Local Hamiltonians with Approximation-Robust Entanglement

Lior Eldar*

April 6, 2015

Abstract

Quantum entanglement is considered, by and large, to be a very delicate and non-robust phenomenon that is very hard to maintain in the presence of noise, or non-zero temperatures. In recent years however, and motivated, in part, by a quest for a quantum analog of the PCP theorem \cite{1,2}, researches have tried to establish whether or not we can preserve quantum entanglement at “constant” temperatures that are independent of system size. This would imply that any quantum state with energy at most, say 0.05 of the total available energy of the Hamiltonian, would be highly-entangled. However to this date, no such systems were found, and moreover, it became evident that even embedding local Hamiltonians on robust, albeit “non-physical” topologies, namely expanders, does not guarantee entanglement robustness \cite{10,4}.

In this study, we indicate that such robustness may be possible after all: first, we relax the approximation condition in a way that is reminiscent of classical approximation problems: instead of asking that any quantum state with fractional energy at most 0.05 be highly-entangled, we just ask that any quantum state violating a fraction at most 0.05 of constraints is highly-entangled. Then, we define a new ”handle” on entanglement of a quantum state by considering what is the minimal-depth Boolean circuit for approximately simulating any tensor-product measurement performed on that state.

We then construct an infinite family of $O(1)$-local Hamiltonians, corresponding to check terms of a quantum error-correcting code with the following property of combinatorial inapproximability: any quantum state that violates a fraction at most 0.05 of all local terms cannot be even approximately simulated by classical circuits whose depth is sub-logarithmic in the number of qubits. In a sense, this implies that even providing a ”witness” to the fact that the local Hamiltonian can be ”almost” satisfied, requires long-range entanglement.

Our construction is but a first step in what, we believe, is a whole range of possible entanglement-robust local Hamiltonians. One could attempt to find robust-entanglement that is also useful for computation, robust against ”spectral” (instead of just ”combinatorial”) approximation, and robust against other, more physically-natural, criteria, like bounded-depth quantum circuits (NLTS \cite{13}).

1 Introduction

1.1 The search for robust forms of entanglement

The phenomenon of quantum entanglement has boggled the minds of researchers for the last 80 years and our understanding of it even today is far from satisfactory. In particular, entanglement
is considered as a very delicate, non-robust property, that is very susceptible to decoherence. It is in fact this non-robustness of entanglement that plays a key role in preventing the construction of a quantum computer.

In condensed matter physics, as well as in quantum complexity theory, entanglement is usually considered as a property of the ground-state of a locally-defined quantum system, namely a local Hamiltonian. Under this framework, the delicate nature of entanglement is loosely stated as the inability to maintain entanglement at “room temperature”. Perhaps more formally, it means that if we consider the set of quantum states, starting from the ground-state, up to energy at most some constant \( \epsilon > 0 \) fraction of the total available energy, we can already find non-entangled states. In the last several years, motivated in part by a search for a quantum analog of the PCP theorem \([1, 2]\), researchers have explored the possibility of having locally-defined systems (i.e. local Hamiltonians) in which the quantum ground-state entanglement does not break-up completely at non-zero temperatures. From a computer-science-theoretic view this implies, in a sense, that even approximation of the ground-energy will require a significant measure of entanglement. Thus far, there have been no such examples. Perhaps this is not so surprising, as most known examples of local Hamiltonians, particularly those that are physically motivated, are embedded on a regular low-dimensional lattice. The ground-energy of such systems can be readily approximated by “cutting-out” boxes out of this grid, and satisfying each box separately, in a tensor-product fashion, while disregarding the boundary constraints of these boxes altogether.

However, this instability of entanglement was mystified even further, when negative results came out indicating that perhaps even embedding local Hamiltonians on the extreme opposite of lattices, namely expanders, and high-degree graphs will not allow us to retain entanglement at non-zero temperature: in \([10]\) the authors show that any 2-local Hamiltonian, with sufficiently high degree / expansion has low-energy states which are tensor-products, i.e. are completely non-entangled. Similarly, in \([4]\), the authors consider the class of commuting local Hamiltonians (not necessarily 2-local), and show that for such Hamiltonians, whose corresponding interaction graph has a so called high “local expansion”, there exist tensor-product approximations to the ground-state.

In \([13]\), Freedman and Hastings have proposed a formal definition of such robustness called NLTS (see section 3, for its definition). Their definition captures the ability of entanglement to exist in all low-energy states, by preventing constant-depth quantum circuits from generating such states. In that paper, they constructed a system with one-sided-NLTS, in which if one is allowed an energy penalty only from a specific type of local terms, then for sufficiently low energy, such states can be shown to have quantum circuit lower-bounds. However, in general, such systems can be assigned a tensor-product state which approximates the ground energy to a vanishing additive error.

1.2 Statement of Main Results

In this work, we provide, to the best of our knowledge, the first example of a quantum system whose entanglement is robust against approximation, in a well-defined sense. Our notion of “robustness” seeks not to enforce entanglement on any low-energy state as in NLTS. Instead, and reminiscent of the classical notion of approximation, we only ask that any quantum state that satisfies a fraction at least, say, 0.95 of all local terms of the initial Hamiltonian, would still preserve a significant amount of entanglement. Our proxy to entanglement is to relate to the complexity of approximating the distribution induced by measuring a quantum state, by some tensor-product basis:

**Definition 1. Quantum states hard for bounded-depth circuits (sketch)**

A quantum state \( |\psi\rangle \) on \( n \) qubits is said to be bounded-depth-hard, if there exists a tensor-product basis \( B \), such that the distribution on corresponding observation values \( m_1, \ldots, m_n \in \{0, 1\}^n \) cannot be approxi-
mately sampled by bounded-depth circuits, with statistical-distance error better than some \(\nu = \Omega(1)\).

We then define a local Hamiltonian to be bounded-depth-hard if all its ground states are bounded-depth-hard. Finally, we define the notion of hardness of approximation of the ground states of a local Hamiltonian as follows:

**Definition 2.** Hamiltonians with combinatorial-approximation-hardness of bounded-depth circuits (c-Type)

A local Hamiltonian \(H = \sum_{i=1}^{m} H_i\) is said to be \(\epsilon\)-c-Type bounded-depth-hard if any \(\epsilon\)-residual Hamiltonian of \(H\) (a subset of the local terms of \(H\) of size at least \(1 - \epsilon\)) is bounded-depth-hard.

Our choice of bounded-depth circuits was motivated, in part, by its connection to error-correcting codes in [19]: in that result, the authors show that bounded-depth circuits cannot approximate well a uniform distribution over a good linear code (e.g. a code with linear distance). Our system of robust entanglement will, in fact, be built using quantum error correcting codes.

Quantum error-correcting codes are systems which protect encoded information by essentially spreading it out over a much larger Hilbert space, using entanglement. As such, they are natural candidates for quantum systems whose distribution induced by tensor-product measurements is hard to simulate. This we show in Claim 2. We prove that quantum CSS code-states are indeed hard to simulate for at least one of two tensor-product bases. These are, incidentally, the bases that corresponds to the dual-orthogonal codes that comprise them - namely the Hadamard basis, and the standard basis. Though perhaps technically interesting, morally - this is not surprising.

However, as mentioned before, previous constructions of (families of) quantum CSS codes, are unable to retain that property after allowing arbitrary removal of some low, but constant fraction of the local checks. In other words, if we allow quantum states to satisfy a fraction at least \(1 - \epsilon\) of all local constraints, instead of exactly 1, then there are already very simple quantum states that answer this criterion. Such quantum states can be readily simulated (in some tensor-product basis) using bounded-depth classical circuits.

In 2009, Tillich and Zémor [21] have, in a breakthrough paper, provided the first example of a quantum 'code' template. By their construction, given a pair of classical codes, one produces a quantum code, while inheriting some of the parameters of the original classical codes. We use their construction, plugging in classical locally-testable codes, and then prove, using known bounded-depth techniques our central lemma:

**Lemma.** (sketch) Let \(C\) be some locally testable parity-check code with soundness parameter \(\rho = \Omega(1)\) and relative minimal distance \(\delta = \Omega(1)\). Let \(C_x = C \times_{TZ} C\) be the Tillich-Zémor product of \(C\) with itself. \(C_x\) is \(\epsilon\)-c-Type bounded-depth-hard with \(\epsilon = \Omega(\delta \rho) = \Omega(1)\).

We then apply the Tillich Zémor product to a set of locally-testable parity checks defining the Hadamard code. The result is a quantum code \(C_x\) whose corresponding Hamiltonian is \(O(1)\) local, and is hard to simulate, even up to combinatorial approximation constant \(c_0 = \Omega(1)\), for any polynomial size circuit of depth \(O(\log^{1-\delta}(n))\), for any \(\delta > 0\). This implies that any quantum state satisfying a fraction at least \(1 - c_0\) of the checks of \(C_x\) is highly-entangled. Alternatively, discarding any subset of the local checks of \(C_x\) of fractional size at most \(c_0\), would not devoid the residual code from its bounded-depth hardness. This is our main theorem:

**Theorem.** (sketch) There exists a constant \(\epsilon > 0\), an explicit infinite family of \(O(1)\)-local Hamiltonians \(\{H_n\}_n\), such that for any constant \(\delta > 0\), and integer \(n\) the following holds: any quantum state \(|\psi_n\rangle\) satisfying a fraction at least \(1 - \epsilon\) of the checks of \(H_n\) cannot be even approximately simulated by circuits of depth less than \(O(\log^{1-\delta}(n))\).

We note that the quantum code derived in this fashion is a code on \(n\) qubits, such that for any ground-state of some \(\epsilon\)-residual code, the number of qubits that are, in some sense, entangled,
scales only as $\tilde{\Omega}(n^{1/4})$. In other words, the scale of "provable" entanglement, is only in a vanishingly small fraction of the original system - though it is sufficiently strong to prevent bounded-depth simulation. Nevertheless, the scale of provable "robust" entanglement is asymptotically much larger than the locality of the Hamiltonian that enforces this behavior which is $O(1)$. This, in a nutshell, the robust behavior of entanglement we attempt to capture.

### 1.2.1 Implication to quantum circuit lower-bounds

The NLTS criterion [13] is arguably a more physically-natural criterion for considering the complexity of generating a quantum state. Under this criterion, quantum states are hard if they require a large-depth quantum circuit in order to be generated from a tensor-product state. To place into context with the NLTS criterion, we note that approximately sampling from the distribution of a quantum state (via a tensor-product basis) using an bounded-depth circuit, is not necessarily a weaker condition than having it generated by quantum circuits of constant depth.

First, while it is known that approximating each complex coefficient of a quantum state is NP-hard, even for quantum states of constant depth [20], our robustness against bounded-depth classical circuits, measures only the statistical distance, which is a much more relaxed condition. Thus, it is possible that quantum states generated by quantum circuits of constant-depth can, in fact, be approximated by classical circuits of constant-depth to a reasonable statistical distance error. We leave this as one of the open questions of this paper.

Furthermore, since bounded-depth circuits have un-bounded fan-in, whereas quantum circuits of constant-depth do not, then for example the OR function on $n$ bits $\text{OR}_n$ is computable by classical bounded-depth circuits, but not computable by quantum circuits of constant-depth. Hence, whereas one can sample from the distribution $x_1, \ldots, x_n, x_{n+1}$ where $x_1, \ldots, x_n$ are uniform i.i.d., and $x_{n+1} = \text{OR}(x_1, \ldots, x_n)$ in bounded-depth, this distribution is not known to be simulatable by quantum circuits of constant depth.

