

Quantum Locally Testable Codes

Dorit Aharonov*

Lior Eldar†

October 22, 2013

Abstract

We initiate the study of quantum Locally Testable Codes (qLTCs). We provide a definition together with a simplification, denoted sLTCs, for the special case of stabilizer codes, and provide some basic results using those definitions. The most crucial parameter of such codes is their *soundness*, $R(\delta)$, namely, the probability that a randomly chosen constraint is violated as a function of the distance of a word from the code (δ , the relative distance from the code, is called the *proximity*). We then proceed to study limitations on qLTCs. In our first main result we prove a surprising, inherently quantum, property of sLTCs: for small values of proximity, the better the small-set expansion of the interaction graph of the constraints, the *less* sound the qLTC becomes. This stands in sharp contrast to the classical setting. The complementary, more intuitive, result also holds: an upper bound on the soundness when the code is defined on *bad* small-set expanders (a bound which turns out to be far more difficult to show in the quantum case). Together we arrive at a quantum upper-bound on the soundness of stabilizer qLTCs set on *any* graph, which does not hold in the classical case. Many open questions are raised regarding what possible parameters are achievable for qLTCs. In the appendix we also define a quantum analogue of PCPs of proximity (PCPPs) and point out that the result of [15] by which PCPPs imply LTCs with related parameters, carries over to the sLTCs. This creates a first link between qLTCs and quantum PCPs [6].

1 Introduction

Quantum error correcting codes have played a crucial role in quantum complexity theory (see, e.g., [32, 33, 11, 12]) and their study is a vastly growing field (see, e.g., [31, 51, 52, 41, 42, 49, 27]); they are related to a variety of issues including resilience to noise and fault tolerance, quantum cryptography, topological order, multi-particle entanglement, and more.

Here, we initiate the study of the quantum analogue of Locally Testable Codes (LTCs). LTCs, first defined in [28, 46, 1], are a particularly interesting class of error correcting codes which played an instrumental role in all proofs of the celebrated PCP theorem [5, 8, 24]; their study had inspired the definition of property testing [29] and the understanding of their limitations and possible constructions has developed into a very interesting field of its own (see for example Goldreich's survey [30]).

To define LTCs, consider the following question: given a code of n -bit strings, defined by $O(1)$ -local constraints, and a word which is of distance $\delta n > 0$ from the code (we say it has *proximity* δ), what is the probability that a randomly chosen constraint is violated? We denote by $R(\delta)$ (called the

*School of Computer Science and Engineering, The Hebrew University, Jerusalem, Israel

†School of Computer Science and Engineering, The Hebrew University, Jerusalem, Israel.

soundness) the lower bound on the probability that *any* word of proximity δ from the code will violate a randomly chosen constraint.

LTCs of excellent soundness at proximities larger than some constant are known, most notably the Reed-Muller code [43], the Hadamard code [9], and Hastad’s long-code [36] which were used in the PCP proofs of [5, 8, 24]. Though of excellent soundness, these codes are not so satisfying when considering other parameters of interest. For example, the rates of the Hadamard and long code are exponentially and doubly exponentially small, respectively. Much research [28, 46] was devoted to optimizing the parameters of LTCs, maintaining constant relative distance and constant *query complexity* (namely, the number of bits in each constraint), and improving the rate. The best known LTCs in this respect are [24, 16] which have constant distance, constant query complexity, and rates which are $1/\text{polylog}$. It is a major open question (called the c^3 problem [34]) whether good (namely, constant relative rate and distance) LTCs exist.

1.1 Quantum Locally Testable Codes - Definition and Motivation

To the best of our knowledge the quantum analogue of LTCs was not defined before. We provide a definition of general quantum Locally Testable Codes (qLTCs) in Definition 14. To define qLTCs, we recall that a quantum code defined by $O(1)$ -local constraints can be viewed as the groundspace (namely, the zero eigenspace) of a local Hamiltonian $H = \sum_{i=1}^m \Pi_i$ whose local terms are projections, which we will refer to as the quantum constraints. We define Quantum Locally Testable Codes (qLTCs) with soundness $R(\delta)$ as those codes for which when a state Ψ is within distance at least δn from the code space, its average energy with respect to the constraints, $\frac{1}{m} \langle \Psi | H | \Psi \rangle$, is at least $R(\delta)$ (for an exact definition see Subsection 3). The average energy is the natural and commonly used analogue, in quantum Hamiltonian complexity, of the probability to detect a violation in a randomly chosen constraint (see for example [6]).

This definition sets the stage for a wide range of interesting questions. What are the limitations on quantum LTCs, and what are possible constructions? Are there qLTCs which achieve, or get close to, the best classical LTCs in terms of parameters, or are the quantum versions of those codes inherently limited by some quantum phenomenon? What can we learn from qLTCs regarding the notion of local testability of proofs, a notion which in the classical setting is tightly related to that of LTCs [30], and which is still widely evasive in the quantum setting [6]?

Our motivation in introducing qLTCs in order to study the above questions stems not only from trying to import the interesting classical local-testability paradigm into the quantum setting, but also from their strong relations to questions which are of inherent interest to quantum information, quantum complexity as well as to quantum physics. We highlight here several such connections.

An important motivation is to gain insight into the widely open quantum PCP conjecture [2], a quantum analogue of the PCP theorem; it states, roughly, that it is quantum-NP hard to approximate the ground energies of local Hamiltonians even to within a constant fraction. This conjecture is tightly related to deep questions about multiparticle entanglement, and there has been much recent work attempting to make progress on it (see the recent survey [6] and references therein). In the classical setting, LTCs have been instrumental in PCP theory [5, 8, 24] and are intimately related to the notion of local testability of proofs [30], and understanding the limitations of their quantum counterparts might shed light on the qPCP problem.

Another important open question is that of the feasibility of quantum self correcting memory. This is a medium in which a quantum state is maintained almost intact for a long time without active error

correction, even at constant temperatures; errors are corrected passively by the interaction with the environment. Clearly such a system is of high practical as well as theoretical interest, and the topic has been studied extensively in recent years (e.g., [18, 21, 22, 23, 19, 35, 50]). It is of major interest to devise feasible constructions of quantum self correcting memory. A crucial role in this area is played by the *energy barrier* of the quantum code, which is the amount of energy required in order to move from one codeword to an orthogonal one. This notion, which has also been studied extensively (see, e.g., [44]), is tightly related to the soundness of the code, which can be viewed as the *energy cost* of large errors; understanding qLTCs might thus provide insights into possible constructions of self-correcting memories.

A fundamental open question related to both of the above is whether multiparticle entanglement can be made robust at room temperatures. The question was formalized by Hastings in terms of the NLTS (No Low-energy Trivial States) conjecture [37], which, roughly, states that there exist local Hamiltonians such that all their low-energy states are highly entangled. Such Hamiltonians are necessary for the qPCP conjecture to hold ([37], and see also [6]). NLTS Hamiltonians and qLTCs seem related: while in qLTCs, low energies imply closeness to the code, in NLTS Hamiltonians they imply high entanglement, which is well known to be necessary for code states. Indeed, some weak connections between the two notions were already proven¹.

In the following, we will investigate the behavior of qLTCs in various scenarios. The behavior of LTCs is usually explored in one of two contexts: as an error-correcting code, or in relation to locally testable proofs (see [30]); depending on the context, one is interested in different parameters. In particular, in the context of error correction, the interesting regime of proximities, namely distance of the word from the code, is at most half the distance of the code; in this regime, the error can still be corrected. In the context of PCPs, on the other hand, much larger distances can be of interest, since a cheating prover may provide witnesses of arbitrary distance from the code. At any given point, we will mention the range which we will be considering.

1.2 Contributions

1.2.1 Definition and Basic Examples

We provide a general definition of qLTCs in Definition 14. Being probably the richest and most well-studied class of quantum codes, stabilizer codes [31] are compelling to work with. We thus provide a simpler definition for stabilizer LTCs (denoted sLTC – Definition 15) and prove that it coincides with the definition of qLTCs on stabilizer codes, in Claim 3.

An illuminating example to consider is Kitaev’s 2D toric code [39], which turns out to have very bad soundness, since a string-like error of any length – e.g., an error made of Pauli operators applied on a $\Theta(\sqrt{n})$ long line-segment of qubits – only violates two constraints – those that intersect its two edges. So, at small (up to $1/\sqrt{n}$) values of proximity, the soundness is bounded from above by $1/\sqrt{n}$. One can in fact extend this phenomenon to derive bounds on the soundness for constant values of proximity.

Another illuminating example is the Quantum Reed-Muller codes [48]. Certain classical Reed-Muller code are known to have good (constant) soundness [4]. Quantum Reed-Muller codes can be constructed using classical Reed-Muller codes and their dual, in the usual CSS paradigm [45]. By construction, the resulting code will inherit its soundness from one of the two classical codes that

¹One can show that qLTCs do not have tensor-product states with small (constant) mean energy.

defines the CSS code – the one with the worse soundness. Unfortunately, the rate and distance of the quantum Reed-Muller codes are much worse even than the optimal classical Reed-Muller codes, as is expected from CSS codes [45] (more details will be provided in the journal version).

1.2.2 Bound on the soundness of sLTCs on small set expanders

We provide two upper bounds on the soundness of qLTCs at low, constant values of proximities $\delta > 0$. We focus on sLTC's on n qudits, which are *good* quantum codes, defined by m $k = O(1)$ -local check terms, where each qudit participates in $D_L = O(1)$ constraints. For such codes, we consider bounds on the soundness at values of proximities which are at most some constant; this constant is a function of k, D_L , and in particular, $\delta < 1/k$. Usually, in the classical setting, it is much easier to derive LTCs whose soundness is good (large) for those *small* proximity values. Here, we show that in this supposedly *easier* range of parameters, qLTCs are severely limited compared to their classical counterparts.

To make the statement of the results simpler, we observe that the soundness $R(\delta)$, is bounded above by the number of constraints that touch the erred qudits, divided by m : hence it is at most $\delta n D_L / m = k\delta$ (using $D_L n = km$). It is more informative to present our results in terms of the *relative soundness* $r(\delta) = R(\delta)/k\delta$, which is the soundness normalized by its maximal value (for exact definition see Definition 16).

Our first main result proves that good qLTCs exhibit a severe limitation on their relative soundness, when set on good expanders. More precisely, consider the bi-partite graph of the code defined with n bits on the left side, m constraints on the other side, and edges connecting each constraint to all of its bits. We say that the bi-partite graph is an ε small-set expander if every small (size $k = O(1)$) subset of bits, is examined nearly by as many constraints as it possibly can, namely, by at least $(1 - \varepsilon)kD_L$ constraints. Theorem 1 shows that in the quantum setting, when the underlying bi-partite graph of the sLTC code is an ε small set expander, the relative soundness is $O(\varepsilon)$. In other words, the better the expansion, the worse the soundness. This holds for all proximities smaller than some constant δ_0 . More formally, we show:

Theorem 1 *Let C be a good stabilizer code, on n d -dimensional qudits, of relative distance > 0 , and a k -local generating set $\mathcal{G} \subset \Pi_d^n$, such that each qudit is examined by D_L generators. Put $\delta_0 = \min \left\{ \frac{1}{k^3 D_L}, \frac{1}{2n} \text{dist}(C) \right\}$. Suppose the bi-partite interaction graph of \mathcal{G} is ε -small set expanding, for $\varepsilon < 1/2$. Then, for all $0 < \delta < \delta_0$, we have $r(\delta) \leq 2\varepsilon$.*

See subsection 3 for exact definitions of Stabilizer codes and their generators, and Definition 16 for the exact definition of relative soundness.

Theorem 1 stands in sharp contrast to the classical domain. Classically, codes can easily be constructed on good expanders so that for small proximities their soundness is excellent; We provide an explicit such example whose relative soundness is arbitrarily close to 1 by plugging the *lossless expanders* constructed in [20], into the expander code construction of Sipser and Spielman [47]. This implies good classical codes with constant query complexity and with almost optimal soundness for any proximity δ smaller than some constant (see Claim (5 in Appendix C).

1.2.3 Bound on the soundness of general qLTCs

Our second main result is an upper bound on the relative soundness which holds for sLTCs set on *any* underlying bi-partite graph, not necessarily small-set expanders.

Theorem 2 (Roughly) *For any good stabilizer code C of k -local terms ($k \geq 4$) over d -dimensional qudits, where each qudit interacts with $O(1)$ local terms, errors of fractional weight $\delta < \delta_0 \leq 1$, for $\delta_0 = \Omega(1)$ have relative soundness at most $\alpha(d)(1 - \gamma_{\text{gap}})$ for some constant function $\gamma_{\text{gap}} = \gamma_{\text{gap}}(k, d) > 0$.*

$\alpha(d)$ in the above theorem is defined to be $1 - 1/d^2$; this is a technical upper bound on the relative soundness of qLTCs defined on d -dimensional qudits, stemming quite easily from the size of the alphabet d (see subsection 5.1); Theorem 2 shows that the soundness is further bounded by some seemingly deeper quantum phenomenon. We stress that this upperbound, which is not exhibited in classical codes, is found in the range of parameters of δ (small constants) in which it is supposed to be *easiest* to achieve soundness for LTCs, e.g., our Claim 5.

