arXiv:2012.01453v3 [quant-ph] 22 Nov 2024

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

Ramis Movassagh[1,2] and Yingkai Ouyang[3]

[1]IBM Research, MIT-IBM Watson AI lab, Cambridge MA, 02142, USA
[2]Google Quantum AI, Los Angeles, CA, 90291, USA
[3]School of Mathematical and Physical Sciences, University of Sheffield, Sheffield, UK

Implementing robust quantum error correction (QEC) is imperative for harnessing the promise of quantum technologies. We introduce a framework that takes *any* classical code and explicitly constructs the corresponding QEC code. Our framework can be seen to generalize the CSS codes, and goes beyond the stabilizer formalism (Fig. 1). A concrete advantage is that the desirable properties of a classical code are automatically incorporated in the design of the resulting quantum code. We reify the theory by various illustrations some of which outperform the best previous constructions. We then introduce a local quantum spin-chain Hamiltonian whose ground space we analytically completely characterize. 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.

Overview

In a way *information* is an ultimate basic entity in Nature. It is the information content that gives rise to the vast complexity of the physical world even though all known matter is built from a few subatomic particles. Information processing is a way by which we can view the physical processes, information preservation is how physical properties remain invariant in time, and error correction is how a physical state is restored when it deviates from its original form. One can argue that better understanding of the information preservation and processing is the next frontier of science that bridges the micro and macro. Quantum theory is currently the best we have that accounts for the majority of physical phenomena. Therefore quantum information science beckons us towards a deeper understanding of the world.

Computation is our way of synthesizing information processing for useful tasks. Therefore, quantum computation promises to be the most powerful model of computation available to us based on our current theories of nature.

Ramis Movassagh: movassagh@google.com
Yingkai Ouyang: y.ouyang@sheffield.ac.uk

As stated above, preserving information and error correction are necessary parts 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.

Classical error correction, which applies to the standard (classical) model of computation is a mature and evolved field. However, the successes there do not easily carry over to the quantum realm. The main difficulty is that possible quantum errors that can corrupt the computation or a state in the memory are richer than classical errors– besides bit-flip errors that classical information suffers, there can be errors in the phases. Moreover, nature herself provides innate resources for the protection and correction of information. These beg the questions:

1. To what extent can one import discoveries in classical coding to the quantum realm?

2. Since the bulk of matter often resides in its ground state, are there simple physical quantum systems amenable to experimental realizations in the lab whose ground states sustain good quantum codes?

In this paper we address both of these questions in two parts, which we now overview:

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 are supported on classical codewords of length n. However, our formalism goes beyond the CSS and its generalization (the stabilizer formalism). We are able to identify codes outside the known paradigms. In the simplest case, we encode a logical qubit as follows

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

where C_0 and C_1 are disjoint subsets of C, and each

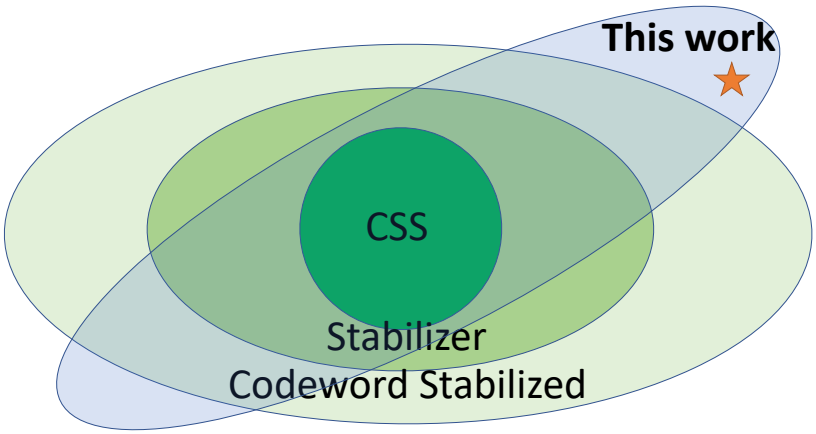

Figure 1: Comparison of the codes attainable within this work with Calderbank-Shor-Steane (CSS) [1, 2], quantum stabilizer [3, 4], and codeword-stabilized (CWS) [5] codes. Inclusion of stabilizers and CWS is not strict as our codewords are supported on disjoint sets. The star on the upper right indicates that we can identify codes outside of the previous frameworks.

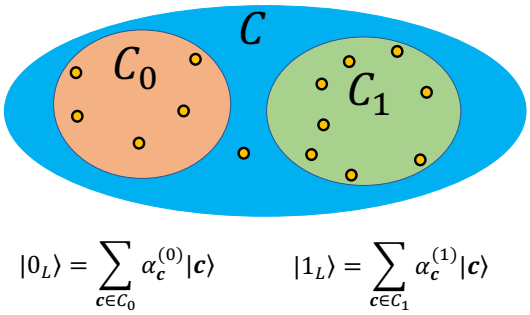

Figure 2: The encoding of one logical qubit from two disjoint subsets of a classical code C.

$\boldsymbol{c}$ 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 criteria [6] to a linear algebra problem, we construct an explicit algorithm that can determine these unknowns.

Using our framework we find constant excitation codes that outperform the best-known comparable codes [7, 8].

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. 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 $M \leq q^{c\,n}$ with $0 < c < 1$ resulting in quantum codes with constant rates, and q is the dimension of each qudit.

Let $V_q(r)$ be the volume of the Hamming ball of radius r defined by

$$V_q(r) = \sum_{w=0}^{r} \binom{n}{w} (q-1)^w. \tag{3}$$

We prove (see Theorem 1):

Theorem. *Take a classical code C of length n on a q-ary alphabet with the distance of d_X. If $|C| \geq 2V_q(d_Z - 1)$, then Alg. 1 and Alg. 2 in the paper explicitly derive M logical states as in Eq. (2) with bit- and phase-flip distances of d_X and d_Z respectively. Further, if C is chosen as a random code, with probability that approaches 1 as n goes to infinity, we have $2 \leq M \leq q^{c\,n}$ and $0 < c < 1$. The overall distance is* $\min(d_X, d_Z)$.