### 1.3 Outline of the techniques

#### 1.4 Classical techniques

Before describing the intuition behind our construction, it may be useful to survey the techniques we are using. The first two techniques, are related to classical results on bounded-depth sampling, namely [19], and are the low-noise sensitivity theorem, and the iso-perimetric inequality on the boolean hypercube. The first property (see Lemma 1 due to [9, 18]) states that given a bounded-depth circuit with uniform random input, for any average input $x \in \{0, 1\}^n$, perturbed by a random error $e$ at $p = O(1)$ locations, the difference between $x$ and $x + e$ at the output of that circuit scales at most logarithmically with the input size. The second property (see Lemma 2 due to [16, 17]) relates to the fact that for any partition of the boolean hypercube into two constant-measure sets, there exists a constant fraction of all single bit-flip edges that are arched between these sets.

Aside from these two classical techniques, we use known constructions of classical locally-testable codes (see Definition 7). Classical locally testable codes are a very important class of error-correcting codes, that have been the turnkey for all known constructions of PCP’s (see [15] for a detailed survey). In this paper, given a locally testable code, we are interested in it’s robustness - how it would behave, if we discard a small constant fraction of its local checks. Such robustness was explored in it’s classical context in [12]. Essentially, we require a simple property that follows immediately from local testability: that any codeword of an $\epsilon$-residual code is close to the original code. This, in some sense, is reading local testability in reverse: instead of asking for the penalty assigned to a word that is distant from the code, we ask for the distance of a word from the
code space, whose penalty is upper-bounded, by the fraction of local checks that we've initially discarded.

1.5 Quantum techniques

On the quantum side, we devise a useful statement that any quantum CSS code must super-pose with comparable projections, on some partition of the logical space, either in the "position" basis, or in the "momentum" basis. This lemma, called the Heisenberg uncertainty principle for CSS codes, Lemma [3] is then used as a turnkey for the main claims of this paper. Essentially, this lemma forces any quantum state of a CSS code to behave like a "CAT" state in either one of two simple bases.

The main technical effort of this work is a rather detailed analysis of the Tillich-Zémor product code [21]. The Tillich-Zémor code is a very elegant graph-product technique, denoted by $C_x = C \times_{TZ} C$, in which one can provably show that the resulting quantum code inherits some of the properties of the original codes, namely its locality (LDPC), and coding rate. This construction produces a quantum code $C_x$ given a pair of classical codes, using a natural hypergraph product $C_x = C_1 \times_{TZ} C_2$, where the product operation is a graph product of the respective Tanner graphs of the input classical codes $C_1, C_2$.

We exploit a somewhat subtle property of the Tillich-Zémor product, which is that for "reasonable" input classical codes (with no constant-bits), the logical space of the output quantum code has large equivalence classes up to a very structured logical subgroup. This logical subgroup is actually isomorphic to words of the original codes $C_1, C_2$, and in the case that $C_x$ is subjected to constraint removal, correspond to words from "noisy" versions of the comprising codes $C_1, C_2$ when subjected to a similar constraint removal process. We use this observation critically to construct a contradiction to bounded-depth sampling, described in the next section.

1.6 Overview of construction and proof

Quantum circuit lower-bounds have not been investigated thoroughly in the literature. However, there are very simple cases where this is possible. One such example is the quantum CAT state:

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle^\otimes n + |1\rangle^\otimes n).$$

In this state, any pair of qubits is correlated perfectly, and this implies that any quantum circuit generating $|\psi\rangle$ needs to correlate (entangle) all pairs, so if this is a local quantum circuit, it requires depth $\Omega(\log(n))$. This notion is resonated, in a result on classical codes by Lovett and Viola [19], who show circuit lower bounds on approximating the uniform distribution on good error-correcting codes, when starting from a uniform input distribution on the binary cube. In the example of the CAT state, one can view this as the uniform distribution over the repetition code of $n$ bits.

We note that the CAT state can be generated in depth $O(1)$ if we allow un-bounded fan-out. However, the equivalence of bounded fan-out and unbounded fan-out in the computation model of circuits, (any circuit of unbounded fan-out and constant depth can be reduced to a circuit of bounded fan-out and another constant depth), does not hold for the sampling paradigm: the new circuit will not be able to take in a uniform distribution over the binary cube, and will require very tailored correlations between these bits. In the quantum case, the no-cloning theorem, makes the definition of quantum circuits of un-bounded fan-out even less natural. In this paper, we thus restrict ourselves to classical circuits with bounded fan-out, unbounded fan-in, and depth up to some polylog function of the input size.
Step 1: CSS code-states are bounded-depth-hard  
Our construction begins with the following statement: quantum CSS codes must, in one of at least two simple bases, superpose on two far-away sets, each with some constant probability. These sets are the cosets of the large code, modulo the dual of the other code. These bases correspond to either the Hadamard basis, or the standard qubit basis. This property, in which we have some non-negligible “uncertainty” in either the “momentum” basis or the “position” basis is described in the Heisenberg uncertainty lemma for CSS codes (see Lemma 3). Any quantum CSS code with linear distance, can thus be imagined as super-posing on two distant parallel affine spaces (see figure 5). This, we define formally as a distance partition (see Definition 18). By a slight generalization of the no-go-theorem for sampling uniformly from classical codes [19], one gets that quantum states of CSS codes with large distance, cannot be simulated too accurately by bounded-depth circuits.

Step 2: Connection to locally testable codes  
Next, we investigate the robustness of locally testable codes when subjected to removal of constraints. Locally testable codes (LTC’s) are a very important family of LDPC codes (see [15]) that have the following property: the probability that a random LDPC check is violated by word $w$ is proportional to $w$’s distance from the code. Inspired by the work of [12], we examine LTC’s from a different perspective: what can be said of words that satisfy a fraction, say, 0.99 of all local constraints? Suppose $C$ is some LTC with distance $\Omega(n)$. If we discard some small fraction $\varepsilon$ of the checks of $C$, then any word in the residual code $C'$ must be close to $C$, since it violates a fraction at most $\varepsilon$ of the checks, and $C$ is locally testable. Thus, local testability can be read in reverse: instead of asking what is the probability of catching words far from the code, we ask how close are words that satisfy most constraints.

We now use this observation in the quantum case: In [5] quantum locally testable codes qLTC’s were defined, as analogs of classical LTC’s: for a qLTC a quantum state is penalized by a random local check of the code with probability that scales with its distance from the code-space. Currently there are no known constructions of qLTC’s. However, we try to hypothesize, what would we gain if we had at our disposal a qLTC with linear distance? Could it be that we get a similar phenomenon, in which any ground state of the residual code is close to the original ground space and thus highly entangled, as any original ground state?

In theorem [1] we show that qLTC’s with linear distance are in fact $c$-type bounded-depth-hard. This is described pictorially in figure 6. qLTC’s based on CSS codes, inherit the property that any quantum state satisfying most constraints, must be close to the original code-space. Returning to the affine-space image: if any original code-state super-poses on affine plates with large spacing, then after deleting a constant, but sufficiently small fraction of the constraints, the space between the plates becomes “noisy”, being populated with newly added words, but does not vanish completely. This, despite the fact that the code distance per-se may go as low as 1.

Step 3: Constructing a Tillich-Zemor code using classical LTC’s  
We now turn our attention to the Tillich-Zémor code, and carry out the next natural step, i.e. apply it to a pair of classical LTC’s, in the hope that the result is a quantum qLTC. Unfortunately, this is hard to show. Furthermore, even if local testability was somehow inherited into the quantum code, the minimal distance of the resulting code is $O(\sqrt{n})$ by the upper-bound of [21]. As such, we cannot hope that theorem [1] is applicable. Pictorially, upon discarding a constant fraction of the local checks, the entire space between the affine plates may be covered with new codewords, completely obliterating any chance to identify proper distance partitions (see Definition 18), that could potentially resist bounded-depth simulation.

To our rescue, comes an interesting structure that appears in the Tillich-Zémor code. The Tillich-Zémor code acts on the Hilbert space $V \times V \cup C \times C$, where $(V, C)$ corresponds to the Tanner graph of the original classical code $C$. There exists a logical subgroup of $C$, which is isomorphic to $C$: these are formed by words of the form $w = c \cdot e_i^T$, (the word $w$ has 0’s for all bits in
$C \times C$) where $c$ is any codeword $c \in C$, and $e_i$ some singleton vector, corresponding to some row of $V \times V$. (By symmetry, a similar structure appears for the columns of $V \times V$, and the rows/columns of $C \times C$.)

$$C \times |n| \simeq \left\{ w = v \cdot e_i^T, v \in C, i \in |V| \right\}$$

Furthermore, this isomorphism can be extended to the case where constraints are removed from $C_i'$ in the following way: let $w \in F_2^n$ be some word in the residual code $L'_w$ such that $w$ is supported only on the $i$-th column of $V \times V$, i.e. $V \times v_i$. Then $w|_{V \times v_i}$ must correspond to a codeword of the classical code $C_i'$ that is induced by restricting all operators $L'_w \times V$ to $V \times v_i$, as linear constraints over $F_2$. We now try to use this special group, in order to translate the robustness of $C$ to constraint removal as a classical LTC, into quantum robustness of $C_x$.

**Step 4: Putting it all together**  So having constructed a Tillich-Zémor product $C_x$ from a classical LTC $C_x$, we would like to show that any ground-state of any $\varepsilon$-residual code of $C_x$ is hard to approximate by low-depth classical circuits. This is the claim of our main lemma\footnote{4}.

Consider the Heisenberg lemma applied to some code-state $|\psi\rangle$ of an $\varepsilon$-residual code $C_x'$. By choosing a basis for the logical space of $C_x'$, which includes such special logical words $w \in C_x \subseteq C_x'$, we are promised that $|\psi\rangle$ super-poses non-trivially on the pair of complementary orthogonal spaces spanned by logical operators with, and without $w$. Since the above happens for every column / row, then w.h.p. a given state $|\psi\rangle$ super-poses non-trivially along such words $w$, for a good fraction of the rows / columns.

Assume, towards contradiction, that $|\psi\rangle$ is not hard for BD-circuits. Then for any tensor-product basis there exists a bounded-depth circuit $C_{bd}$ simulating the distribution of measuring $|\psi\rangle$ in that basis. This is true, in particular, for the basis in which the Heisenberg uncertainty lemma predicts that $|\psi\rangle$ will super-poses non-trivially along a good fraction of the special words $w$. So from now on, we fix such a basis, say the standard qubit basis, and consider each quantum state in $C_x'$ as a super-position of strings, which supposedly $C_{bd}$ can sample from with sufficient accuracy, according to the square-amplitudes of each string. In particular, each such string belongs to the Pauli $X$ code comprising the residual CSS code $C_x'$.

Let us now consider the implication of the low noise-sensitivity theorem in such a scenario. Since for a random string $x$, that is flipped by an error $e$ at $O(1)$ random locations, the difference between the outputs of $x$ and $x + e$ on $C_{bd}$ is logarithmic in size, i.e. a vanishing fraction of the total number of output bits, there exists a column $i$ such that $x, x + e$ cannot differ at the output of $C_{bd}$ on any bit outside the $i$-th column that is adjacent to $\text{supp}(w)$, i.e. bits that share some constraint in $C_x$. Formally:

$$[C_{bd}(x) \oplus C_{bd}(x + e)]|_{\Gamma(V \times v_i)} = 0,$$

This implies, that the string

$$\mathcal{E} = C_{bd}(x) \oplus C_{bd}(x + e),$$

has the property that $\mathcal{E}|_{V \times v_i} \in C_i'$; i.e. its restriction to the $i$-th column is a codeword of the residual code generated by taking the restriction of all remaining check terms and restricting them to that column $V \times v_i$. This, in itself may not seem so special.

However, by the Heisenberg lemma above, we can also assume that, in addition, the following “miracle” happens: $C_{bd}(x)$, and $C_{bd}(x + e)$ each belongs to a different coset w.r.t. some special word $w \in C_x$ supported on the $i$-th column. Thus $\mathcal{E}$, when expressed as a sum over basis elements, where this basis contains $w$, it must have $w$ in it’s decomposition.