1.2.4 Quantum PCPs of Proximity

LTCs are tightly connected [30] to PCP's of proximity (PCPPs), which are proof systems defined very similarly to PCPs (See [15]). For the reader familiar with PCPs, they too consider a verifier who gets access to an untrusted proof, however, PCPPs differ from PCPs in two important aspects: first, they are weaker, in the sense that they are required to reject only inputs that are *far* from the language, whereas in PCPs any input out of the language should be rejected. On the other hand, the verifier is charged not only for the number of queries out of the proof, but also for the number queries out of (part of) the input. For a formal definition see Appendix G.

Ben Sasson et. al [15] provide a standard construction of an LTC from a PCPP. Given a PCPP for membership in a code, and an error correcting code C , they construct an LTC code C' , which inherits its soundness parameter from the soundness parameter of the PCPP and its distance from the code C (Construction 4.3, and Proposition 4.4 in [15], see Appendix G).

In Appendix G, we suggest a definition of quantum PCPPs, and show that a similar result to that of [15] holds in the quantum setting. The meaning of the definition of qPCPP and of the above described connection, and their relevance and importance to the quantum PCP conjecture, are far from clear (see for example [6] for doubts regarding the classical approach to proving the quantum PCP conjecture, and the direct applicability of quantum Error correcting codes in this context). Still we provide these definitions and results in the appendix, to make the point that a syntactic connection does carry over also in the quantum regime. It is a widely open question to give deep meaning to the connection between qLTCs and quantum local testability of proofs, as is known in the classical case [30].

1.3 Overview of Proofs of Theorems 1 and 2

1.3.1 Bounds on sLTC codes on Expanders

To prove theorem 1, we want to use good small-set expansion in order to construct an error which will not have a large energy penalty (namely, will not violate too many constraints) but which will be of large weight. More precisely, the error should have a large weight modulo the centralizer of the stabilizer group (see Definition 15), and yet should not violate too many stabilizer generators (recall

that an error violates a stabilizer generator, or constraint, if it does not commute with it; see definition 7).

The key idea is that in a small-set expander, intersections between stabilizer generators which consist of more than one qudit are rare (See fact 2). The size of the intersection matters since for two generators that intersect on a single qubit, the restrictions of those operators to that qubit must *commute*, because the two generators commute overall (see definition 7). We note that it cannot be that *all* generators when restricted to a given qudit commute, because this would mean this qubit is trivial for the code (see remark at the end of Subsection 2.3). An error defined on a qudit in such a way that it commutes with the majority of the generators acting on it, will violate only a small fraction of the constraints acting on that qudit.

To extend this to errors of larger weight (up to some small constant fraction), we apply the above idea to each of the generators in a large “sparse” set of generators, namely a set in which each two terms are of at least some constant distance apart in the interaction bi-partite graph. (formally, a 1-independent set of terms; see Definition 18). It is not difficult to see that due to the distance between the generators, the error weight remains large even modulo the centralizer.

1.3.2 Upper bound on soundness for stabilizer sLTCs on any graph

To prove theorem 2, we want to prove that regardless of the graph they are set on, the relative soundness of qLTCs is bounded from above by some constant strictly smaller than 1. We use the bound of theorem (1) (the “surprising” side) augmented with a claim that quantum stabilizer codes not only suffer from the quantum effect of Theorem (1) but also cannot avoid the classical effect by which codes with *poor* small-set expansion have low soundness, namely that large error patterns are examined by relatively few check terms, so the number of constraints they violate is relatively low. Together, this means that for *any* underlying graph, whether a good or a bad small set expander, the relative soundness is non-trivially bounded.

While in the classical case, the fact that poor expansion implies poor relative soundness, is very easy to argue, in the quantum case the proof turns out to be quite non-trivial, but still a similar phenomenon holds. Let us clarify what we’re trying to show. We want to show that if the expansion is bad, one can construct an error of large weight but which does not have large relative penalty. Suppose we would like to show that the soundness function $r(\delta)$ is small, for some range of proximity values $(0, \delta_0]$. Consider a set of qudits S whose fractional size is some $\delta \in (0, \delta_0]$, and which has positive expansion error $\varepsilon > 0$. A priori, if we have an error supported on S , then the maximal number of violations is at most $|S|D_L(1 - \varepsilon)$, by the assumption on the expansion. This might seem as though it proves the result trivially. The technical problem here, however, is that an error on S may just “seem” to be large, whereas possibly, may be represented much more succinctly modulo the centralizer group. This problem is, once again, inherently quantum - it corresponds, essentially, to showing that a given error has large weight even modulo to the *dual* code, namely the code spanned by the generators themselves. We would hence like to devise an error pattern, that cannot be down-sized significantly by operations in the centralizer group, but would still “sense” the non-expanding nature of S , and hence have fewer-than-optimal violations.

To this end we prove the Onion fact (Fact 7) which might be of interest of its own. It states that given an error on at most $k/2$ of the k qudits supporting a generator, its weight cannot be reduced modulo the centralizer within the k -neighborhood of the generator (the k neighborhood is, roughly, the qudits belonging to the set of terms of distance k from that generator in the interaction graph).

The “Onion” in the name is due to the fact that the proof (given in Subsection 5.3.3) works via some hybrid argument on the onion-like layers $\Gamma^{(i)}(u)$ surrounding the qudits of a generator u .

Our idea is to concentrate the error on a large set of far away generators whose k -neighborhoods are non-intersecting (we call those generators “islands”). We now argue as follows. If we draw a random error on the qudits belonging to these “islands”, with probability calibrated so that the expected number of errors per “island”, is, say, 1 error, the following will occur: on one hand, many islands have more than one error, so they “sense” the sub-optimality of expansion. On the other hand, only a meager fraction, exponentially small in k , of the “islands” with at least two errors, will have more than $k/2$ errors; only those, by the Onion fact (fact 7) can be potentially reduced modulo the centralizer. Hence with high probability, the weight of the random error, cannot be significantly reduced modulo the centralizer, yet it still has less-than-optimal number of violations due to the expansion.

1.4 Related work

Theorem 1 is related to our recent result [3] in which it was shown that when a quantum local Hamiltonian, whose terms mutually commute, is set on a good small-set expander, then the approximation of its ground energy lies in NP. In that result, the better the small-set expansion, the better the approximation. In other words, as the expansion improves, the problem becomes less interesting from the quantum point of view. Another result of the same spirit was derived by Brandao and Harrow [17] for non-commuting 2-local Hamiltonians on standard expanders. In both results good expansion poses a limitation on the expressiveness of quantum constraint systems. We note that the starting point of both the proof of our Theorem 1 and the result of [3] are Facts 1 and 2 regarding the percentage of unique neighbors in good small set expanders; however, the proofs proceed from that point onwards in very different directions.

Dinur and Kaufman [26] showed that classical LTC codes *must* be set on a good small-set expander. More precisely, given a code with soundness $R(\delta) = \rho \cdot \delta$ for all $\delta > \delta_0$ for some constant δ_0 , the edge expansion of the underlying graph is at least $c\rho$, for some constant c . This might seem to provide another classical contrast to our Theorem 1, in addition to our Claim 5. However, [26] does not use bi-partite graph expansion but rather the graph in which an edge connects any two nodes that participate in a common constraint; the two notions of expansion are very different and hence direct comparison to the [26] result is not possible.

1.5 Discussion and Further directions

Many open questions arise regarding qLTCs. Can we find other qLTCs with much better parameters than those mentioned in this article? It is a natural starting point to check known quantum codes that have good self-correcting properties, or high energy barrier [35, 44]. Do qLTCs exist with parameters which are as good as those of [24, 16], namely, constant distance, constant query complexity, constant soundness for all proximities larger than some constant $\delta_0 > 0$, and rate which is inverse polylogarithmic? If not, can we prove appropriate upper bounds on qLTCs?

The upper bounds we provided here point to an inherently quantum phenomenon, which constitutes an obstacle against local testability for qLTCs in the low-proximity range of parameters. Both of our main theorems, reflect, in fact, a deeper phenomenon called *monogamy of entanglement* which was identified also in [3] for commuting local Hamiltonians, and [17] for 2-local general Hamiltonians. Es-

entially, this phenomenon limits the amount of entanglement that a single qudit with $O(1)$ quantum levels can “handle”. In quantum codes, based on commuting check terms, the entanglement of code states arises from the fact that the operators actually do not commute per qubit, but only over sets of qubits. Incidentally, per-qubit non-commutativity is also the phenomenon responsible for the energy “penalty” received by certain (sparse) errors. Hence, in cases where monogamy of entanglement is a significant factor, for example in small-set expander geometry, we witness an inherent decline in the energy “penalty” of such errors, thus upper-bounding the quantum local testability. It is thus the combination of *monogamy of entanglement* in small-set expanders, and the poor local testability of non-expanders, that are responsible for the apparently quantum phenomenon. Whether Theorem 2 hints at a more profound limitation on quantum local testability, that holds also for larger values of δ , calls for further research. Perhaps refuting the c^3 open problem is doable in the quantum case?

Finally, the link between quantum local testability of proofs and qLTCs, so crucial in the classical world [30], is far from clear in the quantum setting. We have merely touched upon it (see the result of quantum PCPPs in the appendix), however, much further clarification of this connection, is called for.

Organization of paper In Section 2 we provide the necessary background on quantum error correcting codes and on small-set expanders. Section 3 provides definitions of quantum locally testable codes (qLTCs) and stabilizer qLTCs, and basic results. Section 4 provides bounds on the soundness of quantum LTCs on small-set expanders, and Section 5 provides an absolute bound on soundness of stabilizer LTCs regardless of the expansion of their underlying graph. Finally, In the Appendices we provide several proofs which are on the more technical side. In Appendix G we provide our definition of quantum PCPPs and the construction and proof of the induced qLTC.

2 Background

2.1 The Pauli groups

Definition 1 Pauli Group

The group Π^n is the n -fold tensor product of Pauli operators $A_1 \otimes A_2 \otimes \dots \otimes A_n$, where $A_i \in \{I, X, Y, Z\}$, along with multiplicative factors $\pm 1, \pm i$ with matrix multiplication as group operation.

The Pauli group can be generalized to particles of any dimensionality d :

Definition 2 The Pauli group generalized to F_d

Let $X_d^k : |i\rangle \mapsto |(i+k) \pmod d\rangle$, $P_d^\ell |j\rangle \mapsto w_d^{j\ell} |j\rangle$ be the generalized bit and phase flip operators on the d -dimensional Hilbert space, where $w_d = e^{2\pi i/d}$ is the primitive d -th root of unity. Let Π_d be the group generated by these operators and all roots of unity of order d . The group Π_d^n is the n -fold tensor product of Pauli operators $A_1 \otimes A_2 \otimes \dots \otimes A_n$, where $A_i \in \{X_d^k P_d^\ell\}$ along with these multiplicative factors.

The weight of a Pauli operator is defined to be the number of locations where it is non-identity.

2.2 General Quantum Error Correction

Definition 3 Quantum Code

A quantum code on n qudits is given by a set of (m) projections Π_i . The code is defined to be the simultaneous 0 eigenstates of all those projections.

Definition 4 Quantum Error detection 1[40]

Let $C \subseteq \mathcal{H}$ be a quantum code on n qudits. Let Π_C be the orthogonal projection onto C . We say that the set of errors \mathcal{E} is detectable by C if for any $E \in \mathcal{E}$, we have:

$$\Pi_C E \Pi_C = \gamma_E \Pi_C, \quad (1)$$

where γ_E is some constant which may depend on E .

Definition 5 Quantum Error detection 2[40]

A set \mathcal{E} is detectable by C , if for any $|\psi\rangle, |\phi\rangle \in C$ with $\langle\psi|\phi\rangle = 0$, and any $E \in \mathcal{E}$, $\langle\psi|E|\phi\rangle = 0$.

Claim 1 [40] Definitions (5) and (4) are equivalent:

The proof can be found in the Appendix. Definition (5) gives rise to the following natural definition:

Definition 6 Distance of a code[40]

Let C be a quantum code detecting error set $\mathcal{E} \subset \Pi_d^n$. C has distance $\text{dist}(C)$ if for any two orthogonal code states $|\phi\rangle, |\psi\rangle$, and any $E \in \mathcal{E}$ of weight at most $\text{dist}(C) - 1$, we have $\langle\phi|E|\psi\rangle = 0$.

2.3 Stabilizer Quantum Error Correcting Codes

Definition 7 Stabilizer Code

A stabilizer code C is defined by an Abelian subgroup $A = A(\mathcal{G}) \subset \Pi_d^n$, generated by a set $\mathcal{G} \subset \Pi_d^n$. The codespace is defined as the mutual 1-eigenspace of all elements in \mathcal{G} (we require that $-I \notin \mathcal{G}$ so that this codespace is not empty). An element $E \in \Pi_d^n$ is said to be an error if it does not commute with at least one element of \mathcal{G} , i.e. $E \notin \mathbf{Z}(\mathcal{G})$, where $\mathbf{Z}(\mathcal{G})$ is the centralizer of \mathcal{G} . An element $E \in \Pi_d^n$ is said to be a logical operation, if it commutes with all of \mathcal{G} , but is not generated by \mathcal{G} , i.e., $E \in \mathbf{Z}(\mathcal{G}) - A$. A stabilizer code is said to be k -local if each term $g \in \mathcal{G}$ is an element of Π_d^n , with weight exactly k .