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) [9] with linear distance and constant expected rate, provided that the underlying classical code has these parameters. The trade-off is between the expected number of logical states and the approximation error as given by Eq. (33).

In addition to giving asymptotic results, this formalism works equally well to construct finite size

codes. To illustrate, we show examples of quantum codes that can be constructed from classical 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. The formalism introduced here is shown in relation to other known formalism in Fig. 1.

Our framework allows one to have the following perspective on designing quantum codes: instead of choosing from existing quantum codes the best quantum codes that suits a given physical system, one can impose the constraints imposed by the physical system a priori, and then construct quantum codes that respect these constraints. There is a big distinction between the two approaches of quantum code design. In the former approach, we might encounter a situation where the best available quantum code does not simultaneously have all the nice properties that we would like to have, whereas in this case, we flip the problem on its head. Namely, once we can cast physical constraints in the language of classical coding theory, we have a systematic approach to design bespoke quantum codes that respects the required physical constraints. In the second part of our paper, we illustrate this with a concrete 2-local spin chain Hamiltonian, and design quantum codes for it. This illustrates a systematic approach towards realising robust quantum codes in quantum matter.

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 [10]. Local Hamiltonians are considered more physical than the general Hamiltonians. In particular the most physical are 2-local interactions, and many have investigated the encoding of quantum codes in their ground spaces.

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 [11]. Kitaev's toric code is an example of topological order and paved the way for the topological model of quantum computation. The compass model [12] is 2-local on a lattice, and has recently been proposed as a candidate to encode quantum codes in the eigenbasis of the Hamiltonian [13]. 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 the perfect quantum error correction setting.

Brandao *et al.* [14] gave both constructive and non-constructive proof of the existence of AQECCs within the low-energy sector for a multitude of yoquantum spin chains including ferromagnetic Heisenberg model and spin-1 Motzkin spin chain [14]. The challenges that remained were that the quantum error correction criteria was only approximately satisfied (hence AQECCs), errors had to be on consecutive set of spins for general spin chains, 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.

Recently, it was also shown that by leveraging on a clock-work construction, one can design AQECCs with linear distance that reside within the ground-space of 10-local Hamiltonians [15]. However the challenge remained for constructing exact linear distance codes that reside within the ground space of a 2-local Hamiltonian.

Our work overcomes these challenges. We construct explicit codes that exactly correct errors with linear distance that encode one logical qubit (we could have easily encoded a qudit as well). 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 sub-strings. By leveraging on existing constructions of binary codes, we construct candidate classical codes for our algorithm to run. See the following table for a comparison.

Properties	Brandao et al [14]	This work
QECC	Apprx. $\epsilon = O(N^{-1/8})$	Exact
Distance d	$d = \Omega(\log(N))$	$d = \Theta(N)$
Rate	Vanishes	Vanishes
Error restriction	consecutive spins	None
Code space	Low-energy eigenstates	Exact g.s.

We now give details of the main features of the Hamiltonian and its ground space. Let us consider a spin chain of length n with open boundary conditions and the local Hilbert space dimension of $2s+1$, where $s \geq 1$ is a positive integer. We take a representation in which $|j\rangle$ denotes the $s_z = j$ state of a spin-s particle, such that $\hat{S}_z|j\rangle = j\,|j\rangle$ where $j \in \{0, \pm1, \pm2, \cdots, \pm s\}$.

The local Hamiltonian whose ground space contains the quantum code is $H_n = H_n^J + H_n^s$, where $H_n^J = J\sum_{k=1}^{n}(|0\rangle\langle 0|)_k$. The Hamiltonian H_n^s, is defined by

$$H_n^s = \sum_{k=1}^{n-1}\left\{\sum_{m=-s}^{s} P_{k,k+1}^m + \sum_{m=1}^{s} Q_{k,k+1}^m\right\}, \qquad (4)$$

and the local terms are projectors acting on two neighboring spins $k, k+1$ are

$$P^m = |0 \leftrightarrow m\rangle\langle 0 \leftrightarrow m|, Q^m = |00 \leftrightarrow \pm m\rangle\langle 00 \leftrightarrow \pm m|, \qquad (5)$$

Local Projector	Local Moves	Interpretation
P^m	$0m \longleftrightarrow m0$	spin transport
Q^m	$00 \longleftrightarrow m, -m$	spin interaction

Table 1: Map between interactions and corresponding moves in the underlying Markov chain. Here *spin transport* means locally exchanging spin m with 0, and *spin interaction* means local creating or annihilating $m, -m$.

where $|0 \leftrightarrow m\rangle \equiv \frac{1}{\sqrt{2}}[|0,m\rangle - |m,0\rangle]$, $|00 \leftrightarrow \pm m\rangle \equiv \frac{1}{\sqrt{2}}[|0,0\rangle - |m,-m\rangle]$, and we denoted by $|j,\ell\rangle$ the spin state $|s^z_k = j, s^z_{k+1} = \ell\rangle$. We will be mostly interested in $s > 1$.

Since H^s_n is free of the sign problem (i.e., stoquastic), the local projectors define an effective Markov chain, which have the following correspondence:

We prove that the ground state degeneracy is exponentially large in the number of spins ($n \gg 1$):

$$\dim(\ker(H^s_n)) = \frac{\left(-2 + r_+^{n+1} + r_-^{n+1}\right)}{2(s-1)} \approx \frac{r_+^{n+1}}{2(s-1)},$$

where $r_\pm \equiv (1 \pm \sqrt{1-1/s})$, and $\ker(M)$ the kernel of the operator M. Let us denote by $\mathrm{Ent}_q : [0,1] \to [0,1]$ the q-ary entropy function defined by $\mathrm{Ent}_q(x) = -x\log_q x - (1-x)\log_q(1-x) + x\log_q(q-1)$. Our main theorem is (this is Theorem 2 in the paper):

Theorem. *Let $0 < \tau \leq 1/4$ be a real and positive constant. There exist quantum codes in $\ker(H_n)$ that encode one logical qubit and have the distance of $2\tau n$ whenever*

$$\mathrm{Ent}_2(2\tau) + \mathrm{Ent}_{2s+1}(2\tau)\log_2(2s+1) + o(1) \leq 1.$$