Let us recap: the above analysis translates into the following event that happens w.h.p.: if we sample the output of the purported circuit on a random input, and the output of that input with few random bits flipped, and take the XOR of the two strings, we get a string which must have "jumped a coset" $w \in C_x$ for $w = c \cdot e_i^T$, for some $c \in C$, and that some word of $C_i'$ is present
in the $i$-th column. This, is the result of "colliding" the low noise-sensitivity theorem with the Heisenberg lemma.

At this point, we bring in the local testability of $C$. We can assume w.l.o.g. that only an $\varepsilon$-fraction of the local checks on the $i$-th column were removed. This is because we remove only an $\varepsilon$ fraction on average from each column. Since $C$ was chosen to be classically locally-testable the words of $C'_i$ must cluster around those of $C$. Hence the restriction of $C_{bd}(x) \oplus C_{bd}(x+\varepsilon)$ to the $i$-th column is actually "close" to some non-zero word of $C$, and thus has large weight. This yields a contradiction to the low noise-sensitivity theorem, and concludes the proof.

As a higher-level mathematical statement, the behavior of the Tillich-Zémor code $C_\times$ under removal of local checks, is not that we have a proper distance partition, which allows us to claim immediately that it resists bounded-depth simulation, but rather, that a small perturbation of the input sees a large distance partition on average. This is depicted pictorially in figure 8.3.

**Step 5: The construction** In lemma 4 it is shown that $C_\times$, built from a locally testable code $C$ with minimal distance $\delta_{\text{min}}$ and soundness parameter $\rho$ is such that any quantum circuit satisfying at least $1 - O(\varepsilon\delta)$ of the checks cannot be even approximately simulated by classical circuits of almost log-depth. The next step is to provide an explicit construction, which is our main theorem 2: we propose to use the Hadamard code, which has a large fractional minimal distance (1/2), and soundness parameter. However, the Tanner graph of the Hadamard code is such that the degree of each constraint is 3 (by the linearity test) but the degree of each bit is linear in $n$. Thus by the TZ-construction, the locality of the output Hamiltonian would be $\sqrt{n}$, which is highly non-local. To that end, we first perform a degree-reduction step on the Tanner graph of $C$, similar to (11). The output of this degree reduction is still a set of parity check codes. Hence, we can now apply the TZ-construction and extract a local Hamiltonian with the same asymptotic property of entanglement robustness.

### 1.7 Discussion and open questions

**Stepping up the complexity hierarchy** We believe that this result is but a first step in achieving a much larger class of robust forms of entanglement. One could imagine that this class of local Hamiltonians that are approximation-robust to bounded-depth-sampling, can be then extended to local Hamiltonians whose ground states are complete for the class of quantum circuits of bounded-depth, logarithmic depth, and even BQP-complete, and remain so even after discarding a constant fraction of the local terms. This last statement would, in some sense, amount to a Hamiltonian version of the fault tolerance theorem 3, with Hamiltonian implementation errors replacing environment-induced errors. Of course, devising a class of QMA-complete local Hamiltonians which are approximation-robust, would amount to proving the qPCP conjecture.

**Spectral versus combinatorial** In this work we have shown that there are quantum codes such that any quantum state that satisfies most constraints still has, in a sense, long-range correlations. However, this does not imply that any state with low-energy has such long-range correlations. In particular, our result "covers" all quantum super-positions that correspond to combinatorial approximation of the original Hamiltonian, i.e. to some ground-state of a residual Hamiltonian, but this does not cover all possible low-energy superpositions. Thus, a main task one should also seek to achieve, is to extend our combinatorial hardness to full spectral hardness, i.e. not only that any $\varepsilon$-residual Hamiltonian has bounded-depth-hard ground states, but also that any low-energy state is bounded-depth-hard. We have not been able to prove such a connection thus far.

Interestingly enough, we claim, that proving spectral-hardness of approximation for bounded-depth, would in fact, place a limitation on the extendability of the result of Brandão-Harrow 10 in
2.1 Notation

2 Preliminary facts and definitions

The following sense: spectral-approximation hardness for this construction implies that for every degree $d$ one can find a $k$-local Hamiltonian, with qubit degree at least $d$, such that all low-energy states are bounded-depth hard, and thus, no low-energy state is a tensor-product state. In such a scenario, the theorem shown in [10] where any 2-local Hamiltonian of sufficiently large degree has a good tensor-product approximation to the ground state, cannot be extended to some sufficiently large integer $k = O(1)$, and indicates that 2-local systems may be inherently less robust.

**Quantum locally testable codes and linear distance** As mentioned above, one could avoid the intricate analysis of the Tillich-Zémor construction, if we had at our disposal good quantum locally-testable codes with linear distance. Furthermore, using good qLTC’s to get approximation-robust bounded-depth-hard systems, would provide us with provable entanglement of linear scale $\Omega(n)$, as opposed to $\Omega(n^{1/4})$ as in the current construction. Unfortunately, even quantum LDPC codes with linear distance are not known. Given this current connection, we believe that this should increase the importance of this problem. Could it be that the fact that quantum LDPC codes with linear distance are not known implies some inherent quantum barrier to the qPCP? Recent progress in [6] indicates that we need not be too pessimistic in this respect.

**Quantum circuit lower bounds** Finally, we believe that a more in-depth study of quantum circuit lower bounds will inevitably lead to new results in this respect. More specifically, given the central role of the low-noise sensitivity theorem for classical bounded-depth circuits, it seems reasonable to conjecture the existence of a quantum analog which would, perhaps, show that the central role of the low-noise sensitivity theorem for classical bounded-depth circuits, it seems that circuit lower bounds will inevitably lead to new results in this respect. More specifically, given this current connection, we believe that the system constructed in our main theorem is in fact, also NLTS or cNLTS.

2 Preliminary facts and definitions

2.1 Notation

- Let $U_n$ denote the uniform distribution on $n$-bit strings, and for $0 \leq p \leq 1$, let $\mu_p$ denote the uniform distribution on $n$ bit strings with weight exactly $\lceil p \cdot n \rceil$.
- For bit strings $x, y$ let $x \oplus y$ denote their bit-wise sum over $\mathbb{F}_2$ (XOR).
- For subsets $A, B \subseteq \{0, 1\}^n$, let $A + B$ denote the set of all possible pairwise sums $x \oplus y$ with $x \in A, y \in B$. In particular, when $B$ has one element $x$, we may, omit the set notation and write $A + x$.
- Let $B_n = \{0, 1\}^n$ denote the boolean hypercube on $n$ bits.
- For a linear subspace $A \subseteq B_n$ over $\mathbb{F}_2$, we denote by $A^\perp$, the dual of $A$ as
  \[ A^\perp = \{ x \in B_n, \langle w, x \rangle = 0, \forall w \in A \}. \]
- Let $C$ be a parity-check code on $n$ bits, defined by the Tanner graph $G = (V, C; E)$ where $V$ correspond to the set of bits, $C$ correspond to the set of checks, and $E$ is the set of edges where each check $c \in C$ is connected to all the bits it checks in $V$. The transpose of the code $C$, denoted by $C^T$, is defined by exchanging the roles of the bits, and checks, i.e. it is the code whose Tanner graph is $G = (C, V; E)$.
- Let $S, T, S \subseteq T \subseteq B_n$ denote some linear subspaces. Then $T / S$ denotes the quotient space, defined by identifying any two strings $x, y \in T$, for which there exists some $s \in S$, such that $x \oplus s = y$. Also, $T - S$ denotes the set of strings in $T$ that are not in $S$. In particular, $T / S$ has a representation in terms of elements of $T - S$, and the 0 element (representing $S$).
- Let $S, T$ be as above, and let $R$ be some representation of $S / T$. For $x \in T$, we define $\coset(x)$, as the representative of $x$ by $R$. 


2.2 Quantum codes and local Hamiltonians

**Definition 3. CSS code**
A quantum CSS code on $n$ qubits is a subspace of the Hilbert space of $n$ qubits. It is defined by a pair of linear subspaces of $L_x, L_z \subseteq \mathcal{B}_n$, such that

$$L^\perp \subseteq L_x, L^\perp_x \subseteq L_z.$$ 

It is thus denoted $C = C(L_x, L_z)$.

**Definition 4. Coset-state basis**
A CSS code $C(L_x, L_z)$ has a natural basis of the following form: $|C(w)\rangle \propto \sum_{v \in L^\perp_x} |v \oplus w\rangle$, where $v \in L_x$, and the strings are written in the standard basis, and similarly for $w \in L_z$ where the summation is then over $v \in L^\perp_x$, and the strings are written in the Hadamard basis.

Since $L^\perp$ is a sub-code of $L_z$, then any pair of cosets of $L_z/L^\perp_x$ are disjoint as subsets of $\mathcal{B}_n$. Hence for any $w_1, w_2 \in L_z/L^\perp_x$, either $|C(w_1)\rangle = |C(w_2)\rangle$ (i.e. same coset), or $\langle C(w_1)|C(w_2)\rangle = 0$ for different cosets.

**Definition 5. $k$-local Hamiltonian**
A $k$-local Hamiltonian $H \geq 0$ is a positive semidefinite operator on an $n$-th fold tensor product space $\mathbb{C}^{2^\otimes n}$, that can be written as a sum $H = \sum_{i=1}^{m} H_i$, where each $H_i$ is a positive-semidefinite matrix, $H_i \geq 0$, and each $H_i$ may be written as $H_i = h_i \otimes I$, where $h_i \geq 0$ is a $2^k \times 2^k$ matrix.

Given a local Hamiltonian $H = \sum_i H_i$, we may sometimes use $H$ to denote the set of its local terms $H = \{H_i\}_{i=1}$, depending on the context.

**Definition 6. The Hamiltonian of the code**
A CSS code $C = (L_x, L_z)$ whose duals can be locally generated, by $H_x, H_z$ (i.e. $C$ is a quantum LDPC) can be assigned a Hamiltonian $H(C)$, whose terms correspond to the generators of the CSS code in the following way: for each $e \in H_x$, let $P_x(e)$ denote the Pauli element that is Pauli-X on all indices $i \in [n]$ for which $e(i) = 1$, and identity otherwise. Then

$$H = H(C) = \{P_x(e), e \in H_x\} \cup \{P_z(e), e \in H_z\}.$$ 

In particular, if $C$ is a quantum LDPC code of locality $k$, then its corresponding Hamiltonian $H(C)$ is a $k$-local Hamiltonian.

2.3 Locally-testable codes

**Definition 7. Classical locally-testable code**
A code $C \subseteq \mathcal{B}_n$ is said to be locally-testable with parameter $\rho$, if there exists a set of check terms $C_i$, such that

$$\text{Prob}_i [C_i(w) = 1] \geq \rho \cdot \text{dist}(w, C),$$

where $\text{dist}(w, C)$ is the minimal Hamming distance of $w$ from any word $v \in C$. In particular $C_i(w) = 0$ for all $i$, iff $w \in C$.

Similarly, a quantum locally testable code, can be defined, following [5]

**Definition 8. Quantum locally testable code (strong)**
Given a Hilbert space $H$, a quantum locally testable code $C \subseteq H$, with $m$ local projection checks $C_i$, and soundness constant $s > 0$, is a quantum code, such that for any quantum state $|\psi\rangle$ we have:

$$\frac{1}{m} \text{tr}(H(C)|\psi\rangle\langle\psi|) \geq s \cdot \frac{1}{n} \text{dist}(|\psi\rangle, C).$$

where $\text{dist}(|\psi\rangle, C)$ is the maximal integer $w_0$ such that for all tensor-product Paulis $P$ with weight at most $w_0$, we have $P|\psi\rangle \perp C$. 