To fit with the terminology of Definition 3, consider for each generator g the projection Π_g which projects on the orthogonal subspace to the 1 eigenspace of g .

Definition 8 Succinct representation

A k -local set of generators \mathcal{G} is said to be succinct, if there does not exist a different generating set \mathcal{G}' , such that $A(\mathcal{G}) = A(\mathcal{G}')$ and $\text{wt}(g) < k$ for some $g \in \mathcal{G}'$.

The following is a well known fact [31] which will be useful later on, and we prove it in appendix (D).

Lemma 1 Stabilizer Decomposition

Let C be a stabilizer code on n qudits, and consider the sets $EC = \{E|\phi\rangle, |\phi\rangle \in C\}$ with $E \in \Pi_d^n$. Then two sets $EC, E'C$ are either orthogonal or equal to each other, and $\{EC\}_{E \in \Pi_d^n}$ span the entire Hilbert space. Moreover, consider the partition of the entire Hilbert space to sets of states which are mutual eigenvectors of all generators of C with exactly the same set of eigenvalues for each generator. Then this partition is exactly the partition derived by the EC 's, and two orthogonal EC 's have two lists of eigenvalues which differ on at least one generator. In particular, any n qudit state $|\psi\rangle$ may be written as a sum of orthogonal vectors

$$|\psi\rangle = \sum_i E_i |\eta_i\rangle,$$

where $E_i \in \Pi_d^n$ and $|\eta_i\rangle \in C$.

Definition 9 Weight of an error in stabilizer codes

Let C be a stabilizer code on n d -dimensional qudits, with generating set $\mathcal{G} \subset \Pi_d^n$. For $E \in \Pi_d^n$, we denote:

1. The number of locations in which E is non-identity - by $\text{wt}(E)$.
2. The weight of E modulo the group $A(\mathcal{G})$ - by $\text{wt}_{\mathcal{G}}(E)$: $\text{wt}_{\mathcal{G}}(E) = \min_{f \in A(\mathcal{G})} \{\text{wt}(fE)\}$.
3. The weight of E modulo the centralizer $\mathbf{Z}(\mathcal{G})$ - by $\text{wt}_{\mathbf{Z}(\mathcal{G})}(E)$: $\text{wt}_{\mathbf{Z}(\mathcal{G})}(E) = \min_{z \in \mathbf{Z}(\mathcal{G})} \{\text{wt}(zE)\}$.

The above claims give rise to the following definition of distance in a stabilizer code:

Definition 10 Distance of a stabilizer code

Let C be a k -local stabilizer code on n d -dimensional qudits, with generating set $\mathcal{G} \subset \Pi_d^n$. The distance of C is defined as the minimal weight of any logical operation on C :

$$\text{dist}(C) = \min_{E \in \mathbf{Z}(\mathcal{G}) - A(\mathcal{G})} \text{wt}(E).$$

Claim 2 Equivalence of distance definitions A stabilizer code C has $\text{dist}(C) \geq \rho$ by definition 10, iff it has distance $\geq \rho$ by definition 6.

The proof is given in the appendix subsection (E). A code C on n qudits is said to have a constant relative distance $\delta > 0$, if its distance is at least δn . We will make use of the following assumption which we isolate so that we can refer to it later on:

Remark: If there is a qudit q such that all states in the code look like $|\alpha\rangle$ tensor with some state on the remaining qudits, for some fixed one-qudit state $|\alpha\rangle$ of that qudit q , we say that q is *trivial* for the code. We will assume in the remainder of the paper that for all codes we handle, no qudits are trivial for the code, since such qudits can be simply discarded.

2.4 Interaction graphs and their expansion

We assume in the rest of the paper that each qudit participates in exactly D_L constraints. We define bi-partite expanders, similar to [47], [20], who used them to construct locally-testable classical codes. Note that we require expansion to hold only for sets of constant size k .

Definition 11 Bi-Partite Interaction Graph

Let C be a quantum code on n d -dimensional qudits, whose check terms $\{\Pi_i\}_i$ are k -local. We define the bi-partite interaction graph of C $G = G(C) = (L, R; E)$ as follows: the nodes L correspond to the qudits, the nodes R correspond to the check terms, and the set of edges connect each constraint $\Pi_i \in R$ to all the qudits in L on which it acts non-trivially. We note that G is left D_L -regular, and right k -regular.

Definition 12 Bi-partite expansion

Let $G = (L, R; E)$ be a bi-partite graph, that is left D_L -regular, right k -regular. A subset of qudits $S \subseteq L$ is said to be ε -expanding, if $|\Gamma(S)| \geq |S|D_L(1 - \varepsilon)$, where $\Gamma(S)$ is the set of neighbors of S in this graph. ε is called the expansion error for this set. G is said to be ε -small-set-expanding, if every subset $S \subseteq L$, $|S| \leq k$ has expansion error at most ε .

We state two technical facts on good bi-partite expanders that will be useful later on. The proofs are in the appendix (B).

Fact 1 Consider $S \subseteq L$ in a bi-partite graph $G(L, R; E)$ and let S be ε -expanding, for $\varepsilon < \frac{1}{2}$. Then a fraction at most 2ε of all vertices of $\Gamma(S)$ have degree strictly larger than 1 in S .

Fact 2 Let $S \subseteq L$ in a bi-partite graph $G = (L, R; E)$, such that S is ε expanding, for $\varepsilon < \frac{1}{2}$. Then there exists a vertex $q \in S$, such that the fraction of neighbors of q with at least two neighbors in S is at most 2ε .

2.5 Notation

We denote as follows. d is the dimension of the qudits involved. For a bi-partite graph we denote $G = (L, R; E)$, L denotes the left set of vertices of size $|L| = n$ (corresponding to qudits), R denotes the right vertices $|R| = m$ (corresponding to constraints), and E is the set of edges between L and R . D_L will denote the left degree of a bi-partite graph. k will denote the locality of the constraints, namely the right degree of the graph. Given $S \subseteq R$ (or L) in a bi-partite graph, $\Gamma(S)$ denotes the neighbor set of S in L (or R). $\mathcal{N}(q)$ will denote the qudit-neighborhood of a qudit q in L , namely all the qudits participating in all the constraints acting on q (so, $\mathcal{N}_q = \Gamma^{(2)}(q)$). We will use ε to denote the expansion error for bi-partite graphs (as in Definition 12). We will use δ (and sometimes μ) to denote the proximity, namely, the relative distance of a word from a code.

3 Locally-testable quantum codes

In this section we define locally testable quantum codes, both in the general case, and in the specific case of stabilizer codes. We then show that our definitions coincide for stabilizer codes.

3.1 Local testability of general quantum codes

We first generalize definition (6), from a definition of distance of a code to a definition of distance from a code:

Definition 13 Distance from a quantum code

Let C be a quantum code detecting error set $\mathcal{E} \subset \Pi_d^n$. For any two orthogonal states $|\phi\rangle, |\psi\rangle \in \mathcal{H}$, we define the Hamming distance between them $\text{dist}_C(|\phi\rangle, |\psi\rangle)$ as the maximal integer ρ , such that for any $E \in \mathcal{E}$, with $\text{wt}(E) \leq \rho - 1$, we have $\langle \psi | E | \phi \rangle = 0$. Similarly, given a state $|\phi\rangle$ orthogonal to C , we say that the distance of $|\phi\rangle$ from C denoted by $\text{dist}(|\phi\rangle, C)$ is the minimum over all $|\psi\rangle \in C$ of $\text{dist}_C(|\phi\rangle, |\psi\rangle)$.

We note here that the distance of a state from the code in the above, can be much larger than the distance of the code. This, akin to the classical case, where locally-testable codes are required to identify words far from the code, even if they cannot be (uniquely) decoded, so that these codes can be used as proof systems.

Definition 14 Quantum Locally Testable Codes (qLTC)

Let $R = R(\delta)$ be some function $R(\delta) : [0, 1] \mapsto [0, 1]$, this is called the soundness function. Let C be a quantum code on n d -dimensional qudits, defined as the groundspace of $H = \sum_{i=1}^m \Pi_C^i$, where Π_C^i are m k -local projections for some constant k . We say that C is quantum locally testable with soundness $R(\delta)$, if:

$$\forall \delta > 0, |\Psi\rangle : \text{dist}(|\Psi\rangle, C) \geq \delta n \mapsto \frac{1}{m} \langle \Psi | H | \Psi \rangle \geq R(\delta).$$

The query complexity of the code is defined to be k .

3.2 Local testability of quantum stabilizer codes

We now show that local testability defined above (Definition 14) has a natural interpretation in the context of stabilizer codes.

Definition 15 Local Testability for Stabilizer Codes (sLTC)

Let $R(\delta)$ be some function $R(\delta) : [0, 1] \mapsto [0, 1]$. We say that a stabilizer code C on n d -dimensional qudits is an sLTC with query complexity k and soundness $R(\delta)$, if there exists a generating set \mathcal{G} for C , where each element has support k , such that the following holds: for any $E \in \Pi_d^n$ with $\text{wt}_{\mathbf{Z}(\mathcal{G})}(E) \geq \delta n$, a uniformly random generator $g \in \mathcal{G}$ does not commute with E w.p. at least $R(\delta)$.

3.2.1 Equivalence of definitions of locally testable codes

We now show that the definition of stabilizer locally testable codes (Definition 15) is in fact a special case of the general quantum locally testable codes (Definition 14).

Claim 3

1. If C is a Stabilizer code with generating set \mathcal{G} , which is an sLTC with query complexity k , and soundness $R(\delta)$, then the set of projections $\{\Pi_g\}_{g \in \mathcal{G}}$, where $I - \Pi_g$ is the projection on the 1-eigenspace of g , defines a qLTC with query complexity k , and soundness $R(\delta)$.
2. If C is a qLTC with query complexity k , and soundness $R(\delta)$, defined by a set of projections $\{\Pi_g\}_{g \in \mathcal{G}}$, such that the set $\{I - \Pi_g\}_{g \in \mathcal{G}}$ spans an Abelian subgroup of Π_d^n , then C is also an sLTC with query complexity k , and soundness $R(\delta)$.

Proof: sLTC \mapsto qLTC

By definition of a stabilizer code, for any $|\phi\rangle \in C$, we have $g|\phi\rangle = |\phi\rangle$ for all $g \in \mathcal{G}$, so $\Pi_g|\phi\rangle = 0$ for all $g \in \mathcal{G}$. Next, consider a state $|\phi\rangle$ orthogonal to C , such that $\text{dist}(|\phi\rangle, C) \geq \delta n$. We would now like to show that a projection chosen randomly from $\{\Pi_g\}_{g \in \mathcal{G}}$ is violated by $|\phi\rangle$ with probability at least $R(\delta)$. Consider the following orthogonal decomposition of ϕ as implied by lemma (1):

$$|\phi\rangle = \sum_i \alpha_i |\alpha_i\rangle = \sum_i \alpha_i E_i |\eta_i\rangle, \quad (2)$$

where $E_i \in \Pi_d^n$, $|\eta_i\rangle \in C$, and $E_i |\eta_i\rangle$ are orthogonal. We claim that for each i , $\text{wt}_{\mathbf{Z}(\mathcal{G})}(E_i) \geq \delta n$: otherwise, it is easy to see that there exists some $E' \in \Pi_d^n$, $\text{wt}(E') < \delta n$, such that for at least one i , we have $E' E_i \in \mathbf{Z}(\mathcal{G})$. Since for any $J \in \mathbf{Z}(\mathcal{G})$, $JC = C$, we have that alternatively, $E' |\alpha_i\rangle \in C$. Since E' is unitary, and the $|\alpha_i\rangle$'s are orthogonal, then the $E' |\alpha_i\rangle$'s are orthogonal, thus $E' |\phi\rangle$ has a non-zero projection on C . Contrary to the assumption that $\text{dist}(|\phi\rangle, C) \geq \delta n$.

