Robust Quantum Entanglement at (Nearly) Room Temperature

Lior Eldar
Yifat, Israel
eldar.lior@gmail.com

Abstract

We formulate an average-case analog of the NLTS conjecture of Freedman and Hastings (QIC 2014) by asking whether there exist topologically ordered systems with corresponding local Hamiltonians for which the thermal Gibbs state for constant temperature cannot even be approximated by shallow quantum circuits. We then prove this conjecture for nearly optimal parameters: we construct a quantum error correcting code whose corresponding (log) local Hamiltonian has the following property: for nearly constant temperature (temperature decays as $1/\log^2\log(n)$) the thermal Gibbs state of that Hamiltonian cannot be approximated by any circuit of depth less than $\log(n)$, and it is highly entangled in a well-defined way. This implies that appropriately chosen local Hamiltonians can give rise to ground-state long-range entanglement which can survive without active error correction at temperatures which are nearly independent of the system size: thereby improving exponentially upon previously known bounds.

2012 ACM Subject Classification Theory of computation → Quantum complexity theory

Keywords and phrases Quantum error-correcting codes, Quantum Entanglement, Quantum Locally-Testable Codes, Local Hamiltonians, quantum PCP, NLTS

Digital Object Identifier 10.4230/LIPIcs.ITCS.2021.49

Related Version A full version of the paper is available at `https://arxiv.org/abs/1911.04461v3`.

Acknowledgements The author thanks Dorit Aharonov, Simon Apers, Aram Harrow, Matthew Hastings and Anthony Leverrier for their useful comments and suggestions. He also thanks anonymous reviewers for their helpful comments and suggestions.

1 General

In order to perform universal quantum computation, one should at the very least be able to store quantum states for long periods of time. While the Fault Tolerance theorem [1] makes this possible using active error correction, in parallel, and in part due to the limitations of the FT theorem (see e.g. [4]) a huge research effort was devoted to finding quantum systems that can retain quantum information passively - namely a self-correcting quantum memory.

Self-correcting quantum memories are often referred to as topologically-ordered systems (or TQO) which is a phase of matter that exhibits long-range entanglement at 0 temperature. Since 0 temperature states are essentially theoretical objects that one does not expect to encounter in the lab, the race was on to find TQO systems whose long-range entanglement can survive at very high temperatures - ideally at a constant temperature $T > 0$ that is independent of the system size.

In recent years there has been progress in ruling out such robustness for low-dimensional systems like the 2-D and 3-D Toric Code, but there has been an indication that perhaps in 4 dimensions and above, robustness is more likely (see Section 2.1.2 for a summary of these results). Intriguingly, it seems that quantum mechanics does not fundamentally limit the ability to store quantum states for long times, at least for high-dimensional systems. Despite

that there remains today a large gap between our physical intuition and our ability to provide formal proofs on the existence of robust systems. Hence the problem of establishing the existence of robust TQO systems, even for high dimensions is wide open.

2 Topological Quantum Order (TQO)

TQO is a phase of matter (i.e. in addition to the traditional gas, liquid, and solid states) defined as the zero eigenspace of a local Hamiltonian which is "robust" in the sense that there can be no transition between orthogonal zero eigenstate without a phase transition (See survey of TQO in [19]). Formally one says that a system is ε-TQO if any sufficiently local observable O is unable to discern orthogonal states of the groundspace - i.e. there exists some $z \neq 0$ such that

$$\|POP - zP\| \leq \varepsilon$$

where P is the projection onto the groundspace.

In the language of quantum computing, TQO is mostly synonymous with quantum error correcting codes, and specifically topological quantum codes - these are ε-TQO systems with $\varepsilon = 0$. Under error-correction terminology the TQO property of robustness of ground-state degeneracy is the quantum error-correcting minimal distance: i.e. the system can retain its logical encoded state in the presence of sufficiently small errors.

Thus, TQO systems have the promise that at zero temperature, their entanglement can passively sustain itself (i.e. without active error-correction) as a form of self-correcting quantum memory. It is this stability that brought forth the immensely influential paradigm of the topological quantum computer by Kitaev [14, 8], and even initiated large-scale engineering efforts in trying to build such a set-up [9].

However, since a physicist attempting to prepare a TQO state in a lab can only expect to encounter a Gibbs state (i.e. a thermal state) of the Hamiltonian governing the TQO for some low temperature, then for TQO to serve as a self-correcting quantum memory a necessary property for such a system is that it retains its long-range entanglement at some non-zero temperature $T > 0$ that is independent of the size of the system.

A natural treatment of robustness of TQO systems can be made using quantum circuit lower bounds, a form of analysis initially considered in [11]. Under TQO terminology, topologically ordered states *cannot* be generated from a tensor product state using a shallow circuit, whereas a state is said to be "trivial" if it *can* be generated from product states by shallow circuits - namely it is nearly equivalent to a product state in its lack of quantum entanglement. With this terminology in mind we consider the following conjecture:

▶ **Conjecture 1** (Robust Circuit Depth for Topologically Ordered Systems). *There exists a number $\beta > 0$ and a family of topologically-ordered systems (local Hamiltonians) $\{H_n\}_n$ on n qubits such that for all $\gamma \geq \beta$ we have: Any quantum circuit U that approximates the thermal Gibbs state $e^{-\gamma H}$ to vanishing trace distance has depth $\Omega(\log(n))$.*

In words: the conjecture posits the existence of a TQO system (say, a quantum error-correcting code) for which one can show a circuit lower bound for the thermal state for all T from 0 (i.e. the ground-state) up to some constant temperature. Such a system exhibits "robustness" in the sense that the circuit lower bound for approximating its Gibbs state does not collapse when temperature is increased, with the logarithmic bound potentially allowing the coupling of *every* pair of qubits in the system, using a locally-defined quantum circuit.

Similar variants of this conjecture have been studied in physics literature: for example, in [20] Yoshida provides a negative solution to a similar conjecture for codes embeddable in 2 or 3 dimensional lattices. On the other hand, in [11, 13] the authors provided an indication to the affirmative of this conjecture by considering the 4-dimensional Toric Code: for example, Hastings [11] assumes the existence of certain error operators from which he derived a related property. In [3] the authors use an approximation of thermal systems called the weak Markovian limit, and conclude that certain topological measurements are preserved at constant temperatures for exponentially long time in the system size (exponential coherence times). However, to the best of our knowledge there is no formal proof of conjecture 1.

Here, we make progress towards affirming this conjecture formally by proving conjecture 1 for nearly-optimal parameters:

▶ **Theorem** (sketch). (Robust TQO at nearly Room Temperature). *There exists a* log*-local family of quantum error-correcting codes* $\{\mathcal{C}_n\}_n$ *with polynomial minimal distance* $n^{\Omega(1)}$ *(in particular, a topologically-ordered system) and a corresponding family of commuting local Hamiltonians* $\{H_n\}_n$ *such that for any* $\beta_n = O(\log^2\log(n))$ *the following holds: any quantum circuit* V *that acts on* $a \geq n$ *qubits and approximates the thermal state at temperature at most* $T_n = 1/(\kappa\beta_n)$ *on a set of qubits* S*,* $|S| = n$*:*

$$\left\| \frac{1}{Z} e^{-\beta_n H_n} - \mathrm{tr}_{-S}(V|0^{\otimes a}\rangle\langle 0^{\otimes a}|V^\dagger) \right\|_1 = o(1), \quad Z = \mathrm{tr}(e^{-\beta_n H_n})$$

satisfies a circuit lower bound:

$$d(V) = \Omega(\ln(n)).$$

Our proof will actually show a stronger statement: namely that the thermal Gibbs state of these codes, for sufficiently low, yet nearly constant temperature, can be decoded using a shallow circuit to a bona-fide quantum code state. This implies that the Gibbs state retains topological order (up to a shallow decoder) at very high temperatures: if we initialize our system in some ground-state of the TQO, and allow it to thermalize, we can later recover that code-state with little extra cost (see Section 2.1.7 discussing the possible implementation error of such a set-up). In particular, it implies that appropriately chosen local Hamiltonians can give rise to ground-state multi-partite entanglement which can survive without active error correction at nearly-constant temperatures.

2.1 Some Perspective

2.1.1 The Thermal Gibbs State

This study explores quantum circuit lower bounds on arguably the most natural of physical states - namely the thermal Gibbs state $e^{-\beta H}$ - which can be formed by coupling a ground-state of a physical system H to a "heat bath" at temperature $1/\beta$ - meaning it is allowed to interact indefinitely with an environment to which we have no access to. (see definition 3)

2.1.2 The Regimes of "Inverse-Temperature" β

We consider here a summary of prior art: the temperature at which one can establish an $\Omega(\log(n))$ (i.e. "global") circuit lower bound for the Gibbs state of a Hamiltonian:

Hamiltonian	Temperature	Result	Comments
QECC with large distance	0	Folklore	
2 or 3-D systems	$O(1/\text{poly}(n))$ [1]	[20]	No-go theorem
Projective Code	$\Omega(1/\text{polylog}(n))$	This work	By definition, Without amplification
Amplified Projective Code	$\Omega(1/\text{polyloglog}(n))$	This work	With amplification
4-D Toric Code	$\Omega(1)$	[11]	Heuristic argument.