10
One can also define weak-sense qLTC’s, where the energy w.r.t. $H(C)$ is measured only for quantum states which are $\epsilon$-far from $C$ for some constant $\epsilon > 0$. We now state a relatively simple fact due to [5] connecting classical and quantum CSS locally-testable codes:

**Fact 1.** Let $C$ be a quantum CSS code corresponding to two linear codes $L_x, L_z \subseteq \mathbb{F}_2^n$. Suppose $C$ is strong-sense qLTC, with parameter $\rho$. Then each of $L_x, L_z$ are strong-sense LTCs with parameter at least $\rho$.

**Fact 2.** Let $C$ be a locally-testable code with parameter $\rho$ and minimal distance $\delta$. Let $C'$ be a code, generated by discarding a fraction at most $\epsilon$ of the checks of $C'$. If $B$ is a base for $C'$ containing a base for $C$ then for any $b \in C \cap B$ the following holds:

$$\forall b' \in \text{Span}(B - \{b\}), \text{dist}(b', b) \geq (\delta - \epsilon / \rho)n.$$  

**Proof.** For any $\epsilon$-residual code $C'$ if $x$ violates a fraction at most $c$ of the checks of $C'$, then it violates a fraction at most $c + \epsilon$ of the checks of $C$, and so it is at distance from $C$ is at most $(c + \epsilon) / \rho$. In particular, any word $w \in C'$ is $\epsilon / \rho$-close to $C$. Thus

$$C' = C + C_{\text{new}},$$

where $C_{\text{new}}$ is a set of words each of weight at most $\epsilon n / \rho$. Consider some $b' \in \text{Span}(B - \{b\})$. Write $b' = c_0 + c_n$, where $c_0 \in C, c_n \in C_{\text{new}}$. Since $B$ includes a basis for $C$, then $c_0$ has a representation in terms of $B \cap C$. But $b' \in \text{Span}(B - \{b\})$ so this representation cannot include $b$. Therefore by the minimal distance of $C$, we have

$$\text{dist}(b', b) \geq \text{dist}(c_0, b) - \text{wt}(c_n) \geq (\delta - \epsilon / \rho)n,$$

where the last inequality follows from the definition of minimal distance of the original code $C$.

2.4 Bounded-depth circuits

**Lemma 1.** [9, 18, 19] Low noise-sensitivity theorem

Let $C : B_m \mapsto B_n$ be some bounded-depth circuit $BD(d, s)$. Let $x \sim U_m, e \sim \mu_{p/m}$. Then

$$E_{x \sim U_m, e \sim \mu_{p/m}}[\text{dist}(C(x), C(x + e)) = O(n \cdot p \cdot \log^d(s) / m)].$$

2.5 Boolean hypercube expansion

**Lemma 2.** [19] Let $S_0, S_1$ be two subsets of $B_m$ of fractional size $\epsilon$ each, i.e.

$$|S_0| \geq 2^m \cdot \epsilon, |S_1| \geq 2^m \cdot \epsilon.$$

Put

$$p = \log(2 / \epsilon),$$

and let $x \sim U_m$, and $e \sim \mu_{p/m}$. Then

$$\text{Prob}(x \in S_0 \land x + e \in S_1) \geq \epsilon^2.$$

3 Defining quantum systems of robust entanglement

In [13] Freedman and Hastings defined an NLTS system as a local Hamiltonian, in which there are no easy-to-generate states with energy at most some $\epsilon$-fraction of the total available energy of the system.
Definition 9. Unitary-trivial states
A family of quantum states $\{ |\psi_n \rangle \}_{n}$ is said to be unitary-trivial, if there exists a constant $c_0$, such that for infinitely many integers $n$, there exists a quantum unitary circuit $U_n$ of depth $O(1)$, such that

$$|\langle \psi | U | 0^{\infty} \rangle| \geq c_0.$$  \hspace{1cm} (1)

Definition 10. NLTS (spectral robustness)
Let $\{ H_n \}_{n \in \mathbb{N}}$ be a family of local Hamiltonians, where for each $n$, $H_n$ has $m = m(n)$ local terms. We say that $\{ H_n \}_{n \in \mathbb{N}}$ is $\varepsilon$-NLTS if there exists some constant $\varepsilon$, such that if $\{ |\psi_n \rangle \}_{n}$ is a family of quantum states, with with $\langle \psi_n | H_n | \psi_n \rangle \leq \varepsilon m$, then $\{ |\psi_n \rangle \}_{n}$ is not unitary-trivial.

This definition was motivated, in part, to prevent the following form of NP-approximation of the ground-energy of such system: a prover sends a (polynomial-size) description of the shallow quantum circuit, and the verifier probabilistically computes the expectation value of the Hamiltonian, conjugated by this unitary circuit, on the all-zero state. The verifier is thus able to accept/reject correctly, with high probability. Since the circuit has depth $O(1)$, and each term of $H$ is local, each local term of $UHU^+$ is local, so this computation can be carried out efficiently.

Here, we define a combinatorial version of NLTS, called cNLTS, where we require that any quantum state satisfying a fraction at least, say, 0.99 of all local terms, cannot be generated by shallow circuits.

Definition 11. residual Hamiltonian
Let $H = \sum_{i=1}^{m} H_i$ be some local Hamiltonian of $m$ local terms. An $\varepsilon$-residual Hamiltonian $H'$ of $H$ is derived from $H$ by removing at most $\varepsilon$ fraction of its local terms.

Similarly, an $\varepsilon$-residual code, of a quantum code $C$ is the ground space of an $\varepsilon$-residual Hamiltonian of $H = H(C)$.

Definition 12. cNLTS (combinatorial robustness)
A family of local Hamiltonians $H_n$, where $H_n$ has $m = m(n)$ local terms is said to be $\varepsilon$-combinatorial-NLTS, if for any corresponding family of $\varepsilon$-residual Hamiltonians $H'_n \subseteq H_n$ the following holds: any infinite family of ground states of the residual Hamiltonians: $\{ |\psi_n \rangle \}_{n}$ with $H'_n | \psi_n \rangle = 0$, is not unitary-trivial.

Clearly, NLTS implies cNLTS, because if we would have a ground state of some $\varepsilon$-residual Hamiltonian that can be easily generated, it would imply that this state, has energy at most $\varepsilon$ in the original system, ruling out that this system is NLTS. However, it is not known if cNLTS implies NLTS.

Under both definitions, quantum unitary circuits, are merely local functions of their inputs. This, contrary to classical circuits of bounded depth, where we allow unbounded fan-in gates. Hence, one can easily find examples that separate these two classes. For example, the OR function on $n$ bits, $OR_n$, can be computed by bounded-depth circuits, trivially, but cannot be computed by quantum circuits of depth $O(1)$.

This provides motivation to define a classical-circuit analog of cNLTS, namely a class of quantum systems whose ground-states are hard to generate, in a robust way. These are local Hamiltonian systems, in which any quantum state that satisfies at least, say 0.99 of all local terms cannot be simulated by bounded-depth classical circuits in the following sense: there exists some tensor-product measurement, such that the distribution induced by measuring such states using these observables cannot be simulated by bounded-depth circuits too accurately. \footnote{We construct this notion gradually, using the following sequence of definitions:}

$^1$ Proving hardness for sampling via bounded-depth circuits, is in some sense, more powerful than showing hardness for computing a function using such circuits: for example, as noted in \cite{19} constant-depth circuits are able to sample uniformly from the distribution of $n + 1$ bit strings, where the first $n$ are i.i.d. uniform, and the last is the parity of the first $n$, but cannot compute the parity function itself.
Definition 13. **Bounded-depth circuits**

BD\((d, s)\) is the set of boolean circuits, consisting of AND gates and OR gates, each of unbounded fan-in, organized into a bounded number of layers. The depth of the circuit \(d\) is the number of layers, and the size of the circuit \(s\) is the number of gates. Fixing the input size to \(n\) we use the short-hand BD to refer to the set of BD\((d, s)\) circuits of size \(s = \text{poly}(n)\), and depth \(d = O(\log^{1-\varepsilon}(n))\), for any constant \(\varepsilon > 0\).

Definition 14. **Quantum states hard for bounded-depth circuits**

A quantum state \(|\psi\rangle\) on \(n\) qubits is said to be hard for BD, if there exists a tensor-product basis \(B\), such that the distribution on corresponding observation values \(m_1, \ldots, m_n \in \{0, 1\}^n\) cannot be approximately sampled by BD circuits, with statistical-distance error better than \(\delta\), for some \(\delta = \Omega(1)\).

Definition 15. **bounded-depth-hard local Hamiltonians**

A local Hamiltonian \(H\) is said to be BD-hard, if any ground state of \(H\) is hard for BD.

Definition 16. **Hamiltonians whose BD-hardness if robust against combinatorial approximation (c-Type BD-hard)**

A local Hamiltonian \(H = \sum_{i=1}^{m} H_i\) is said to be \(\varepsilon\)-combinatorial-approximation-hard for BD if any ground state of any \(\varepsilon\)-residual Hamiltonian of \(H\) is hard for BD.

Definition 17. **Hamiltonians with spectral-approximation-hardness of BD (s-Type BD-hard)**

A local Hamiltonian \(H = \sum_{i=1}^{m} H_i\) is said to be \(\varepsilon\)-spectral-approximation-hard for BD if any quantum state \(|\psi\rangle\) with \(\frac{1}{m} \langle \psi | H | \psi \rangle \leq \varepsilon\) is hard for BD.

Clearly, a local Hamiltonian that is \(\varepsilon\) s-Type hard for bounded-depth is also \(\varepsilon\) c-Type hard for bounded-depth.

Using a similar s-Type (spectral) and c-Type (combinatorial) notation, one can say that if qPCP holds then there are local Hamiltonians which are s-Type QMA-hard, i.e. it is QMA-hard to approximate their energy. Also, NLTS and cNLTS correspond to systems which are s-Type and c-Type hard for constant-depth quantum circuits, in the sense that quantum circuits of constant depth cannot generate states of these Hamiltonians whose energy is below some small \(\varepsilon\) (for NLTS) or who violate at most an \(\varepsilon\) fraction of the local terms (for cNLTS). We conjecture that a similar relation holds for BD-hard systems, i.e. that if qPCP holds (i.e. s-Type QMA-hard systems exist) then s-Type and c-Type BD-hard systems exist. Theorem 2 of this paper shows the existence of c-Type BD-hard systems. Also, it is easy to check that any local Hamiltonian with tensor-product ground-states can be neither cNLTS nor c-Type BD-hard. The above is summarized in the diagram below.

![Diagram](image)

**Figure 1:** Possible behavior of approximation-resistant local Hamiltonians.
4 Classical circuit lower bounds for quantum states

The natural candidates for locally-defined systems whose ground-states are hard to simulate are quantum codes. In quantum error-correction, encoded information is protected by spreading it out over a larger Hilbert space, using long-range entanglement. As such, one would expect that at least quantumly, such long-range correlations cannot be generated by quantum circuits that do not mix together many qubits, namely constant-depth quantum circuits.

Indeed, it is a relatively straightforward observation, that the local indistinguishability property of quantum error correction, which prevents us from telling apart two orthogonal code-states by local observables (i.e. observables whose support is smaller than the minimal distance of the code), implies that generating such code-states using quantum circuits requires large depth: Towards a contradiction, assume that shallow circuit $U$ is able to generate some quantum code-state $|\psi\rangle$ from the all-zero state $|0^{\otimes n}\rangle$. Further suppose that this code has at least one logical qubit and diverging distance. This implies that the local projections (i.e. $U|0\rangle\langle 0|U^\dagger$, for each qubit $i$), can tell apart $|\psi\rangle$ from any state $|\phi\rangle$ orthogonal to $|\psi\rangle$, since for any such $|\phi\rangle$ we have $\langle 0^{\otimes n}|U^\dagger\phi\rangle = 0$. This, in contradiction to the minimal distance of the code.