Second, there are explicit quantum codes which encode one logical qubit with a distance of $2\tau n$ whenever

$$1/2 - \tau/0.11 \geq \log_2(2s+1)\mathrm{Ent}_{2s+1}(2\tau).$$

Remark. *We call the constructions given by optimizing (58) and (59) as the Gilbert-Varshamov (GV) [16, Chpt. 1] and Justesen construct [16, Chpt. 10, Thm. 11] respectively. The GV construct arises from choosing a random C, while the Justesen construct uses the classical Justesen code to define C.*

Our work side-steps the Bravyi-Terhal no-go theorem [17] which asserts that in one-dimension one cannot have stabilizer codes with system-size dependent distance. We also side-step the more general no-go result given by Gschwendtner et al. [18] which states that the degenerate ground space of gapped Hamiltonians can only be QECs with a constant distance. The reason we can side-step these no-go results is because our work considers QEC as a strict subspace of the ground space of Hamiltonians. In particular, this work could pave the way for constructing the quantum codes with linear distance within 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, 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 [19], which may be of independent interest.

0.1 Practical considerations

Here, we explain why the quantum codes we can construct, particularly the non-stabilizer codes, are interesting from a practical point of view.

A particular family of non-stabilizer codes that our paper can construct, and also show potential in a practical setting, are permutation-invariant quantum codes. Permutation-invariant codes can be efficiently prepared using either the usual Boykin gate set [20] (Clifford + T gates) set [21], or quantum control type of operations such as Rabi oscillations [22], or geometric phase gates [23]. In particular, geometric phase gates can be performed in a very practical way, because they only need (1) a linear interaction between the collective angular momentum operator of the qubits and a bosonic mode, and the bosonic mode to be initialized in a coherent state (a laser mode). The paper [23] showed that geometric phase gates can be performed in variety of physical systems. Good candidate systems for geometric phase gates include ion traps and cold neutral atoms.

Furthermore, there is potential to do quantum error correction on permutation-invariant codes in a practical way, as described in Ref. [24]. Ref. [24] proposes to perform quantum error correction by (1) measuring the total angular momentum of sequences of consecutive qubits, (2) performing geometric phase gates, and (3) performing logical gate teleportation operations. Ref. [24] explains how each one of these operations can be performed in a practical way, by using the interaction between collective spin operators and one or more bosonic modes, combined with homodyne and heterodyne measurements on these bosonic modes. Hence permutation-invariant codes have strong potential to be practical codes. Hence our paper's formalism does encompass codes with practical potential.

Our paper's code construction formalism also encompasses a particular class of quantum codes that reside in a decoherence free subspace of errors that act coherently [25, 26, 27, 28], and are hence 'error-avoiding' quantum codes. There has been recent work on constant-excitation codes, which are quantum error correction codes that avoid coherent errors in one axis (in Refs. [7, 8]). Using the code construc-

tion formalism in our paper and also by considering non-stabilizer codes, we construct new constant-excitation codes with improved distance-rate parameters for fixed code length.

We leave questions regarding the fault-tolerance of quantum codes that can be constructed using our framework as an open problem, and we are optimistic about its ultimate resolution.

0.1.1 Why introduce a Hamiltonian?

Theoretical considerations– This model is of theoretical interest because it allows for the encoding of linear distance codes in its ground space. Encoding quantum information in the ground space of physical Hamiltonians has a long history dating back to Kitaev's toric code [10]. A motivation for our work was the nice work of Brandao *et al.* [14] where existence of codes in low energy eigenstates of local translation invariant spin chains were found. In this work we came up with explicit and exact constructions and overcome some of the limitations of that work. These were detailed in the introduction and will be elaborated on below.

Our work may also be useful in bringing new insights into conformal field theories from quantum codes [29], by allowing any classical code to be used in the quantum coding framework.

Applied and engineering considerations– Finding new quantum codes can help hasten the dream of fault-tolerant quantum computation. Our method is distinct from other widely used methods to construct quantum codes from classical codes, such as for CSS codes, stabilizer codes, and codeword-stabilized codes. A key feature of our code construction is that we can take as input a general classical code, and demand that the quantum code we construct must be supported on the computational basis vectors that are labelled by these classical codewords. The non-trivial solution of the nullspace then gives us the amplitudes over with the logical zero and logical one of our quantum code will assume.

Our proposal to engineer a two-local Hamiltonian to stabilize quantum information is in line with the ideas utilizing quantum control techniques to suppress the noise before employing quantum error correction. We differ from traditional approaches in quantum control procedures where one typically applies dynamical decoupling pulses to create an essentially a trivial identity Hamiltonian that acts on the system when no quantum gates are performed. In this situation, however, local errors are not energetically penalized. In contrast, one might envision that quantum control methods can engineer a Hamiltonian that energetically penalizes the dominant noise rates that occur in a quantum system before introducing quantum error correction [30, 31].

In many practical physical systems, noise is biased and can be dominated by bit-flip or phase-flip type errors. We consider a biased noise model that is dominated by bit-flip type errors. On a spin-system, we expect our Hamiltonian to energetically penalize bit-flip errors. This would allow our engineered Hamiltonian to greatly suppress the noise rates of the dominant (bit-flip) type of errors. The remaining errors can then be cleaned up using our quantum code with a linear distance. The advantage of engineering our Hamiltonian, as compared to, for instance, the surface code Hamiltonian, is that the Hamiltonian terms that we require are two-local, whereas the surface code requires many-body interactions, which is challenging to realize in practice.

The Hamiltonian we will introduce has the form $H_n = \sum_{k=1}^{n-1} H_{k,k+1}$; see Eq.(47). Its ground space has a strict subspace that is the quantum code. We could make the model sums of commuting local terms by considering a new Hamiltonian that skips all (say) even interactions and write $H'_n = \sum_{k\ odd} H_{k,k+1}$. The ground space of H'_n contains the ground space of H_n and therefore also includes the quantum code. One could continue this way and eventually get a Hamiltonian that is trivial (*i.e.*, no interaction) $H'' = I$ for which any quantum code is in the "ground space". The price one pays following this crooked path is that Nature will help less and less in suppressing the rate at which errors appear.

