Towards Local Testability for Quantum Coding

Anthony Leverrier, Vivien Londe, Gilles Zémor

Towards Local Testability for Quantum Coding

Anthony Leverrier
Inria, Paris, France
anthony.leverrier@inria.fr

Vivien Londe
Microsoft, Issy-les-moulineaux, France
https://vivienlonde.github.io/
vivien.londe@microsoft.com

Gilles Zémor
Institut de Mathématiques de Bordeaux, UMR 5251, France
zemor@math.u-bordeaux.fr

Abstract

We introduce the *hemicubic codes*, a family of quantum codes obtained by associating qubits with the p-faces of the n-cube (for $n > p$) and stabilizer constraints with faces of dimension $(p \pm 1)$. The quantum code obtained by identifying antipodal faces of the resulting complex encodes one logical qubit into $N = 2^{n-p-1}\binom{n}{p}$ physical qubits and displays local testability with a soundness of $\Omega(1/\log(N))$ beating the current state-of-the-art of $1/\log^2(N)$ due to Hastings. We exploit this local testability to devise an efficient decoding algorithm that corrects arbitrary errors of size less than the minimum distance, up to polylog factors.

We then extend this code family by considering the quotient of the n-cube by arbitrary linear classical codes of length n. We establish the parameters of these *generalized hemicubic codes*. Interestingly, if the soundness of the hemicubic code could be shown to be constant, similarly to the ordinary n-cube, then the generalized hemicubic codes could yield quantum locally testable codes of length not exceeding an exponential or even polynomial function of the code dimension.

2012 ACM Subject Classification Theory of computation → Error-correcting codes

Keywords and phrases Quantum error correcting code

Digital Object Identifier 10.4230/LIPIcs.ITCS.2021.65

Related Version A full version of the paper is available at https://arxiv.org/abs/1911.03069.

Funding *Anthony Leverrier*: Agence Nationale de la Recherche (ANR): QuantERA project QCDA.
Gilles Zémor: Agence Nationale de la Recherche (ANR): ANR-18-CE47-0010 project QUDATA.

Acknowledgements We would like to thank Benjamin Audoux, Alain Couvreur, Omar Fawzi, Antoine Grospellier and Jean-Pierre Tillich for many fruitful discussions on quantum codes.

1 Quantum LDPC codes, local testability and robustness of entanglement

Entanglement is arguably the central concept of quantum theory and despite decades of study, many questions about it remain unsolved today. One particular mystery is the robustness of phases of highly entangled states, such as the ones involved in quantum computation. Given such a state, does it remain entangled in the presence of noise? A closely related question concerns low-energy states of local Hamiltonians: while ground states, *i.e.*, states of minimal energy, are often highly entangled, is it also the case of higher energy states? These questions are related through the concept of quantum error correction: logical information is often encoded in a quantum error correcting code (QECC) in order to be processed during a quantum computation, and the ground space of a local Hamiltonian is nothing but a special case of a QECC called quantum low-density parity-check (LDPC) code.

12th Innovations in Theoretical Computer Science Conference (ITCS 2021).
Editor: James R. Lee; Article No. 65; pp. 65:1–65:11
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Physically it indeed makes sense to implement quantum error correction by relying on local interaction, for example by encoding the quantum state in the degenerate ground space of a local Hamiltonian, that is an N-qubit operator $H \propto \sum_i \Pi_i$, where each Π_i is a projector acting nontrivially on a small number q of qubits (we talk of q-local terms). By "small", one usually means constant or sometimes logarithmic in N. A quantum stabilizer code is a subspace of the space $(\mathbb{C}^2)^{\otimes N}$ of N qubits defined as the common $+1$ eigenspace of a set $\{S_1, \dots, S_m\}$ of commuting Pauli operators, that is, the space

$$\mathrm{span}\{|\psi\rangle \in (\mathbb{C}^2)^{\otimes N} \;:\; S_i|\psi\rangle = |\psi\rangle, \forall i \in [m]\}.$$

Such a code is said to be *LDPC* if all the generators S_i act nontrivially on at most q qubits for small q. With this language, a quantum LDPC stabilizer code corresponds to the ground space of the local Hamiltonian $H = \frac{1}{m}\sum_{i=1}^m \Pi_i$, with $\Pi_i = \frac{1}{2}(I - S_i)$.