However, when dealing with quantum codes, with some of the check terms removed, the local indistinguishability promise fades away with the code distance. In fact, for any “reasonable” quantum code, one can bring down the quantum error-correction distance to 1, by “isolating” at least one qubit, i.e. removing all its incident check terms. Thus, any argument, classical or quantum, that relies on the error-correcting distance is bound to fail.

Hence, we attempt to prove lower-bounds using a property of a different kind. This property, named distance partition is the one by which measuring the quantum state using some tensor-product measurement, results in a distribution of strings, in which one can identify a partition of the output hyper-cube into two constant-measure sets $S_1, S_2$, that are distant from each other in Hamming distance.

**Definition 18. Distance partition**

A distribution $D$ on $n$ bit strings is said to have a distance partition with parameter $d$, if one can identify a partition of $\text{supp}(D)$ as $\text{supp}(D) = S_1 \sqcup S_2$, such that $\text{Prob}_D(S_1) = \Omega(1)$, $\text{Prob}_D(S_2) = \Omega(1)$, and

$$\text{dist}(S_1, S_2) = \min_{x \in S_1, y \in S_2} \text{dist}(x, y) \geq d.$$ 

This property is inspired by the lower-bound on generating the quantum CAT state, supported on strings of maximal distance, and on classical results [19] preventing shallow circuits from sampling from good codes, i.e. from sets whose pairwise distance is large. Indeed, using this definition, and following [19] we show the following basic fact:

**Claim 1. Classical circuit lower-bound for distance partition**

Let $D$ be some distribution on $n$-bit strings, for which there exist a distance partition with parameter $d = \text{poly}(n)$. Then any BD circuit generating distribution $D'$ given any number of $m = \Omega(n)$ random bits, has

$$|D - D'|_1 = \Omega(1).$$

**Proof.** For simplicity of presentation, we first analyze the case where $D = D'$, and then extend to some constant statistical-distance. Let $S_0, S_1$ be some partition of $B_n$ into two sets, each with prob. at least $\delta = \Omega(1)$ each under $D$, and $\text{dist}(S_1, S_2) = \Omega(n)$. Assume, toward a contradiction a BD circuit $f$ that simulates $D$ exactly, using $m$ random bits. Consider a partition of $B_m$ into equivalence classes corresponding to the support of $D$. Then $f^{-1}(S_0), f^{-1}(S_1) \subseteq B_m$ form a partition of $B_m$ with measure $\Omega(1)$ each, w.r.t. a uniform distribution on $B_m$.

Applying lemma [2] with parameter $p = O(1/\delta)$, we conclude that a fraction $\Omega(1)$ of all edges have one end in $f^{-1}(S_0)$, and the other in $f^{-1}(S_1)$. Therefore, a uniformly random $m$-bit string $s$,
with a random $p$ bit-flip error $e$, w.p. $\Omega(1)$ corresponds to an edge between $f^{-1}(S_0)$ and $f^{-1}(S_1)$, and so for some $c_0 > 0$,

$$E_{x \sim U_m, e \sim \mu_1/m} [\text{dist}(f(x), f(x + e))] \geq c_0 \cdot \text{dist}(S_0, S_1) = \Omega(d) = \Omega(n^d), \text{ for some } \delta > 0. \quad (2)$$

On the other hand, by the low noise-sensitivity theorem of Lemma 1 for a BD$(d, s)$ function $f$, a random $m$-bit string $x$, and a $p$-flip random noise $e$ to $x$, $f(x + e)$ differs from $f(x)$ by only a small amount:

$$E_{x \sim U_m, e \sim \mu_1/m} [\text{dist}(f(x), f(x + e))] = O(n \cdot \log^d(s)/m). \quad (3)$$

Substituting the parameters $m = \Omega(n), s = \text{poly}(n), d = \log^{1-\epsilon}(n)$ we get

$$E_{x \sim U_m, e \sim \mu_1/m} [\text{dist}(f(x), f(x + e))] = o(n^\delta), \forall \delta > 0 \quad (4)$$

in contradiction to equation (2). Thus, BD circuits cannot sample exactly from $D$.

Now consider the case where the circuit outputs some distribution $D'$ at statistical distance at most $\nu = \Omega(1)$ from $D$. Consider again two disjoint sets $S_0, S_1$ of constant measure at least $\delta > 2\nu$ at the output. Applying lemma 2 with $p = O(1/\nu) = O(1)$, we get that choosing $x \sim U_m, e \sim \mu_{p/m}$ have w.p. $\Omega(1)$:

$$x \in f^{-1}(S_0) \land x + e \in f^{-1}(S_1). \quad (5)$$

Therefore,

$$E_{x \sim U_m, e \sim \mu_{p/m}} [\text{dist}(f(x), f(x + e))] = \Omega(n^d). \quad (6)$$

Same as above, this leads to a contradiction via lemma 1.

$$\square$$

5 Warm-up: quantum CSS codes cannot be sampled by bounded-depth circuits

In this section, we show that a natural ”sanity-check” passes successfully, i.e. that quantum CSS codes cannot be sampled by bounded-depth circuits. We stress though, that such a claim is by no means ”robust”. As mentioned before, known constructions of quantum CSS codes, despite having code-states that are hard for BD, are not $s$-Type robust, and even not $c$-Type robust for any $\epsilon > 0$. This is mainly because these are physically-motivated constructions, and thus usually allow for embedding on a regular lattice of low-dimension. As an archetypal example, consider the 2-D Toric Code. The $\epsilon$-residual code defined by discarding all check terms at the boundary of sufficiently large regular boxes cut out of the grid would allow local diagonalization of the residual code, and in particular, bounded-depth simulation.

Our claim on quantum CSS codes is as follows:

**Claim 2. Code-states of CSS codes with large distance are hard for BD circuits**

Let $C$ be a quantum CSS code on $n$ qubits, with $\delta_{\text{min}} = \text{poly}(n)$. Any $|\psi\rangle \in C$ is BD-hard.

To prove this claim, we require a certain turnkey lemma, which will be useful in all other ensuing claims. This lemma states, that any CSS code state must have a certain (constant) degree of ”uncertainty” in either one of the standard basis or Hadamard basis:

**Lemma 3. Heisenberg’s uncertainty principle for quantum CSS codes**

Let $B_x, B_z$ be two bases of $L_x/L_x^\perp, L_z/L_z^\perp$, and $b_x \in B_x, b_z \in B_z$ elements for which $\langle b_x, b_z \rangle = 1$. For any quantum code state $|\psi\rangle \in C$ either one of the following two holds:

1. $|\psi\rangle$ has projection $\Omega(1)$ on the span of coset states whose cosets are in $\text{Span}(B_z - b_z)$, and simultaneously projection at least $\Omega(1)$ on the span of cosets of the form $\text{Span}(B_z - b_z) + b_z$. 

2. \(|\psi\rangle\) has projection at least \(\Omega(1)\) on the span of coset states whose cosets are in \(\text{Span}(\mathcal{B}_x - b_x)\), and simultaneously projection at least \(\Omega(1)\) on the span of cosets of the form \(\text{Span}(\mathcal{B}_x - b_x) + b_x\).

Proof. By taking appropriate linear combinations with \(b_x, b_z\) in \(\mathcal{B}_x, \mathcal{B}_z\) respectively, we can assume that the following holds:

\[
\forall b \in \mathcal{B}_x, \ b \neq b_x, \ \langle b, b_z \rangle = 0, \quad \forall b \in \mathcal{B}_z, \ b \neq b_z, \ \langle b, b_x \rangle = 0.
\]  \(\text{(7)}\)

Let \(\alpha_w\) denote the complex constants in the decomposition of \(|\psi\rangle\) in the coset-state basis for \(\mathcal{L}_z / \mathcal{L}_z^\perp\), i.e.

\[
|\psi\rangle = \sum_{w \in \mathcal{L}_z / \mathcal{L}_z^\perp} \alpha_w |C(w)\rangle, \quad \text{where} \quad |C(w)\rangle = \sum_{u \in \mathcal{L}_z^\perp} |u \oplus w\rangle.
\]  \(\text{(8)}\)

Let \(\Pi_0\) denote the projection onto the space spanned by coset states \(|w\rangle\), for \(w \in \text{Span}(\mathcal{B}_z - b_z)\). Then either

\[
\langle \psi | \Pi_0 | \psi \rangle \geq 1/5 \quad \text{(9)}
\]
or

\[
\langle \psi | I - \Pi_0 | \psi \rangle \geq 1/5.
\]  \(\text{(10)}\)

Let us assume the former, w.l.o.g. If, in addition, the projection on the orthogonal space is large, i.e.:

\[
\langle \psi | I - \Pi_0 | \psi \rangle \geq 1/5, \quad \text{(11)}
\]
then we sample strings \(s\), whose coset linearly depends on \(b_z\) w.p. \(p_1 \in \{1/5, 4/5\}\), and does not linearly depend on \(b_z\) w.p. \(p_2 \in \{1/5, 4/5\}\). This is the first case of the lemma. Otherwise, consider \(|\psi\rangle\) in the Hadamard basis:

\[
H^{\otimes n} |\psi\rangle = \sum_{w \in \mathcal{L}_z / \mathcal{L}_z^\perp} \alpha_w \sum_{u \in \mathcal{L}_z} (-1)^{u \cdot w} |u\rangle.
\]  \(\text{(12)}\)

By equation \((11)\), we can write:

\[
H^{\otimes n} |\psi\rangle = \alpha \sum_{w \in \text{Span}(\mathcal{B}_z - b_z)} \alpha_w \sum_{u \in \mathcal{L}_z} (-1)^{u \cdot w} |u\rangle + \beta |\phi\rangle, \quad |\alpha|^2 \geq 4/5, \ |\beta|^2 < 1/5.
\]  \(\text{(13)}\)

Let us now compare the amplitudes from the first summand, of a pair of strings \(u, u \oplus b_x\), for arbitrary \(u \in \text{Span}(\mathcal{B}_x)\): we have

\[
|\alpha_u| = \left| \sum_{w \in \text{Span}(\mathcal{B}_z - b_z)} \alpha_w (-1)^{u \cdot w} \right|
\]  \(\text{(14)}\)

\[
|\alpha_{u \oplus b_x}| = \left| \sum_{w \in \text{Span}(\mathcal{B}_z - b_z)} \alpha_w (-1)^{(u \oplus b_x) \cdot w} \right| = \left| \sum_{w \in \text{Span}(\mathcal{B}_z - b_z)} \alpha_w (-1)^{u \cdot w} \cdot (-1)^{b_x \cdot w} \right|
\]  \(\text{(15)}\)

But by equation \((7)\), \((-1)^{b_x \cdot w} = 1\) for all \(w \in \text{Span}(\mathcal{B}_z - b_z)\) and so the above is equal to

\[
\left| \sum_{w \in \text{Span}(\mathcal{B}_z - b_z)} \alpha_w (-1)^{u \cdot w} \right| = |\alpha_u|,
\]  \(\text{(16)}\)

where the last equality is by equation \((14)\). Hence in particular, a string \(s\) belongs to a coset that is linearly dependent, or linearly independent of \(b_x\) w.p. at least

\[
\left| \sqrt{\frac{1}{2}} - \sqrt{\frac{1}{5}} \right|^2 \geq \frac{1}{20},
\]  \(\text{(17)}\)

and so \(p_1, p_2 = \Omega(1)\).
In order to use the lemma above, we require the following standard property of any CSS code:

**Fact 3. Anti-commuting checks**

Let $C$ be a CSS code on $n$ qubits, $C = (\mathcal{L}_x, \mathcal{L}_z)$. There exist bases $B_x$ for $\mathcal{L}_x / \mathcal{L}_x^\perp$, $B_z$ for $\mathcal{L}_z / \mathcal{L}_z^\perp$ such that $\langle b_x, b_z \rangle = 1$, for all $b_x \in B_x, b_z \in B_z$.