0.2 Discussions and open problems

This paper provides a rigorous framework for the systematic construction of a quantum codes from any classical code. We illustrate the theory through a series of examples and proved that new quantum codes with linear distance and constant rate can be constructed using this work. Our formalism encapsulates the CSS formalism, and has an intersection with stabilizer and codeword-stabilized (CWS) formalisms (see subsection 1.5.2). However, there are codes inside the stabilizer and CWS formalism that our formalism does not capture. For example, the five-qubit code is not covered by our formalism because the corresponding classical code has a distance of one. Alg. 2 can construct logical states beyond a logical qubit. The relation of our work to the previous is faithfully depicted in the Venn diagram (Fig. 1) shows.

Our formalism can take as the input any classical linear, self-orthogonal code, and then derive the corresponding CSS code. This is because CSS codes, which rely on these types of classical codes, can also be completely cast within our framework. It will be interesting to classify all quantum codes that can be obtained within our framework if one were to start with classical linear, self-orthogonal codes.

Another open problem would be to find an alternative way of getting at our logical qu*d*it construction by directly using the large freedom in choosing codes

in our construction (namely the high-dimensional kernel of the matrix A in Eq. (13) and Fig. 3). It would also be interesting to see an extension of our formalism to encompass all stabilizer codes, and indeed, any arbitrary quantum code. With the exception of permutation invariant codes (subsection 1.5.3), most of the analysis herein takes the classical codewords and uses them to define a product basis over which the logical quantum states are defined. The extension of our results to include non-product basis for the logical codewords calls for further investigation.

Another interesting problem is to find a Hamiltonian whose ground space is quantum code with a macroscopic distance, and the local and global ground states satisfy a consistency criterion as defined in [32]. This would then serve as the first example of topological quantum order in one-dimension. We would have found it easy to prove a gap above the degenerate ground space of the local Hamiltonian herein; however, since the code occupies a subspace of the ground space one would need to prove a *local gap* lower bound. This means that in order to move from a subspace of the ground space to another subspace an operator with a large support needs to be applied.

1 Part 1: Explicit quantum codes from classical codes

1.1 Constructing a logical qubit with linear distance

In this section, we want to design q-ary quantum codes with bit-flip distance of d_X and a phase-flip distance of d_Z using a q-ary classical code $C \subset \{0,1\ldots,q-1\}^n$ as an input. The minimum distance of the quantum code is then $d = \min(d_X, d_Z)$.

To correct errors on q-ary quantum codes, we consider errors in the generalized Pauli basis. Let us denote by ω the primitive root of unity $\omega \equiv \exp(2\pi i/q)$. The Z and X type Pauli matrices are respectively given by

$$Z = \sum_{j=0}^{q-1} \omega^j |j\rangle\langle j| , \quad X = \sum_{j\in\mathbb{Z}_q} |j\rangle\langle j+1| . \tag{6}$$

And any Pauli operator is equivalent to $X^a Z^b$ up to a phase for some $a, b = 0,\ldots,q-1$. We consider the set Pauli operators on n qudits $\mathcal{P}_n = \{X^a Z^b : a, b = 0,\ldots,q-1\}^{\otimes n}$ that span the space of linear operators on n qudits. Given any Pauli in $\mathcal{P}_n$ that has the form $P = X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n}$, we denote $\mathrm{wt}_X(P) = \mathrm{wt}(\mathbf{a})$ and $\mathrm{wt}_Z(P) = \mathrm{wt}(\mathbf{b})$, where $\mathbf{a} = (a_1,\ldots,a_n)$, $\mathbf{b} = (b_1,\ldots,b_n)$, and $\mathrm{wt}(\cdot)$ denotes the Hamming weight of the vector. It is easy to see that for any non-negative integer $r \le n$, we have $\sum_{w=0}^{r} |\mathcal{Z}_w| = V_q(r)$, where $V_q(r) = \sum_{w=0}^{r} \binom{n}{w}(q-1)^w$ is the volume of the q-ary Hamming ball of radius r as before.

For the KL criteria to hold for a quantum code with logical codewords $|0_L\rangle$ and $|1_L\rangle$ on n qubits with a bit-flip distance of d_X and a phase-flip distance of d_Z, it suffices to require that for all generalized Pauli matrices P such that $\mathrm{wt}_X(P) \le d_X - 1$ and $\mathrm{wt}_Z(P) \le d_Z - 1$, these hold:

$$\langle 0_L|P|0_L\rangle = \langle 1_L|P|1_L\rangle \tag{7}$$
$$\langle 0_L|P|1_L\rangle = 0 . \tag{8}$$

Eqs. (7) and (8) are the *non-deformation* and *orthogonality* conditions respectively. If we demand that

1. $\mathrm{dist}(C) \ge d_X$: the minimum distance of C is at least d_X
2. $\mathrm{Supp}(0_L) \cap \mathrm{Supp}(1_L) = \emptyset$: (the logical codewords $|0_L\rangle$ and $|1_L\rangle$ are supported on distinct codewords in C),

then the orthogonality condition (Eq. (8)) trivially holds. To verify the non-deformation condition (Eq. (7)), we note that $\langle 0_L|P|0_L\rangle = \langle 1_L|P|1_L\rangle = 0$ whenever P is not diagonal. Hence the only non-trivial cases to be verified are the diagonal generalized Pauli operators, where the set of diagonal Pauli operators of weight w is

$$\mathcal{Z}_w = \{Z^{z_1} \otimes \cdots \otimes Z^{z_n} \ : \ \mathrm{wt}(\mathbf{z}) = w\} . \tag{9}$$