Our main theorem establishes the existence of log-local Hamiltonians for which the thermal state $e^{-\beta H}$ for $\beta = (\text{loglog}(n))^2$ requires a logarithmic circuit depth. Therefore it improves exponentially on previous work in terms of the provable highest temperature as a function of system size n at which circuit lower bounds can be maintained.

Notably, observe that the rate of errors experienced by quantum states from this ensemble scales like $n/\text{polylog}(n)$ - i.e. a nearly linear fraction. Such error rates result in error patterns whose weight is much larger than the minimal error-correcting distance of the quantum code, and hence it is not immediately clear, at least from an information-theoretic perspective, whether these states - that formally cannot protect quantum information - can be assigned circuit lower bounds.

2.1.3 Is it Entangled?

Any quantum system satisfying Conjecture 1 has a highly entangled ground-space, because for $T = 0$ a Gibbs state can be any (possibly pure) ground-state of a topologically ordered system. That said, for $T > 0$ the circuit lower bound is applied to mixed states: assigning a quantum circuit lower bound for the task of approximating a quantum mixed state (as opposed to a pure state) does not necessarily indicate the existence of quantum correlations but rather the presence of long-range correlations, which may or may not be quantum. In fact, by using the argument of Lovett and Viola [17] one can show a $\Omega(\log(n))$ circuit lower bound for the Gibbs state at constant temperature $T = \Omega(1)$ of any good classical locally testable code, though, this bound breaks for $T = 0$ since any classical string codeword, which is unentangled, is a valid Gibbs state.

However, as noted above even this somewhat weaker notion of a quantum system with a highly-entangled ground-space that retains a quantum circuit lower bound at very high temperature isn't known to exist (at least formally), and is related to major open questions in quantum complexity theory. See in this context the NLTS conjecture discussed in the section 2.1.6.

2.1.4 Quantum Circuit Lower Bounds

This work adds to the set of available tools for showing quantum circuit lower bounds - by combining quantum locally-testable codes, an analysis of the thermal state as a truncated Markov chain, and a local decoder that relies on these two properties to decode a thermal state to a bona-fide quantum code-state which can be assigned a circuit lower bound by information-theoretic arguments. Previous works have either used quantum locally testable codes [5] to argue direct circuit lower bounds, or local decoders [11, 16] but as far as we know these strategies were never used in conjunction. We outline our strategy in more detail in Section 2.3

2.1.5 Energy versus error

An important distinction that one needs to make early on is that having a quantum state with low-energy *does not* necessarily imply it is generated by applying few errors to a ground-state. This is only true if the Hamiltonian governing the quantum state is a so-called qLTC [2]. qLTC's are quantum analogs of locally-testable codes (and see Definition 7).

Like their classical counterparts qLTC's are (local) Hamiltonians for which large errors necessarily result in a large number of violations from a set of local check terms. To give an example - consider Kitaev's 2-dimensional Toric Code [14] at very low-temperature, say $T = O(1/\sqrt{n})$. At that temperature the probability of an error of weight $\sqrt{n}$, at least one which is composed of strings of weight $\sqrt{n}$ is proportional to the probability of observing an error of constant energy, i.e.: $e^{-\beta O(1)}$ i.e. comparable to the probability of a single error. So, unless additional structure of the problem is used, for all we know the number of errors could be $\Omega(n)$. The reason for the above is that the Toric Code is known to have very poor soundness as a locally testable code: in fact one can have an error of size $\sqrt{n}$ with only two violations.

2.1.6 The relation to NLTS

Conjecture 1 above is a mixed-state analog (albeit with a slightly more stringent requirement on the circuit depth) of the NLTS conjecture due to Freedman and Hastings [7] - which posits the existence of local Hamiltonians for which *any* low-energy state can only be generated by circuits of diverging depth. As far as we know neither conjecture is stronger than the other.

Arguably, the only known strategy to establishing the NLTS conjecture, outlined in [5], is to show a construction of quantum locally-testable codes (qLTC's) with constant soundness and linear minimal quantum error correcting distance. However, such a statement by itself requires the construction of quantum LDPC codes with distance growing linearly in the number of qubits - a conjecture now open for nearly 30 years. Thus our inability to make progress on qLDPC is a significant barrier to any progress on the NLTS conjecture.

In this work, we show that by considering a mixed-state (or average-case) analog of NLTS (while still placing a more stringent requirement on the circuit depth) one can break away from this strategy using the tools we already have today - namely qLTC's with 1/polylog soundness and code distance which is sub-linear in n, in this case $\sqrt{n}$, and achieve a construction with nearly optimal parameters. Nevertheless, it could be the case that the construction provided here is in fact NLTS - meaning there are no trivial states of the code Hamiltonian for sufficiently small constant temperature.

2.1.7 Implementation Error

Above, we mentioned the ability of the proposed system to allow thermalization of an initialized state, and still be able to recover that state using a local decoder. Arguably, one can argue against such a statement that one also needs to account for the implementation error of the Hamiltonian governing the TQO state, as well as the decoding Hamiltonian. There exist analogous claims against active fault-tolerance in the form of implementation error of the error-correcting unitary circuits.

However, we conjecture that the system we construct, insofar as the check terms of the Hamiltonians are concerned $\{C_i\}$, is in fact robust against implementation error by virtue of local testability. Recall that a locally testable code (see Definition 7) satisfies the following operator inequality: $\frac{1}{m}\sum_{i=1}^{m} C_i \succeq \frac{s}{n} D_{\mathcal{C}}$. where $D_{\mathcal{C}}$ is an operator that relates a state to its distance from the code-space.

On can check that if the LHS above suffers from an additive error quantified by a Hermitian error operator $\mathcal{E}$, $\frac{1}{m}\sum_{i=1}^{m} C_i + \mathcal{E}$ then using standard results about stability of Hermitian operators under Hermitian perturbation, the resulting code will still be, for sufficiently weak error $\mathcal{E}$, a locally testable code albeit with slightly worse parameters, and for a smaller range of distances from the codespace: it will not be able to faithfully test very small errors, but only large errors.

Still, this code will possess the key property that we use here to argue the main theorem: that for sufficiently low temperature (depending on the strength of the implementation error $\|\mathcal{E}\|$) - the code reins in the error weight to small weights, and these errors are far apart to allow for local error correction. Notably, the actual shallow decoder used in the argument will also suffer from implementation noise, undoubtedly, but as a theoretic argument about entanglement, it is only important to account for implementation error of the Hamiltonian, and not the decoding circuit.

Hence the system proposed has apparently two advantages: not only it is able to sustain long-range entanglement for high temperatures as established in Theorem 31, one doesn't even need to implement it precisely to gain the first advantage. We leave for future research to quantify precisely the degree to which this system is robust against implementation error.

2.2 Some Open Questions

We end this section with several questions for further research. First, it is desirable to improve (reduce) the value of β and improve (reduce) the locality of checks (currently they are log-local). We note that a limiting factor to decreasing β is the maximal size set for which one can show near-optimal expansion, for qLTC's.

An interesting extension of this work is to extend it to actual quantum information - namely show the system can store an arbitrary quantum state for long periods of time: notably here we have only showed that one can recover the uniform distribution on code-states, but it is not immediately clear that it can preserve a single arbitrarily encoded code-state. In addition, it would be insightful to understand the actual coherence time of such a system as a self-correcting quantum memory - we conjecture that it is polynomial in n.

Finally, one could explore the possibility that the constructed code in fact satisfies the NLTS condition: namely that any low-energy state is highly entangled.

2.3 Overall Strategy

In figure 1 we outline the main steps of our argument. To recall, the main goal of this study is to demonstrate that the thermal state $e^{-\beta H}/Z$ is hard to produce for sufficiently small β, and show the same for any ground-state of H - mixed or pure.

Our overall strategy is to demonstrate a *shallow* quantum circuit that allows to correct this thermal state to some code-state of a quantum code with large minimal distance. For a quantum code with large minimal error-correcting distance it is a folklore fact (made formal here) that any quantum state in that codespace is hard to approximate (the gray-shaded box in Figure 1), thereby satisfying the hardness-of-approximation requirement for groundstates. Furthermore, together with the existence of a shallow decoder, it implies a lower-bound on the circuit depth for $e^{-\beta H}$ as the lower-bound on a circuit generating a quantum code-state, minus the depth of the decoder. Thus, working in the diagram of Figure 1 backwards we translate our overall theorem to demonstrating a shallow error-correcting circuit from a thermal state to a code-state with polynomial distance.

2.3.1 Translating Energy to Error

The strategy outlined above requires us to demonstrate a shallow decoder for thermal states of sufficiently low temperatures. Here we are faced with a severe obstacle: a thermal Gibbs state is defined in terms of energy, whereas the natural language for decoders is the language of "errors" (whether they are average-case or worst-case). Hence we need a scheme to argue about the error distribution of the Gibbs state.