Using lemma [3] and the definition above, we now prove our claim:

**Proof of Claim [2]**

Proof. Let $|\psi\rangle$ be some code-state of $C$. By Fact 3 above, one can find bases $B_x, B_z$ whose with $\langle b_x, b_z \rangle = 1$, for all $b_x \in B_x, b_z \in B_z$. According to lemma [3], any code state $|\psi\rangle$ has overlap at least $\Omega(1)$, with the logical span of both $\text{Span}(B_x - b_x)$, and $\text{Span}(B_x - b_x) + b_x$ or both of $\text{Span}(B_z - b_z)$ and $\text{Span}(B_z - b_z) + b_z$. Suppose the former is the case, and let $D_\psi$ denote the distribution on $B_n$ induced by measuring $|\psi\rangle$ in the tensor $Z$ basis. Define $S_0$ as the set of all strings belonging to cosets of $\text{Span}(B_x - b_x)$, and $S_1$ as all strings of cosets of $\text{Span}(B_x) + b_x$. Then $S_0, S_1$ each have measure $\Omega(1)$ under $D_\psi$, and furthermore for any $s \in S_0, t \in S_1$, $\text{dist}(s, t) \geq wt(b_z) \geq \delta_{\text{min}} = \text{poly}(n)$. Therefore, by Claim [2] no BD circuit can sample from $D_\psi$, with error lower than $\nu$, for some $\nu = \Omega(1)$. Hence, $|\psi\rangle$ is bounded-depth-hard.}

---

**Figure 2:** Depiction of the distance-partition of a quantum CSS code with large distance. Any code-state must super-pose non-negligibly in at least one of the two bases, on two distinct affine spaces separated by a large distance.

Since one can get large quantum error-correcting distance using local checks, i.e. quantum LDPC, then simply appending such a quantum LDPC to a QMA-complete local Hamiltonian implies immediately:

**Corollary 1.** There exist QMA-complete local Hamiltonians that are also BD-hard.
6 A bit further: quantum locally-testable codes

We now connect between quantum locally testable codes (see definition of qLTC’s in Definition 8) and robust-entanglement systems: we show that if a quantum locally testable code also has a large distance, then states satisfying almost all constraints are not only close to some original code-state, as in the classical case, but also retain some non-negligible measure of long-range correlations from the entangled code-space of the code:

**Theorem 1.** Let $C$ be a quantum locally-testable CSS code with soundness $\rho > 0$, and fractional minimal distance $\delta_{\min} > 0$. Then $C$ is $\varepsilon$-c-Type hard for BD for $\varepsilon = \Omega(\delta \rho)$.

*Proof.* Let $C' = (\mathcal{L}'_x, \mathcal{L}'_z)$ be some $\varepsilon$-residual code of $C$, with subspaces $\mathcal{L}_x \subseteq \mathcal{L}'_x \subseteq B_n, \mathcal{L}_z \subseteq \mathcal{L}'_z \subseteq B_n$. Let $a_j, b_j$ be two words of the original code-space $\mathcal{L}_x - \mathcal{L}'_x, \mathcal{L}_x - \mathcal{L}'_z$, respectively, with $\langle a_j, b_j \rangle = 1$. Let $|\psi\rangle$ be some code-state of $C'$. Let $B_x, B_z$ be bases of $\mathcal{L}'_x/\mathcal{L}'_x$ and $\mathcal{L}'_z/\mathcal{L}'_z$, respectively, containing $b_j, a_j$, respectively. Then by lemma 3 the state $|\psi\rangle$ has, w.l.o.g. projection $c_0 = \Omega(1)$ on the space of coset states whose corresponding elements of $B_x$ are spanned with, or without $b_j$. In this case, we can fix the tensor-product basis as $\sigma_x$.

Towards a contradiction, let $C : B_n \mapsto B_n$ be some BD circuit approximating $|\psi\rangle$, to statistical distance error $c_1 = \Omega(1)$ - this constant will be determined at the end of the proof. Let $S_0, S_1$ denote the partition of $B_n$ induced by cosets spanned without $b_j$, and with $b_j$, respectively:

\begin{align*}
S_0 &= \{ x : \text{coset}(x) \in \text{Span}(B_x - b_j) \} , \\
S_1 &= \{ x : \text{coset}(x) \in \text{Span}(B_x - b_j) + b_j \} .
\end{align*}

Since $\mathcal{L}_x'$ is generated by discarding a fraction at most $\varepsilon$ of the checks of $\mathcal{L}_x'$, any $x \in \mathcal{L}_x'$ violates a fraction at most $\varepsilon$ of the checks of $\mathcal{L}_x'$. But on the other hand, since $C$ is a qLTC, and a CSS code, then by fact 1 the code $\mathcal{L}_x$ is locally testable. Therefore, any $x$ sampled from $|\psi\rangle$, i.e. $x \in \mathcal{L}_x'$, is $\varepsilon \rho / \rho$-close to some word in $\mathcal{L}_x$. Hence:

\[ x = u_0 + u_1, \text{wt}(u_1) \leq \varepsilon \rho, u_0 \in \mathcal{L}_x, \]

and so expanding $\text{coset}(x)$ in terms of $B_x$, we get:

\[ \text{coset}(x) = w_0 + w_1, \text{wt}(w_1) \leq \varepsilon \rho, w_0 \in \mathcal{L}_x / \mathcal{L}_x' . \]

Let $x \in S_0, y \in S_1$. Then $\text{coset}(x)$’s expansion in $B_x$ includes $b_j \in \mathcal{L}_x / \mathcal{L}_x'$, whereas $\text{coset}(y)$’s expansion does not. Thus,

\[ \text{coset}(x \oplus y) = \text{coset}(x) \oplus \text{coset}(y) = w_0 + w_1, \text{wt}(w_1) \leq 2\varepsilon \rho, w_0 \in (\mathcal{L}_x / \mathcal{L}_x' - b_j) + b_j . \]

But since $w_0$’s expansion in terms of the elements of $B_x \cap (\mathcal{L}_x / \mathcal{L}_x')$ includes $b_j$, then by the minimal distance $\delta_{\min} > 0$ we have $\text{wt}(w_0) \geq \delta_{\min} n$. Hence, we can write:

\[ x \oplus y = w_0 \oplus w_1 \oplus z, \text{wt}(w_0) \geq \delta_{\min} n, \text{wt}(w_1) \leq 2\varepsilon \rho, z \in \mathcal{L}_x' . \]

By definition of error-correction distance, we know that

\[ \forall a \in \mathcal{L}_x / \mathcal{L}_x', b \in \mathcal{L}_x', \text{wt}(a \oplus b) \geq \delta_{\min} \cdot n \]

But since $\mathcal{L}_x' \subseteq \mathcal{L}_x$ then

\[ \forall a \in \mathcal{L}_x / \mathcal{L}_x', b \in \mathcal{L}_x' / \mathcal{L}_x', \text{wt}(a \oplus b) \geq \delta_{\min} \cdot n \]

Thus, by the triangle inequality,

\[ \text{wt}(x \oplus y) \geq \text{wt}(w_0 \oplus z) - \text{wt}(w_1) \geq \delta_{\min} n - 2\varepsilon \rho = \Omega(n) . \]
Therefore,
\[
dist(S_0, S_1) = \min_{x \in S_0, y \in S_1} \text{dist}(x, y) = \Omega(n). \tag{27}
\]

Let \( \mathcal{D} \) be some distribution for which
\[
\text{Prob}_{\mathcal{D}}(S_0) \geq c_0 \quad \text{and} \quad \text{Prob}_{\mathcal{D}}(S_1) \geq c_0. \tag{28}
\]

Let \( \mathcal{D}' \) be some distribution for which \( |\mathcal{D} - \mathcal{D}'| \leq c_1 \). Choose the statistical distance error constant \( c_1 \), so that for any such \( \mathcal{D}, \mathcal{D}' \) we have:
\[
\text{Prob}_{\mathcal{D}}'(S_0) \geq \nu \quad \text{and} \quad \text{Prob}_{\mathcal{D}}'(S_1) \geq \nu, \tag{29}
\]

for some \( \nu = \Omega(1) \). Put \( p = \log(2/\nu) = O(1) \). Then applying the hypercube expansion Lemma 2 to the equation above, we get that
\[
E_{x \sim U_m, e \sim \mu_{p/m}}\left[ \text{dist}(C(x), C(x + e)) \right] = \Omega(n), \tag{30}
\]

whereas by lemma 1
\[
E_{x \sim U_m, e \sim \mu_{p/m}}\left[ \text{dist}(C(x), C(x + e)) \right] = O(p \cdot n^\nu) = O(n^\nu), \forall \nu > 0. \tag{31}
\]
in contradiction.

![Distance partition = poly(n) minimal distance = 1.](image)

**Figure 3:** Robustness of qLTC code-states against approximation: The distance partition image for a CSS code of large distance, with a fraction of the checks removed: New codewords (light blue), appear adjacent to the old codewords (dark blue). The minimal distance can plummet to 1, drawn here as the distance between a new codeword and an old codeword, but by local testability, one can still find a distance partition: this by “decoding” the new codewords back to the old code subspace.

7 **The Tillich-Zémor hypergraph product**

In this section, we survey the Tillich-Zémor hypergraph product (TZ for short). We provide here only the very basic definitions that are required to prove our main theorem, and refer the reader to...
the original paper [21], for an in-depth view. The TZ-product code takes in two classical codes defined by their constraint Tanner graphs, and generates a product of these graphs. Then it attaches a CSS code to the product graph. Formally stated:

**Definition 19. The Tillich-Zémor hypergraph product**

Given two codes defined by two bi-partite constraint graphs $C_1 = (V_1, C_1), C_2 = (V_2, C_2)$ the Tillich-Zémor product of these codes, denoted by $C_1 \times_{TZ} C_2$, is defined by the hypergraph product of the corresponding graphs. Its Hilbert space is comprised of qubits corresponding to $(V_1 \times V_2) \cup (C_1 \times C_2)$, and check terms are of the following form:

$$H_x = C_1 \times V_2, H_z = V_1 \times C_2.$$  

The product $C_1 \times V_2$, for example, is interpreted in the following way: each constraint $(c_1, v_2)$ is connected to all elements $(u, v_2) \in V_1 \times V_2$, where $u \in V_1$ is incident on check term $c_1 \in C_1$, and also, to all elements $(c_1, u) \in C_1 \times C_2$ where $u \in C_2$ is incident on bit $u \in V_2$. It follows from this definition that $C_\times$ is a CSS code $C_\times (L_x, L_z)$, where:

$$L_x = \ker(H_x), L_z = \ker(H_z).$$

If $|V_1| = n_1, |V_2| = n_2, |C_1| = m_1, |C_2| = m_2$, then $C_\times$ is a quantum CSS code on $n_1 n_2 + m_1 m_2$ qubits, with $n_1 m_2 + n_2 m_1$ local checks.

![Figure 4: An example of a check term $(c_k, v_j)$ of $H_x$. It is a parity check on all bits $(v_m, v_j)$ in the $j$-th column of $V \times V$ such that $v_m$ is examined by $c_k$ in the original code $C$, and on all bits in the $k$-th row of $C \times C$ that corresponds to checks incident on $v_j$ in $C$.](image)

We now state several useful facts on this construction, which can all be found in [21]. For a parity-check code $C$ given by its Tanner graph $(V, C)$ we denote its transpose code $C^T$ as the parity check code whose Tanner graph is $(C, V)$. The following holds:
Fact 4. Properties of the Tillich-Zémor code[21]

1. If $C_1, C_2$ have locality parameters $l_1, l_2, l_1^T, l_2^T$, respectively, ($l_1^T$ is the degree of each vertex $v \in V$ in the bi-partite Tanner graph of $C$), then $C_x$ has locality parameter $l_1 + l_2^T$ for $H_x$, and $l_2 + l_1^T$ for $H_z$.

