}\|_\infty = \sqrt{\langle\rho| \, \Pi_{S^0} \, |\rho\rangle \cdot \langle\rho| \, \Pi_{S^1} \, |\rho\rangle} = \sqrt{D(S^0) D(S^1)} \geq \mu. \tag{13}$$

Thus, $2^{3t} \geq \frac{u^2}{400 \cdot \log \frac{1}{\mu} \cdot n}$, which rearranges into the fact statement. □

Proof of Fact 2: By construction,

$$\epsilon n \geq \mathrm{tr}(\mathbf{H}\psi) \geq \mathrm{tr}(\mathbf{H}_{\mathsf{z}}\psi) = \mathop{\mathbf{E}}_{y \sim D_{\mathsf{z}}} |H_{\mathsf{z}} y|. \tag{14}$$

Here, the last equality holds since for a Pauli operator Z^a, $\langle y| \, \frac{\mathbb{1} - Z^a}{2} \, |y\rangle = \frac{1 - (-1)^{a.y}}{2} = a.y$. Let $q \overset{\mathsf{def}}{=} D_{\mathsf{z}}(G_{\mathsf{z}}^{\epsilon_1})$ be the probability mass assigned by D_{z} to $G_{\mathsf{z}}^{\epsilon_1}$. Then,

$$\mathop{\mathbf{E}}_{y \sim D_{\mathsf{z}}} |H_{\mathsf{z}} y| \geq 0 \cdot q + (1 - q) \cdot \epsilon_1 m_{\mathsf{z}} = (1 - q)\epsilon_1 m_{\mathsf{z}}. \tag{15}$$

Therefore, $D_{\mathsf{z}}(G_{\mathsf{z}}^{\epsilon_1}) \geq 1 - \epsilon n/(\epsilon_1 m_{\mathsf{z}})$. A similar argument shows that $D_{\mathsf{x}}(G_{\mathsf{x}}^{\epsilon_1}) \geq 1 - \epsilon n/(\epsilon_1 m_{\mathsf{x}})$. With the choice $\epsilon_1 = \frac{200n}{\min\{m_{\mathsf{x}}, m_{\mathsf{z}}\}} \cdot \epsilon$, we get the statement of the fact. □

Proof of Fact 3: It is easy to check that $C_{\mathsf{z}} \supseteq \{(x \oplus v, x) : x \in \mathbb{F}_2^n, v \in C\}$, since $H_{\mathsf{z}} = [H, H]$. For equality, notice that for any $(x, x \oplus v') \in C_{\mathsf{z}}$, then $Hx \oplus Hx \oplus Hv' = 0 \implies v' \in C$.

For local testability, we want to show $\forall x, v' \in \mathbb{F}_2^n$,

$$\frac{|H_{\mathrm{Z}}(x \oplus v', x)|}{m} \geq 2\rho \cdot \frac{d((x \oplus v', x), C_{\mathrm{Z}})}{2n}. \tag{16}$$

We first note that $|H_{\mathrm{Z}}(x \oplus v', x)| = |Hv'|$. Moreover, $d((x \oplus v', x), C_{\mathrm{Z}}) = d(v', C)$. By ρ-local testability of C, C_{Z} is locally testable with soundness 2ρ. This also proves (by Fact 17 of [EH17]) that Q is locally testable with soundness 2ρ. □

Proof of Fact 4: Let $\langle A \rangle = \mathrm{tr}(A\psi)$. Likewise, for B. If we define $C = \langle A \rangle A + \langle B \rangle B$ and $\lambda = \langle A \rangle^2 + \langle B \rangle^2$, then notice that

$$C^2 = \langle A \rangle^2 A^2 + \langle A \rangle \langle B \rangle (AB + BA) + \langle B \rangle^2 B^2 = \langle A \rangle^2 + \langle B \rangle^2 = \lambda \tag{17}$$

and that $\lambda = \langle C \rangle$. Since variance is non-negative, $\lambda^2 = \langle C \rangle^2 \leq \langle C^2 \rangle = \lambda \implies 0 \leq \lambda \leq 1$. Therefore, $\mathrm{tr}(A\psi)^2 + \mathrm{tr}(B\psi)^2 \leq 1$ which implies the statement. □

[a] Proofs of Facts 1 and 2 are copied from [ABN22], with permission.

References

[AAG22] Anurag Anshu, Itai Arad, and David Gosset. An area law for 2d frustration-free spin systems. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2022, page 12–18, New York, NY, USA, 2022. Association for Computing Machinery. doi:10.1145/3519935.3519962. 5

[Aar16] Scott Aaronson. More Wrong Things I Said in Papers — scottaaronson.blog. `https://scottaaronson.blog/?p=2854`, 2016. [Accessed 08-Oct-2022]. 2

[ABN22] Anurag Anshu, Nikolas P. Breuckmann, and Chinmay Nirkhe. NLTS Hamiltonians from good quantum codes, 2022. doi:10.48550/ARXIV.2206.13228. 2, 3, 6

[CHN+22] Andrew Cross, Zhiyang He, Anand Natarajan, Mario Szegedy, and Guanyu Zhu. Quantum locally testable code with exotic parameters, 2022. doi:10.48550/ARXIV.2209.11405. 2, 3

[EH17] L. Eldar and A. W. Harrow. Local hamiltonians whose ground states are hard to approximate. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 427–438, 2017. doi:10.1109/FOCS.2017.46. 2, 3, 4, 6

[FH14] Michael H. Freedman and Matthew B. Hastings. Quantum systems on non-k-hyperfinite complexes: A generalization of classical statistical mechanics on expander graphs. *Quantum Info. Comput.*, 14(1–2):144–180, January 2014. 2

[Nir22] Chinmay Nirkhe. *Lower bounds on the complexity of quantum proofs*. PhD thesis, EECS Department, University of California, Berkeley, Aug 2022. `http://www2.eecs.berkeley.edu/Pubs/TechRpts/2022/EECS-2022-184.html`. 2, 4

[Vid20] Thomas Vidick. It happens to everyone. . . but it's not fun — mycqstate.wordpress.com. `https://mycqstate.wordpress.com/2020/09/29/it-happens-to-everyonebut-its-not-fun/`, 2020. [Accessed 08-Oct-2022]. 2