To our aid come quantum locally testable codes (qLTCs) [2] (and see Definition 7). The main use of locally testable codes is to rein in the error weight of low-energy states. We use this property in conjunction with the well-known Metropolis-Hastings algorithm (or MH) on Hamiltonians corresponding to the check terms of qLTC's. The MH algorithm is a standard tool in physics to simulate the thermal Gibbs state by a random walk where transition probabilities between quantum states are dictated by their relative energies (see Section 7).

Applying this tool to local Hamiltonians corresponding to qLTCs we show that the thermal Gibbs state $e^{-\beta H}$, for H corresponding to a qLTC, can in fact be approximated by a so-called "truncated" MH process. These arguments correspond to the top Vanilla-colored boxes in the diagram.

As a general note, as far as we know, no previous work using qLTC's made such a translation from energy to error weight: in [5] the authors show that qLTC's with linear distance are NLTS, but since such codes are not known to exist, they end up proving a somewhat weaker version called NLETS thus bypassing the energy-to-error translation. On the other hand, such a translation is probably the most natural way to proceed w.r.t. quantum codes: we do not know how to treat "energies" on quantum states, but if we can model the errors they experience we can leverage our vast knowledge of quantum *error-correction* to handle them. Hence, we believe that the use of the MH random process is of conceptual importance and will be useful elsewhere, since it allows for the first time, to bring the analysis from a point we want to argue about ("energies") to a point where we have powerful analysis tools ("errors").

2.3.2 Shallow Decoding from Local Expansion

To recap the flow of arguments: the arguments about the MH random process (Vanilla-colored boxes in Figure 1) allow us to argue that the thermal Gibbs state $e^{-\beta H}$, for a qLTC Hamiltonian H, can be simulated by sampling an error according to an MH random walk that is controlled by the inverse temperature β and the soundness of the qLTC. We would now like to leverage that property to demonstrate a shallow decoder for this state.

A key observation towards that end (corresponding to the bottom Vanilla-colored box) is that while the MH random process is not an i.i.d. process, it does in fact conform to a somewhat weaker characterization called "locally-stochastic" (or "locally-decaying") [15, 6, 10], which are a main source of inspiration of this work. A noise is locally-stochastic if the probability of a large cluster of errors decays exponentially in its size (see Definition 23).

Concretely, using the truncated MH random process we conclude (orange box) that for sufficiently large β (low temperature) the errors experienced by the Gibbs state are locally-stochastic, and hence typically form only small clusters whose size is, say, at most $\log(n)$.

In effect, a stronger notion is true: we show that local-stochasticity of these random errors means that their clusters are also far away from each other - in the sense that even if we "blow up" each cluster by a factor of $1/\alpha$ (for small $\alpha > 0$) they are still at most the size above. This definition is called α-subset and it too, is due to [15, 6].

In these works, error patterns that are locally-stochastic were shown to be amenable to correction by a local decoder, since intuitively, these errors can be "divided-and-conquered" locally. In this context, the notion of α-subsets was used to handle the possibility that the decoder can introduce errors to qubits which weren't initially erred, by arguing that even if such an event occurs it will not cause the initial clusters to aggregate together to form large, undecodable clusters.

Our choice for a shallow "local-decoder" is to use a straightforward quantum generalization of the Sipser-Spielman decoder (notably, a variant of this decoder was used in [15]). This decoder is desirable since it is able, under certain conditions to decode an error of weight w in time $\log(w)$, and do so locally. That would imply that for error patches of logarithmic size, the decoder would run in depth $O(\text{loglog}(n))$ - i.e. a very shallow decoder.

However, such a decoder comes attached with a very stringent condition: it requires the Tanner graph of the code to be a very strong bi-partite expander. That condition is too stringent for our purposes, since we also need the quantum code to be locally-testable, and it is not known how to make even classical local-testability co-exist with the code's Tanner graph being a bi-partite expander.

In our study, we relax the stringent expansion condition, and require that only very small errors, i.e. those of logarithmic size which we've shown to be the typical error size for the Gibbs state - those errors are required to expand well ("small-set expansion"), while requiring nothing for linear-weight errors, which is the regime of interest of the standard Sipser-Spielman decoder. Hence, we are able to use a code whose Tanner graph is not a true expander. This while still being able to use the Sipser-Spielman approach to a fast parallel decoder by considering only small sets. These arguments are outlined in the pink-shaded boxes in the middle of the diagram.

2.4 The construction

To recap again, starting from the previous section, our goal is to find quantum a code, whose thermal state can be corrected quickly and in parallel. We've shown that if a code is qLTC then the Gibbs state can be essentially modeled as an error process that is locally-stochastic. Locally-stochastic errors can be decoded quickly, if the underlying topology is a good expander - at least for the typical error size. Hence, our interim goal is to find a quantum code $\mathcal{C}$ that satisfies simultaneously three requirements:

1. It has a minimal quantum error-correcting distance that is some polynomial in the number of qubits n, say $\sqrt{n}$ - to allow a circuit lower bound for proper code-states.
2. It is *locally-testable* - to allow translation from energies to errors in the truncated-MH modeling of the Gibbs state.
3. Expansion of the bi-partite Tanner graph corresponding to the checks of the code, for errors of small weight (or "small-set expansion") - to allow for shallow decoding using the Sipser-Spielman algorithm.

2.4.1 The Choice of Quantum Code

In [12] Hastings found a way to make progress on the qLTC conjecture [2] by considering high-dimensional manifolds: he showed that by tessellating a high-dimensional sphere using a regular grid (or some other topology for improved rate) the resulting quantum code on n qubits has soundness $1/\text{polylog}(n)$. We make a crucial use of his approach here.

Recently, Leverrier et al. [16] have proposed the projective code, which is an arguably simpler variant of this high-dimensional construction whereby a length-3 complex chain of p-faces of the binary N-cube (modulo the all-ones vector), for $p = \Omega(N)$ is used to derive

a quantum code on n qubits with distance scaling like n^c, for some constant $c > 0$. This code has improved soundness compared to the one in [12]. Our construction is based on the projective code on n qubits, using p-faces of the N-dimensional cube for $p = N/2$, where $N = \Theta(\log(n))$.

On one hand, by the minimal distance of the projective code one immediately gains a circuit lower bound of $\Omega(\log(n))$ on the minimal depth circuit generating its ground-state (corresponding to the gray-shaded block in Figure 1. This satisfies the first requirement above. It is also a qLTC with reasonable $(1/\log^2(n))$ soundness, (see navy-shaded block in Figure 1) thus satisfying the second requirement.

However, the last critical advantage that we gain by using this code, as opposed to say the original high-dimensional manifold of Hastings, is not its improved soundness parameter but rather the underlying structure of the high-dimensional cube: namely its property of small-set expansion that exists in addition to its non-negligible soundness. This property of small set expansion is the turnkey for allowing the application of a shallow decoder to combat the typical errors of a thermal state with large β parameter.

More specifically, we make crucial use of the structure of the N-cube to establish the third requirement - namely, show that small error sets expand significantly - i.e. have many unique incident constraints. This emanates from the fact that small subsets of p-faces of the n-cube for $p = n/2$ have many adjacent $p + 1$-faces and many adjacent $p - 1$-faces.

2.4.2 Efficient Soundness Amplification

The flow of arguments until this point results in lemma 27 which roughly states that a qLTC with soundness s and qubit degree D has the property that its thermal state for sufficiently large inverse temperature: $\beta \geq \log(D)/s$. has error patterns that form clusters of only logarithmic size. Such errors admit a shallow-depth parallel decoding scheme resulting in a circuit lower bound for approximating this thermal state.

Consider, for example the projective code of [16]. We have $D = \log(n), \quad s = 1/\log^2(n)$ Using these parameters one would only be able to establish a circuit lower bound for $\beta = \text{polylog}(n)$. Hence, by the behavior of β as a function of D and s one sees it is desirable to trade-off increased degree for improved soundness so long as these two quantities are increased/decreased in a commensurate manner.

Using standard probabilistic analysis we show that it is sufficient to choose a random family of $\Omega(n\log^2(n))$ subsets - each set comprised of $1/s$ checks in order to achieve a qLTC with constant soundness and query size q/s. This corresponds to the second navy-shaded box in Figure 1.

This amplification procedure results in a somewhat peculiar situation that we'd like to point out: the thermal Gibbs state $e^{-\beta H}$ is defined w.r.t. the Hamiltonian $H = H(\mathcal{C}_{pa})$ where $\mathcal{C}_{pa}$ is the result of the amplification of the projective code formed by choosing a sufficiently large random family of subsets of check terms of size $1/s$ each. However, the decoding procedure, using the Sipser-Spielman algorithm uses the original checks of $\mathcal{C}$ to locate and correct errors, and not the amplified ones: this is because we do not establish local expansion for the amplified checks, only for the original checks. Still, both sets of checks share the same code-space - namely the original projective code $\mathcal{C}$. Hence, the set of checks used for *testing* are not the same as the ones used for *correcting errors*.

