NLTS Hamiltonians from classical LTCs

Zhiyang He\textsuperscript{1} and Chinmay Nirkhe\textsuperscript{2}

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

In this short note, we provide a completely self-contained construction of a family of NLTS Hamiltonians \[\{H^{(n)}\}_{n=1}^{\infty}\] based on ideas from \[\text{[ABN22]}, \text{[CHN}^{+}\text{22]}\text{ and [EH17]}\]; 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 \[\text{[ABN22]}\]. We recommend \[\text{[Nir22]}\] for an introduction to the NLTS problem and a proof of the result of \[\text{[ABN22]}\].

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

Like \[\text{[ABN22]}\], 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 $H$. 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 \[\text{[ABN22]}\]). 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 $\text{dist}(S^0, S^1)$ is the minimum Hamming distance between elements of the sets, then the depth of the circuit is at least

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

(1)

A fruitful technique (used in \[\text{[EH17]}\text{, Theorem 45]}\] and \[\text{[ABN22]}\text{, Theorem 1]}\] 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 $C_z \supseteq C_x^\perp$. The code $C_z$ is the kernel of a row- and column-sparse matrix $H_z \in \mathbb{F}_2^{m_z \times 2n}$; the same for $C_x$ and $H_x \in \mathbb{F}_2^{m_x \times n}$. The following fact due to Markov’s inequality proves large support.

**Fact 2** (From Theorem 1 of \[\text{[ABN22]}\]). We define $G^\delta_x$ as the set of vectors which violate at most a $\delta$-fraction of checks from $C_x$, i.e. $G^\delta_x = \{ y : |H_{zy}| \leq \delta m_z \}$. We similarly define $G^\delta_z$. Consider a state $\psi$ on $n$ qubits such that $\text{tr}(H\psi) \leq \epsilon n$. Let $D_x$ and $D_z$ be the distributions generated by measuring the $\psi$ in the (Hadamard) $X$- and (standard) $Z$- bases, respectively. Then, with the choice $\epsilon_1 = \frac{200}{\min\{m_x, m_z\}} \cdot \epsilon$,

$$D_x(G^\delta_x), D_z(G^\delta_z) \geq \frac{99}{100} \epsilon.$$

(2)
Next, we see that $G_2^{e_1}$ (and, likewise, $G_x^{e_1}$) 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 $\rho$. Consider, the quantum CSS code $Q$ defined by $H_k = H_z = [H, H] \in \mathbb{F}_2^m \times 2n$.

**Fact 3** (Part of Theorem 1.1 of [CHN+22]). $C_x = C_z$ are LTCs with soundness $2\rho$.

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 $w \defeq (x \oplus v, x) \in C_z$. Pick a linearly independent basis \{\(v = v_1, \ldots, v_k\)\} $\in \mathbb{F}_2^n$ for $C$. Define the sets
\[
C_0^v = \left\{ y \oplus \left( \sum_{j=1}^k a_j v_j \right), y \right\} : a_2, \ldots, a_k \in \mathbb{F}_2, y \in \mathbb{F}_2^n, \right\},
\]
\[
C_1^v = C_0^v \oplus (v, 0) = C_0^v \oplus (0, v) = \left\{ w \oplus \left( z \oplus \left( \sum_{j=1}^k b_j v_j \right), z \right) \right\} \left| b_2, \ldots, b_k \in \mathbb{F}_2, z \in \mathbb{F}_2^n \right\}.
\]
Then $C_z = C_0^v \cup C_1^v$. Since the field is $\mathbb{F}_2$, the distance between any two points $c_0 \in C_0^v$ and $c_1 \in C_1^v$ is
\[
\left| v \oplus \sum_{j=1}^k (a_j + b_j) v_j \right|.
\]

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 $C_0^v$ and $C_1^v$ is $\geq d$. Since $C_z$ is a LTC with soundness $2\rho$, by the definition of local testability, we know that $G_2^{e_1}$ is contained in $B_r(C_z)$, the ball of radius $r \defeq \frac{\epsilon/m}{\rho}$ about $C_z$. Then,
\[
G_2^{e_1} \subset S_v^0 \cup S_v^1 \text{ where } S_v^0 \defeq B_r(C_0^v) \text{ and } S_v^1 \defeq B_r(C_1^v).
\]

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 $A^2 = B^2 = I$. For any state $|\psi\rangle$, $\frac{1}{2} \geq \min(\text{tr}(A\psi)^2, \text{tr}(B\psi)^2)$.

To apply this uncertainty 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 $\frac{1}{2} \geq \text{tr}(A\psi)^2$, then using Fact 2 we have that
\[
D_2(S_v^0), D_2(S_v^1) \geq \frac{1}{2} - \frac{1}{2\sqrt{2}} - 2 \cdot \frac{1}{100} > \frac{1}{10}.
\]
Therefore, the distribution is well-spread. Likewise, if $\frac{1}{2} \geq \text{tr}(B\psi)^2$, 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 $H_k = H_z = [H, H]$ 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 $\rho$. Let $H$ be the corresponding local Hamiltonian consisting of $2m$ terms and $2n$ qubits. Then for
\[
\epsilon < \frac{dp}\ln(400n^2)
\]
and every state $\psi$ such that $\text{tr}(H\psi) \leq \epsilon n$, the circuit depth of $\psi$ is at least $\frac{1}{3} \log \left( \frac{d^2}{\epsilon^2} \right)$.
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

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

[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

[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

[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.