In general, for any diagonal Pauli operator P, the expectations $\langle 0_L|P|0_L\rangle$ and $\langle 1_L|P|1_L\rangle$ are complex numbers. This is in contrast to the case where P are Kraus operators of the amplitude damping channel, in which all such expectations are real, or when P are diagonal operators and $q = 2$. For Eq. (7) to hold, the following has to hold for all Paulis P with a weight at most $d-1$:

$$\mathrm{Re}\left(\langle 0_L|P|0_L\rangle\right) - \mathrm{Re}\left(\langle 1_L|P|1_L\rangle\right) = 0$$
$$\mathrm{Im}\left(\langle 0_L|P|0_L\rangle\right) - \mathrm{Im}\left(\langle 1_L|P|1_L\rangle\right) = 0 ,$$

The quantum code we define depends on a "balanced" real non-zero column vector $\mathbf{x} = (x_1, x_2, \ldots, x_m)^T$ in the sense that

$$\sum_{i=1}^{m} x_i = 0.$$

Let $x_k^+ = \max\{x_k, 0\}$, $x_k^- = -\min\{x_k, 0\}$, and $x = x_1^+ + \cdots + x_m^+$. We can decompose the vector $\mathbf{x}$ into its positive and negative components $\mathbf{x} = \mathbf{x}^+ - \mathbf{x}^-$ where $\mathbf{x}^+ = (x_1^+,\ldots,x_m^+)^T$ and $\mathbf{x}^- = (x_1^-,\ldots,x_m^-)^T$ respectively. We also have $x = \|\mathbf{x}^+\|_1 = \|\mathbf{x}^-\|_1 = \|\mathbf{x}\|_1/2$. For example, using this notation $\mathbf{x} = (1,2,-1,-1,-1)^T$ gives $\mathbf{x}^+ = (1,2,0,0,0)^T$ and $\mathbf{x}^- = (0,0,1,1,1)^T$, and $x = 3$.

In our construction of quantum codes using the classical code C, we only consider logical codewords that are linear combinations over labels in C with

only real coefficients. Hence, we define the two logical codewords of our quantum code as

$$|0_L\rangle = \frac{1}{\sqrt{x}}\left(\sqrt{x_1^+}|\mathbf{c}_1\rangle + \cdots + \sqrt{x_m^+}|\mathbf{c}_m\rangle\right), \quad (10)$$

$$|1_L\rangle = \frac{1}{\sqrt{x}}\left(\sqrt{x_1^-}|\mathbf{c}_1\rangle + \cdots + \sqrt{x_m^-}|\mathbf{c}_m\rangle\right). \quad (11)$$

Since that $x_j^+ x_j^- = 0$ for all $j \in [m]$, the logical states $|0_L\rangle$ and $|1_L\rangle$ have disjoint supports.

We next clarify the connection between $\mathbf{x}$ and the non-deformation conditions by constructing a real matrix A that enforces these conditions. Roughly speaking, this matrix has rows labeled by diagonal Pauli errors of weight at most $d_Z - 1$ and columns labeled by the states $|\mathbf{c}_1\rangle, \ldots, |\mathbf{c}_m\rangle$. While the ordering of the rows of A is unimportant, we will collect the rows in groups corresponding to the weights of P. The matrix A is defined by

$$\begin{aligned} A = &\sum_{P\in\mathcal{Z}_0}\sum_{k=1}^{m}|P\rangle\langle k| \\ &+\sum_{w=1}^{d-1}\sum_{P\in\mathcal{Z}_w}\sum_{k=1}^{m}\{\mathrm{Re}\left(\langle\mathbf{c}_k|P|\mathbf{c}_k\rangle\right)|P,0\rangle\langle k| \\ &\qquad +\mathrm{Im}\left(\langle\mathbf{c}_k|P|\mathbf{c}_k\rangle\right)|P,1\rangle\langle k|\}\,. \end{aligned} \quad (12)$$

In matrix representation A is a wide rectangular matrix and writes

$$A = \begin{bmatrix} 1 & \cdots & 1 \\ a_{2,1} & \cdots & a_{2,m} \\ \vdots & \cdots & \vdots \\ a_{2V_q(2t)-1,1} & \cdots & a_{2V_q(2t)-1,m} \end{bmatrix} \equiv \begin{bmatrix} \mathbf{a}_1^T \\ \mathbf{a}_2^T \\ \vdots \\ \mathbf{a}_{2V_q(2t)-1}^T \end{bmatrix} \quad (13)$$

where $\mathbf{a}_r = (a_{r,1}, \ldots, a_{r,m})^T$ are column vectors. The reason for introducing the matrix A is that the non-deformation condition for correcting t errors using the vector $\mathbf{x}$ is enforced by the constraint (see Fig.3)

$$A\mathbf{x} = 0\,.$$

Lemma 1. *Let $\mathbf{x}$ be a non-zero real vector such that $A\mathbf{x} = 0$. Let $|0_L\rangle$ and $|1_L\rangle$ be logical codewords that depend on $\mathbf{x}$ as in Eqs. (10) and (11). Then $\langle 0_L|P|0_L\rangle = \langle 1_L|P|1_L\rangle$ for any diagonal Pauli of weight at most $d_Z - 1$.*

Proof. Recall that $x = x_1^+ + \cdots + x_m^+$. Since each $|\mathbf{c}_k\rangle$ is a product state, we have $\langle\mathbf{c}_j|P|\mathbf{c}_k\rangle = 0$ for all distinct j and k, and for all diagonal Pauli of weight at most $d_Z - 1$. We can use the definitions of logical codewords (Eqs. (10) and (11)) to write

$$\begin{aligned} &x\left(\langle 0_L|P|0_L\rangle - \langle 1_L|P|1_L\rangle\right) \\ &= \sum_{k=1}^{m} x_k^+\langle\mathbf{c}_k|P|\mathbf{c}_k\rangle - \sum_{k=1}^{m} x_k^-\langle\mathbf{c}_k|P|\mathbf{c}_k\rangle \\ &= \sum_{k=1}^{m} x_k\langle\mathbf{c}_k|P|\mathbf{c}_k\rangle \end{aligned}$$

where on the second line we used $x_k = x_k^+ - x_k^-$. Using Eq. (12) we see that $\langle\mathbf{c}_k|P|\mathbf{c}_k\rangle = \langle P,0|A|k\rangle + i\langle P,1|A|k\rangle$. Therefore