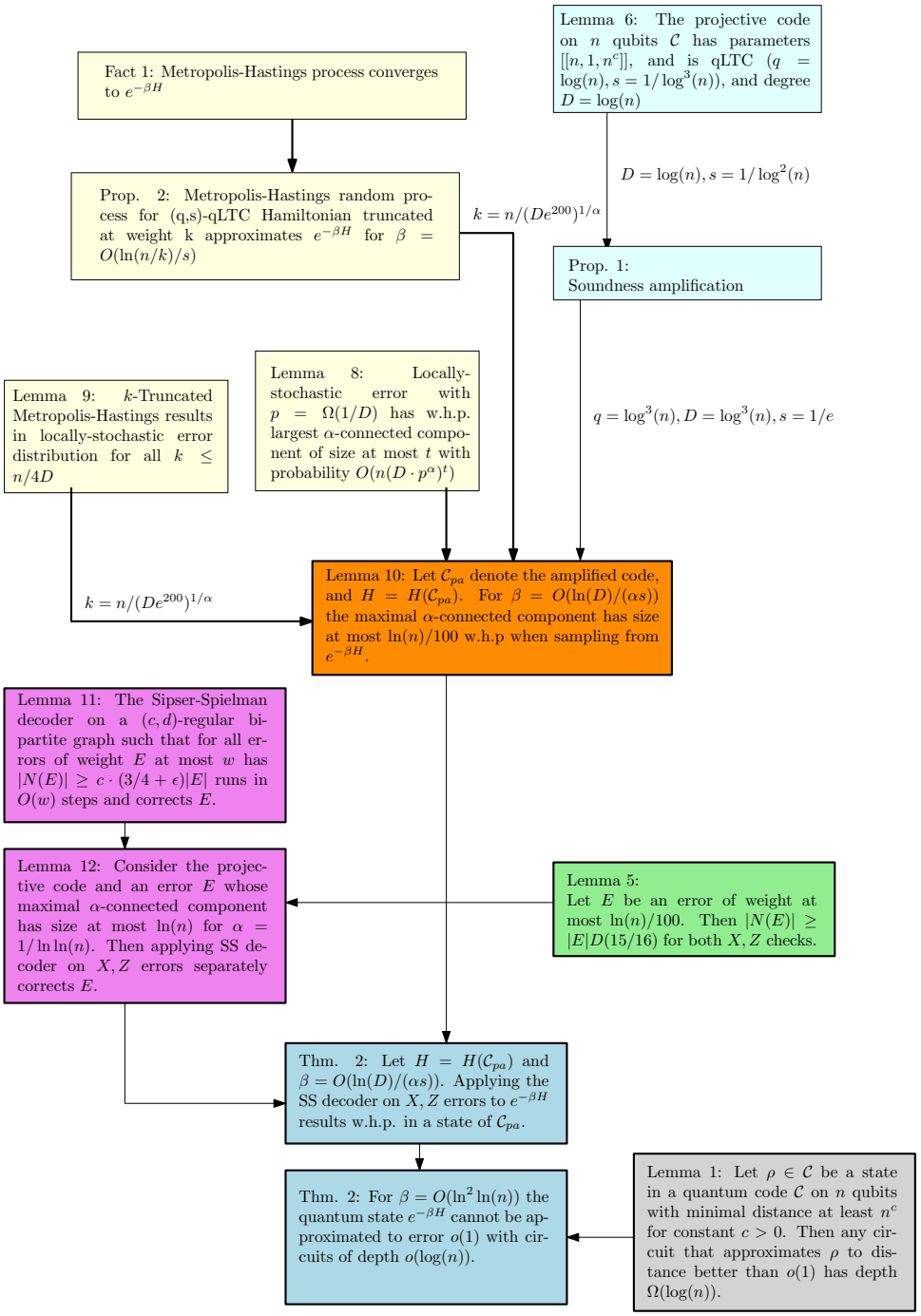

Figure 1 Flow of the main arguments.

3 Notation

A quantum CSS code on n qubits is a pair of codes $\mathcal{C} = (\mathcal{C}_x, \mathcal{C}_z)$, where $\mathcal{C}_x, \mathcal{C}_z$ are subspaces of $\mathbb{F}_2^n$. For a thermal state $\rho = (1/Z)e^{-\beta H}$, β signifies the "inverse temperature" $\beta = 1/(\kappa T)$ where κ is the Boltzmann constant, and $Z = \mathrm{tr}(e^{-\beta H})$ is the partition function of this state. For a finite discrete set S, $|S|$ denotes the cardinality of the set. For $\mathcal{E} \in \{0,1\}^n$ the support of $\mathcal{E}$, $\mathrm{supp}(\mathcal{E})$ is the set of non-zero positions of $\mathcal{E}$. $|\mathcal{E}|$ is the Hamming weight of $\mathcal{E}$. For quantum density matrices A, B, the trace distance between A, B is denoted by $\|A - B\|_1$, and the quantum fidelity between these states is denoted by $\mathcal{F}(A, B)$. A density matrix ρ of rank r is said to be a *uniform mixture* if it can be written as $\rho = \frac{1}{r}\sum_{i=1}^{r} |u_i\rangle\langle u_i|$ where $\{|u_i\rangle\}$ are an orthonormal set of vectors.

We say that a quantum circuit U on a set T of N qubits approximates a quantum state ρ on a set $S \subseteq T$ of $n \leq N$ qubits, to error δ if $\left\|\mathrm{tr}_{T-S}\left(U|0^{\otimes n}\rangle\langle 0^{\otimes n}|U^\dagger\right) - \rho\right\|_1 \leq \delta$

In this work, we will consider random error models $\mathcal{E}$ supported on the n-th fold tensor product Pauli group $\mathcal{P}^n$, where $\mathcal{P} = \{X, Z, Y, I\}$. For an error $\mathcal{E}$ $\mathcal{E} = \mathcal{E}_1 \otimes \ldots \otimes \mathcal{E}_n, \quad \mathcal{E}_i \in \mathcal{P}$ we denote by $|\mathcal{E}|$ the Hamming weight of $\mathcal{E}$ - namely the number of terms $\mathcal{E}_i$ that are not equal to I. Often we will use $|\mathcal{E}|$ to denote the minimal weight of $\mathcal{E}$ modulo a stabilizer subgroup of $\mathcal{P}^n$. For a stabilizer code $\mathcal{C}$ with local check terms $\{C_i\}_{i=1}^m$, $C_i \in \mathcal{P}^n$, the Hamiltonian $H = H(\mathcal{C})$ is the local Hamiltonian $\sum_{i=1}^m (I - C_i)/2$ - i.e. its ground-space is the intersection of the 1-eigenspaces of all check terms C_i.

The N-cube is the binary cube in N dimensions. We will use capital N to denote the dimension of the cube. The projective cube results in a code of n qubits. When considering n in the context of the projective cube we will use lower-case n to denote the number of qubits, i.e. $n = 2^N$.

The letter a will be used to denote an initial set of qubits $a \geq n$ that also include any ancillary qubits used to generate the state of n qubits, i.e. to generate a mixed state on n qubits one applies a unitary transformation on the state $|0^{\otimes a}\rangle\langle 0^{\otimes a}|$, traces out $a - n$ qubits.

Let $G = (V, E)$ be a graph. For a set $S \subseteq V$ the set $\Gamma(S) \subseteq V$ is the set of all vertices that neighbor S in G. The degree of a vertex $v \in V$ is the number of edges incident on that vertex. The degree D of a graph is the maximal degree of any vertex $v \in V$. A graph is D-regular if the degrees of all vertices are equal. We will use $a \propto b$ to signify that $a = c \cdot b$ for some c that does not depend on b. Throughout the paper we will use the binary logarithm $\log(n)$ in the context of quantum circuit lower bounds, and the natural logarithm $\ln(n)$ in the context of errors occurring on a thermal state $e^{-\beta H}$.

4 Preliminaries I: Thermal Gibbs State of a Local Hamiltonian

When considering the thermal Gibbs state for a local Hamiltonian $H = \sum_i H_i$, $\|H_i\| \leq 1$, care needs to be taken as to how to scale the energy of the Hamiltonian. On one hand, we would like the Gibbs state of a Hamiltonian H to be invariant under scaling of H, or perhaps rewriting H as a sum of possibly lower-rank projections. On the other hand, we note that it is unreasonable to expect to have a family of local Hamiltonians $\{H_n\}_n$ with entanglement at room temperature (i.e. constant $\beta > 0$), if the norm of H_n doesn't grow with the number of qubits n. Hence, we introduce the definition of energy density - which captures the average "energy" invested into a qubit in the system:

▶ **Definition 2** (Energy density). *A local Hamiltonian on n qubits with m local terms $H = \sum_{i=1}^m H_i$, $\|H_i\| \leq 1$ is said to have energy density $\lambda = m/n$.*

The thermal Gibbs state is defined for a local Hamiltonian as follows:

▶ **Definition 3** (Gibbs state of a local Hamiltonian). *Let $H = \sum_{i\in[m]} H_i$, be a local Hamiltonian on n qubits $\mathcal{H} = \mathbf{C}^{\otimes n}$, m local terms, and energy density $\lambda = m/n$. The Gibbs state of H for finite $\beta > 0$ is the following density matrix: $\frac{1}{Z}e^{-\beta\tilde{H}}$ where $Z = \mathrm{tr}(e^{-\beta\tilde{H}})$ and $\tilde{H} = H/\lambda$. For $\beta \to \infty$ the Gibbs state is any $\rho \in \ker(H)$.*

Remark about the definition

One could also define the Gibbs state more strictly for $T = 0$ or $\beta \to \infty$ as the uniform mixture over codestates. Such a definition would not change the "quantumness" of the conjecture 1 nor the proof: the conjecture requires that at 0 temperature the system be topologically-ordered, so it must be highly entangled. As to the proof - it shows a circuit lower bound for every mixed ground-state, and in particular the uniform mixture thereof. The more relaxed definition here for $T = 0$ is designed to include every state which is a stationary distribution of the Metropolis-Hastings algorithm, and indeed any mixed/pure ground-state is such a stationary distribution.