If E_i and $g \in \mathcal{G}$ do not commute, $E_i g = \omega g E_i$, for some $\omega \neq 1$. In particular, $E_i |\eta_i\rangle$ is a ω eigenstate of g . This means it is orthogonal to the 1-eigenspace of g , and therefore:

$$\langle \alpha_i | \Pi_g | \alpha_i \rangle = 1.$$

Yet, by the sLTC property of C , for each i , E_i does not commute with a fraction at least $R(\delta)$ of the generators of \mathcal{G} . Thus, a randomly chosen check term is violated by $|\alpha_i\rangle$ with probability at least $R(\delta)$, so

$$\frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} \langle \alpha_i | \Pi_g | \alpha_i \rangle \geq R(\delta).$$

Since by lemma (1) the decomposition above coincides with the simultaneous eigenbasis of \mathcal{G} , we have:

$$\frac{1}{|\mathcal{G}|} \langle \phi | \sum_{g \in \mathcal{G}} \Pi_g | \phi \rangle = \frac{1}{|\mathcal{G}|} \sum_i \sum_{g \in \mathcal{G}} |\alpha_i|^2 \langle \alpha_i | \Pi_g | \alpha_i \rangle \geq R(\delta).$$

qLTC \mapsto sLTC

First, by definition, the set of states that are in the mutual groundspace of the Π_g 's, are stabilized (i.e. eigenvalue 1) w.r.t. the terms \mathcal{G} , and vice versa. Now, let $E \in \Pi_d^n$, whose weight modulo $\mathbf{Z}(\mathcal{G})$ is at least δn . Let $|\phi\rangle \in C$ be any code state, and denote $|\psi\rangle = E|\phi\rangle$. We claim that $\text{dist}(|\psi\rangle, C) \geq \delta n$. Otherwise there exists $E' \in \Pi^n$, $\text{wt}(E') < \delta n$, such that $E'|\psi\rangle$ has a non-zero projection on C , hence $E'E|\phi\rangle$ has a nonzero projection on C , so by lemma (1), we have that $E'EC = C$. Therefore, $E'E$ commutes with all \mathcal{G} , and hence $E'E \in \mathbf{Z}(\mathcal{G})$, which implies that $\text{wt}_{\mathbf{Z}(\mathcal{G})}(E) < \delta n$, in contradiction. By the qLTC property of C , we have

$$\langle \psi | \sum_{g \in \mathcal{G}} \Pi_g | \psi \rangle \geq |\mathcal{G}| \cdot R(\delta). \quad (3)$$

Since $|\psi\rangle = E|\phi\rangle$, then for any generator g $g|\psi\rangle = gE|\phi\rangle = \omega E g|\phi\rangle = \omega E|\phi\rangle$, for some $\omega \in \mathbf{C}$. So for any $g \in \mathcal{G}$ $|\psi\rangle$ is some eigenstate of g . Hence $|\psi\rangle$ is either in the 1-eigenspace of Π_g or in its 0-eigenspace, so by equation (3) it violates a fraction at least $R(\delta)$ of all generators \mathcal{G} . ■

4 Bound on the soundness of stabilizer LTCs on small-set expanders

In this section we prove theorem 1. We define the *relative soundness* formally:

Definition 16 Relative Soundness Define

$$r(\delta) : [0, 1] \mapsto [0, 1],$$

as follows: $r(\delta) = R(\delta)/\Theta(\delta)$, where $\Theta(\delta) \equiv \min\{\delta k, 1\}$.

We note that in the all the following, we will be interested in $\delta < 1/k$ and in this range $r(\delta) = R(\delta)/k\delta$.

4.1 A useful fact about restrictions of stabilizers

Definition 17 Restriction of stabilizers

For a $E \in \Pi_d^n$, let $E|_q$ denote the q -th component of the tensor product E , and let $E|_{-q}$ denote the tensor product of all terms except the q -th. Similarly, for a generating set \mathcal{G} , we denote by $\mathcal{G}|_q$ as the set $\{g|_q, g \in \mathcal{G}\}$, and similarly for $\mathcal{G}|_{-q}$.

We now prove a useful fact: that the restrictions to a given qudit q of all the generators of a stabilizer code with absolute distance strictly larger than 1 cannot all commute.

Fact 3 Let C be a stabilizer code with absolute minimal distance strictly larger than 1. Then for any qudit q , and any generator g acting on q , there exists another generator $h(q)$ acting on q such that $[g|_q, h|_q] \neq 0$.

Proof: Assume on the negative, that there is a qudit q , and a generator g , such that for all other generators h , we have $[g|_q, h|_q] = 0$. Let $Q = g|_q$. We have that $Q' = Q \otimes I_{-q}$, namely the tensor product with identity on the other qubits, commutes with all $g \in \mathcal{G}$, and thus $Q' \in \mathbf{Z}(\mathcal{G})$. However, Q' cannot be inside $A(\mathcal{G})$, since otherwise q is in some constant state (the 1 eigenvector of Q) $|\alpha\rangle$ for all code states, and thus q is trivial for the code (see remark at the end of Subsection 2.3). Hence, $Q' \in \mathbf{Z}(\mathcal{G}) - A(\mathcal{G})$, so the distance of the code by definition (10) is 1, in contradiction to our assumption. ■

4.2 Proof of Theorem 1

In the proof we will make use of "sparse" sets of constraints, defined as follows.

Definition 18 1-independent set of constraints

For a given constraint u , consider $\Gamma^3(u)$, the set of qudits acted upon by constraints which act on qudits in u . A set of constraints U is said to be 1-independent if for any two constraints $u, w \in U$, $\Gamma^3(u) \cap \Gamma^3(w) = \emptyset$.

Proof: (Of theorem 1)

Generating the error We want to construct an error $E \in \Pi_d^n$, $wt_{\mathbf{Z}(\mathcal{G})}(E) \geq \delta n$, that will not violate too many constraints in \mathcal{G} . Let C be a stabilizer code with a k -local generating set \mathcal{G} , such that the bi-partite interaction graph of C is an ε small-set bi-partite expander. Let U be a 1-independent set of constraints of size δn . We note that since $\delta \leq \frac{1}{k^3 D_L}$ a 1-independent set of this size must exist, by a simple greedy algorithm. For a given constraint $u \in U$, and $i \in [k]$, let $\alpha_i(u)$ denote the number of generators $g \in \mathcal{G}$ that act on a qudit i in u and intersect u in at least one other qudit. Then for each $u \in U$ we define $q(u)$ to be a qudit of minimal $\alpha_i(u)$ over all $i \in [k]$. Let $T = \{q(u) | u \in U\}$. Let us define an error pattern:

$$E = \bigotimes_{u \in U} u|_{q(u)}.$$

We first note that $E \notin \mathbf{Z}(\mathcal{G})$; This is true by Fact (3): for each qudit q in the support of E , $E|_q$ does not commute with $h|_q$ for some $h \in \mathcal{G}$. But since T is induced by a 1-independent set, h does not touch any other qudit in the support of E except q , so this implies $[h, E] = [h|_q, E|_q] \neq 0$. We will now show that E has large weight modulo $\mathbf{Z}(\mathcal{G})$, but is penalized by a relatively small fraction of \mathcal{G} .

Weight Analysis By definition, we have that $wt(E) = |T| = |U| = \delta n$. We claim that:

$$wt_{\mathbf{Z}(\mathcal{G})}(E) = |T| \tag{4}$$

Since δ was chosen to be smaller than half the distance of the code C , $wt_{\mathbf{Z}(\mathcal{G})}(E) = wt_{\mathcal{G}}(E)$ and so it suffices to lower-bound $wt_{\mathcal{G}}(E)$.

Suppose on the negative that $wt_{\mathcal{G}}(E) < |T|$. Then there exists $\Delta \in A(\mathcal{G})$, such that $E' = \Delta E$ has $wt(E') < |T|$. Since the weight of E' is strictly smaller than that of E , there must be one qudit q_0 in T , s.t. on the neighborhood $\mathcal{N}(q_0)$ the weight of E' is strictly smaller than that of E , which is 1; namely, E' must be equal to the identity on all the qudits in the qudit-neighborhood of q_0 . Here, we have used the fact that the qudit-neighborhoods of different qudits in T are non-intersecting. This is true by the fact that the qudits were chosen by picking one qudit from each constraint out of a 1-independent set of constraints (definition 18). This means that Δ must be equal to the inverse of

E on this neighborhood. But this inverse is exactly the following: It is equal to $E|_{q_0}^{-1}$ on q_0 , and to the identity on all other qudits in the neighborhood. By construction, $E|_{q_0}$ on q_0 , (and therefore also $E^{-1}|_{q_0} = \Delta_{q_0}$) does not commute with $h|_{q_0}$, for some $h \in \mathcal{G}$. Since Δ is identity on all qudits of h other than q_0 , this implies that Δ does not commute with h , in contradiction to the fact that $\Delta \in A(\mathcal{G})$.

soundness Analysis We upper-bound the number of generators that do not commute with E . For each $u \in U$, the number of generators $g \in \mathcal{G}$ that do not commute with $E|_{q(u)}$ is at most the number of generators that share at least two qudits with u . By fact (2) there exists a qudit $q \in \Gamma(u)$ such that the fraction of its check terms with at least two qudits in $\Gamma(u)$ is at most 2ε ; since we chose $q(u)$ to be the qudit that minimizes that fraction over all qudits on which u acts, we have that for $q(u)$, the fraction of terms acting on it that intersect u with at least 2 qudits is at most 2ε . Thus, the absolute number of generators acting on $q(u)$ that intersect u in at least two qudits is at most $2\varepsilon D_L$. Hence the overall number of generators violated by E is at most $2\varepsilon |T| D_L$. By Equation 4 this is equal to $2\varepsilon D_L \text{wt}_{\mathbf{Z}(\mathcal{G})}(E)$. Using $D_L n = mk$, we have $R(\delta) \leq 2\varepsilon k \delta$ and so $r(\delta) \leq 2\varepsilon$. ■

We now show that a slightly stronger version of the above theorem holds. This version will be used for showing Theorem (2).

Claim 4 *Let C be a good stabilizer code, with a k -local succinct generating set, where each qubit is examined by D_L constraints. If there exists a 1-independent set of constraints $U \subseteq R$, s.t. $|U| = \delta n$ for some $0 < \delta < 1/k$, and $\Gamma(U)$, the set of qudits that the constraints in U act on satisfies $|\Gamma(U)| \geq |\Gamma(U)| D_L (1 - \varepsilon)$, then for any $\delta' \leq \delta$ we have that $r(\delta') \leq 2\varepsilon$.*

Proof: For a set $S \subseteq L$, let $\Gamma_1(S)$ denote the number of neighbors of S having a single neighbor in S , and let $\Gamma_{\geq 2}(S) \equiv \Gamma(S) - \Gamma_1(S)$. Put $S = \Gamma(U)$, and let $S = \bigsqcup_{i=1}^k S_i$, denote a partition of S into k disjoint sets, where each S_i takes a single (arbitrary) qubit from each $\Gamma(u)$, $u \in U$. By assumption, $|\Gamma(S)| \geq |S| D_L (1 - \varepsilon)$, whereas the total degree of S is $|S| D_L$. Hence, $|\Gamma_{\geq 2}(S)| \leq |S| D_L \varepsilon$, so $|\Gamma_1(S)| \geq |S| D_L (1 - 2\varepsilon)$. Since each unique neighbor of S examines exactly one partition S_j , there exists a partition S_0 examined by at least $|S_0| D_L (1 - 2\varepsilon) = \delta n D_L (1 - 2\varepsilon)$, constraints from $\Gamma_1(S)$.

Now, given any $\delta' \leq \delta$, let S'_0 be a subset of S_0 of size $\delta' n$, maximizing the ratio $|\Gamma_1(S'_0)|/|S'_0|$, over all sets $S' \subseteq S_0$ of this size. Since each element of $\Gamma_1(S)$ examines just one element of S , such a set exists, with ratio at least $D_L (1 - 2\varepsilon)$. A tensor-product error \mathcal{E} defined by taking, for each $u \in U$ the restriction to its qubit in S'_0 , we have by equation (4) $\text{wt}_{\mathbf{Z}(\mathcal{G})}(E) = \delta' n$, whereas the maximal penalty is at most $2\varepsilon D_L \delta' n$. Since $\delta' \leq \delta < 1/k$ it follows that $r(\delta') \leq 2\varepsilon$. ■

5 An upper-bound on soundness

We now show an absolute constant strictly less than 1, upper-bounding the relative soundness of any good quantum stabilizer code spanned by k -local generators, whose qudits are acted upon by D_L stabilizers each. We start with an easy alphabet based upper bound.

5.1 Alphabet-based bound on soundness

In attempting to understand soundness of good stabilizer codes, one must first account for limitations on the soundness that seem almost trivial, and occur even when there is just a single error.

Definition 19 Single error soundness

Let $t(d) = 1/(d^2 - 1)$; The single error relative soundness in dimension d is defined to be $\alpha(d) = 1 - t(d)$.

The motivation for the above definition is as follows. For any qudit q , there always exists $Q \in \Pi_d$, $Q \neq I$, such that a fraction at least $t(d)$ of the generators touching q are equal to Q when restricted to q . If we consider a single-qudit error on q to be equal to Q , then it would commute with $t(d)$ of the generators acting on q ; thus they can violate at most $\alpha(d)$ of the constraints acting on q . Hence, one can expect that it is possible to construct an error of linear weight, whose relative soundness $r(\delta)$ is bounded by the single error relative soundness using qudits whose neighboring constraints are far from each other.

Indeed, we show:

Fact 4 Alphabet bound on soundness

For any good stabilizer code C on n d -dimensional qudits, with a k -local succinct generating set \mathcal{G} , whose left-degree is D_L , we have $r(\delta) \leq \alpha(d)$, for any $\delta \leq 1/(k^3 D_L)$.