Entanglement can be quantified in many ways, but a relevant definition is to say that a quantum state is highly entangled (or displays *long-range entanglement*) if it cannot be obtained by processing an initial product state via a quantum circuit of constant depth. By contrast, a quantum state that can be obtained that way, and which is therefore of the form $U_{\mathrm{circ}}\big(\otimes_{i=1}^n |\phi_i\rangle\big)$ for some $|\phi_i\rangle \in \mathbb{C}^2$, is said to be *trivial.* An important property of trivial states is that they admit an efficient classical description and that one can efficiently compute the value of local observables such as Π_i for such states: this is because the operator $U_{\mathrm{circ}}^\dagger \Pi_i U_{\mathrm{circ}}$ remains local (since the circuit has constant depth) and its expectation can therefore be computed efficiently for a product state. In particular, such a classical description can serve as a witness that a local Hamiltonian admits a trivial state of low energy. It is well known how to construct N-qubit Hamiltonians with highly entangled ground states, for instance by considering a Hamiltonian associated with a quantum LDPC code with non-constant minimum distance [9], but the question of the existence of local Hamiltonians such that low-energy states are non-trivial remains poorly understood.

The no low-energy trivial state (NLTS) conjecture asks whether there exists a local Hamiltonian such that all states of small enough (normalized) energy are nontrivial [20]. More precisely, is there some $H = \frac{1}{m}\sum_{i=1}^m \Pi_i$ as above, such that there exists a constant $\alpha > 0$ such that all states ρ satisfying $\mathrm{tr}(\rho H) \le \alpha$ are nontrivial? What is interesting with the NLTS conjecture is that it is a consequence of the quantum PCP conjecture [1], and therefore corresponds to a possible milestone on the route towards establishing the quantum PCP conjecture. We note that there are several versions of the quantum PCP conjecture in the literature, corresponding to the quantum generalizations of equivalent versions of the classical PCP theorem, but not known to be equivalent in the quantum case, and that the multiprover version was recently established [28]. Here, however, we are concerned with the Hamiltonian version of the quantum PCP conjecture which still remains wide open. This conjecture is concerned with the complexity of the *Local Hamiltonian* problem: given a local Hamiltonian as before, two numbers $a < b$ and the promise that the minimum eigenvalue of the Hamiltonian is either less than a, or greater than b, decide which is the case. The quantum PCP conjecture asserts that this problem is QMA-hard when the gap $b - a$ is constant. This generalizes the PCP theorem that says that the satisfiability problem is NP-hard when the relative gap is constant [11]. Here, QMA is the class of languages generalizing NP (more precisely generalizing MA), where the witness can be a quantum state and the verifier is allowed to use a quantum computer. Assuming that NP $\not\subseteq$ QMA, we see that Hamiltonians with trivial states of low energy cannot be used to prove the quantum PCP conjecture since the classical description of such states would be a witness that could be checked efficiently by a classical verifier. In other words, if the quantum PCP conjecture is true, it implies that NLTS holds. The converse statement is unknown.

Eldar and Harrow made progress towards the NLTS conjecture by establishing a simpler variant, called NLETS [15], by giving an explicit local Hamiltonian where states close to ground states are shown to be nontrivial. (See also Ref. [29] for an alternate proof exploiting approximate low-weight check codes.) The subtlety here is that closeness is not defined as "low energy" as in NLTS, but by the existence of a low weight operator mapping the state to a ground state. Viewing the ground space as a quantum LDPC code, [15] shows that states which are δN-close to the code (for some sufficiently small $\delta > 0$) are nontrivial. The NLTS conjecture asks for something stronger: that all states with energy less than a small, constant, fraction of the operator norm of the Hamiltonian are nontrivial. Of course, states close to the codespace have a low (normalized) energy or syndrome weight, but the converse does not hold in general, and this is what makes the NLTS conjecture difficult to tackle.

One case where the distance to the code is tightly related to the syndrome weight is for *locally testable codes* (LTC): classical locally testable codes are codes for which one can efficiently decide, with high probability, whether a given word belongs to the code or is far from it, where efficiency is quantified in the number of queries to the coordinates of the word. To see the link between the two notions, the idea is to distinguish between codewords and words far from the code by computing a few elements of the syndrome and deciding that the word belongs to the code if all these elements are zero. An LTC is such that any word at constant relative distance from the code will have a constant fraction of unsatisfied checknodes, that is a syndrome of weight linear in the blocklength. The Hadamard code which maps a k-bit word x to a string of length 2^k corresponding to the evaluations at x of all linear functions provides such an example with the syndrome corresponding to all possible linearity tests between the bits of the word: indeed, any word that satisfies most linearity tests can be shown to be close to the codespace [6].