$$\begin{aligned} &x\left(\langle 0_L|P|0_L\rangle - \langle 1_L|P|1_L\rangle\right) \\ &= \sum_{k=1}^{m} x_k\left(\langle P,0|A|k\rangle + i\langle P,1|A|k\rangle\right) \\ &= \sum_{k=1}^{m}\left(\langle P,0|Ax_k|k\rangle + i\langle P,1|Ax_k|k\rangle\right) \\ &= \langle P,0|A\mathbf{x} + i\langle P,1|A\mathbf{x}\,, \end{aligned}$$

because $\mathbf{x} = \sum_{k=1}^{m} x_k|k\rangle$. Since the first row of A is all ones, $A\mathbf{x} = 0$ implies $\langle 0_L|0_L\rangle = \langle 1_L|1_L\rangle$. Moreover, in the above, P is an arbitrary diagonal Pauli of weight at most $d_Z - 1$, and the requirement $A\mathbf{x} = 0$ implies $\langle 0_L|P|0_L\rangle = \langle 1_L|P|1_L\rangle$ for any diagonal Pauli of weight at most $d_Z - 1$. □

The condition $A\mathbf{x} = 0$ is satisfied for any $\mathbf{x} \in \ker(A)$. It is then important to understand the structure of the kernel. Since A is real, any vector in its kernel must be real, which we then use to design an explicit quantum code that obeys the generalized orthogonality conditions above. Whenever $|C| \geq 2V_q(d_Z - 1)$, that is the number of codewords in C is strictly greater than the number of rows in A, by the rank-nullity theorem, A must have a non-trivial kernel. We thus have the following existence theorem for quantum codes that reside within the ground space of H_n.

Lemma 2. *(Existence) Let C have a minimum distance at least d_X. If $|C| \geq 2V_q(d_Z - 1)$, then Alg. 1 constructs a quantum code with one logical qubit and with a bit-flip and phase-flip distance of d_X and d_Z respectively. Moreover, this quantum code can be constructed from any nonzero $\mathbf{x} \in \ker(A)$.*

This lemma shows that we can derive the logical codewords of our quantum code from a classical code, and only requires C to have a minimum distance of d_X and for $|C|$ to be at least twice the size of the q-ary Hamming ball of radius $d_Z - 1$.

We proceed to derive a more explicit expression for the entries of the matrix A in Eqs. (12) and (13). We will show that these entries are elements of a finite-sized set given by

$$\{\cos(2\pi k/q)\,,\ \sin(2\pi k/q)\ :\ k = 0, \ldots, q-1\}\,. \quad (14)$$

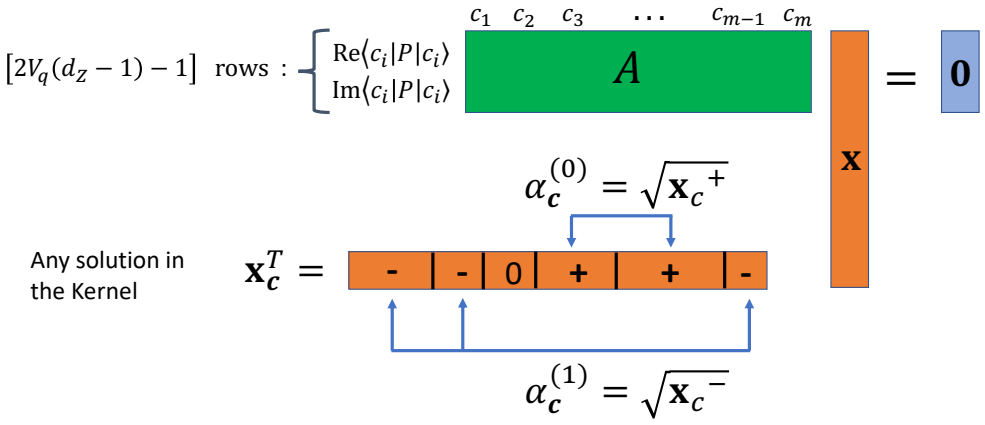

Figure 3: Illustration of $A\mathbf{x} = 0$ in Lemma 1, where the matrix A has $[2V_q(d_z-1)-1]$ rows and m columns (top of this figure). The vector $\mathbf{x_c}$ has m real components and denotes any solution in the kernel. Since the first row of A is all ones (P corresponds to the identity matrix), the vector $\mathbf{x_c}$ is balanced– the sum of all entries is equal to zero.

For any classical string $\mathbf{c} = (c_1, \ldots, c_n)^T \in C$ with $c_i = 0, 1, \ldots, q-1$, the quantum state is $|\mathbf{c}\rangle = |c_1, c_2, \ldots, c_n\rangle$, and when $P = Z^{z_1} \otimes \cdots \otimes Z^{z_n}$, we have

$$\langle \mathbf{c}|P|\mathbf{c}\rangle = \prod_{j=1}^{n} \langle c_j|Z^{z_j}|c_j\rangle$$

$$= \prod_{j=1}^{n} \langle c_j| \sum_{k\in\Sigma_c} (\omega^k)^{z_j} |k\rangle\langle k|c_j\rangle \tag{15}$$

$$= \prod_{j=1}^{n} \omega^{z_j c_j} = \omega^{\mathbf{z}^T\mathbf{c}} \tag{16}$$

$$= \cos\left(\frac{2\pi\, \mathbf{z}^T\mathbf{c}}{q}\right) + i \sin\left(\frac{2\pi\, \mathbf{z}^T\mathbf{c}}{q}\right). \tag{17}$$

The first row of A is all ones, and all other entries are given by

$$A' = \sum_{w=1}^{d_Z-1} \sum_{\mathrm{wt}(\mathbf{z})=w} \sum_{\mathbf{c}\in C} \left[\cos\left(\frac{2\pi\, \mathbf{z}^T\mathbf{c}}{q}\right) |\mathbf{z}, 0\rangle\langle \mathbf{c}| + \sin\left(\frac{2\pi\, \mathbf{z}^T\mathbf{c}}{q}\right) |\mathbf{z}, 1\rangle\langle \mathbf{c}|\right]. \tag{18}$$

Since $\mathbf{z}^T\mathbf{c}$ is always an integer, it follows that the entries of A must take values from the set in (14).

