Constructing quantum codes from *any* classical code and their embedding in ground space of local Hamiltonians

Ramis Movassagh [*] Yingkai Ouyang [†]

We introduce a framework for constructing a quantum error correcting code from *any* classical error correcting code. This includes CSS codes [5] and goes beyond the stabilizer formalism [8] to allow quantum codes to be constructed from classical codes that are not necessarily linear or self-orthogonal (Fig. 1). We give an algorithm that explicitly constructs quantum codes with linear distance and constant rate from classical codes with a linear distance and rate. As illustrations for small size codes, we obtain Steane's 7−qubit code [15] uniquely from Hamming's [7,4,3] code [13], and obtain other error detecting quantum codes from other explicit classical codes of length 4 and 6. Motivated by quantum LDPC codes and the use of physics to protect quantum information, we introduce a new 2-local frustration free quantum spin chain Hamiltonian whose ground space we analytically characterize completely. By mapping classical codewords to basis states of the ground space, we utilize our framework to demonstrate that the ground space contains explicit quantum codes with linear distance. This side-steps the Bravyi-Terhal no-go theorem [3] because our work allows for more general quantum codes beyond the stabilizer and/or linear codes. This model may be called an example of *subspace* quantum LDPC codes with linear distance.

1 Overview

Error correction is a necessary part of any reliable computation. On one hand, one can protect against errors by designing error correcting codes that allow for reliable recovery of the encoded information. On the other hand, nature herself provides innate resources for the protection and correction of information. These beg the questions:

1. Since quantum computers generalize classical computers, to what extent can one import the remarkable discoveries in classical coding [13] to the quantum realm?

2. Since the bulk of matter often resides in its ground state, are there physical quantum systems (e.g., 2-local Hamiltonians) whose ground states can sustain good quantum codes?

In this paper we address both of these questions in two parts:

Part 1 introduces a framework that takes any classical code and algorithmically constructs an explicit quantum code. The challenge in designing quantum codes is to not only correct the bit-flip errors, but also to correct phase-flip errors. We construct quantum codes with asymmetric distances given by d_X and d_Z for the bit-flip and phase-flip errors respectively. Similar to CSS codes, the logical codewords that are supported on codewords of length n are labeled by a *classical* code C. In the simplest case, we encode a logical qubit as follows

$$|0_L\rangle = \sum_{\mathbf{c}\in C_0} \alpha_{\mathbf{c}}^{(0)} |\mathbf{c}\rangle, \quad |1_L\rangle = \sum_{\mathbf{c}\in C_1} \alpha_{\mathbf{c}}^{(1)} |\mathbf{c}\rangle, \tag{1}$$

[*] IBM Quantum Research, MIT-IBM AI lab, Cambridge, MA 02142, U.S.A.
[†] Department of Physics and Astronomy, University of Sheffield, Sheffield, UK

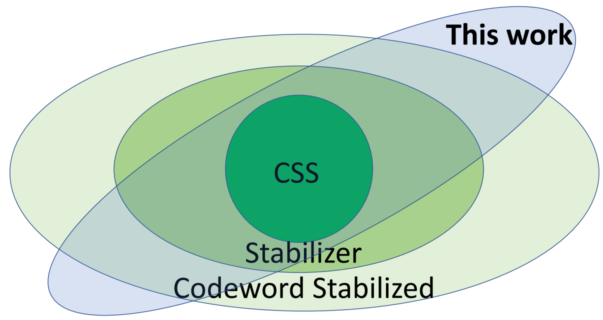

Figure 1: Comparison of the codes attainable within this work with Calderbank-Shor-Steane (CSS) [5, 15], quantum stabilizer [4, 8], and codeword-stabilized (CWS) [6] codes. Inclusion of stabilizers and CWS is not strict as our codewords are supported on disjoint sets.