While LTCs have been extensively studied in the classical literature [19] and provide a crucial ingredient for the proof of the classical PCP theorem, their quantum generalization is relatively new and much less understood. The concept was only recently introduced in a paper by Aharonov and Eldar [2] which showed that the classical approaches to local testability seem to fail in the quantum world: for instance, defining a code on a (hyper)graph with too much expansion seems to be a bad idea. In any case, if quantum LTCs with constant minimum distance existed, they would provide a proof of the NLTS conjecture [15], and this motivates trying to understand whether such codes can exist. Let us, however, mention that while classical LTCs are useful for performing alphabet reduction in the context of the PCP theorem, the same doesn't seem to apply in the quantum regime since it is known that directly quantizing Dinur's combinatorial proof of the PCP theorem [11] is bound to fail [8, 1].

An additional difficulty in the quantum case is that good quantum LDPC codes are not even known to exist. While taking a random LDPC code yields a code with linear minimum distance with high probability in the classical case, the same statement is not known to hold in the quantum setting. Even restricting our attention to codes only encoding a constant number of logical qubits, it is hard to find families of codes with minimum distance much larger than $\sqrt{N}$: a construction due to Freedman, Meyer and Luo gives a minimum distance $\Theta(N^{1/2} \log^{1/4} N)$ [18] while recent constructions based on high-dimensional expanders yield a polylogarithmic improvement [23, 16, 24] and hold the current record for quantum LDPC codes. (Note that considering subsystem codes [30] or approximate codes [10, 5] is helpful to get a large minimum distance [4, 29, 7].) For these reasons, while a lot of work on classical LTCs focusses on codes with linear minimum distance and aims at minimizing the length of the code, the current goals in the quantum case are much more modest at this point.

A possible formal definition of a quantum LTC was suggested by [15], which we detail now. Recall that the objective is to relate two notions: the distance of a state to the code, and the energy of the state. A quantum code, or equivalently, its associated Hamiltonian, will be locally testable if any word at distance t from the code (or the ground space) has energy $\Omega(t)$ and if this energy can be estimated by accessing only a small number of qubits (this is why we insist on having local terms in the Hamiltonian). First, one defines a quantum version of the Hamming distance as follows. Consider the code space $\mathcal{C} \subset (\mathbb{C}^2)^{\otimes N}$ and define its t-fattening $\mathcal{C}_t$ as the span of states at distance at most t from $\mathcal{C}$:

$$\mathcal{C}_t := \mathrm{Span}\{(A_1 \otimes \cdots \otimes A_n)|\psi\rangle \ : \ |\psi\rangle \in \mathcal{C}, |\{i \ : \ A_i \neq I\}| \leq t\},$$

where the A_i are single-qubit Pauli matrices. States at distance t belong to $\mathcal{C}_t$, but not to $\mathcal{C}_{t-1}$, which we formalize by considering the projector $\Pi_{\mathcal{C}_t}$ onto $\mathcal{C}_t$ and forming the *distance operator*

$$D_{\mathcal{C}} := \sum_t t(\Pi_{\mathcal{C}_t} - \Pi_{\mathcal{C}_{t-1}}).$$

Informally, the eigenspace of $D_{\mathcal{C}}$ with eigenvalue t corresponds to states which are at distance t from the code. We now define the averaged normalized Hamiltonian $H_{\mathcal{C}}$ associated with the quantum code $\mathcal{C}$ with q-local projections $(\Pi_1, \ldots, \Pi_m)$:

$$H_{\mathcal{C}} = \frac{1}{m}\sum_{i=1}^{m} \Pi_i.$$

The normalization by m ensures that $\|H_{\mathcal{C}}\| \leq 1$. With these notations, we say that a q-local quantum code $\mathcal{C} \subseteq (\mathbb{C}^2)^{\otimes n}$ is an (s, q)-quantum LTC with soundness $s \in [0, 1]$ if[1]

$$H_{\mathcal{C}} \succeq \frac{s}{N} D_{\mathcal{C}}, \qquad (1)$$

where $A \succeq B$ means that the operator $A - B$ is positive semidefinite. In words, condition (1) means that any low-energy state is close to the codespace in terms of the quantum Hamming distance, and that simple energy tests allow one to distinguish codewords from states far from the code. More precisely, one can distinguish between a codeword (with energy 0) and a state at distance δN from the code (therefore with energy $\geq s\delta$) by measuring approximately $1/(s\delta)$ terms of the Hamiltonian. Ideally, one would want the soundness s and the locality q to be constant, so that accessing a constant number of qubits would suffice to distinguish codewords from states at distance greater than δN from the code, for constant $\delta > 0$.