5 Preliminaries II :Quantum Error-Correcting Codes

We require the basic definition of stabilizer codes and CSS codes

▶ **Definition 4** (Quantum Stabilizer Code and Quantum CSS Code). *A stabilizer group $\mathcal{G} \subseteq \mathcal{P}^n$ is an Abelian subgroup of $\mathcal{P}^n$. The codespace $\mathcal{C}$ is then defined as the centralizer of $\mathcal{G}$, denoted by $C[\mathcal{G}]$, or equivalently - the mutual 1-eigenspace of $\mathcal{G}$. A CSS code $\mathcal{C} = (\mathcal{C}_x, \mathcal{C}_z)$ is a stabilizer code where the check terms (i.e. generators of the group) are tensor-products of either only Pauli X or only Pauli Z. In particular regarding $\mathcal{C}_x, \mathcal{C}_z$ as $\mathbb{F}_2$ subspaces of $\mathbb{F}_2^n$ we have $\mathcal{C}_x \subseteq \mathcal{C}_z^{\perp}$ and vice versa.*

In this work, we will require some bounds on the minimal depth of a quantum circuit to generate a quantum code state. We recall a slight rephrasing of Prop. 45 in [5] to mixed states: [2]

▶ **Lemma 5** (Robust circuit lower bound for CSS code-states, [5]). *Let $\mathcal{C}$ be a quantum CSS code of non-zero number of logical qubits $k > 1$ on n qubits with minimal distance n^{ε} for some $\varepsilon > 0$. Let ρ_{gs} be a mixture on a set of code-states of $\mathcal{C}$ and let V be a unitary circuit on $N \geq n, N = \mathrm{poly}(n)$ qubits that approximates ρ_{gs}: $\rho = \mathrm{tr}_T\left(V|0^{\otimes N}\rangle\langle 0^{\otimes N}|V^{\dagger}\right) \quad \|\rho - \rho_{gs}\|_1 \leq n^{-2}, \quad \rho_{gs} \in \mathcal{C}$ Then the depth of V is $\Omega(\log(n))$.*

5.1 Quantum Locally Testable Codes

In [2] Aharonov and the author defined quantum locally testable codes (qLTC's). We state here a version due to Eldar and Harrow [5]: a quantum locally testable code can be defined by the property that quantum states on n qubits at distance d to the codespace have energy $\Omega(d/n)$.

[2] The only change required to achieve a mixed-state version of Prop. 45 is to construct distant subsets C_0, C_1 of $\mathbb{F}_2^n$ that each has a non-negligible probability, when measuring the ground-state ρ in one of the X/Z bases. Such sets are readily available: consider some eigenbasis of the code: In at least one of the Z or X bases the state ρ has support at least $1/2$ on basis vectors such that each of them is a "well-partitioned" pure-state. One then constructs the sets C_0, C_1 by "cutting in half" each such well-partitioned eigenstate, sending each half to a different set. By the minimal distance of the code, the "half" of each eigenstate is far from any "half" of any other eigenstate.

▶ **Definition 6.** *If V is a subspace of $(\mathbf{C}^2)^{\otimes n}$ then define its t-fattening to be $V_t := \mathrm{Span}\{(A_1 \otimes \cdots \otimes A_n)|\psi\rangle : |\psi\rangle \in V, \#\{i : A_i \neq I\} \leq t\}$. Let Π_{V_t} project onto V_t. Then define the distance operator $D_V := \sum_{t \geq 1} t(\Pi_{V_t} - \Pi_{V_{t-1}})$.*

This reflects the fact that for quantum states, Hamming distance should be thought of as an observable, meaning a Hermitian operator where a given state can be a superposition of eigenstates.

▶ **Definition 7** (Quantum locally testable code)**.** *An (q, s)-quantum locally testable code $\mathcal{C} \subseteq (\mathbb{C}^2)^{\otimes n}$, is a quantum code with q-local projection $C_1, \ldots, C_m$ such that $\frac{1}{m}\sum_{i=1}^m C_i \succeq \frac{s}{n} D_{\mathcal{C}}$. s is called the soundness parameter of the code.*

We note that the soundness parameter s in this definition generalizes the standard notion of soundness of a classical LTC as a special case, where all C_i's are diagonal in the computational basis. In particular, if the quantum code is a stabilizer code, then the definition of quantum local testability can be further simplified to resemble classical local testability more closely:

▶ **Definition 8** (Stabilizer Locally-Testable Codes (sLTC))**.** *An sLTC is a quantum stabilizer code that is qLTC. An equivalent group-theoretic of an sLTC is as follows: $\mathcal{C}$ is a stabilizer code generated by stabilizer group $\mathcal{G}$. It is $(q, s) -$ sLTC if there exists a set S of q-local words in the stabilizer group $g_1, \ldots, g_t \in \mathcal{G}$ such that for $P \in \mathcal{P}^n$ we have $\mathsf{P}_{g \sim U[S]}([g, P] \neq 0) \geq (|P|/n) \cdot s$ where $|P|$ is the Hamming weight of P modulo the centralizer of G, $C[\mathcal{G}]$: $|P| = \min_{z \in C[\mathcal{G}]} wt(P + z)$ where for $x \in \mathcal{P}^n$ $wt(x)$ counts the number of non-identity entries in x.*

See [5] and [2] for the derivation of this definition as a special case of Definition 7: the operator $\mathcal{D}_{\mathcal{C}}$ penalizes a quantum state according to the "weighted" distance of that state from the codespace, whereas in definition 8 the penalty is defined w.r.t. each Pauli error separately, and as a function of the standard Hamming weight of the error, modulo the code.

Given a (q, s)-sLTC one can generate a sLTC with parameters $(\lceil q/s \rceil, 1/e)$ by amplification as follows:

▶ **Proposition 9** (Randomized Amplification)**.** *Given is a (q, s) sLTC on n qubits with $\mathrm{poly}(n)$ checks. There exists a qLTC $\mathcal{C}_{amp}$ of $\mathrm{poly}(n)$ checks with parameters $(\lceil q/s \rceil, 1/e)$ where each qubit is incident on at most $D' = \lceil q \log^2(n)/s \rceil$ checks.*

6 Preliminaries III: Expansion of Small Errors on the Projective Hypercube

The main observation of this section is that while the projective code is a qLTC with a mild soundness parameter $1/\log^2(n)$, the soundness parameter for *small* errors is much better, and in fact for very small errors, their boundary (i.e. the Hamming weight of their image) is very close to maximal. We begin with a couple of standard definitions:

▶ **Definition 10** (Shadow)**.** *Let $[n]^r$ denote the set of all r-subsets of $[n]$, and let $\mathcal{A} \subseteq [n]^r$. The lower shadow of $\mathcal{A}$ is the set of all $r-1$ subsets which are contained in at least one element of $\mathcal{A}$: $\partial^- \mathcal{A} = \{A - \{i\} : A \in \mathcal{A}, i \in A\}$ and the upper shadow of $\mathcal{A}$ is the set of all $r+1$ subsets that contain at least one element of $\mathcal{A}$: $\partial^+ \mathcal{A} = \{A + \{i\} : A \in \mathcal{A}, i \notin A\}$*

Recall our notation that n denotes the dimension of the cube, and $N = 2^n$ signifies the number of qubits in the context of the quantum error correcting code generated by the projective code of dimension n. We define p-faces as follows:

▶ **Definition 11** (p-face, set of p-faces, subspaces of p-faces)**.** *For integer $n \geq 1$ a p-face is a word in $\{0,1,*\}^n$ that contains exactly p positions with $*$. We denote by $\mathcal{K}_p^N$ as the set of p-faces of the n-th cube. Let C_p^N denote the space spanned by $\mathcal{K}_p^N$ with coefficients from $\mathbb{F}_2$.*

One can think about a p-face as a subset of $\{0,1\}^n$ of all points that are equal to the p-face in its non-$*$ positions. Under this notation one can naturally define upper and lower shadow of p-faces as follows:

▶ **Definition 12** (Shadow of p-faces of $\mathcal{K}_p^N$)**.** *The lower-shadow ∂^- of a p-face f is the set of all $p-1$ faces derived by replacing any $*$ entry with either 0 or 1. The upper-shadow ∂^+ of a p-face f is the set of all $p+1$ faces that can be derived by replacing any non-$*$ entry of p with $*$.*

To connect the definitions above, note that the $\mathbb{F}_2$-boundary operator ∂_{p+1} associated with the $\mathbb{F}_2$-complex chain $\{C_p^n\}_p$ maps each $p+1$-face f to a summation over the set of p-faces $\partial^- f$ with coefficient 1 in $\mathbb{F}_2$, whereas the co-boundary map ∂_p^T sends each $p-1$ face f to a summation over the set of p-faces $\partial^+ f$ with coefficient 1.