Proof: Similarly to Theorem (1), given the parameters assumed in the statement of the fact, there exists a 1-independent set of constraints U of size δn . For each constraint $u \in U$ we select arbitrarily some qubit $q = q(u) \in \Gamma(u)$ and examine the restrictions to q of all stabilizers acting non-trivially on q . Let $P(q)$ denote the set of all such restrictions. Let $MAJ(q)$ denote the element of Π_d that appears a maximal number of times in $P(q)$. We then set $E = \bigotimes_{u \in U} MAJ(q(u))$. We first realize that E is an error: we want to show that there exists a generator g such that E and g do not commute. Otherwise, E commutes with all generators; Since by construction, each generator intersects E with at most one qudit, this means that the restrictions to q also commute: $[E|_q, g|_q] = 0$ for all $q(u)$ acted upon by E . This is a contradiction by Fact (3); hence, there must be a generator which does not commute with E , so E is indeed an error. Similarly to the proof of Equation (4) in the proof of Theorem (1), we also have $wt_{\mathbf{Z}(\mathcal{G})}(E) = \delta n$. Furthermore, for each qudit q , the fraction of generators on q , whose restriction to q does not commute with $E|_q$ is at most $\alpha(d)$, since the number of appearances of $E|_q = MAJ(q)$ in $P(q)$ is at least $t(d) = 1 - \alpha(d)$. Hence the number of violated constraints is at most $\alpha(d) \cdot |U| \cdot D_L = \alpha(d)\delta n D_L$. Since $\delta < 1/k$ it follows that $r(\delta) \leq \alpha(d)$. ■

We note that classically, there is no direct analogue to the requirement of non-commutativity to achieve constraint violation. No analogue of the $\alpha(d)$ thus exists.

5.2 Separation from alphabet-based soundness

In this section we show that the alphabet-based bound on the relative soundness in fact cannot be achieved, and the relative soundness is further bounded by a constant factor strictly less than 1, which is due to what seems to be an inherently quantum phenomenon. We will use the geometry of the underlying interaction graph to achieve this separation, by treating differently expanding instances and non-expanding instances. Before stating the main theorem of this section, we require a generalization of definition 18 and a simple fact.

Definition 20 t -independent set of constraints Let C be a quantum code with a set of k -local constraints, whose underlying bi-partite graph is $G(C) = (L, R; E)$. A set of constraints $U \subseteq R$ is said to be t -independent if for any $a, b \in U$ we have $\Gamma^{(2t+1)}(u) \cap \Gamma^{(2t+1)}(v) = \Phi$.

The following fact can be easily derived by a greedy algorithm:

Fact 5 Let $\eta = \eta(k, D_L) = k^{-(2k+1)} D_L^{-(2k-1)}$. For any quantum code C whose bi-partite graph $G(C)$ is left D_L -regular, and right k -regular, there exists a k -independent set of size at least ηn .

Proof: Pick a constraint u , remove all constraints in $\Gamma^{(4k)}(u)$, and repeat. The number of constraints we have removed for each constraint is $(kD_L)^{2k}$. Hence, we can proceed for $m/(kD_L)^{2k}$ steps. We get that the fraction of constraints is at least $k^{-(2k)} D_L^{-(2k)}$, and since $mk = nD_L$, we get the desired result. ■

Theorem (2) Let C be a stabilizer code on n d -dimensional qudits, of minimal distance at least k , and a k -local ($k \geq 4$) succinct generating set $\mathcal{G} \subset \Pi_d^n$, where the right degree of the interaction graph of \mathcal{G} is D_L . Then there exists a function $\gamma_{gap} = \gamma_{gap}(k) > \min\{10^{-3}, 0.01/k\}$ such that for any $\delta \leq \min\{\text{dist}(C)/2n, \eta/10\}$, (for η as defined in Fact 5) we have $r(\delta') \leq \alpha(d)(1 - \gamma_{gap})$. where $\delta' \in (0.99\delta, 1.01\delta)$.

The proof of the theorem will use, on one hand, claim (4) which upper-bounds the soundness of expanding instances, and on the other hand a lemma on non-expanding instances, which tries to "mimic" the behavior of the classical setting, in which non-expanding topologies suffer from poor soundness. We now state this lemma:

Lemma 2 Let C be a stabilizer code on n qudits of dimension d , with minimal distance at least k and a k -local ($k \geq 4$) succinct generating set \mathcal{G} , where the left degree of the interaction graph of \mathcal{G} is D_L . Let $\gamma_{gap} = \gamma_{gap}(k) = \min\{10^{-3}, 0.01/k\}$. If there exists a k -independent set U of size $|U| = \delta n$, with $\delta < \text{dist}(C)/2n$, such that the bi-partite expansion error of $\Gamma(U)$ is at least $\varepsilon = 0.32$, i.e. $|\Gamma(\Gamma(U))| = |\Gamma(U)|D_L(1 - \varepsilon')$ for some $\varepsilon' \geq 0.32$ then

$$r(\delta') \leq \alpha(d) \cdot (1 - \gamma_{gap}),$$

for some $\delta' \in (0.099\delta, 0.101\delta)$.

The proof of this Lemma is technically non-trivial, and we defer it to a separate section. From this lemma, it is easy to show theorem (2):

Proof: (of theorem 2) The parameters of the theorem allow us to apply directly fact (5); hence there exists a k -independent set S of size at least ηn , for η as defined in Fact (5). Since $\delta \leq \eta/10$ there exists a k -independent set S of size 10δ . Now, either:

1. S has expansion error at least 0.32. By lemma (2), we have

$$r(\mu) < \alpha(d)(1 - \gamma_{gap}),$$

for some $\mu \in (0.099 \cdot (10\delta), 0.101 \cdot (10\delta)) = (0.99\delta, 1.01\delta)$, and $\gamma_{gap}(k)$ from lemma (2), which is at least $\min\{10^{-3}, 0.01/k\}$.

2. The set S is ε -expanding for $\varepsilon < 0.32$. In which case, since S is in particular R -independent, then by claim (4), the soundness $r(\delta') \leq 2\varepsilon < 2/3 - 0.01 \leq \alpha(d) - 0.01$, for all $\delta' \leq |S|/n$. In particular $r(\mu) < \alpha(d)(1 - 0.01/k)$.

Taking the higher of these two bounds we get the desired upper-bound for $r(\mu)$. ■

5.3 Proof of Lemma (2)

In the following we first define the error; We provide the proof that the expected penalty of this error is small in fact (6), then state and prove the Onion fact in sub-subsection 5.3.3 and use it to prove Fact (8), in which we show that the error has large weight modulo the group. Finally we combine all the above to finish the proof of the lemma.

5.3.1 Constructing the error

Let $U \subseteq R$ be a k -independent set as promised by the conditions of the lemma. Then $|U| = \delta n$, and denoting $S = \Gamma(U)$, we have that $|S| = \delta n k$. Therefore, $|\Gamma(S)| = |S| D_L (1 - \varepsilon')$, for some $\varepsilon' \geq 0.32$. Let \mathcal{E} be the following random error process: for each qudit of S independently, we apply I w.p. $1 - p$ for $p = 1/(10k)$, and one of the other elements of Π_d with equal probability $p \cdot t(d)$, where t is defined in Definition (19).

$$\mathcal{E} = \bigotimes_{i \in S} \mathcal{E}_i, \text{ where } \mathcal{E}_i = \begin{cases} I_i & \text{w.p. } 1 - 1/(10k) \\ X_d^k P_d^l & \text{w.p. } t/(10k) \end{cases}$$

We note here that the choice of p is such that on average, each k -tuple has only a small number of errors; the expectation of the number of errors is an absolute constant $1/10$ (not a fraction of k). This will help, later on, to lower-bound the weight of the error modulo the group.

5.3.2 Analyzing Penalty

We first claim, that on average, \mathcal{E} has a relatively small penalty w.r.t. \mathcal{G} , using the fact that the expansion error is at least 0.32 as in the condition of Lemma 2. For any \mathcal{E} , let $\text{penalty}(\mathcal{E})$ denote the number of generators of \mathcal{G} that do not commute with \mathcal{E} .

Fact 6

$$\mathbf{E}_{\mathcal{E}} [\text{Penalty}(\mathcal{E})] \leq p \alpha |S| D_L (1 - 0.02/k)$$

Proof: Let $G = (L, R; E)$ denote the bi-partite graph corresponding to \mathcal{G} , with R being the generators of \mathcal{G} and L the qudits. Let $S = \Gamma(U)$ be as before. Let the error process \mathcal{E} be the one defined above. For any constraint $c \in \Gamma(S)$ which is violated when applied to this error, observe that there must be a qudit $i \in \text{supp}(c)$ such that $[c|_i, \mathcal{E}_i] \neq 0$. We now would like to bound the number of constraints violated by \mathcal{E} using this observation, and linearity of expectation.

For an edge $e \in E$ connecting a qudit i in S and a constraint c in $\Gamma(S)$, let $x(e)$ denote the binary variable which is 1, iff the error term \mathcal{E}_i on does not commute with $c|_i$. In other words, an edge marked by 1 is an edge whose qudit causes its constraint to be violated. By construction, for each $e \in E$ which connects the qudit i and the constraint c we have

$$\mathbf{E}_{\mathcal{E}} [x(e)] = p(1 - t). \tag{5}$$

This is true since a constraint c restricted to the qudit i , $c|_i$ does not commute with the error restricted to the same qudit i , \mathcal{E}_i , iff both \mathcal{E}_i is non-identity (which happens with probability p) and is not equal to $c|_i$.

If we had just added now $x(e)$ over all edges going out of S (whose number is $|S|D_L$), then by linearity of expectation, this would have given an upper bound on the expected number of violated constraint equal to

$$\sum_e p(1-t) = p|S|D_L\alpha(d). \quad (6)$$

Unfortunately this upper bound does not suffice; to strengthen it we would now like to take advantage of the fact that many of those edges go to the same constraint, due to the fact that the expansion is bad; thus, instead of simply summing these expectation values, we take advantage of the fact that two qudits touching the same constraint cannot contribute twice to its violation. Observe that it may even be the case that some edges may cause constraints to become "unviolated", so the actual bound may be even lower.

Let $E_{inj} \subseteq E$ be a subset of the edges between S to $\Gamma(S)$ chosen by picking a single edge for each constraint in $\Gamma(S)$. For an edge $e \in E$ let $c(e)$ denote the constraint incident on e , and let $e_{inj}(c(e))$ denote the edge in E_{inj} that is connected to $c(e)$.

We now bound the expectation by subtracting $x(e)$ from the sum, if the Boolean variable $x(e_{inj}(c(e)))$ is 1; this avoids counting the violation of the same constraint twice due to the two edges. We have:

$$\mathbf{E}_{\mathcal{E}} [Penalty] \leq \mathbf{E}_{\mathcal{E}} \left[\sum_{e \in E_{inj}} x(e) + \sum_{e \notin E_{inj}} (1 - x(e_{inj}(c(e)))) \cdot x(e) \right].$$

Expanding the above by linearity of expectation:

$$\begin{aligned} \mathbf{E} [Penalty] &\leq \sum_{e \in E_{inj}} \mathbf{E}_{\mathcal{E}} [x(e)] + \sum_{e \notin E_{inj}} \mathbf{E}_{\mathcal{E}} [x(e)] - \sum_{e \notin E_{inj}} \mathbf{E}_{\mathcal{E}} [x(e_{inj}(c(e))) \cdot x(e)] = \\ &\sum_{e \in E} \mathbf{E}_{\mathcal{E}} [x(e)] + \sum_{e \notin E_{inj}} \mathbf{E}_{\mathcal{E}} [x(e_{inj}(c(e))) \cdot x(e)]. \end{aligned}$$

We have already calculated the first term in the sum in Equation 6; We now lower bound the correction given by the second term. We use the fact that for any $e \notin E_{inj}$

$$\mathbf{E}_{\mathcal{E}} [x(e_{inj}(c(e)))x(e)] = \mathbf{E}_{\mathcal{E}} [x(e_{inj}(c(e)))]\mathbf{E}_{\mathcal{E}} [x(e)]$$

since \mathcal{E} is independent between different qudits. We can thus substitute Equation 5, and get:

$$\mathbf{E}_{\mathcal{E}} [Penalty] \leq p\alpha|S|D_L - |S|D_L\varepsilon(p\alpha)^2.$$

where we have used the fact that $|E \setminus E_{inj}| = |S|D_L\varepsilon$. This is equal to

$$p\alpha|S|D_L(1 - p\alpha\varepsilon).$$

Using $p = 1/(10k)$, $\varepsilon \geq 0.32$, $\alpha(d) \geq 2/3$, we get the desired bound. ■

5.3.3 The Onion fact (7)

Fact 7 Onion fact

Let C be a stabilizer code on n qudits with a succinct generating set \mathcal{G} of locality k , such that $\text{dist}(C) \geq k$. Let $E \in \Pi_d^n$ s.t. $\text{supp}(E) \subseteq \Gamma(u)$ for some generator $u \in \mathcal{G}$. Finally let $\Delta \in A(\mathcal{G})$, and let $E_{\mathcal{G}} = \Delta \cdot E$. Then, for any $i \in [k]$, if $\text{wt}(E|_{\Gamma(u)}) = i$, then $\text{wt}(E_{\mathcal{G}}|_{\Gamma(2k+1)(u)}) \geq \min\{i, k - i\}$.

Proof: If $\Delta|_{\Gamma(u)} = I$ then

$$\text{wt}(E_{\mathcal{G}}|_{\Gamma(2k+1)(u)}) \geq \text{wt}(E_{\mathcal{G}}|_{\Gamma(u)}) = \text{wt}(E|_{\Gamma(u)}) = i, \quad (7)$$

so in this case we are done.

Otherwise, $\Delta|_{\Gamma(u)}$ is non-identity, and so has at least one non-identity coordinate. Since Δ is non-identity, by the assumption on the succinctness of \mathcal{G} we have $\text{wt}(\Delta) \geq k$.