Known constructions of quantum LTCs are rare. For instance, quantum expander codes yield one example of (s, q)-quantum LTCs with both $s = O(1), q = O(1)$, but with the *major caveat* that Eq. (1) doesn't hold in general, but only on the restriction of the Hilbert space consisting of states $O(\sqrt{N})$-close to the codespace [27]. In fact, there exist states at distance $\Omega(\sqrt{N})$ violating only a single projection Π_i. This means that such codes cannot be used to establish the NLTS conjecture. By allowing the locality to be logarithmic in the number of qubits instead of constant, that is $q = O(\log N)$, a recent construction of Hastings [21] yields a quantum LTC with soundness $s = O\left(\frac{1}{\log^2 N}\right)$, without any restriction on the validity of Eq. (1). The construction is a generalization of the toric code where instead of taking the product of two 1-cycles of length p, one rather considers the product of two d-cycles of area p^d for the appropriate values of $p = \omega(1)$ and $d = \omega(1)$.

[1] In a previous version of this manuscript, `https://arxiv.org/abs/1911.03069v1`, we were additionally normalizing the Hamiltonian by q, leading to a soundness value of s/q. We remove this extra factor here, in accordance with the literature in classical and quantum locally testable codes.

Our results

In this work, we present a different construction of a quantum LTC which shares with Hastings' the property that it is set in a high-dimensional space with $d = \Theta(\log N)$ and therefore a similar locality[2] $q = \Theta(\log N)$. Our code, however, achieves a slightly better soundness $r = \Omega\left(\frac{1}{\log N}\right)$, and in fact, we were not able to rule out that the soundness is not constant, which would be optimal. While this hemicube code only encodes a single logical qubit, we can introduce a generalized family of codes with polynomial rate. These codes are obtained starting with the chain complex associated to the n-dimensional Hamming cube, where we identify faces corresponding to the same coset of a classical code of length n. A CSS quantum code is obtained by placing qubits on the p-faces and stabilizers either on $(p-1)$-faces or $(p+1)$-faces, with constraints given by the incidence relations between the faces in the cube. While this construction is arguably quite natural, computing the parameters (dimension and minimum distance) of this code family turned out to be rather subtle, relying in nontrivial arguments from algebraic topology. The parameters of the CSS code resulting from the quotient of the cube by a linear code of parameters $[n, k, d]$ are

$$\left[\!\!\left[2^{n-p-k}\binom{n}{p}, \binom{p+k-1}{p}, \min\left\{\binom{d}{p}, 2^{n-p-k}\right\} \right]\!\!\right]$$

when qubits are placed on p-faces for $p \leq d-2$. Whether these codes are also locally testable is left as an open question. In that case, these would provide the first examples of quantum LTCs of exponential or even polynomial length in the code dimension. Remember indeed that both the hemicubic and Hastings' codes have constant dimension.

2 Construction of the hemicubic code

We start with the simplest member of our quantum code family, corresponding to the quotient of the n-cube by the repetition code. It has been known since Kitaev [25] that one can associate a quantum CSS code with any chain complex of binary vector spaces of the form: $C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0$, where the boundary operators ∂_2 and ∂_1 satisfy $\partial_1\partial_2 = 0$. One first defines two classical codes $\mathcal{C}_X = \ker \partial_1$ and $\mathcal{C}_Z = (\operatorname{Im} \partial_2)^\perp = \ker \partial_2^T$. These codes satisfy $\mathcal{C}_Z^\perp \subseteq \mathcal{C}_X$ since $\partial_1\partial_2 = 0$ and the resulting quantum CSS code is the linear span of $\left\{\sum_{z \in \mathcal{C}_Z^\perp} |x+z\rangle \;:\; x \in \mathcal{C}_X\right\}$, where $\{|x\rangle \;:\; x \in \mathbb{F}_2^N\}$ is the canonical basis of $(\mathbb{C}^2)^{\otimes N}$ and N is the dimension of the central space C_1 of the chain complex. One obtains in this way a quantum code of length N and dimension $\dim(\mathcal{C}_X/\mathcal{C}_Z^\perp) = \dim(\mathcal{C}_X) + \dim(\mathcal{C}_Z) - N$. Its minimum distance is given by $d_{\min} = \min(d_X, d_Z)$ with $d_X = \min\{|w| \;:\; w \in C_X \setminus C_Z^\perp\}$ and $d_Z = \min\{|w| \;:\; w \in C_Z \setminus C_X^\perp\}$. Here, $|w|$ stands for the Hamming weight of the word w.