Importantly, in this work, we will focus on the p-faces of the projective cube as the combinatorial set $\mathcal{K}_p^N$, and not on the corresponding $\mathbb{F}_2$-space C_p^N. This is because we are interested in establishing a combinatorial expansion property of the boundary maps ∂^+, ∂^-, to be later used in conjunction with the Sipser-Spielman decoder.

However, we will use, in a black box fashion, the properties of these maps, as maps over an $\mathbb{F}_2$ complex chain that appeared in [16]: these properties are namely the soundness and minimal distance of a quantum code derived by the pair (∂^+, ∂^-).

In this study, we consider p-faces of the n-hypercube. While this resembles the case of subsets of $[n]^r$ there is a major difference - since now any $*$-entry replaced, can assume a value either 0 or 1, and the isoperimetric inequality needs to account for this larger set. Bollobas and Radcliffe provide an isoperimetric inequality for the regular grid [Thm. 10, Bollobas and Radcliffe]. Their bounds are useful especially when the set of faces is exponentially large in the dimension of the embedding space. For our purposes though, we are interested in set of p-faces that are polynomial in that dimension so simpler bounds are available as follows:

▶ **Lemma 13.** *Let $\mathcal{A} \subseteq \mathcal{K}_{p-1}^n$ be a set of $(p-1)$-faces for $p = n/2$, $|\mathcal{A}| \leq n/32$. Then $|\partial^+ \mathcal{A}| \geq |\mathcal{A}| \cdot (n/2+1) \cdot (15/16)$. Let $\mathcal{A} \subseteq \mathcal{K}_{p+1}^n$ be a set of $p+1$-faces for $p = n/2$, $|\mathcal{A}| \leq n/8$. Then $|\partial^- \mathcal{A}| \geq 2 \cdot |\mathcal{A}| \cdot (n/2+1) \cdot (15/16)$*

6.1 The Projective Code

▶ **Definition 14** (The Projective Cube)**.** *Let $\mathcal{K}_p^N$ denote the set of p-faces of the N-th cube. The projective cube, denoted by $\tilde{\mathcal{K}}_p^N$ is formed by identifying $x \sim \bar{x}$ iff $x = \bar{x} + \mathbf{1}$ Let $\tilde{C}_p^N$ denote the space spanned by $\tilde{\mathcal{K}}_p^n$ with coefficients in $\mathbb{F}_2$.*

In this study, we will use build upon the projective code defined by Leverrier et al. [16]:

▶ **Definition 15** (Projective code)**.** *Extend the operators ∂^+, ∂^- from $\mathcal{K}_p^N$ to $\tilde{\mathcal{K}}_p^N$ and consider the complex chain formed by the $\mathbb{F}_2$ span of $\tilde{\mathcal{K}}_p^N$, namely the spaces $\{\tilde{C}_p^N\}_p$: $\tilde{C}_{p+1}^N \to^{\partial_{p+1}} \tilde{C}_p^N \to^{\partial_p} \tilde{C}_{p-1}^N$ the quantum CSS code (see Definition 4) defined by $\mathcal{C}_x = \ker(\partial_p), \mathcal{C}_z = (\mathrm{Im}\partial_p)^\perp$ is called the (N,p)-projective code and denoted by $\mathcal{C}_{N,p} = (\mathcal{C}_x, \mathcal{C}_z)$.*

▶ **Lemma 16** (Properties of the projective code, [16])**.** *For every sufficiently large N there exists $n = 2^{\Omega(N)}$ such that the (N,p)-projective code $\mathcal{C}_{N,p}$ for $p = N/2$ has parameters $[[n, 1, n^c]]$, for some constant $c > 0$. It has soundness $1/\log^2(n)$ and each qubit is incident on at most $D = 2\log(n)$ checks.*

We conclude this section by reducing the isoperimetric inequality for the projective cube to the isoperimetric inequality for the N-cube.

▶ **Lemma 17** (Isoperimetric inequalities for the projective hypercube). *Let $\mathcal{C} = (\mathcal{C}_x, \mathcal{C}_z)$ denote the (N, p)-projective code with $p = N/2$. Let $\mathcal{E}$ be a subset of errors of weight at most $N/64$. Then the number of checks $\mathcal{C}_x$ incident on $\mathcal{E}$ is at least $|\mathcal{E}| \cdot (N/2) \cdot (15/16)$ and the number of $\mathcal{C}_z$ checks incident is at least $|\mathcal{E}| \cdot (N) \cdot (15/16)$*

Some context

To provide some context, we note that at first sight it is unclear why considering such small weight ($N/64$) may provide a non-trivial result: after all, for the regime of temperatures we are considering the typical error has nearly linear weight - i.e. $n/\text{polylog}(n)$, and since $n = 2^N$ the weight considered above is merely $\text{polylog}(n)$. The reason is that as we later show in the proof, the typical error of the Gibbs state is not arbitrary, but can be further characterized as being formed on very small clusters - clusters of logarithmic size (see Lemma 27). We would like the check terms of the p-th projective code $\mathcal{C}_{N,p}$ to be such that *any* error of logarithmic size expands very well in the Tanner graph of the code. The isoperimetric inequality provided here on this very restricted error model will allows us to argue that we can use a Sipser-Sipelman type decoder to correct all errors of the thermal state with high probability.

7 Behavior of Errors in the Gibbs State of qLTCs

7.1 The Thermal Gibbs by the Metropolis-Hastings Algorithm

As mentioned in the introduction, a recurring barrier in the emergent field of robust quantum entanglement is to establish a connection between the energy of a state, w.r.t. some local Hamiltonian, and the "error" experienced by that state.

The main observation in this section is that specifically for qLTC's the Gibbs state can be formulated as a random error process (and specifically, a discrete finite Markov process) where the errors occur independently at each step, with an error rate that is comparable to the energy parameter of the state. This will then allow us to conclude that for sufficiently small energy of the Gibbs state the resulting errors can only form very small clusters.

▶ **Definition 18** (The Metropolis-Hastings Random Process Stabilizer Hamiltonians). *Let $\mathcal{G}$ be a stabilizer group with a corresponding Hamiltonian $H = H(\mathcal{G})$ on n qubits $H = \sum_{i=1}^{m} H_i$ with m local terms, and $\lambda(H) = \lambda = m/n$. Let $\beta \geq 0$ be finite. Define a Markov random process $\mathcal{M}$ on a finite graph $G = (V, E)$ whose vertex set V is formed by considering the uniform mixture τ_0 on the set of zero-eigenstates of H, and an additional vertex for each unique state formed by applying a Pauli error applied to τ_0: $V := \{P \cdot \tau_0 \cdot P, \quad P \in \mathcal{P}^n\}$ For any two vertices τ_i, τ_j such that $\tau_j = P\tau_i P$ where P is a single qubit Pauli $P \in \mathcal{P}$ we define the following transition probabilities: $\forall i \neq j \quad \mathcal{M}_{i,j} = \frac{1}{4n} \min\left\{1, \exp\left\{\beta(E_{\tau_i} - E_{\tau_j})/\lambda\right\}\right\}$ and $\mathcal{M}_{i,i} = 1 - \sum_{j \neq i} \mathcal{M}_{i,j}$ where $E(\tau_i) = \text{tr}(\tau_i H)$*

We note that under the definition above, any two vertices connected by an element of the stabilizer group $g \in \mathcal{G}$, i.e. $\tau_i = g\tau_j g^\dagger$ will correspond to the same vertex - since it preserves the uniform distribution on the codespace. In particular we have $|V| = |\mathbb{F}_2^n/\mathcal{C}_x| = |\mathbb{F}_2^n/\mathcal{C}_z|$. More generally for stabilizer codes, each vertex corresponds to a minimal weight error modulo the stabilizer group. Also note, that the transition probabilities $\mathcal{M}_{i,j}$ correspond to a 2-step process, where at the first step one samples a uniformly random index $k \in [n]$ and then

applies a uniformly random Pauli error $\mathcal{E}$ on that index with probability corresponding to the exponent of energy differences. We also note that the normalization by factor of $4n$ stems from the size of the single-qubit Pauli group $|\mathcal{P}| = 4$.