Moreover, we claim that $\text{wt}(\Delta|_{\Gamma(2k+1)(u)}) \geq k$. Otherwise, consider the following process. Start with the generator u , and consider the qudits in $\Gamma(u)$. Now add the qudits in $\Gamma^{(3)}(u)$ (namely the qudits that are acted upon by generators intersecting u). Then add the next level, and so on for k levels, by which point we have added all qudits belonging to $\Gamma^{(2k+1)}(u)$. By the pigeonhole principle, if $\text{wt}(\Delta|_{\Gamma(2k+1)(u)}) < k$, then there must exist a level t , $1 \leq t \leq k$, such that Δ has zero support on qudits added in this level.

We now claim that $\tilde{\Delta} = \Delta|_{\Gamma^{(2(t-1)+1)}(u)}$, is in the centralizer $\mathbf{Z}(\mathcal{G})$ but its weight is less than k . This, together with the fact that $\tilde{\Delta} \notin A(\mathcal{G})$, shown in the next paragraph, contradicts the assumption that $\text{dist}(C) \geq k$. To see that $\tilde{\Delta}$ is in the centralizer, we observe first that Δ commutes with all elements of \mathcal{G} that act only on qudits in $\Gamma^{(t-1)}(u)$, and since $\tilde{\Delta}$ agrees with Δ on $\Gamma^{(2(t-1)+1)}(u)$, $\tilde{\Delta}$ also commutes with them. We also observe that $\tilde{\Delta}$ trivially commutes with all elements in \mathcal{G} whose support does not intersect $\Gamma^{(2(t-1)+1)}(u)$. Hence we only need to worry about those terms that act on at least one qudit in $\Gamma^{(2t+1)}(u) - \Gamma^{(2(t-1)+1)}(u)$ and at least one qudit in $\Gamma^{(2(t-1)+1)}(u)$. Let v be some such term. Note that v does not act on any qudit outside $\Gamma^{(2t+1)}(u)$ by definition. We know that Δ commutes with v . But by the choice of t , we know that Δ is trivial on those qudits added at the t -th level, and hence Δ restricted to $\Gamma^{(2t+1)}(u)$ (which contains the qudits of v) is the same as Δ restricted to $\Gamma^{(2(t-1)+1)}(u)$. And so Δ restricted to $\Gamma^{(2(t-1)+1)}(u)$ commutes with v .

We showed that $\tilde{\Delta}$ is in $\mathbf{Z}(\mathcal{G})$. If it also belongs to $A(\mathcal{G})$, this contradicts succinctness of \mathcal{G} ; otherwise it is in $\mathbf{Z}(\mathcal{G}) - A(\mathcal{G})$ implying the distance of C is at most $k - 1$, contrary to assumption. This means that $\text{wt}(\Delta|_{\Gamma(2k+1)(u)}) \geq k$. Therefore, we now know by the triangle inequality on the Hamming distance, that

$$\text{wt}(E_{\mathcal{G}}|_{\Gamma(2k+1)(u)}) \geq \text{wt}(\Delta|_{\Gamma(2k+1)(u)}) - \text{wt}(E|_{\Gamma(2k+1)(u)}) = \quad (8)$$

$$\text{wt}(\Delta|_{\Gamma(2k+1)(u)}) - \text{wt}(E|_{\Gamma(u)}) \geq k - i.$$

Taking the minimal of the bounds from Equations (7),(8) completes the proof. \blacksquare

5.3.4 Analyzing error weight

We note that the expected weight of \mathcal{E} is $p|S|$ and since $|S|$ is linear in n , by Chernoff the probability that the weight of \mathcal{E} is smaller by more than a constant fraction than this expectation is

$2^{-\Omega(n)}$. We need to show a similar bound on the weight modulo the centralizer group; given that $\delta < \text{dist}(C)/2n$ we only need to bound the weight modulo $A(\mathcal{G})$. Let $\Delta \in A$ be some element in the stabilizer group and let $\mathcal{E}_{\mathcal{G}} = \Delta \cdot \mathcal{E}$. We now need to lower-bound $wt(\mathcal{E}_{\mathcal{G}})$.

Fact 8 For integer k , let $\hat{k} = \lfloor k/2 \rfloor + 1$. Let $y(k) : [4, \infty] \mapsto \mathbf{R}$ be the function:

$$y(k) = \begin{cases} 1 - 2^{(-\hat{k}+1)\log(k)+k-2.3\hat{k}+4.54} & k \geq 12 \\ 0.9999 & 6 \leq k \leq 11 \\ 0.9992 & k = 5 \\ 0.9985 & k = 4 \end{cases}$$

We claim:

$$\text{Prob}_{\mathcal{E}}(wt(\mathcal{E}_{\mathcal{G}}) < |S|py(k)) = 2^{-\Omega(n)}.$$

Proof: (Sketch. The detailed proof can be found in Appendix (F).) The proof builds on the onion fact (7) as follows: the onion fact shows that "islands" with fewer than $k/2$ errors cannot "lose" error weight modulo the centralizer of \mathcal{G} . The proof uses standard probabilistic arguments, to argue, that the random error pattern we chose, is such, that the vast majority of islands, have fewer than this threshold error weight, and so the overall error weight is virtually unharmed. ■

5.3.5 Concluding the proof of lemma (2)

Proof: By fact (6) the average penalty of \mathcal{E} is small, i.e.

$$\mathbf{E}[Penalty(\mathcal{E})] \leq |S|D_L p \alpha(1 - 0.02/k) \triangleq P.$$

Yet, by fact (8) w.p. exponentially close to 1, we have

$$wt(\mathcal{E}_{\mathcal{G}}) \geq |S|py(k) \triangleq W_{low} \geq |S|p \cdot 0.99.$$

Similarly, by the Hoeffding bound w.p. exponentially close to 1, we have

$$wt(\mathcal{E}_{\mathcal{G}}) < |S|p(1 + 0.01) \triangleq W_{high}.$$

Since all penalties are non-negative, we conclude that *conditioned* on $|wt(\mathcal{E}_{\mathcal{G}})/(|S|p) - 1| < 0.01$, we have $\mathbf{E}[Penalty(\mathcal{E})] \leq P + 2^{-\Omega(n)}$. Therefore, there must exist an error \mathcal{E} , whose weight modulo \mathcal{G} deviates by a fraction at most 0.01 from $|S|p$, and whose penalty is at most $P + 2^{-\Omega(n)}$.

We would like to bound the soundness of this error, which is the ratio of the penalty to its relative weight times D_L . We get that its soundness is at most

$$r = \frac{P + 2^{-\Omega(n)}}{D_L W_{low}} \leq \frac{1}{D_L} \cdot \frac{|S|D_L p \alpha(1 - 0.019/k)}{|S|py(k)} = \alpha \left(\frac{1 - 0.019/k}{y(k)} \right). \quad (9)$$

We now note that in the last expression, for all $k \geq 12$, the ratio $\frac{1-0.019/k}{y(k)}$ is at most $1 - 0.01/k$. For all values of $4 \leq k < 12$ we substitute the appropriate value of $y(k)$ and get similarly that the ratio $\frac{1-0.019/k}{y(k)}$ is at most $1 - 10^{-3}$. Hence, the soundness of the error, r is at most $\alpha(d)(1 - \gamma_{gap})$ where γ_{gap} is as defined in the statement of theorem (2). ■

6 Acknowledgements

The authors would like to thank Eli Ben-Sasson, Irit Dinur and Tali Kaufman for insightful discussions.

References

- [1] S. Arora. *Probabilistic checking of proofs and the hardness of approximation problems*. PhD thesis, UC Berkeley, 1994.
- [2] D. Aharonov, I. Arad, Z. Landau, U. Vazirani *The Detectability Lemma and Quantum Gap Amplification* *arXiv:0811.3412*
- [3] D. Aharonov, L. Eldar, The commuting Local Hamiltonian problem on small-set expanders is in NP. Preliminary version of the results appeared in quant-ph arXiv:1301.3407.
- [4] N. Alon, T. Kaufman, M. Krivelevich, S. Litsyn, D. Ron Testing Reed-Muller codes *IEEE Transactions on Information Theory* (Volume:51 , Issue: 11) , Nov. 2005.
- [5] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. *Proof verification and intractability of Approximation problems*. *J. ACM*, 45(3):501-555, 1998.
- [6] D. Aharonov, I. Arad, T. Vidick *The Quantum PCP Conjecture* *ACM SIGACT News archive Volume 44 Issue 2, June 2013, Pages 47–79*
- [7] S. Arora, S. Safra *Probabilistic checking of proofs: A new characterization of NP* *Journal of the ACM*, 45 (1): 70122, 1998.
- [8] S. Arora, S. Safra *Probabilistic checking of proofs: A new characterization of NP* *Journal of the ACM* 45 (1): 70122.
- [9] S. Arora and B. Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009.
- [10] D. Bacon *Operator Quantum Error Correcting Subsystems for Self-Correcting Quantum Memories* *Phys. Rev. A* 73 012340 (2005)
- [11] H. Buhrman, R. Cleve, J. Watrous, R. de Wolf *Quantum Fingerprinting* *Phys. Rev. Lett.* 87, 167902 (2001)
- [12] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, A. Tapp *Authentication of Quantum Messages* *Proc. 43rd Annual IEEE Symposium on the Foundations of Computer Science (FOCS '02)*, pp. 449-458. IEEE Press, 2002.
- [13] L. Babai, L. Fortnow, L. Levin, M. Szegedy. *Checking Computation in Polylogarithmic Time* *23rd ACM Symp. on Theory of Computation, New Orleans, May 1991*
- [14] Verifying Program Executions Succinctly and in Zero Knowledge [ePrint] E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, M. Virza *33rd International Cryptology Conference (CRYPTO 2013)*

- [15] E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, S. P. Vadhan: *Sound PCPs of Proximity, Shorter PCPs, and Applications to Coding* *SIAM J. Comput.* 36(4): 889-974 (2006).
- [16] E. Ben-Sasson and M. Sudan. *Short PCPs with polylog query complexity.* *SIAM Journal on Computing*, Vol. 38 (2), pages 551607, 2008. (Preliminary Version in 37th STOC, 2005).
- [17] Fernando G.S.L. Brando, Aram W. Harrow, Product-state Approximations to Quantum Ground States, Proc. of the 45th ACM Symposium on theory of computing (STOC 2013), pp. 871-880
- [18] S. Bravyi, B. Terhal *A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes* *New J. Phys.* 11 (2009)
- [19] S. Chesi, D. Loss, S. Bravyi, B. M. Terhal *Thermodynamic stability criteria for a quantum memory based on stabilizer and subsystem codes* *New J. Phys.* 12, 025013 (2010)
- [20] M. R. Capalbo, O. Reingold, S. Vadhan, and A. Wigderson. *Randomness conductors and constant-degree lossless expanders.* In *Proceedings of the ACM Symposium on Theory of Computing (STOC)*, pages 659-668, 2002.
- [21] E. Dennis, A. Kitaev, A. Landahl, J. Preskill *Topological quantum memory* *J. Math. Phys.* 43, 4452 (2002)
- [22] J. Haah *Local stabilizer codes in three dimensions without string logical operators* *Phys. Rev. A* 83, 042330 (2011).
- [23] J. Haah, J. Preskill *Logical-operator tradeoff for local quantum codes* *Phys. Rev. A* 86, 032308 (2012)
- [24] I. Dinur *The PCP theorem by gap amplification.* *Journal of the ACM*, Vol. 54 (3), Art. 12, 2007. *Extended abstract in 38th STOC, 2006.*
- [25] I. Dinur, T. Kaufman *On the structure of NP-hard 3-SAT instances , and a similar question for LTCs* *Talk at the The Fourth Israel CS Theory Day Thursday, March 24 th, 2011.*
- [26] I. Dinur, T. Kaufman *Locally Testable Codes and Expanders* *Pre-Print.*
- [27] E. Fetaya *Bounding the distance of quantum surface codes.* *J. Math. Phys.* 53, 062202 (2012).
- [28] K. Friedl and M. Sudan. *Some improvements to total degree tests.* In *Proc. 3rd Israel Symposium on Theoretical and Computing Systems (Tel Aviv, Israel, 46 Jan. 1995)*, pages 190-198.
- [29] O. Goldreich, S. Goldwasser, D. Ron *Property testing and its connection to learning and approximation* *Journal of the ACM (JACM)*, Volume 45 Issue 4, July 1998, Pages 653-750.
- [30] O. Goldreich *Short Locally Testable Codes and Proofs: A Survey in Two Parts*
- [31] D. Gottesman *Stabilizer Codes and Quantum Error Correction* *Caltech Ph.D. Thesis.*
- [32] D. Gottesman *A theory of fault-tolerant quantum computation* *Phys. Rev. A* 57, 127-137 (1998)
- [33] D. Gottesman *On the Theory of Quantum Secret Sharing* *Phys. Rev. A* 61, 042311 (2000)
- [34] O. Goldreich, M. Sudan *Locally testable codes and PCPs of almost-linear length.* *Journal of the ACM (JACM)* ,Volume 53 Issue 4, July 2006,Pages 558-655.