Our construction relies on the n-dimensional hemicube, where a p-face is formed by a pair of antipodal p-dimensional faces of the Hamming cube $\{0,1\}^n$. A p-face of the Hamming cube is a string of n-elements from $\{0, 1, *\}$ where symbol $*$ appears exactly p times. Let us denote by C_p^n the $\mathbb{F}_2^n$-vector space spanned by p-faces of the hemicube. Boundary ∂_p and coboundary δ_p operators are obtained by extending the natural operators for the Hamming cube to the hemicube

$$\partial_p\, x_1 \dots x_n := \bigoplus_{i \text{ s.t.} x_i = *} x_1 \dots x_{i-1} 0 x_{i+1} \dots x_n \oplus x_1 \dots x_{i-1} 1 x_{i+1} \dots x_n$$

$$\delta_p\, x_1 \dots x_n := \bigoplus_{i \text{ s.t.} x_i \neq *} x_1 \dots x_{i-1} * x_{i+1} \dots x_n$$

[2] We note that in both our construction and Hastings', each qubit is only involved in a logarithmic number of constraints.

and are further extended to p-chains by linearity. We reserve the notation $+$ for the standard addition in $\mathbb{F}_2$ and use $\oplus$ for summing chains. The hemicubic code is then defined as the CSS code obtained from the chain complex

$$C^n_{p+1} \xrightarrow{\partial_{p+1}} C^n_p \xrightarrow{\partial_p} C^n_{p-1}.$$

Choosing $p = \alpha n$ for $0 < \alpha < 1$, the resulting code will be LDPC with generators of logarithmic weight since the boundary and coboundary operators act nontrivially on $O(n) = O(\log N)$ coordinates. The dimension of the hemicubic code corresponds to that of the homology groups $H^n_p = \ker \partial_p / \mathrm{Im}\, \partial_{p+1}$. Since the hemicube, viewed as a cellular complex, has the same topology as the real projective plane, its homology groups all have the same dimension equal to 1. We note that the quantum code obtained here can be described with a completely different approach exploiting Khovanov homology [3]. Obtaining the minimum distance of the code requires more care since one needs to find lower bounds on the weight of minimal nontrivial cycles and cocycles in the hemicube. Summarizing, we establish the following result.

▶ **Theorem 1.** *The hemicubic code is a CSS code with parameters*

$$\left[\!\left[N = 2^{n-p-1}\binom{n}{p}, 1, d_{\min} = \min\left\{\binom{n}{p}, 2^{n-p-1}\right\} \right]\!\right].$$

Let $\alpha^* \approx 0.227$ be the unique nonzero solution of $h(\alpha^*) = 1 - \alpha^*$ where h is the binary entropy function. Then choosing $p = \lfloor \alpha^* n \rfloor$ yields a quantum code family with $d_{\min} \geq \frac{\sqrt{N}}{1.62}$ [3].

3 Local testability of the hemicubic code

We now turn our attention to the local testability of the hemicubic code. This property results from isoperimetric bounds on the hemicube.

▶ **Theorem 2.** *The hemicubic code is locally testable with soundness $s = \Omega\left(\frac{1}{\log N}\right)$.*

This improves over Hastings' construction [22] obtained by taking the product of two n-spheres and which displays soundness $s = \Theta\left(\log^{-2}(N)\right)$. It would be interesting to understand whether the bounds of Theorem 2 are tight or not. At the moment, we believe it might be possible to get rid of the logarithmic factor and obtain a constant soundness for the hemicubic code. This would then match the soundness of the standard Hamming cube, which does not encode any logical qubit since its associated complex has zero homology.

We say that a p-chain X is a *filling* of Y if $\partial X = Y$ and that a p-cochain X is a *cofilling* of Y if $\delta X = Y$. The main tools to establish the soundness of the hemicubic code are upper bounds on the size of fillings (resp. cofillings) for boundaries (resp. coboundaries) in the cube. Denoting the Hamming weight of chains and cochains by $\|\ \|$, we have:

▶ **Lemma 3.** *Let E be a p-chain of C^n_p. Then there exists a p-chain F which is a filling of ∂E, satisfying $\partial F = \partial E$ such that*

$$\|F\| \leq \frac{n-p}{2}\|\partial E\|.$$

Let E be a p-cochain of C^n_p. Then there exists a p-cochain F which is a cofilling of δE, satisfying $\delta F = \delta E$ such that

$$\|F\| \leq (p+1)\|\delta E\|.$$

It is straightforward to translate these results in the language of quantum codes. Let us represent an arbitrary Pauli error of the form $\bigotimes_{i\in E_X, j\in E_Z} X^i Z^j$ by a couple $E=(E_X,E_Z)$ where E_X is the support of the X-type errors and E_Z is the support of the Z-type error. Interpreting E_X as a p-chain and E_Z as a p-cochain, we see that the syndrome of E is given by the pair $(\partial E_X, \delta E_Z)$. In order to compute the soundness of the quantum code, one needs to lower bound the ratio:

$$\min_{(E_X,E_Z)} \frac{\|\partial E_X\| + \|\delta E_Z\|}{\|[E_X]\| + \|[E_Z]\|} \geq \min \left\{ \min_{E_X} \frac{\|\partial E_X\|}{\|[E_X]\|}, \min_{E_Z} \frac{\|\delta E_Z\|}{\|[E_Z]\|} \right\},$$

where the minimum is computed over all errors with a nonzero syndrome, i.e., for p-chains E_X which are not a p-cycle and p-cochains E_Z which are not a p-cocycle. In these expressions, we denote by $[E]$ the representative of the equivalence class of error E, with the smallest weight. Indeed, recall that two errors differing by an element of the stabilizer group are equivalent. The fact that one considers $[E]$ instead of E makes the analysis significantly subtler in the quantum case than in the classical case. A solution is to work backward (as was also done by Dotterer in the case of the Hamming cube [13]): start with a syndrome and find a small weight error giving rise to this syndrome. This is essentially how we establish Lemma 3:

$$\min_{E_X, \partial E_X \neq 0} \frac{\|\partial E_X\|}{\|[E_X]\|} \geq \frac{2}{n-p}, \qquad \min_{E_Z, \delta E_Z \neq 0} \frac{\|\delta E_Z\|}{\|[E_Z]\|} \geq \frac{1}{p+1}.$$

This implies the soundness in Theorem 2 since $n-p, p+1 = \Theta(\log N)$.

While Dotterer established tight bounds for the size of (co)fillings in the Hamming cube, we do not know whether the bounds of Lemma 3 are tight. Right now, we lose a logarithmic factor in the case of the hemicube, but it is not clear that this should be the case. In fact, it is not even excluded that the hemicube could display a *better* soundness than the standard cube. We expand on these ideas in the full version of the paper [26].

4 An efficient decoding algorithm for the hemicubic code

The existence of the small fillings and cofillings promised by the soundness of the code is particularly interesting in the context of decoding since it guarantees the existence of a low-weight error associated to any low-weight syndrome. To turn this into an efficient decoding algorithm, the main idea is to notice that one can efficiently find the required fillings and cofilings and therefore find Pauli errors giving the observed syndrome. While finding the smallest possible fillings or cofillings does not appear to be easy, finding ones satisfying the bounds of Lemma 3 can be done efficiently.

We note, however, that the decoding algorithm does not seem to perform so well against random errors of linear weight. In particular, arguments from percolation theory that would imply that errors tend to only form small clusters and that therefore it is sufficient to correct these errors (similarly to [17] for instance) will likely fail here because of the logarithmic weight of the generators. Indeed, the factor graph of the code has logarithmic degree and there does not exist a constant threshold for the error probability such that below this threshold, errors appear in clusters of size $o(N)$. In addition, and more importantly, our decoding algorithm is not local in the sense that it explores only the neighborhood of some violated constraints to take a local decision, and for this reason, it is not entirely clear whether the algorithm processes disconnected clusters of errors independently.

▶ **Theorem 4.** *The hemicubic code comes with an efficient decoding algorithm that corrects adversarial errors of weight $O(d_{\min}/\log^2 N)$ with complexity $O(n^4 N)$.*

The decoding complexity is quasilinear in the error size and the algorithm can be parallelized to run in logarithmic depth. Finding a filling (or cofilling) can be done recursively by fixing one of the n coordinates and finding fillings in the projective cube of dimension $n-1$. While the choice of the special coordinate is not immediately obvious if one wants to find the smallest filling, it is nevertheless possible to make a reasonably good choice efficiently by computing upper bounds on the final filling size for each possible choice of coordinate. We establish Theorem 4 in the full version of the paper [26].

5 Generalized hemicubic codes: quotients by arbitrary linear codes

A key remark is that identifying antipodal p-faces of the n-cube is equivalent to considering the cosets of the repetition code $\{0^n, 1^n\}$ in the cube complex. It is therefore tempting to generalize this approach by identifying the elements of the cosets of arbitrary linear codes $\mathcal{C}$ with parameters $[n, k, d]$. We form in this way a new complex where two p-faces x and y are identified if there exists a codeword $c \in \mathcal{C}$ such that $x = y + c$. Recall that addition is coordinate-wise here and that $*$ is an absorbing element.