▶ **Fact 19.** *There exists a stationary distribution of $\mathcal{M}$, denoted by ρ_0 and it satisfies: $\rho_0 = \frac{1}{Z}e^{-\beta\tilde{H}}$ where $\tilde{H} = H/\lambda$ and $Z = \mathrm{tr}(e^{-\beta\tilde{H}})$ is the partition function for value β.*

7.2 The Thermal Gibbs Markov Process for qLTC's

As a next step, we consider a *truncated* random process $\mathcal{M}_k$ for integer k where one only considers errors up to some "typical" weight k, beyond which the measure of the stationary distribution of the original process $\mathcal{M}$ is negligible.

▶ **Definition 20** (k-Truncated Markov chain)**.** *Let $\mathcal{C}$ be a quantum stabilizer code on n qubits with m checks, and let $H = H(\mathcal{C})$. Set $\lambda(H) = \lambda = m/n$. Let $\beta \geq 0$ be finite. For any two vertices τ_i, τ_j such that $\tau_j = P\tau_i P$ where P is a single qubit Pauli $P \in \mathcal{P}$ we define the following transition probabilities:*

$$\forall i \neq j \quad \mathcal{M}_{i,j} = \begin{cases} 0 & \text{if } \Delta(\tau_j, \tau_0) > k/n \\ \frac{1}{4n}\min\left\{1, \exp\left\{\beta(E_{\tau_i} - E_{\tau_j})/\lambda\right\}\right\} & o/w \end{cases}$$

where $\Delta(\tau_i, \tau_j)$ is the minimal weight of a Pauli P such that $P\tau_i P = \tau_j$, and $\mathcal{M}_{i,i} = 1 - \sum_{i\neq j}\mathcal{M}_{i,j}$

In general, given the energy parameter $\beta > 0$ one cannot bound a so-called "typical" weight, for which the measure of errors above that weight are negligible in the thermal Gibbs state $e^{-\beta H}$. However, for the specific case of qLTC's such a bound is readily available, via the soundness parameter $\varepsilon > 0$.

▶ **Proposition 21** (Truncated Metropolis Hastings Approximates the Gibbs State of a qLTC)**.** *Suppose in particular that $H = H(\mathcal{C})$ where $\mathcal{C}$ is a (q, s) sLTC, and set $\lambda = \lambda(H)$. Let $0 < \delta < 1/2$ and denote $k = n\delta$. Let ρ_k denote a stationary distribution of the k-th truncated Markov chain $\mathcal{M}_k$. Then for $\beta \geq 5\ln(1/\delta)/s$ the k-th truncated Markov chain approximates the thermal Gibbs state of the scaled Hamiltonian $\tilde{H} = H/\lambda$: $\left\|\rho_k - \frac{1}{Z}e^{-\beta\tilde{H}}\right\| \leq 2n \cdot e^{-2n\cdot\ln(1/\delta)\cdot\delta}$, $\quad Z = \mathrm{tr}(e^{-\beta\tilde{H}})$*

7.3 Percolation Behavior of Random Errors in the Gibbs State of qLTC's

We now recall some of the definitions of Fawzi et al. [6]. The first one is that of an α-subset which is a subset that has a large intersection with some fixed subset:

▶ **Definition 22** (α-subset)**.** *Let $G = (V, E)$ be a graph, $X \subseteq V$, and $\alpha \in [0, 1]$. An α-subset of X is a set $S \subseteq V$ such that $|S \cap X| \geq \alpha \cdot |S|$. We denote by $\mathrm{maxconn}_\alpha(X)$ as the maximum size of an α connected subset of X.*

The second definition is that of a locally-stochastic random error model, which generalizes an independent random error model in that the probability of a set decays exponentially in its size:

▶ **Definition 23** (Locally-stochastic)**.** *Let V be a set of n elements. A random subset $X \subseteq V$ is said to be locally-stochastic with parameter $p \in [0, 1]$ if for every $S \subseteq V$ we have $\mathsf{P}(X \supseteq S) \leq p^{|S|}$*

We now recall Theorem 17 of [6] on the percolation behavior of α-subsets. It states, roughly, that the size of the maximal α-connected component when choosing vertices at random with probability p drops exponentially in dp^α. We rephrase the theorem as the following lemma:

▶ **Lemma 24** (Percolation behavior for locally-stochastic random errors). *Let $G = (V, E)$ be a graph on n vertices, such that each vertex has at most $D = D(n)$ neighboring edges. Let $\alpha > 0$. Let $X \subseteq V$ be a random subset of V that is locally stochastic with parameter p. There exists a constant c such that if $p < c/D$ we have $\mathsf{P}(\mathrm{maxconn}_\alpha(X) \geq t) \leq 2n \cdot (2Dep^\alpha)^t$*

Consider now a local Hamiltonian H, we define its interaction graph as follows:

▶ **Definition 25** (Interaction graph of a local Hamiltonian). *Let $H = \sum_i H_i$ denote a local Hamiltonian on n qubits. The interaction graph of H, $G(H) = (V, E)$ is defined by $V = [n]$ corresponding to the n qubits, and $e = (i, j) \in E$ if qubits i and j share a local term H_e in H.*

We would like to show that the k-th truncated Metropolis-Hastings random process on H is locally-stochastic for sufficiently small k.

To see why this is a non-trivial statement, recall that the MH random process does not induce independent errors, since the probability of adding error to a given qubit depends on the additional energy cost induced by flipping that qubit, and that additional energy depends on the specific error configuration on its neighboring qubits.

In fact this random error model implies that errors are *more likely* to occur near previously sampled errors thus leading to a behavior that is completely opposite to local stochasticity. However, we show that if k is significantly less than n/D then this effect is negligible compared to the probability of sampling an error that is not connected to any other error, and hence approximately these errors are locally-stochastic.

▶ **Lemma 26** (The Thermal Gibbs State is Locally-Stochastic). *Let $\mathcal{C}$ be a stabilizer code and let $H = H(\mathcal{C})$ denote the corresponding local Hamiltonian. Suppose that the corresponding interaction graph $G(H)$ has degree at most D. Let $\alpha \in (0, 1]$, and consider the k-th truncated Markov chain $\mathcal{M}_k$ and its stationary distribution ρ_k, for $k \leq \frac{n}{2e(De^{300})^{1/\alpha}}$ If the energy density is sufficiently large compared to the inverse temperature: $\lambda \geq \beta \ln(n)$ then $\mathcal{E} \sim \rho_k$ is locally-stochastic with parameter at most $p_0 \leq 2ke/n$ with probability at least $1 - (k + 1)n^{-4}$.*

We conclude our central lemma of this section - which is that the thermal Gibbs state $e^{-\beta H}$ where H is a Hamiltonian corresponding to a qLTC, and β is sufficiently large, satisfies a percolation property - namely that the maximal α-connected component of a typical error $\mathcal{E}$ is of logarithmic size:

▶ **Lemma 27** (Typical error components are small for the thermal state of qLTC's). *Let $\mathcal{C}$ be a (q, s)-sLTC on n qubits and let $H(\mathcal{C})$ be its corresponding Hamiltonian, $\lambda(H) = \lambda$. Suppose that the interaction graph of H, $G(H)$, is of degree most D. Let $\alpha > 0$. Let $\tau = \mathcal{E} \cdot \tau_0 \cdot \mathcal{E}$ be a random state (the uniform code mixed state conjugated by a random error $\mathcal{E}$) sampled according to the distribution $e^{-\beta H/\lambda}/Z$ for $(10/\alpha) \cdot \ln(D)/s \leq \beta \leq \lambda/\ln(n)$ Then $\mathsf{P}\left(\mathrm{maxconn}_\alpha \mathcal{E} > \ln(n)/100\right) \leq n^{-3}$*

The range of values β

It is insightful at this point to consider the statement of the lemma w.r.t. the parameter β: the statement of the lemma requires that β is within some range - between $\mathrm{loglog}(n)$ and $\log(n)$. This initially might seem strange as intuitively, increasing β can only improve the ability to correct errors since it corresponds to a regime of much fewer errors - e.g. lower temperature.

However in Lemma 26 it turns out that the analysis is more subtle: indeed we require β to be also sufficiently small so that the error model is locally stochastic: if β is too large (i.e. the temperature is very low) it turns out that a qubit that is hit by an error is much more likely to be hit by another error - this contrary to local stochasticity, whereas for higher temperatures this phenomenon is greatly alleviated.

Hence, the phenomenon of locally stochastic errors, that we exploit to demonstrate a shallow decoder is in fact relevant only for a median range of temperatures: for very low temperatures, the error is no longer locally stochastic, but in that range - the *absolute* number of errors is extremely small to allow worst-case error correction. For higher temperatures, the absolute number of errors is very large but conforms to the locally stochastic model which is treatable by a local decoder. This results in a "win-win" situation, which is handled case-by-case in the proof of the main theorem.

8 A Shallow Decoder for Low Error Rate

The last component of the proof is to demonstrate a shallow circuit that can correct the thermal state $e^{-\beta H}$ to a code-state, for sufficiently large $\beta > 0$ (finite or not). In the previous section we've seen that such a state can be modeled as a random error process with small rate. We would now like to leverage that understanding, together with the small-set expansion property of the n-projective cube to show that the quantum version of the Sipser Spielman decoder yields a shallow decoder.