- [35] J. Haah *Local stabilizer codes in three dimensions without string logical operators* *Phys. Rev. A* 83, 042330 (2011)
- [36] J. Håstad *Some optimal inapproximability results*. *Journal of ACM*, 48:798859, 2001.
- [37] M. B. Hastings *Trivial Low Energy States for Commuting Hamiltonians, and the Quantum PCP Conjecture* *arXiv:1201.3387v1*.
- [38] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and quantum computation*, volume 47 of *Graduate Studies in Mathematics*. AMS, 2002.
- [39] A. Yu. Kitaev *Fault-tolerant quantum computation by anyons*. *Ann. Physics*, 303(1), 2003.
- [40] E. Knill, R. Laflamme, A. Ashikhmin, H. Barnum, L. Viola, W.H. Zurek *Introduction to Quantum Error Correction* <http://arxiv.org/abs/quant-ph/0207170>.
- [41] A.A. Kovalev and L.P. Pryadko, *Fault tolerance of “bad” quantum low density parity check codes* *arXiv:1208.2317*
- [42] A.A. Kovalev and L.P. Pryadko, *Quantum “hyperbicycle” low density parity check codes with finite rate* *arXiv:1212.6703*
- [43] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, (North-Holland, Amsterdam 1977)
- [44] K. Michnicki *3-d quantum stabilizer codes with a power law energy barrier* *arXiv:1208.3496*
- [45] M. A. Nielsen, I. L. Chuang *Quantum Computation and Quantum Information* (10. Anniversary Edition). Cambridge University Press, (2010).
- [46] R. Rubinfeld and M. Sudan. *sound characterizations of polynomials with applications to program testing*. *SIAM Journal on Computing* 25, 2 (Apr. 1996), 252271. (Preliminary Version in 3rd SODA, 1992).
- [47] M. Sipser, D. Spielman. *Expander codes*. *IEEE Transactions on Information Theory* 42(6): 1710-1722 (1996).
- [48] A. Steane *Quantum Reed-Muller Codes* *arXiv:quant-ph/9608026*
- [49] S. Bravyi, D. Poulin and B.M. Terhal, *Tradeoffs for reliable quantum information storage in 2D systems* *arxiv.org: 0909.5200* (2009), *Phys. Rev. Lett.* 104, 050503 (2010).
- [50] B. Yoshida *Feasibility of self-correcting quantum memory and thermal stability of topological order* *Annals of Physics* 326, (2011) 2566-2633
- [51] A. Couvreur, N. Delfosse, G. Zémor *A construction of quantum LDPC codes from Cayley graphs*. *IEEE International Symposium on Information Theory Proceedings (ISIT)*, 2011, pp. 643-647.
- [52] J.P. Tillich, G. Zémor *Quantum LDPC codes with positive rate and minimum distance proportional to $n^{1/2}$* . *IEEE International Symposium on Information Theory (ISIT)* 2009, pp. 799-803.

A Proof of Claim 1

We prove that Definitions (5) and (4) are equivalent:

Proof: If definition (4) holds then for any $E \in \mathcal{E}$, and any two orthogonal states of the code $|\phi\rangle, |\psi\rangle$ have

$$\langle\phi|E|\psi\rangle = \langle\phi|\Pi_C E \Pi_C|\psi\rangle = \gamma_E \langle\phi|\Pi_C|\psi\rangle = \gamma_E \langle\phi|\psi\rangle = \gamma_E 0 = 0.$$

On the other hand, suppose that for any two orthogonal states $|\phi\rangle, |\psi\rangle$ in the code, and any $E \in \mathcal{E}$, we have $\langle\phi|E|\psi\rangle = 0$. Choose some orthogonal basis of the code $C \{ |b_i\rangle \}_{i=1}^m$. Then for each of these basis vectors, we have $\langle b_i|E|b_j\rangle = 0$, for $i \neq j$. Hence, in particular, the operator $E|_C$, i.e., E restricted to C , is a diagonal matrix $\text{diag}(\lambda_1, \dots, \lambda_m)$. We claim, further that $E|_C = \gamma_E I$, for some constant γ_E , and hence $\Pi_C E \Pi_C = \gamma_E \Pi_C$. Suppose, on the negative, that there exist two eigenvalues of $E|_C$ that are different, say $\lambda_1 \neq \lambda_2$. Consider the orthogonal states $|\phi\rangle = \frac{1}{\sqrt{2}}(|b_1\rangle + |b_2\rangle)$, $|\psi\rangle = \frac{1}{\sqrt{2}}(|b_1\rangle - |b_2\rangle)$. Then $|\phi\rangle, |\psi\rangle$ are in the code by linear closure, and are orthogonal, and yet

$$\langle\phi|E|\psi\rangle = \frac{1}{2}\langle b_1|E|b_1\rangle - \frac{1}{2}\langle b_1|E|b_2\rangle + \frac{1}{2}\langle b_2|E|b_1\rangle - \frac{1}{2}\langle b_2|E|b_2\rangle = \frac{1}{2}(\lambda_1 - \lambda_2) \neq 0,$$

contrary to our assumption on E . ■

B Proofs of geometrical facts on small-set expanders

B.1 Proof of fact (1):

For $S \subseteq R$ let $\Gamma_1(S) \subseteq \Gamma(S)$ denote the subset of the neighbors of S with exactly one neighbor in S . Similarly, let $\Gamma_{\geq 2}(S)$ denote the subset of neighbors with at least two neighbors in S .

Proof: The average degree of a vertex in $\Gamma(S)$ w.r.t. $|S|$ is at most $\frac{D_L S}{D_L S(1-\varepsilon)} = \frac{1}{1-\varepsilon}$. Let α_1 denote the fraction $|\Gamma_1(S)|/|\Gamma(S)|$, where $\Gamma_1(S)$ is the set of neighbors of S with degree exactly 1 with respect to S . Then

$$\frac{1}{1-\varepsilon} \geq \alpha_1 1 + (1 - \alpha_1)m,$$

where m is the average degree of a vertex with at least two neighbors in S . Then by simple algebra

$$\alpha_1(m) \geq 1 - \frac{1}{m-1} \cdot \frac{\varepsilon}{1-\varepsilon},$$

so $\alpha_1(m)$ is a monotonously increasing function of m , and since $m \geq 2$, then α_1 is minimized for $m = 2$. Hence,

$$\alpha_1 \geq 1 - \frac{\varepsilon}{1-\varepsilon}.$$

and since $\varepsilon < 1/2$ we have:

$$\alpha_1 \geq 1 - \varepsilon(1 + 2\varepsilon) \geq 1 - 2\varepsilon. \quad \blacksquare$$

B.2 Proof of fact (2):

Proof: By definition, we have $|\Gamma(S)| \geq |S|D_L(1-\varepsilon)$. Let $E_{inj} \subseteq E(S)$ be a subset of the edges incident on S such that each $u \in \Gamma(S)$ has a single neighbor in S connected by an edge of E_{inj} . Then E_{inj} is of size $|\Gamma(S)|$ which is at least $|S|D_L(1-\varepsilon)$. Also $|E(S)| = |S|D_L$, thus $|E(S) - E_{inj}| \leq |S|D_L\varepsilon$. Therefore $|\Gamma_{\geq 2}(S)| \leq |S|D_L\varepsilon$. Hence, $\Gamma_1(S) = \Gamma(S) - \Gamma_{\geq 2}(S)$ is of size at least $|S|D_L(1-\varepsilon) - |S|D_L\varepsilon = |S|D_L(1-2\varepsilon)$. Therefore, when $\varepsilon < 1/2$ there exists a vertex $v \in S$ with at least $D_L(1-2\varepsilon)$ neighbors in $\Gamma_1(S)$. Since v has D_L neighbors in $\Gamma(S)$, then the fraction of neighbors of v with at least two neighbors in S is at most 2ε , when $\varepsilon < \frac{1}{2}$. ■

C Existence of arbitrarily sound classical LTCs on small-set expanders

Claim 5 For any $\varepsilon \in (0, 1/2)$, and $r \in (0, 1)$ there exists a constant $\delta = \delta(r, \varepsilon)$, such that there exists an explicit infinite family of codes $\{C_\varepsilon(n)\}_{n \in \mathbb{N}}$ of n bits, of constant fractional rate r , and constant fractional distance $d = d(\varepsilon, r)$, whose check terms are of locality whose expectation is equal to a constant k , and all errors of weight less than δn have soundness $r(\delta) \geq 1 - 3\varepsilon$. Moreover, the underlying graph of these codes is an ε small-set expander.

Proof: The construction of [20], generates explicitly for any ε, r a left- D_L -regular bi-partite graph $G = (L, R; E)$ such that $|R|/|L| = 1 - r$, and for any subset $S \subseteq L$, $|S| \leq |L|\delta$ the neighbor set of S is of size at least $|S|D_L(1-\varepsilon)$, where D_L is the left degree of G . Note that since the left degree is D_L , the average right degree is $D_L|L|/|R| = D_L \frac{1}{1-r}$, which is a constant given that D_L is a constant.

The code is defined by assigning to each right node a parity check over its incident vertices. Let us lower bound the rate of this code: it is at least $r = (|L| - |R|)/|L|$, since each constraint in R at most halves the dimension of the codespace. The minimal distance of the code is at least δ , since any non-zero word of weight at most δ is rejected, since there exists at least one check term that "sees" just a single bit at state 1, by Fact (1).

Hence, these are so-called "good" codes. Furthermore, their soundness is at least $1 - 3\varepsilon$ since an error on a set of bits S of size $|S| \leq \delta n$, is examined by at least $|S|D_L(1-\varepsilon)$ constraints. By Fact (1) at least $1 - 2\varepsilon$ of those constraints, examine S in exactly one location; all constraints that touch a given error set S in exactly one location will be violated; hence the total number of constraints that will be violated is at least $|S|D_L(1-\varepsilon)(1-2\varepsilon) \geq |S|D_L(1-3\varepsilon)$. Therefore, the soundness function $R(\delta')$ is at least $(1 - 3\varepsilon)\delta'k$, for all $\delta' \in [0, \delta]$. ■

D Proof of Lemma (1): decomposition to cosets of a stabilizer code

Proof: For any $E \in \Pi_d^n$, and any $g \in \mathcal{G}$, we have $Eg = \omega gE$, where $\omega \in \mathbb{C}$. Therefore, for any $|\eta\rangle$ in C , we have $E|\eta\rangle$ is an ω eigenstate of g . Then for any $E \in \Pi_d^n$, we have that EC is some simultaneous eigenspace of \mathcal{G} . But, since Π_d^n , spans over \mathbb{C} all unitaries on n qudits, then it must be that every simultaneous eigenspace of \mathcal{G} is equal to EC for some $E \in \Pi_d^n$. In particular, any state $|\phi\rangle$ may be written as a sum

$$|\phi\rangle = \sum_i E_i |\eta_i\rangle,$$

where $E_i \in \Pi_d^n$, and $|\eta_i\rangle \in C$. ■

E Proof of Claim (2) Equivalence of definitions of code distance

We prove that a stabilizer code C has $\text{dist}(C) \geq \rho$ by definition 10, iff it has distance $\geq \rho$ by definition 6.

Proof: If the minimal weight of a Pauli in $\mathbf{Z}(\mathcal{G}) - A(\mathcal{G})$ has weight at least ρ , then all terms $E \in \Pi_d^n$ of weight strictly less than ρ (namely, at most $\rho - 1$) are either spanned by \mathcal{G} , or outside $\mathbf{Z}(\mathcal{G})$. Take any two orthogonal code states $|\phi\rangle, |\psi\rangle$. If $E \in A(\mathcal{G})$ then all code states are stabilized by E , so we have $\langle\phi|E|\psi\rangle = 1 \cdot \langle\phi|\psi\rangle = 0$. If $E \notin \mathbf{Z}(\mathcal{G})$, E does not commute with some generator, so in particular, E does not preserve the simultaneous 1-eigenspace of all generators, namely, the code. By lemma (1), this implies that EC is orthogonal to C . Thus we have in this case as well: $\langle\phi|E|\psi\rangle = 0$. Hence the minimal distance of the code, according to definition (6) is at least d .