Deriving the parameters of the quantum CSS code associated to these new complexes has been surprisingly challenging. In particular it does not seem particularly obvious that the quantum parameters, especially the minimum distance, should depend only on the parameters $[n, k, d]$ of the classical code $\mathcal{C}$ and not otherwise on its particular structure: it turns out indeed to be the case however. We managed to derive the quantum parameters by exhibiting explicit representatives of the $\mathbb{F}_2$-homology and cohomology classes, through a double induction on p and the classical code dimension k. We obtain a lower bound on the minimum homologically non-trivial cycle weight by exhibiting a set of representatives of a cohomology class all of which must be orthogonal to the cycle, and in particular intersect it. Since a non-trivial cycle meets this bound it is exact. A similar method is used to derive the minimum non-trivial cocycle weight and we obtain the following theorem.

▶ **Theorem 5.** *The quantum code obtained as the quotient of the n-cube by a linear code $[n, k, d]$ admits parameters*

$$\left[\!\left[2^{n-p-k}\binom{n}{p}, \binom{p+k-1}{p}, \min\left\{\binom{d}{p}, 2^{n-p-k}\right\} \right]\!\right]$$

when qubits are placed on p-faces for $p \leq d-2$.

An interesting case is $k = 2$, which yields a quantum code of exponential length (that is, dimension logarithmic in the code length):

$$\left[\!\left[2^{n-p-2}\binom{n}{p}, p+1, \min\left\{\binom{d}{p}, 2^{n-p-2}\right\} \right]\!\right].$$

We are only able to prove a lower bound on the soundness of the code (for X-errors) of $\Omega(1/p!)$. However, a much improved soundness would follow from the conjectured filling and cofilling constants of the original hemicubic complex: generalized hemicubic codes are therefore candidates for quantum locally testable codes of growing dimension, of which no examples are presently known.

6 Discussion and open questions

In this paper, we have introduced a family of quantum code constructions that live on the quotient of the n-dimensional Hamming cube by classical linear codes. Despite the apparent simplicity of the construction, it does not seem to have appeared before in the literature.

Deriving the parameters of these codes turned out to be significantly subtler than expected, and quite surprisingly, the parameters of the quantum code only depend on the parameters of the classical code and not on any additional structure. The simplest member of our quantum code family, the hemicubic code, basically inherits its local testability from the soundness of the Hamming cube, which was established by Dotterer. In our view, the fact that our code construction relies so much on the Hamming cube may be expected to yield additional advantages, through the import of other interesting properties from the cube, as well as tools from Boolean analysis.

The most pressing question is to understand whether the generalized hemicubic codes also display local testability. At the moment, we can only establish it for the simplest member of the family, which only encodes a single logical qubit. If we could show that the codes corresponding to the quotient of the Hamming cube by arbitrary linear codes of dimension k remain locally testable, then this would provide the first examples of quantum locally testable codes of exponential (if $k > 1$) or polynomial (if $k = \Omega(n)$) length. As we discuss in the full version of the paper [26], improving our bound on the soundness of the one-qubit hemicubic code from $\frac{1}{\log N}$ to constant would already prove that the generalized code with $k = 2$ remains locally testable. An indication that such an improvement might be possible comes from the 0-qubit code defined on the standard hypercube (without identifying antipodal faces) which indeed displays constant soundness [12]. More generally, the question of what parameters are achievable for quantum locally testable codes is essentially completely open at the moment.

Another intriguing question is whether the hemicubic code might help towards establishing the NLTS conjecture (albeit with a quasilocal Hamiltonian with terms of logarithmic weight) or more generally whether it is relevant for many-body physics. As mentioned earlier, any quantum LTC with linear minimum distance would yield such a proof [15]. The hemicubic code, however, is restricted by a $O(\sqrt{N})$ minimum distance, and the argument of [15] does not directly apply anymore. This is in particular a line of research followed by Eldar which relies on the hemicubic code and which provides positive partial results [14]. We note that in the physics context of the Local Hamiltonian, it is crucial that every individual quantum system (say, qubit) is acted upon by a small number of terms. In this sense, the problem is somewhat more constrained than in the local testability case where one is typically fine if the number of qubits is much larger than the number of constraints. Our quantum codes satisfy this requirement since each qubit is only involved in a logarithmic number of local constraints.

Finally, while classical LTCs have found a number of applications in recent years, notably for constructing PCPs, it is fair to say that not much is presently known about possible applications of quantum LTCs. At the same time, local testability is a notion that makes perfect sense in the quantum regime and it seems reasonable to think that quantum LTCs might also find applications. Finding explicit families encoding a non-constant number of qubits is a natural first step.

References

1 Dorit Aharonov, Itai Arad, and Thomas Vidick. Guest column: the quantum PCP conjecture. *ACM SIGACT news*, 44(2):47–79, 2013.