where C_0 and C_1 are disjoint subsets of C, and each $\boldsymbol{c}$ is a product state. *A priori*, the subsets C_0 and C_1 and the coefficients are not known. By mapping the Knill-Laflamme (KL) quantum error correction criterion to a linear algebra problem, we construct an explicit algorithm that can determine these unknowns. To design a quantum code that encodes more than one logical qubit, we provide a recursive algorithm. This algorithm finds the disjoint subsets of C and enforces the KL criteria by solving for feasible solutions of a linear program, in time at most $O(MV_q^3(d_Z-1))$, where $V_q(r)$ is the volume of the q-ary Hamming ball of radius r and M is the number of logical states constructed from M disjoint subsets of C. The algorithm outputs the logical states:

$$|j_L\rangle = \sum_{\mathbf{c}\in C_j} \alpha_{\mathbf{c}}^{(j)} |\mathbf{c}\rangle, \quad j \in \{0, 1, \ldots, M-1\}, \tag{2}$$

where $2 \le M \le q^{O(n)}$, resulting in quantum codes with constant rates. We prove:

Theorem 1. *Take a classical code C of length n on a q-ary alphabet with the distance of d_X. If $|C| \ge 2V_{2s+1}(d_Z-1)$, then Alg. (1) and M calls to Alg. (2) in the paper explicitly derives the M quantum logical codewords in (2) with a bit- and phase-flip distances of d_X and d_Z respectively. The overall distance is $\min(d_X, d_Z)$ and the classical runtime of the procedure is $O(MV_q^3(d_Z-1))$.*

Our algorithm has a recursive structure. When the inequality in the theorem is satisfied, the algorithm always constructs two logical codewords. The third and subsequent logical codewords are found recursively by determining the feasibility of a sequence of linear programs.

This recursive algorithm succeeds with high probability and almost surely over random codes. In the rare case that the set of linear constraints have rows that are all non-zero and are of the same sign, the recursion becomes infeasible and algorithm halts. We find that even if this happens we can always construct *Approximate* Quantum Error Correcting Codes (AQECC) [11] with linear distance and constant rate, provided that, the underlying classical code has these parameters. The formalism introduced here is shown in relation to other known formalism in Fig. 1. To obtain a q-ary quantum code with M logical codewords where M is even, the error of the approximation is $\epsilon \le (M/(2\lfloor |C|/(2V_q(d_Z-1))\rfloor))^{1/(2V_q(d_Z-1))}$.

In addition to giving asymptotic results, the formalism introduced works equally well to construct finite size codes. To illustrate, we show examples of quantum codes that can be constructed from classic codes in the classical literature. Among the various, we find that the Steane code is the unique solution of our formalism when the input is Hamming's [7,4,3] code.

Part 2 focuses on the physics of information. Since topological models of quantum computation, it has been recognized that quantum codes may naturally appear in the ground space of physical systems [9]. Most physical are 2-local interactions.

The most celebrated example is Kitaev's toric code that resides in the ground space of a 4-local Hamiltonian, which is an effective Hamiltonian of a perturbed 2-local Hamiltonian [10]. Kitaev's toric code is an example of topological order and paved the way for the topological model of quantum computation. The compass model [7] is 2-local on a lattice, and has recently been proposed as a candidate to encode quantum codes in the eigenbasis of the Hamiltonian [12]. However, the performance of these quantum codes are not well understood and have mainly been numerically investigated. The advantage of our work over the aforementioned works is that we construct a 2-local Hamiltonian, whose quantum error correcting properties we analytically prove.

In a nice recent result, Brandao *et al.* [1] gave a non-constructive proof of the existence, with high probability, of AQECC within a low-energy sector of translation invariant quantum spin chains. A remarkable feature of their result is that they proved the existence of AQECCs for a multitude of translation invariant models [1]. The remainin challenges were that the codes were not explicit, the KL criteria was only approximately satisfied (hence AQECCs), errors had to be on consecutive set of spins, and the codes were in a low-energy sector of the local Hamiltonian (i.e., not the ground space). Moreover, the distance of the code grows logarithmically with the number of spins.