Proving the converse, assume that $\text{dist}(C) < \rho$, i.e. $\min_{E \in \mathbf{Z}(\mathcal{G}) - A(\mathcal{G})} \text{wt}(E) < \rho$. Then, there exists $E \in \Pi_d^n$, of weight less than ρ , that commutes with all generators of \mathcal{G} but not spanned by them, so there exists some state $|\phi\rangle \in C$, such that $E|\phi\rangle \neq |\phi\rangle$, yet $E|\phi\rangle \in C$, (see [31], p. 27). Thus, there exists a non-zero projection of $E|\phi\rangle$ on some other code state $|\psi\rangle$ orthogonal to $|\phi\rangle$. Therefore, $\langle\psi|E|\phi\rangle \neq 0$, contrary to definition (5). ■

F Lower-bound on weight: proof of Fact (8)

Proof: Let $x \sim B(k, p = 1/(10k))$ denote a random variable which is the sum of k i.i.d Boolean variables, each equal to 1 with probability p ; in other words, x is a binomial process; $B(i) = \text{Prob}(x = i)$. Let U be a k -independent set of size $\Omega(n)$, and \mathcal{E} be the error process defined in Subsection (5.3.1). Let $U_i = \{u \in U | \text{wt}(\mathcal{E}|_{\Gamma(u)}) = i\}$ be the set of generators which have exactly i erroneous qudits. Using the Hoeffding bound, for a given $i \in [k]$ and a given any constant $\chi > 0$, we have

$$\text{Prob}_{\mathcal{E}} \left(\left| \frac{|U_i|}{|U|} - B(i) \right| \geq \chi \right) = 2^{-\Omega(n)} \quad (10)$$

By the union bound, we have that for any constant $\chi > 0$:

$$\text{Prob}_{\mathcal{E}} \left(\exists i, s.t. \left| \frac{|U_i|}{|U|} - B(i) \right| \geq \chi \right) = 2^{-\Omega(n)}. \quad (11)$$

Since the set U is a k -independent set, then the sets $\{\Gamma^{(k)}(u)\}_{u \in U}$ are non-intersecting so

$$\text{wt}(\mathcal{E}_{\mathcal{G}}) \geq \sum_{u \in U} \text{wt}(\mathcal{E}_{\mathcal{G}}|_{\Gamma^{(k)}(u)}), \quad (12)$$

By the Onion fact (Fact 7), for each $u \in U_i$ we have $\text{wt}(\mathcal{E}_{\mathcal{G}}|_{\Gamma^{(k)}(u)}) \geq \min\{i, k - i\}$, hence

$$\text{wt}(\mathcal{E}_{\mathcal{G}}) \geq \sum_{i \in [k]} |U_i| \min\{i, k - i\} = \frac{|S|}{k} \sum_{i \in [k]} \frac{|U_i|}{|U|} \min\{i, k - i\}$$

using $k|U| = |S|$. Using equation (11) w.p. close to 1 we have

$$\text{wt}(\mathcal{E}_{\mathcal{G}}) \geq \frac{|S|}{k} \sum_{i \in [k]} (B(i) - \chi) \min\{i, k - i\} \geq \frac{|S|}{k} \left(\sum_{i \in [k]} B(i) \min\{i, k - i\} - 2^{-k^2} \right), \quad (13)$$

for $\chi = 2^{-k^2}/k^2$.

We separate the rest of the proof to two cases: $k \geq 12$ and $4 \leq k < 12$. We start with the case $k \geq 12$. Recall $\hat{k} = \lfloor k/2 \rfloor + 1$. Let

$$A_{loss} = \sum_{i \geq \hat{k}} B(i)(2i - k).$$

Then by equation (13) we have that with probability exponentially close to 1

$$wt(\mathcal{E}_G) \geq \frac{|S|}{k} \left(\sum_{i \in [k]} B(i)i - A_{loss} - 2^{-k^2} \right) = \frac{|S|}{k} (pk - 2^{-k^2} - A_{loss}) \quad (14)$$

In the rest of the proof for $k \geq 12$ we upper-bound A_{loss} and substitute in the above equation to derive the desired result. Using an upper-bound of the binomial, we have:

$$B(\hat{k}) = \binom{k}{\hat{k}} p^{\hat{k}} (1-p)^{k-\hat{k}} \leq 2^k \cdot (10k)^{-\hat{k}} (1-p)^{\hat{k}} \leq k^{-\hat{k}} 10^{-\hat{k}} 2^k \leq 2^{-\hat{k} \log(k) + k - 3.3\hat{k}}, \quad (15)$$

For any $i \geq \hat{k}$ and $p < 1/2$ we have

$$B(i+1) = B(i) \binom{k-i}{i+1} \left(\frac{p}{1-p} \right) < B(i) \frac{p}{1-p} < 2pB(i) \quad (16)$$

Substituting equations (16) and (15) in the expression for A_{loss} we have:

$$A_{loss} = \sum_{i \geq \hat{k}} B(i)(2i - k) \leq 2^{-\hat{k} \log(k) + k - 3.3\hat{k}} \sum_{i \geq \hat{k}} (2p)^{(i-\hat{k})} (2i - k) \quad (17)$$

$$\leq 2^{-\hat{k} \log(k) + k - 3.3\hat{k} + 1 + \hat{k}} \sum_{i \geq \hat{k}} (p)^{(i-\hat{k})} (i - \lfloor k/2 \rfloor) \quad (18)$$

Changing summation $i - \lfloor k/2 \rfloor \mapsto j$ we have the above is at most:

$$2^{-\hat{k} \log(k) + k - 2.3\hat{k} + 1} \sum_{j \geq 1}^{\lfloor k/2 \rfloor} p^{-j+1} j \leq 2^{-\hat{k} \log(k) + k - 2.3\hat{k} + 1} \sum_{j \geq 1}^{\lfloor k/2 \rfloor} p^{-j+1} k \quad (19)$$

$$\leq 2^{-\hat{k} \log(k) + k - 2.3\hat{k} + 1} k \sum_{j \geq 1}^{\lfloor k/2 \rfloor} p^{-j+1} \leq 2^{-\hat{k} \log(k) + k - 2.3\hat{k} + 1} k \cdot 1.1 \leq 2^{(-\hat{k}+1) \log(k) + k - 2.3\hat{k} + 1.2}, \quad (20)$$

where in the last inequality we bound the sum by $\sum_{i \geq 0} 1/p^i$, and set $p = 1/(10k) \leq 1/100$, using $k \geq 12$. Substituting this value in (14) we have that with probability $2^{-\Omega(n)}$ close to 1,

$$\begin{aligned} wt(\mathcal{E}_G) &\geq \frac{|S|}{k} \left(pk - 2^{-k^2} - 2^{(-\hat{k}+1) \log(k) + k - 2.3\hat{k} + 1.2} \right) = \\ &\geq \frac{|S|}{k} \left(pk - 2^{(-\hat{k}+1) \log(k) + k - 2.3\hat{k} + 1.21} \right) \end{aligned}$$

where in the last inequality we used again $k \geq 12$. Continuing, using $p = \frac{1}{10k}$ the above bound is equal to

$$= |S|p \left(1 - 2^{(-\hat{k}+1) \log(k) + k - 2.3\hat{k} + 1.21 + \log_2(10)} \right) \geq |S|py(k),$$

for all $k \geq 12$. For values of $4 \leq k < 12$ we substitute directly k in Equation (13), evaluate, and show it is at least $|S|py(k)$. ■

G Quantum PCP of Proximity

G.1 Classical PCPs of Proximity

We begin by presenting the definitions following [15]. A pair language L is a subset of $\{0, 1\}^n \times \{0, 1\}^\ell$ for $\ell = \text{poly}(n)$. For a pair language L , let $L(x) = \{y \mid (x, y) \in L\}$.

Definition 21 PCP of proximity (PCPP)

For functions $s, \delta : Z^+ \mapsto [0, 1]$, a verifier $V = V(x)$ is a probabilistically checkable proof of proximity (PCPP) system for a pair language L with proximity parameter δ and soundness error s if the following two conditions hold for every pair of strings $(x, y) \in \{0, 1\}^n \times \{0, 1\}^\ell$:

1. *Completeness:* If $(x, y) \in L$ there exists π such that $V(x)$ accepts oracle $y \circ \pi$ with probability 1.
2. *Soundness:* If y is $\delta(|x|)$ -far from $L(x)$, then for every π , the verifier $V(x)$ accepts oracle $y \circ \pi$ with probability at most $s(|x|)$.

If s and δ are not specified, then both can be assumed to be constants in $(0, 1)$.

The query complexity of the verifier V is defined to be the number of coordinates that V queries out of y and π . V is not charged for reading x but is charged for reading y even though it is part of the input. We notice that this is a more stringent restriction than in the case of a PCP proof; however, the requirements on the proof system are weaker - V is supposed to reject only word which are *far* from words in the language.

A good pair language to keep in mind is CIRCUIT-VAL, i.e. the pairs (x, y) , where x is a circuit on n bits of polynomial size, and y is a string on n bits, and $(x, y) \in L$ if $x(y) = 1$, i.e. the circuit x evaluates to 1 on input y . Though this problem lies in P, a simple argument (Proposition 2.4 in [15]) shows that a PCPP for CIRCUIT-VAL, implies a PCP for the NP complete decision language CIRCUIT-SAT, the set of all x , for which there exists y , such that $x(y) = 1$.

G.2 From PCPPs to LTCs

Given a PCPP, [15] provides a standard construction of an LTC with related parameters, as follows. Given is a PCPP for membership in a code, namely, for the pair language of (C, w) , a code and a member in that code. Suppose the proximity parameter of the PCPP is δ , the soundness s and the query complexity k . Suppose also that we are given a code C with distance D . Then, one can construct an error correcting code C' which is an LTC with k -local constraints, whose weighted distance is D , and whose soundness is proportional to the soundness s .

C' is defined as the strings $w \circ \pi$ for all w in C , where π is the proximity proof of w . If one defines the distance by weighting only the coordinates in the first register, then C' trivially has the same distance as C .² The local test for the code C' as an LTC are the k -local tests performed by the verifier of the PCPP; Consider now a word $w' \circ \pi'$ which is δ -far from any $w \circ \pi$ in the code C' , where the distance is measured again by taking into account only the coordinates of the left register. This means that w' is δ -far from a word in the code C , then the tests will reject the word $w' \circ \pi'$ with probability s , which will thus be the soundness of the code for proximity δ .

²In [15] this choice of definition of distance is referred to as equivalent to the one used in [15], in which many repetitions of the string w are taken, so that the weight of the error on the second, proof, register becomes negligible.

G.3 Quantum PCPPs

We now define the quantum analogue of PCP's of proximity. We consider quantum pair languages $L \subseteq \{0, 1\}^n \otimes \mathcal{H}_{prf}$, where \mathcal{H}_{prf} is a Hilbert space of ℓ d -dimensional qudits, for $\ell = \text{poly}(n)$. For a quantum pair language L let $L(x) = \text{Span} \{|\psi\rangle \in \mathcal{H}_{prf}, (x, |\psi\rangle) \in L\}$.

Definition 22 Quantum PCP of proximity

Fix functions $s, \delta : Z^+ \mapsto [0, 1]$. Let $V = V(x)$ be a function from n bit strings x to sets of m k -local projections $\{\Pi_i\}_{i=1}^m$, each acting on $\mathcal{H}_{prf} \otimes \mathcal{H}_{pxmty}$. V is a quantum probabilistically checkable proof of proximity (qPCPP) system, for a quantum pair language L , with proximity parameter δ and soundness error s , if the following two conditions hold for every pair $(x, |\psi\rangle)$:

1. *Completeness:* If $(x, |\psi\rangle) \in L$, there exists $|w\rangle \in \mathcal{H}_{pxmty}$, such that for all check terms $\Pi_i \in V(x)$

$$\Pi_i(|\psi\rangle \otimes |w\rangle) = 0.$$

2. *Soundness:* If $|\phi\rangle$ is a quantum state in $\mathcal{H}_{prf} \otimes \mathcal{H}_{pxmty}$ whose reduced density matrix to \mathcal{H}_{prf} is supported on states, each of distance at least $\delta(|x|)$ from $L(x)$, then

$$\frac{1}{m} \sum_i \langle \phi | \Pi_i | \phi \rangle \geq s(|x|) : .$$

G.4 From qPCPPs to qLTCs

Given is a qPCPP for membership in a quantum code on ℓ qudits, namely, for the pair language L comprised of pairs $(C, |\psi\rangle)$: a code (described by n bits), and an ℓ qudit state in the code. Suppose L has a qPCP of proximity with parameters δ, s for some functions $s, \delta : Z^+ \mapsto [0, 1]$, with projections Π_i . Let C' be the codespace $\subseteq \mathcal{H}_{prf} \otimes \mathcal{H}_{pxmty}$, defined as:

$$\text{Span} \{|\phi\rangle \otimes |\Pi(\phi)\rangle \text{ s.t. } |\phi\rangle \in C\},$$

where $|\Pi(\phi)\rangle$ is some proof of proximity for $|\phi\rangle$ from the qPCPP. Let dist_{prf} denote the distance from the codespace as in definition (13) except it only counts non-identity Paulis acting on the register \mathcal{H}_{prf} .

Claim 6 C' is a qLTC with query complexity k and soundness $R(\delta) = s$ (where the proximity δ is defined with respect to the distance dist_{prf}).

Proof: Set $\{\Pi_i\}_{i=1}^m$ as the check terms for $L(C)$. These are k -local terms, so C' has query complexity k . By definition of the quantum PCP of proximity, for any state $|\phi\rangle$ in the codespace of C' , we have $\Pi_i|\phi\rangle = 0$, for any $\Pi_i \in V(C')$. Let us assume now that $\text{dist}_{prf}(|\phi\rangle, C') \geq \delta(|C|) \cdot \ell$. Then by Definition 13, for any Pauli operator E acting on $\mathcal{H}_{prf} \otimes \mathcal{H}_{pxmty}$, whose support on \mathcal{H}_{prf} is at most $\delta(|C|) \cdot \ell - 1$, we have that $E|\phi\rangle$ is still orthogonal to C' . In particular, for any E whose support is contained in \mathcal{H}_{prf} , and whose weight is at most $\delta(|C|) \cdot \ell - 1$, we have that $E|\phi\rangle$ is still orthogonal to C' . It is easy to see that the reduced state of $|\phi\rangle$ to \mathcal{H}_{prf} is a mixture of orthogonal states $\{|\eta_i\rangle\}_i$, each of which is at least $\delta(|C|) \cdot \ell$ -far from C . By virtue of the soundness of the qPCPP, $|\phi\rangle$ will be rejected by the check terms Π_i with probability at least $s(|C|)$. ■