Remark 1. *In Eq. (18) finding a solution in the kernel amounts to finding linear combination of roots of unity that vanish. See for example section III and references in [33]. There is a vast literature (see chapter 7 in [16]) on this topic and properties of the underlying code that controls the values of the integers $\mathbf{z}^T\mathbf{c}$ can in principle be utilized to give analytic solutions.*

Remark 2. *When $q = 2$, all rows in A' that are labeled by $|\mathbf{z}, 1\rangle$ are equal to zero, because the argument of the sine is always an integer multiple of π.*

This section is summarized in the following algorithm:

Algorithm 1. Input: *A classical code $C \subset \{0, 1, \ldots, q-1\}^n$ with $m \equiv |C|$.*

- *Form the matrix A defined by Eq.(12).*
- *Solve $A\mathbf{x} = 0$ to find $\mathbf{x} \neq 0$. Define $\mathbf{x}^+, \mathbf{x}^- \geq 0$ such that $\mathbf{x} = \mathbf{x}^+ - \mathbf{x}^-$ as in Lemma 1*
- *Let C_0 be the set of codewords $\mathbf{c}_k$ with $k \in supp(\mathbf{x}^+)$. And let C_1 be the set of codewords $\mathbf{c}_k$ with $k \in supp(\mathbf{x}^-)$.*
- *For all $\mathbf{c} \in C_0$, assign $\alpha_{\mathbf{c}}^{(0)} = \sqrt{x_c^+}$, and for all $\mathbf{c} \in C_1$, assign $\alpha_{\mathbf{c}}^{(1)} = \sqrt{x_c^-}$.*

Output: *A logical quantum bit with codewords $|0_L\rangle$ and $|1_L\rangle$ as defined in Eqs. (10) and (11). The code distances are $d_X = dist(C)$ and d_Z that satisfies $m > 2V_q(d_Z-1)-1$.*

1.1.1 Limitations of the formalism

Can we use the classical repetition code with codewords $0\ldots0$ and $1\ldots1$ to make a QEC code with distance 2? There are only two linearly independent columns in the matrix A. Hence, we can only have a non-trivial kernel if we have less than two rows. This is not sufficient for even detecting a single error, which would require a distance to be equal to two. This is consistent with the fact that the quantum repetition code, with codespace spanned by $|0\ldots0\rangle$ and $|1\ldots1\rangle$, cannot deal with phase errors.

Next, we consider a classical code C, and like to design a corresponding QEC code with maximum distance. As an example, we consider a classical code that comprises of the codewords 000000, 001110, 010101, 011011, 100011, 101101, 110110, and 111000. We like to know if our framework allows us to obtain a QEC code with distance 3. However, when we construct the A matrix using our formalism, we find that its nullspace has dimension 0. Hence, there is

no QEC code with support on computational states labelled by C with distance 3.

However if the designed distance is reduced to 2, then we can use our formalism to derive the following error-detecting quantum code

$$|0_L\rangle = \frac{1}{2}\left(|0,0,0,0,0,0\rangle + |0,1,1,0,1,1\rangle + |1,0,1,1,0,1\rangle + |1,1,0,1,1,0\rangle\right) \quad (19)$$

$$|1_L\rangle = \frac{1}{2}\left(|0,0,1,1,1,0\rangle + |0,1,0,1,0,1\rangle + |1,0,0,0,1,1\rangle + |1,1,1,0,0,0\rangle\right) \quad (20)$$

1.2 Constant-excitation codes with better parameters

When spurious classical fields interact uniformly with a system of spins, an effective unitary evolution $U_\theta = \exp(i\theta(Z_1 + \ldots Z_n))$ acts on the spins. Here Z_i applies a phase flip on the ith qubit and the identity operation on the remaining qubits. The unitary operator U_θ, known as a coherent error [7], can severely damage the qubits, especially when quantum control techniques twirl it into a Pauli error basis which cause U_θ can introduce multiple phase-flip errors on the physical system.

Constant-excitation (CE) codes on n qubits with excitation number w are quantum codes that are supported on computational basis states $|\mathbf{x}\rangle$ where $\mathbf{x}$ are n-bit vectors of Hamming weight w. Since any CE code is a subspace of a fixed eigenspace of the operator $Z_1 + \cdots + Z_n$, CE codes are left invariant under the action of any coherent error U_θ for any θ, and hence completely avoid coherent errors [7]. Therefor, CE codes are advantageous to use when coherent errors are the dominant source of errors in quantum systems.

In the construction of [7], the CE codes are obtained by concatenating any quantum code with the dual-rail code [34]. CE codes obtained through this construction must have an even number of qubits and excitation number equal to half the number of qubits. In [8], constructions of CSS-type CE codes are also discussed, where the number of qubits can be odd (such as in a [[5,1,2]] CE code).

Our formalism in this paper further develops the theory of constant excitation codes. To obtain constant-excitation code of distance d, the key ingredient needed is a classical constant weight code on n bits of distance d that has sufficiently many codewords. Now denote $A(n,d,w)$ as the maximal number of classical codewords in a constant weight code on n bits of distance d and weight w. Then our framework can derive CE codes from such constant weight codes whenever

$$A(n,d,w) \geq \sum_{k=0}^{d-1} \binom{n}{k} \quad (21)$$

for some w. Let $\underline{A}(n,d,w)$ denote any lower bound to $A(n,d,w)$. Then $\underline{A}(n,d,w) \geq \sum_{k=0}^{d-1}\binom{n}{k}$ implies that $A(n,d,w) \geq \sum_{k=0}^{d-1}\binom{n}{k}$. Hence we seek lower bounds on $A(n,d,w)$, which we can obtain from the tables in [35]. Note that any constant weight code has $d \geq 2$, and hence we trivially have $A(n,2,w) = \binom{n}{w}$. Since $\binom{4}{2} \geq 1+4$, our framework allows us to construct a four-qubit CE code with two excitations.