Our work overcomes these challenges. We construct explicit codes with linear distance that, for simplicity, encode a logical qubit. We write down a new and explicit 2-local quantum integer spin-s chain parent Hamiltonian, H_n, on n qudits. We analytically prove that its ground space can be spanned by product states. By mapping these product states to classical codewords, we reduce the problem of finding quantum codes in the ground space of our Hamiltonian to that of finding classical codes that must obey some constraints that are induced by the Hamiltonian. The classical coding problem becomes that of finding $q$ary codes with forbidden substrings. By leveraging on existing constructions of binary codes, we construct candidate classical codes for our algorithm to run. Our main theorem is:

Theorem 2. *Let $\tau \le 1/2$ be a real and positive constant. There are explicit quantum codes which encode one logical qubit with a distance of $2\tau n$ whenever $1/2 - \tau/0.11 \ge \log_2(2s+1)\mathrm{Ent}_{2s+1}(2\tau)$, where $\mathrm{Ent}_q(x) = -x\log_q x - (1-x)\log_q(1-x) + x\log_q(q-1)$ is the q-ary entropy function.*

Remark 1. *The explicit construction uses a variant of the Justesen code to define C [13, Chpt. 10, Thm. 11]. We also prove existence of codes with linear distance and better constants using Gilbert-Varshamov (GV) construction [13, Chpt. 1], in which, the codewords are random.*

This side-steps the Bravyi-Terhal no-go theorem [3] because our work allows for more general quantum codes than the stabilizer and/or linear codes. This model may be called an example of *subspace* quantum LDPC codes with linear distance.

This work could pave the way for constructing the first Quantum LDPC codes with linear distance in the ground space of translation invariant local spin chains. We note that had we used *all* of the ground space to construct the codes, this Hamiltonian could have made the case for the first example of topological order in one-dimension [2], which has been conjectured to be impossible. The practical advantage of our work is that such explicit Hamiltonians are easily constructed in the laboratory in the near term, especially in atomic or ion trap architectures. Lastly, the Hamiltonian is a generalization of the highly entangled colored Motzkin spin chain [14], which may be of independent interest.

References

[1] Fernando G. S. L. Brandão, Elizabeth Crosson, M. Burak Şahinoğlu, and John Bowen. Quantum error correcting codes in eigenstates of translation-invariant spin chains. *Phys. Rev. Lett.*, 123:110502, Sep 2019.

[2] Sergey Bravyi, Matthew B Hastings, and Spyridon Michalakis. Topological quantum order: stability under local perturbations. *Journal of mathematical physics*, 51(9):093512, 2010.

[3] Sergey Bravyi and Barbara Terhal. A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes. *New Journal of Physics*, 11(4):43029, 2009.

[4] A Robert Calderbank, Eric M Rains, Peter W Shor, and Neil JA Sloane. Quantum error correction and orthogonal geometry. *Physical Review Letters*, 78(3):405, 1997.

[5] A Robert Calderbank and Peter W Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098, 1996.

[6] A Cross, G Smith, J A Smolin, and Bei Zeng. Codeword stabilized quantum codes. In *IEEE International Symposium on Information Theory, 2008*, pages 364–368, July 2008.

[7] Julien Dorier, Federico Becca, and Frédéric Mila. Quantum compass model on the square lattice. *Physical Review B*, 72(2):024448, 2005.

[8] D Gottesman. A class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A*, 54:1862–1868, 1996.

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

[10] Alexei Kitaev. Anyons in an exactly solved model and beyond. *Annals of Physics*, 321(1):2 – 111, 2006. January Special Issue.

[11] Debbie W Leung, Michael A Nielsen, Isaac L Chuang, and Yoshihisa Yamamoto. Approximate quantum error correction can lead to better codes. *Physical Review A*, 56(4):2567, 1997.

[12] Muyuan Li, Daniel Miller, Michael Newman, Yukai Wu, and Kenneth R Brown. 2d compass codes. *Physical Review X*, 9(2):021041, 2019.

[13] F J MacWilliams and N J A Sloane. *The Theory of Error-Correcting Codes.* North-Holland publishing company, first edition, 1977.

[14] Ramis Movassagh and Peter W Shor. Supercritical entanglement in local systems: Counterexample to the area law for quantum matter. *Proceedings of the National Academy of Sciences*, 113(47):13278–13282, 2016.

[15] Andrew Steane. Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, 1996.