2 Dorit Aharonov and Lior Eldar. Quantum locally testable codes. *SIAM Journal on Computing*, 44(5):1230–1262, 2015.

3 Benjamin Audoux. An application of Khovanov homology to quantum codes. *Ann. Inst. Henri Poincaré Comb. Phys. Interact*, 1:185–223, 2014.

4 Dave Bacon, Steven T Flammia, Aram W Harrow, and Jonathan Shi. Sparse quantum codes from quantum circuits. In *Proceedings of the forty-seventh annual ACM symposium on Theory of Computing*, pages 327–334, 2015.

5 Cédric Bény and Ognyan Oreshkov. General conditions for approximate quantum error correction and near-optimal recovery channels. *Physical review letters*, 104(12):120501, 2010.

6 Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-testing/correcting with applications to numerical problems. *Journal of computer and system sciences*, 47(3):549–595, 1993.

7 Thomas C Bohdanowicz, Elizabeth Crosson, Chinmay Nirkhe, and Henry Yuen. Good approximate quantum ldpc codes from spacetime circuit hamiltonians. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 481–490, 2019.

8 Fernando GSL Brandao and Aram W Harrow. Product-state approximations to quantum ground states. In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*, pages 871–880. ACM, 2013.

9 S Bravyi, MB Hastings, and F Verstraete. Lieb-robinson bounds and the generation of correlations and topological quantum order. *Physical Review Letters*, 97(5):050401, 2006.

10 Claude Crépeau, Daniel Gottesman, and Adam Smith. Approximate quantum error-correcting codes and secret sharing schemes. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 285–301. Springer, 2005.

11 Irit Dinur. The PCP theorem by gap amplification. *Journal of the ACM (JACM)*, 54(3):12, 2007.

12 Dominic Dotterrer. *The (co) isoperimetric problem in (random) polyhedra.* PhD thesis, University of Toronto, 2013.

13 Dominic Dotterrer. The filling problem in the cube. *Discrete & Computational Geometry*, 55(2):249–262, 2016.

14 Lior Eldar. Robust quantum entanglement at (nearly) room temperature. *manuscript*, 2019.

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

16 Shai Evra, Tali Kaufman, and Gilles Zémor. Decodable quantum ldpc codes beyond the $\sqrt{n}$ distance barrier using high dimensional expanders. *arXiv preprint*, 2020. `arXiv:2004.07935`.

17 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*, pages 521–534. ACM, 2018.

18 Michael H Freedman, David A Meyer, and Feng Luo. Z2-systolic freedom and quantum codes. *Mathematics of quantum computation, Chapman & Hall/CRC*, pages 287–320, 2002.

19 Oded Goldreich. Short locally testable codes and proofs: A survey in two parts. In *Property testing*, pages 65–104. Springer, 2010.

20 Matthew B Hastings. Trivial low energy states for commuting Hamiltonians, and the quantum PCP conjecture. *Quantum Information & Computation*, 13(5-6):393–429, 2013.

21 Matthew B Hastings. Quantum codes from high-dimensional manifolds. In *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017.

22 Matthew B Hastings. Quantum codes from high-dimensional manifolds. In *LIPIcs-Leibniz International Proceedings in Informatics*, volume 67. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017.

23 Tali Kaufman, David Kazhdan, and Alexander Lubotzky. Isoperimetric inequalities for ramanujan complexes and topological expanders. *Geometric and Functional Analysis*, 26(1):250–287, 2016.

24 Tali Kaufman and Ran J Tessler. Quantum LDPC codes with $\Omega(\sqrt{n}\log^k n)$ distance, for any k. *arXiv preprint*, 2020. `arXiv:2008.09495`.

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

26 Anthony Leverrier, Vivien Londe, and Gilles Zémor. Towards local testability for quantum coding. *arXiv preprint*, 2019. `arXiv:1911.03069`.

27 Anthony Leverrier, Jean-Pierre Tillich, and Gilles Zémor. Quantum expander codes. In *Foundations of Computer Science (FOCS), 2015 IEEE 56th Annual Symposium on*, pages 810–824. IEEE, 2015.

28 Anand Natarajan and Thomas Vidick. Low-degree testing for quantum states, and a quantum entangled games PCP for QMA. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 731–742. IEEE, 2018.

29 Chinmay Nirkhe, Umesh Vazirani, and Henry Yuen. Approximate low-weight check codes and circuit lower bounds for noisy ground states. In *45th International Colloquium on Automata, Languages, and Programming (ICALP 2018)*, volume 107, page 91. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2018.

30 David Poulin. Stabilizer formalism for operator quantum error correction. *Physical Review Letters*, 95(23):230504, 2005.