Inspired by the decoding algorithm of Fawzi et al. [6] we propose an algorithm for decoding a random error $\mathcal{E}$ in depth proportional to $\log(\mathrm{maxconn}_\alpha(\mathcal{E}))$. It is based on a parallel version of the Sipser-Spielman decoder, which we state as follows:

▶ **Lemma 28** ([18], Theorem 11)**.** (Parallel decoder for small-set expander graphs). *Let C be a code on n bits and let G denote the Tanner graph of C. Suppose G is a (c,d)-bi-regular graph on n vertices. The parallel decoder $\mathcal{A}$ is an algorithm that given error $\mathcal{E} = \mathcal{E}_1$ iteratively replaces it with errors $\mathcal{E}_i$ for $i \geq 1$. At step i the algorithm may modify bits only in the support of $\mathcal{E}_i \cup \Gamma(\mathcal{E}_i)$, and in particular, examines for each bit k only $\Gamma(k)$. If, in addition, at the beginning of iteration i we have: $|\Gamma(\mathcal{E}_i)| \geq |\mathcal{E}_i| \cdot c \cdot (3/4 + \varepsilon)$ for some constant $\varepsilon > 0$, then after step i the weight of the residual error $\mathcal{E}_i$ decreases by a multiplicative factor: $|\mathcal{E}_{i+1}| \leq |\mathcal{E}_i| \cdot (1 - 4\varepsilon)$*

Our quantum decoder is an application of the Sipser-Spielman decoder on the individual X, Z errors.

▶ **Algorithm 29** (Shallow Decoder $\mathcal{B}$)**.**
Input: a quantum state ρ on n qubits, a set of X checks $\mathcal{C}_x$ and a set of Z checks $\mathcal{C}_z$.
1. *Run the decoder $\mathcal{A}$ w.r.t. Z errors using $\mathcal{C}_x$.*
2. *Run the decoder $\mathcal{A}$ w.r.t X errors using $\mathcal{C}_z$.*

▶ **Lemma 30.** *Consider the projective code $\mathcal{C} = (\mathcal{C}_x, \mathcal{C}_z)$ on n qubits with $p = n/2$, and let $\mathcal{E} \in \mathcal{P}^n$ denote an error with far-away and small connected components:* $\mathrm{maxconn}_\alpha(\mathcal{E}) \leq \ln(n)/100, \quad \alpha = 1/(\gamma \mathrm{loglog}(n))$ *where $\gamma = \log(1 - 4 \cdot (3/16))$ is the constant implied by Lemma 28 for $\varepsilon = 3/16$. Then shallow decoder $\mathcal{B}$ runs in depth at most $2\gamma \log^2 \log(n)$ steps and satisfies: $\mathcal{B} \circ \mathcal{E} \circ \rho = \rho \quad \forall \rho \in \mathcal{C}$*

We note here that the decoder $\mathcal{B}$ requires extra ancillary bits for syndrome computation, hence the notation $\mathcal{B} \circ \mathcal{E} \circ \rho$ signifies a quantum channel, where some of the qubits are discarded after computation.

9 Global Entanglement for Thermal States

9.1 The construction

1. **Step 1 – The projective code:**
   Fix n as the number of qubits in the code. As the basis for our construction we consider the (N, p) projective code $\mathcal{C}$ for $p = N/2$. By Lemma 16 we can choose $N = \Theta(\log(n))$ such that $\mathcal{C}$ is a qLTC $[[n, 1, n^c]]$ for some $c > 0$ with qLTC parameters $(q = \log(n), s = 1/\log^2(n))$. By construction, the interaction graph of $H(\mathcal{C})$, i.e. $G(H(\mathcal{C}))$ is D-regular with $D = 2 \cdot \log(n)$ and the local Hamiltonian H has $m = 2n \cdot \log(n)$ check terms.
2. **Step 2 – Amplification:**
   We apply Proposition 9 to conclude the existence of a qLTC, denoted by $\mathcal{C}'$ with parameters $(q' = \lceil \log^3(n) \rceil, s' = 1/e)$ and $\lambda = \log^4(n)$. The interaction graph of the Hamiltonian of $\mathcal{C}'$, i.e. $G(H(\mathcal{C}'))$ has degree at most $D' \leq \lceil \log^7(n) \rceil$.
3. **Step 3 – Union:**
   Finally, we consider the union of the checks of $\mathcal{C}$ and $\mathcal{C}'$ and denote the union by $\mathcal{C}_{pa}$ - this is our construction. We denote the number of checks by m_{pa}. We have that, $\mathcal{C}_{pa}$ is $[[n, 1, n^c]]$ quantum code, and is qLTC with parameters: $(q_{pa} = \log^3(n), s_{pa} = 1/2e, D_{pa} \leq 2\log^7(n))$ and $\lambda_{pa} \geq 2\log^4(n)$.

We note that the the amplified code $\mathcal{C}'$ has constant soundness for all *non-zero* distances, but it is not clear a-priori why it should also satisfy $\ker(\mathcal{C}) = \ker(\mathcal{C}')$. Hence, the union of $\mathcal{C}$ and $\mathcal{C}'$ is taken in order to enforce the ground-state of the final code to equal that of $\mathcal{C}_{pa}$. This slightly reduces the soundness, and increases the degree of the interaction graph of the final code. Also note that the check terms of $\mathcal{C}_{pa}$ commute in pairs.

9.2 Main Theorem

We now state formally our main theorem.

▶ **Theorem 31.** *Let $\mathcal{C}_{pa}$ denote the code constructed above on n qubits, and let $H = H(\mathcal{C}_{pa})$, $\lambda = \lambda(H)$ and inverse temperature: $\beta \geq 20e \cdot \log^2\log(n)$ Any quantum circuit U on $a \geq n$ qubits that approximates the thermal state of $\tilde{H} = H/\lambda$ on a set of qubits S, $|S| = n$, at inverse temperature β, $\left\| \mathrm{tr}_{-S}(U|0^{\otimes a}\rangle\langle 0^{\otimes a}|U^\dagger) - e^{-\beta\tilde{H}}/Z \right\|_1 \leq 0.1n^{-2}$ has depth at least $d(U) = \Omega(\log(n))$*

References

1 Dorit Aharonov and Michael Ben-Or. Fault-tolerant quantum computation with constant error rate. *SIAM J. Comput.*, 38(4):1207–1282, July 2008.

2 Dorit Aharonov and Lior Eldar. Quantum locally testable codes. *SIAM J. Comput.*, 44:1230–1262, 2015.

3 R. Alicki, Michal Horodecki, P. Horodecki, and R. Horodecki. On thermal stability of topological qubit in kitaev's 4d model. *Open Systems and Information Dynamics*, 17, November 2008.

4 Robert Alicki, Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Dynamical description of quantum computing: Generic nonlocality of quantum noise. *Phys. Rev. A*, 65:062101, May 2002.

5 Lior Eldar and Aram Wettroth Harrow. Local hamiltonians whose ground states are hard to approximate. *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 427–438, 2015.

6 Omar Fawzi, Antoine Grospellier, and Anthony Leverrier. Efficient decoding of random errors for quantum expander codes. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2018, pages 521–534, New York, NY, USA, 2018. ACM.

7 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.

8 Michael H. Freedman, Alexei Kitaev, Michael J. Larsen, and Zhenghan Wang. Topological quantum computation. *Bull. Amer. Math. Soc. (N.S*, pages 31–38, 2002.

9 Elizabeth Gibney. Inside microsofts quest for a topological quantum computer. *Nature*, 2016.

10 Daniel Gottesman. Fault-tolerant quantum computation with constant overhead. *Quantum Info. Comput.*, 14(15-16):13380–1372, November 2014.

11 Matthew B. Hastings. Topological order at nonzero temperature. *Phys. Rev. Lett.*, 107:210501, November 2011.

12 Matthew B. Hastings. Quantum codes from high-dimensional manifolds. In *ITCS*, 2017.

13 Matthew B. Hastings, Grant H. Watson, and Roger G. Melko. Self-correcting quantum memories beyond the percolation threshold. *Phys. Rev. Lett.*, 112:070501, February 2014.

14 A.Yu. Kitaev. Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303(1):2–30, 2003.

15 A. Leverrier, J. Tillich, and G. Zémor. Quantum expander codes. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*, pages 810–824, October 2015.

16 Anthony Leverrier, Vivien Londe, and Gilles Zémor. A construction of quantum (almost) locally testable codes. *Quantum Information Processing (QIP)*, 2019.

17 Shachar Lovett and Emanuele Viola. Bounded-depth circuits cannot sample good codes. In *IEEE Conference on Computational Complexity*, 2011.

18 M. Sipser and D. A. Spielman. Expander codes. *IEEE Transactions on Information Theory*, 42(6):1710–1722, November 1996.

19 Xiao-Gang Wen. Topological order: From long-range entangled quantum matter to a unified origin of light and electrons. *ISRN Condensed Matter Physics*, 2013, October 2012. doi:10.1155/2013/198710.

20 Beni Yoshida. Feasibility of self-correcting quantum memory and thermal stability of topological order. *Annals of Physics*, 326(10):2566–2633, 2011.