2. $\delta_{\min}(C_x) \geq \min \{\delta_{\min}(C_1), \delta_{\min}(C_2), \delta_{\min}(C_1^T), \delta_{\min}(C_2^T)\}$

3. $\rho(C_x) = \rho(C_1) \cdot \rho(C_2) + \rho(C_1^T) \cdot \rho(C_2^T)$.

These logical operators of $C_x$ can assume very complex forms, due in part, to the fact that the rate of the code scales like $\rho(C_1) \cdot \rho(C_2)$. Hence, the TZ-product of codes with linear rate is linear itself, i.e. scales like $\Omega(|V|^2)$. However, a particularly interesting subset of the logical operators, which is a subgroup w.r.t. addition modulo $F_2$, has a very succinct and useful form. We exploit the structure of this group to "inherit", in some sense, the classical property of local testability:

Fact 5. Group of logical operators isomorphic to the original code
For any $x \in C_1$, and $y \notin C_1^\perp$, the word

$$ (x \cdot y^T)_{V_1 \times V_2} \cup 0_{C_1 \times C_2} \in \mathcal{L}_x - \mathcal{L}_z^\perp. $$

Similarly, for any $x \in C_2^T$, and $y \notin C_1^{T\perp}$ any word of the form

$$ 0_{V_1 \times V_2} \cup (y \cdot x^T)_{C_1 \times C_2} \in \mathcal{L}_x - \mathcal{L}_z^\perp. $$

In particular, if $C_1, C_2, C_1^T, C_2^T$ have no constant bits as classical codes, then $x e_i^T \in \mathcal{L}_x / \mathcal{L}_z^\perp$, for any $x \in C_1$ and singleton $e_i, i \in [n_2]$. Thus

$$ C_1 \times [n_2] \simeq \{z \in \mathcal{L}_x, z = x \cdot e_i^T | x \in C_1, i \in [n_2]\}. $$

The first part of the claim is by [21]. The second part is a simple conclusion thereof. A similar statement holds for $\mathcal{L}_z / \mathcal{L}_x^\perp$.

8 Robust bounded-depth-hard systems exist

In this section, we show how to construct c-Type bounded-depth-hard systems, without using code distance directly. Our strategy will be to use the product code of Tillich-Zémor, and analyze its logical space, in order to derive a contradiction to the noise-insensitivity of bounded-depth circuits. In particular, the behavior we will be looking for is not a proper distance partition, since such a partition may not necessarily exist. This is because the TZ product allows to get codes of distance at most $O(\sqrt{n})$ whereas we allow discarding a constant fraction of the local checks, which implies that all such partitions can get destroyed (see Figure 8.3).

Instead, we will identify a certain subgroup of the logical space $\mathcal{L}_x / \mathcal{L}_z^\perp$ (or its complementary logical basis), which is isomorphic to the original codes comprising the TZ product. Taking the TZ-product of a classical locally-testable code $C$, i.e. $C_x = C \times_{TZ} C$, generates a code, that although cannot be proven to be qLTC per-se, has the property that this subgroup of its logical space inherits the classical “local testability” of $C$. Specifically, they will retain their large ($\Omega(\sqrt{n})$) minimal weight, even after discarding a constant (sufficiently small) fraction of the checks of $C_x$. By assuming, towards a contradiction, the existence of a BD circuit, sampling from some $\varepsilon$-residual code $C_x'$, we will see that it must super-pose non-trivially along this very specific subgroup of the logical space, and by its robustness, this will imply that such a circuit cannot have low noise-sensitivity.

Lemma 4. Let $C$ be some classical LTC which is a parity-check code, no constant bits, local testability parameter $\rho > 0$ and relative minimal distance $\delta_{\min} > 0$, and whose Tanner graph has right and left degrees $O(1)$. Let $C_x = C \times_{TZ} C$ be the quantum Tillich-Zémor product code of $C$ with itself. Then $C_x$ is $\varepsilon$-c-Type hard for BD with parameter $\varepsilon = \Omega(\delta \rho)$. 

21
8.1 The construction

Let $C$ be a locally testable code on $n$ bits, $m$ checks, with parameter $\rho > 0$, and relative minimal distance $\delta_{\text{min}} > 0$. $C$ is defined by the parity-check Tanner graph $(V, C; E)$. Where we denote $V = \{v_1, v_2, \ldots, v_n\}$. Neither $C$ nor $C^T$ have constant bits - i.e. for each $x \in C, i \in V$, there exists $y \in C$ such that $x(i) \neq y(i)$. Let $C_x$ denote the Tillich-Zémor product of $C$ with itself, i.e.:

$$C_x = C \times_{TZ} C.$$  

$C_x$ is a code on $n^2 + m^2$ qubits. Denote by $H_x, H_z$ the checks of $C_x$.

In this proof, we will consider residual codes $C'_x$ of $C_x$: i.e. we are allowed to discard any $\epsilon$ fraction of the local checks, arbitrarily from both $H_x$ and $H_z$. We then examine the code-space that is constrained by those residual checks. Our goal will be to show that any ground-state of such residual codes is BD-hard. For some residual code $C$, let $C'_j \subseteq \{0, 1\}^n$ denote the classical code induced on $V \times v_j$ by the checks $h|_{V \times v_j}$ for all $h \in H'_j$, i.e.

$$C'_j = \{x \in F_2^n | \forall h \in H'_j, h|_{V \times v_j} x = 0\}.$$  

8.2 Properties of $C_x$

Fact 6. Heisenberg uncertainty pairs

Let $C'_x$ be some $\epsilon$-residual code of $C_x$. There exist sets $I \subseteq [n], J \subseteq [n], $ each of size $\Omega(n)$, such that for all pairs $(i, j)$ with $i \in I, j \in J$ a fraction at least $1 - \epsilon$ of the checks of $C_x$ incident on each of $V \times v_j, v_i \times V_j$ are retained by $C'_x$. Moreover, for each $(i, j) \in I \times J$ there exist codewords of $L_x/L_x^\perp$: $a_{ij}$ supported on $v_i \times V$, and $b_{ij}$, supported on $V \times v_j$, with $\langle a_{ij}, b_{ij} \rangle = 1$.

The first part of the fact follows from a simple probabilistic argument. The second part follows from the TZ construction in fact 5 any index $(i, j)$ is incident on two words of the form $x_i x_j^T, e_i x_j^T$, where $x_i, x_j \in C$.

8.3 Proof of lemma 4

Proof. Fix some state $|\psi\rangle \in C'_x$. Consider one of two tensor product bases: the standard-basis on all qubits $\sigma^n$, and the Hadamard basis on all qubits $\sigma^n$. We will show that $|\psi\rangle$ is hard for BD by proving that the distribution induced by $|\psi\rangle$ on at least one of $\sigma^n, \sigma^n$ cannot be approximated by BD circuits to error better than $c_1$, for some $c_1 = \Omega(1)$.

Let us apply lemma 3 to each uncertainty pair $(i, j) \in I \times J$ of the set whose existence is promised by fact 6. Lemma 3 predicts, that for each $(i, j)$ either $a_{ij}$ or $b_{ij}$ induce a constant-measure partition of the logical space.

This implies, in the latter case - that, w.p. at least $c_2 = \Omega(1)$, $x$ sampled from $D_\psi$ belongs to a coset in Span($B_x - b_{ij}$), and, w.p. at least $c_2$ to Span($B_x - b_{ij}$) + $b_{ij}$, where $B_x$ is any completion of $b_{ij}$ to a logical basis of $L_x / L_x^\perp$. In the former case - w.p. at least $c_2$, these $x$ belongs to Span($B_x - a_{ij}$) and w.p. at least $c_2$, to Span($B_x - a_{ij}$) + $a_{ij}$, where $B_x$ is any completion of $a_{ij}$ to a logical basis of $L_x / L_x^\perp$.

This implies that, w.l.o.g., there exist some linear-size "uncertainty" subset of $J$, denoted suggestively by $J_h \subseteq J, |J_h| = \Omega(n)$ with the following property: for any $j \in J_h$ we have that $|\psi\rangle$ super-poses with probability at least $c_2$, each, on any partition of the coset space along some codeword $b_{ij}$ supported on $j$-th column. In particular, such partitions correspond to the $\sigma^n$ basis, for all $j \in J_h$, so this will be our basis of choice to derive a contradiction.

Assume, towards contradiction, that $A$ is some BD circuit for approximating $|\psi\rangle$ to statistical distance at most $c_1 = \Omega(1)$, using $r = \Omega(n^2 + m^2)$ random bits. Similar to the proof of theorem 1 choose $c_1$ so that any distribution at distance at most $c_1$ from a distribution which has measure at
least \( c_0 \) on two distinct sets, has still measure at least \( c_3 = \Omega(1) \) on each set. Put \( p = \log(2/c_3) \), and let

\[
x \sim U_r, y = x + e, e \sim \mu_{p/r},
\]

and put

\[
z = A(x) \oplus A(y).
\]

By the low noise-sensitivity theorem in lemma [1]

\[
\forall v > 0 \ E_{x,v}[\text{wt}(z)] = o(n^v)
\]

On the other hand, hypercube expansion property in Lemma [2] implies that for any pair of constant-measure subsets, a fraction \( \Omega(1) \) of all weight-\( p \) edges are arched between these two sets. In particular, this holds for the partition induced by the pre-images of the partition of the logical space along \( b_{i,j} \).

By applying Markov’s inequality to Equation [33] and taking the union bound w.r.t. the above event we derive the following conclusion: let \( B_x \) be some logical basis containing \( b_{i,j} \). Then

\[
\text{Prob}_{x,v \sim U[n]} \bigg( \forall v > 0, \text{wt}(z) = o(n^v) \land \text{coset}(z) \in \text{Span}(B_x - b_{i,j}) + b_{i,j} \bigg) = \Omega(1).
\]

In words, with some constant probability, a random string at the input, and a random weight-\( p \) error are such, that the sum (mod 2) of their outputs w.r.t. circuit \( A \) is a string \( z \) with the following property: on one hand it has very little weight, but on the other hand, for a random column \( j \) of \( V \times V \), is contained in some non-zero coset corresponding to a word \( b_{i,j} \) supported on \( V \times v_j \).