[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

Appendix

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

$$H_U = \sum_{i=1}^{n'} U |i\rangle\langle i| U^\dagger$$

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

$$P(0) = 1, \quad |P(i/n')| \leq \exp\left(-\frac{f^2}{100n'}\right) \leq \exp\left(-\frac{f^2}{100 \cdot 2^n}\right) \quad \text{for} \ i = 1, 2, \ldots, n'. \quad (9)$$

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, $P(H_U)$, such that

$$\| |\rho\rangle\langle \rho| - P(H_U) \|_{\infty} \leq \exp\left(-\frac{f^2}{100 \cdot 2^n}\right) \quad (10)$$

1Proofs of Facts 1 and 2 are copied from [ABN22], with permission.
Furthermore, $P(H_U)$ is a $f \cdot 2^f$ local operator. Setting $u \overset{\text{def}}{=} \text{dist}(S^0,S^1)$ and choosing $f \overset{\text{def}}{=} \frac{u}{2\sqrt{n}}$, we obtain
\begin{equation}
\| \rho \| P(H_U) \rho \|_{\infty} \leq \exp \left( -\frac{u^2}{400 \cdot 2^3 \cdot n} \right). \tag{11}
\end{equation}

Let $\Pi_{S^0}, \Pi_{S^1}$ be projections onto the strings in sets $S^0,S^1$ respectively. Note that $\Pi_{S^0} P(H_U) \Pi_{S^1} = 0$, which implies
\begin{equation}
\| \Pi_{S^0} |\rho\| \Pi_{S^1} \|_{\infty} \leq \exp \left( -\frac{u^2}{400 \cdot 2^3 \cdot n} \right). \tag{12}
\end{equation}

However,
\begin{equation}
\| \Pi_{S^0} |\rho\| \Pi_{S^1} \|_{\infty} = \sqrt{\langle \rho | \Pi_{S^0} |\rho\| \Pi_{S^1} |\rho\|} = \sqrt{D(S^0)D(S^1)} \geq \mu. \tag{13}
\end{equation}

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

**Proof of Fact 2**: By construction,
\begin{equation}
\epsilon n \geq \text{tr}(H_{\psi}) \geq \text{tr}(H_{\psi} |\psi\| \leq \mathbf{E}_{y \sim D_z} |H_z y|). \tag{14}
\end{equation}

Here, the last equality holds since for a Pauli operator $Z^a$, $\langle y | \frac{Z^a}{2} | y \rangle = \frac{1-(-1)^{a,y}}{2} = a \cdot y$. Let $q \overset{\text{def}}{=} D_z (G_z^{e_1})$ be the probability mass assigned by $D_z$ to $G_z^{e_1}$. Then,
\begin{equation}
\mathbf{E}_{y \sim D_z} |H_z y| \geq 0 \cdot q + (1-q) \cdot \epsilon_1 m_z = (1-q)^{\epsilon_1 m_z}. \tag{15}
\end{equation}

Therefore, $D_z (G_z^{e_1}) \geq 1 - \epsilon n / (\epsilon_1 m_z)$. A similar argument shows that $D_q (G_q^{e_1}) \geq 1 - \epsilon n / (\epsilon_1 m_q)$. With the choice $\epsilon_1 = \frac{\text{min}(m_x, m_z)}{200n} \cdot \epsilon$, we get the statement of the fact. \qed

**Proof of Fact 3**: It is easy to check that $C_z \supseteq \{(x \oplus v, x) : x \in \mathbb{F}_2^n, v \in C\}$, since $H_z = [H, H]$. For equality, notice that for any $(x, x \oplus v') \in C_z$, then $H x \oplus H x \oplus H v' = 0 \implies v' \in C$. For local testability, we want to show $\forall x, v' \in \mathbb{F}_2^n$,
\begin{equation}
\frac{|H_z (x \oplus v', x)|}{m} \geq 2\rho \cdot \frac{d((x \oplus v', x), C_z)}{2n}. \tag{16}
\end{equation}

We first note that $|H_z (x \oplus v', x)| = |H v'|$. Moreover, $d((x \oplus v', x), C_z) = d(v', C)$. By $\rho$-local testability of $C$, $C_z$ is locally testable with soundness $2\rho$. This also proves (by Fact 17 of \cite{EH17}) that $Q$ is locally testable with soundness $2\rho$. \qed

**Proof of Fact 4**: Let $\langle A \rangle = \text{tr}(A \psi)$. 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
\begin{equation}
C^2 = \langle A \rangle^2 A^2 + \langle A \rangle (AB + BA) + (B^2) B^2 = \langle A \rangle^2 + \langle B \rangle^2 = \lambda \tag{17}
\end{equation}

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, $\text{tr}(A \psi)^2 + \text{tr}(B \psi)^2 \leq 1$ which implies the statement. \qed