Assume from now on that this is the case. Consider now, for given \( j \), the immediate neighborhood of \( V \times v_j \) under \( H_x \), and denote by \( \Gamma_x(V \times v_j) \). By definition of the TZ-code (see Definition [19]), we have:

\[
\Gamma_x(V \times v_j) \subseteq C \times C.
\]

Furthermore, for each \( (c_1, c_2) \in C \times C \), we have that the number of \( H_x \) check terms incident on \( (c_1, c_2) \) is, by construction, the degree of each constraint \( c_2 \) in the Tanner graph of \( C \), which is \( O(1) \). Thus each non-zero bit in \( z|_{C \times C} \) covers at most \( O(1) \) unique terms of \( H_x \), so the fraction of neighborhoods \( \Gamma_x(V \times v_j), j \in [n] \) covered by \( z \) is \( o(n^{v-1}) \). But since \( |\mathcal{J}_b| = \Omega(n) \), we conclude that for some \( j \in \mathcal{J}_b \) the neighborhood of \( V \times v_j \) under \( H_x \) (which is in \( C \times C \)) has weight \( 0 \) in \( z \), i.e.

\[
\exists j \in \mathcal{J}_b \text{ s.t. } \Gamma_x(V \times v_j) = 0.
\]

Since \( H'_x|_{\psi} = 0 \) then all \( H'_x \) checks are satisfied as parity checks on \( V \times v_j \cup \Gamma_x(V \times v_j) \). Together with the above, this implies that the restriction of all \( H'_x \) checks to \( V \times v_j \) are satisfied solely by the bits of \( V \times v_j \), i.e.

\[
z|_{V \times v_j} \in \mathcal{C}'_j.
\]

Also, for any basis \( B_x \) of \( \mathcal{L}'_x \) containing \( b_{i,j} \), we have

\[
z \in \text{Span}(B_x - b_{i,j}) + b_{i,j}.
\]

At this point, one may be tempted to claim that we’re in fact done: by equation [36] \( z|_{V \times v_j} \) is contained in \( \mathcal{C}'_j \), and by equation [37] \( z \) is a summation containing the “heavy” word \( b_{i,j} \), which is a non-zero word of the noisy locally-testable code \( \mathcal{C}'_j \). Thus, it seems that this column contains a non-zero word of some residual LTC code of \( C \), which must have large weight. However, the problem is that there may be choices of bases \( B_x \) for which both of these equations hold, but somehow, the restriction of \( z \) to \( V \times v_j \) has weight \( 0 \) for example if \( z \) is a sum of \( b_{i,j} \) and some other, much larger word of \( \mathcal{L}'_x \), that is identical to \( b_{i,j} \) on \( V \times v_j \).
Our plan is thus to construct some specific basis $B_x(z)$ for which this cannot happen, and we exploit the fact that equation \ref{eq:37} which itself follows from lemma \ref{lem:8} in fact holds for any basis containing $b_{i,j}$: we thus initialize $B_x$ with a set of bases $B^i_{col}$ of the form:

$$B^i_{col} = \left\{ z e_i^T, x \in C'_i \right\}_{i \in [n]}$$

Hence, in particular, we have $B^i_{col} \ni b_{i,j} e_j^T = b_{i,j} e_j$ for some $b_j \in C'_j$, so equation \ref{eq:37} is applicable. Let

$$z_q = z \oplus \left( [z|_{\mathcal{V} \times \mathcal{V}_j}, 0]|_{\mathcal{V} \times \mathcal{V}_j} \right) \in B_x,$$

i.e., erase the bits of $z$ in $\mathcal{V} \times \mathcal{V}_j$. Since by equation \ref{eq:36} we have $z|_{\mathcal{V} \times \mathcal{V}_j} \in C'_j$ then $[z|_{\mathcal{V} \times \mathcal{V}_j}, 0]|_{\mathcal{V} \times \mathcal{V}_j} \in \mathcal{L}'$, and so $z_q \in \mathcal{L}'$. We add $z_q$ as necessary to $B_x$. Finally, we complete $B_x$ to a basis of $\mathcal{L}'$ arbitrarily. Expressing $z$ in the new basis $B_x$, we get by Equations \ref{eq:36}, \ref{eq:37} and \ref{eq:38} and by construction of $B_x$:

$$z = z_q \oplus z_{col}, \text{ s.t.}$$

$$z_{col} \in \text{Span}(B^i_{col} - b_{i,j} e_j^T) + b_{i,j} e_j^T$$

$$z|_{\mathcal{V} \times \mathcal{V}_j} = 0.$$ 

and so

$$z|_{\mathcal{V} \times \mathcal{V}_j} = z_{col}|_{\mathcal{V} \times \mathcal{V}_j} \in \text{Span}(B^i_{col}|_{\mathcal{V} \times \mathcal{V}_j} - b_j) + b_j.$$ 

But $j \in \mathcal{J}_b$ so $j \in \mathcal{J}$, thus $\mathcal{V} \times \mathcal{V}_j$ retains at least $1 - \varepsilon$ of its check terms in $C'_x$. We can apply fact \ref{fact:2} to $b_j$ w.r.t. $C'_j$ and claim:

$$\text{wt}(z|_{\mathcal{V} \times \mathcal{V}_j}) \geq \text{dist}(b_j, \text{Span}(B^i_{col}|_{\mathcal{V} \times \mathcal{V}_j} - b_j)) \geq (\delta_{\text{min}} - \varepsilon/\rho) n.$$ 

and so

$$\text{wt}(z) \geq (\delta_{\text{min}} - \varepsilon/\rho) n.$$ 

This implies $\text{wt}(z) = \Omega(n)$ for an appropriate choice of $\delta_{\text{min}}$ as above. Hence, w.p. $\Omega(1)$, we get $\text{wt}(z) = \Omega(n)$, thus

$$E_{x,e} \left[ \text{dist}(A(x), A(x + e)) \right] = \Omega(n).$$

This, contradicts equation \ref{eq:33}.

\section{8.4 Deriving a $c$-Type BD-hard local Hamiltonian}

By the well-known affine-test due to \cite{8}, there exists a set of 3-local parity checks that define the Hadamard code in a locally-testable way. Explicitly, given the Hadamard code on $\mathbb{F}_2^n$, we consider the set of all parity checks of the form

$$T = \{ f(x) \oplus f(y) \oplus f(x + y) | x, y \in \mathbb{F}_2^n \}.$$ 

However, the Tanner graph $G_{\text{Hadamard}} = (L, \mathcal{R}; \mathcal{E})$, defined by these local checks, is such that the left degree (i.e., the degree of each bit) is $\Omega(n)$. Hence, by fact \ref{fact:1} applying directly the Tilich-Zémor product to this graph, would generate a code with check terms whose locality is prohibitively large, i.e. polynomial in the number of qubits.

However, we claim that by essentially applying a degree-reduction procedure used in Dinur’s combinatorial proof of the PCP theorem \cite{11}, we would get a locally-testable code with constant left and right degrees: we replace each bit $x_i$ with a cloud of bits $\tilde{X}_i$. For each original test $t = f(x) \oplus f(y) \oplus f(x + y) \in T$, we write it as a parity check on 3 unique variables $x_t, y_t, z_t$: $x_t$ is
δ_{\text{min}} = \text{poly}(n)

L_{\perp} z + b_1 L_{\perp} z + b_2

\text{minimal distance} = 1.

Effective distance partition experienced by a random \( O(1) \) bit-flip at the input to a bounded-depth circuit.

Figure 5: Tillich-Zémor product-code construction. Since \( \delta_{\text{min}} = (\sqrt{n}) \), removing a constant fraction of the code, can obliterate any distance partition altogether. Thus, the new codewords (light blue) can crowd the entire space between the old codewords (dark blue). However, an average \( O(1) \)-weight bit flip at the input, causes, on average, the output string to “jump” to a far-away coset of a specific kind, \( S_{\text{col}} \). These are marked here in yellow.

in the cloud \( X \) corresponding to variable \( x \), \( y \), and \( z \) in the cloud corresponding to \( x \oplus y \). Then, we further constrain separately each cloud \( X_i \) by a set of equality constraints corresponding to an expander graph on \( n \) vertices. Such an expander graph has constant degree, and furthermore, each equality constraint can be implemented by a simple \( \text{XOR} \)-parity check. Thus, we can apply lemma 4 and conclude our main theorem:

**Theorem 2.** Let \( G \) be an expander graph on \( n \) bits with regular degree \( d = O(1) \). Let \( G_{\text{Had}} \) denote the bi-partite graph corresponding to the tests \( T \) of the Hadamard code on \( n \) bits. Let \( G_{\text{ltc}} \) denote the bi-partite graph corresponding to the locally testable code derived by reducing the degree of \( G_{\text{Had}} \) using \( G \). Let \( C_{\text{ltc}} \) be its corresponding code. Let \( C_{\times} = C_{\text{ltc}} \times_{\text{TZ}} C_{\text{ltc}} \). Then \( H(C_{\times}) \) is an \( O(1) \)-local Hamiltonian that is c-Type hard for BD with parameter \( \epsilon = \Omega(1) \).

9 Acknowledgements

The author thanks Dorit Aharonov, and Jeongwan Haah for useful conversations, Aram Harrow and Cedric Lin for useful and detailed comments and Alex Lubotzky for pointing out the fundamental importance of the Tillich-Zémor construction. The author thanks the Templeton foundation for they support of this work.
References

[1] S. Aaronson, The Quantum PCP Manifesto. Blog: “Shtetl-Optimized”, http://www.scottaaronson.com/blog/?p=139
[2] D. Aharonov, I. Arad, T. Vidick The Quantum PCP Conjecture arXiv:1309.7495
[3] D. Aharonov, M. Ben-Or Fault-tolerant quantum computation with constant error. STOC ’97 Proceedings of the twenty-ninth annual ACM symposium on Theory of computing Pages 176-188, 1997.
[4] D. Aharonov, L. Eldar The commuting local Hamiltonian on locally-expanding graphs is in NP Quantum Information Processing, 2014, (DOI: 10.1007/s11128-014-0877-9)
[5] D. Aharonov, L. Eldar Quantum locally-testable codes QIP, 2014.
[6] D. Bacon, S. T. Flammia, A. W. Harrow, J. Shi Sparse Quantum Codes from Quantum Circuits. http://arxiv.org/abs/1411.3334.
[7] E. Ben-Sasson, V. Guruswami, T. Kaufman, M. Sudan, M. Viderman Locally Testable Codes Require Redundant Testers (2010) SIAM J. Comput., 39(7), 3230-3247.
[8] M. Blum, M. Luby, R. Rubinfeld Self-testing/Correcting with Applications to Numerical Problems. JCSS, Vol. 47, No. 3, pp. 549-595, 1993.
[9] R. Boppana The average sensitivity of bounded-depth circuits. Information Processing Letters 63(5), 257-261. ISSN 0020-0190, 1997.
[10] F. Brandão, A. W. Harrow Quantum Information Processing Proc. of the 45th ACM Symposium on theory of computing (STOC 2013), pp. 871-880
[11] I. Dinur The PCP theorem by gap amplification Proc. 38th ACM Symp. on Theory of Computing, pp. 241–250, 2006.
[12] I. Dinur, M. Sudan, A. Wigderson Robust local testability of tensor products of LDPC codes. Proceedings of the 9th international conference on Approximation Algorithms for Combinatorial Optimization Problems, and 10th international conference on Randomization and Computation Pages 304-315, Springer-Verlag Berlin, Heidelberg 2006.
[13] M. H. Freedman, M. B. Hastings Quantum Systems on Non-k-Hyperfinite Complexes: A Generalization of Classical Statistical Mechanics on Expander Graphs arxiv.org/abs/1301.1363
[14] J. Fitzsimons, T. Vidick A multiprover interactive proof system for the local Hamiltonian problem. arXiv:1409.0260.
[15] O. Goldreich, Short locally testable codes and proofs: a survey in two parts. Property testing, Pages 65-104, Springer-Verlag Berlin, Heidelberg 2010
[16] L. H. Harper Optimal Assignments of Numbers to Vertices. SIAM Journal on Applied Mathematics 12(1), 131-135, 1964.
[17] S. Hart A note on the edges of the n-cube. Discrete Mathematics 14(2), 157-163, 1976
[18] N. Linial, Y. Mansour, N. Nisan Constant depth circuits, Fourier transform, and learnability. J. of the ACM 40(3), 607-620. ISSN 0004-5411, 1993.
[19] S. Lovett, E. Viola Bounded-depth circuits cannot sample good codes (2010) Computational Complexity, June 2012, Volume 21, Issue 2, pp. 245-266
[20] B. M. Terhal, D. P. DiVincenzo Adaptive Quantum Computation, Constant Depth Quantum Circuits and Arthur-Merlin Games Quant. Inf. Comp. Vol. 4 (No. 2), pages 134–145 (2004)
[21] J.P. Tillich, G. Zémor Quantum LDPC codes with positive rate and minimum distance proportional to $\sqrt{n}$ ISIT, Seoul, 2009