Using lower bounds on $A(n,d,w)$ from [35] where $d = 2, 4$, we obtain a table of CE codes, specifying what n_{new} and n_{prev} are, where n_{new} and n_{prev} denote how many qubits previous CE codes [7, 8] and our CE codes need respectively.

The table illustrates that our CE codes, for a fixed distance, use fewer qubits than previous CE codes.

Distance (d)	n_{prev}	n_{new}
2	5[8], 8 [7]	4 ($w=2$)
4	20 [7]	15 ($w=7,8$)

In the above table, for the constructions using the concatenation framework of [7], the codes used are the four-qubit error detection code concatenated with the dual-rail code, and a [[10,1,4]] stabilizer code concatenated with the dual-rail code. While there might be some other error model in which the dual-rail code might outperform the CE codes we construct, this analysis is beyond the scope of our paper.

Using the quantum Gilbert-Varshamov bound for quantum codes we know that $[[n,1,d]]$ asymptotically exist if $1 - \text{Ent}_4(d/n) \geq 0$. Let $d_{\text{QGV}} \approx 0.18929$ be such that $1 - \text{Ent}_4(d_{\text{QGV}}/n) = 0$. Then concatenation of such codes with dual-rail codes gives CE codes with asymptotic relative distance of $d_{\text{QGV}}/2 \approx 0.0946$. Such CE codes do not attain the quantum Gilbert Varshamov bound.

Next we turn our attention to the asymptotic structure of constant weight codes [35] When the Gilbert bound is applied to constant weight codes, one can obtain [35, Theorem], which provides the lower bound

$$A(n,2\delta,w) \geq \frac{\binom{n}{w}}{\sum_{i=0}^{\delta-1}\binom{w}{i}\binom{n-w}{i}} \geq \frac{\binom{n}{w}}{\binom{w}{\delta}\binom{n-w}{\delta}}. \quad (22)$$

Hence to construct asymptotic CE codes with $w = n/2$, it suffices to require that

$$\binom{n}{n/2}\binom{n/2}{\delta}^2 \geq \sum_{k=0^{2\delta-1}} \binom{n}{k}. \quad (23)$$

or equivalently

$$1 - 2\text{Ent}_2(d/n) \geq 0, \quad (24)$$

where $d = 2\delta$. The maximum possible asymptotic value of d/n is approximately 0.11 which is larger than 0.0946. Hence we prove that there are CE codes that asymptotically outperform those obtained using the concatenation construction of [7].

1.3 Constructing logical states with linear distance and constant rate

In building a single logical qubit we used any one non-zero solution in the kernel of A to identify two disjoint subsets C_0 and C_1. Since the number of rows is $2V_q(d_Z-1)-1$ and the number of columns by Gilbert-Varshamov bound satisfies $m \geq q^n/V_q(d_Z-1)$, from Lemma 2 and the asymptotic relation of the volume of the Hamming ball and the q-ary entropy function, we find that the ratio of the number of columns to the number of rows is asymptotically exponentially large

$$\frac{1}{n}\log_q\left(\frac{m}{\#\text{ rows}}\right) \geq 1 - 2\mathrm{Ent}_q\left(\frac{d_Z}{n}\right) \tag{25}$$

where $d_Z/n \in [0,(q-1)/q]$. Here we exploit this to derive roughly $q^{n(1-2\mathrm{Ent}_q(d_Z/n))}$ logical quantum states, and hence obtaining a linear rate $r \approx (1-2\mathrm{Ent}_q(d_Z/n))$. Below we think of $M \propto m/(\#\text{ rows})$.

We now generalize the construction of two quantum states (a logical qubit) to more quantum states (a logical qu*d*it). Suppose we identify M subsets $\{C_0, C_1, \ldots, C_{M-1}\}$ such that $C_i \subset C$ for all $i \in \{0,\ldots,M-1\}$ and that the subsets are pairwise disjoint $C_i \cap C_j = \emptyset$ for all $i \neq j$. Define the logical qudit as

$$\begin{aligned} |0_L\rangle &= \sum_{\boldsymbol{c}\in C_0} \alpha_{\boldsymbol{c}}^{(0)} |\boldsymbol{c}\rangle \\ |1_L\rangle &= \sum_{\boldsymbol{c}\in C_1} \alpha_{\boldsymbol{c}}^{(1)} |\boldsymbol{c}\rangle \\ &\vdots \\ |(M-1)_L\rangle &= \sum_{\boldsymbol{c}\in C_{M-1}} \alpha_{\boldsymbol{c}}^{(M-1)} |\boldsymbol{c}\rangle\,. \end{aligned} \tag{26}$$

where for every $j = 1,\ldots,M-1$, we have the normalization

$$\sum_{\boldsymbol{c}\in C_0} \left(\alpha_{\boldsymbol{c}}^{(0)}\right)^2 = \sum_{\boldsymbol{c}\in C_j} \left(\alpha_{\boldsymbol{c}}^{(j)}\right)^2 \tag{27}$$

Clearly these states are orthonormal. The KL criteria then writes

$$\Pi\, P\, \Pi = c_P\, \Pi \tag{28}$$

where $\Pi = |0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L| + \cdots + |(M-1)_L\rangle\langle (M-1)_L|$ is a projector of (potentially exponentially large) rank M. The orthogonality and non-deformation conditions now write:

$$\langle i_L|P|j_L\rangle = c_P\,\delta_{i,j}\,, \quad i,j \in \{0,1,2,\ldots,M-1\}\,.$$

We first check orthogonality. Since the subsets are pairwise disjoint and futhermore C has a minimum distance of d_X, we have $\langle i_L|P|j_L\rangle = 0$ for all $i \neq j$ for and all diagonal Paulis. Moreover, $\langle i_L|P|j_L\rangle = 0$ if $1 \leq \mathrm{wt}_X(P) \leq d_X - 1$, which is inherited from the classical code's distance d_X. We now turn our attention to the non-deformation condition. As before it is clear that $\langle i_L|P|i_L\rangle = 0$ for all $i \in \{0,1,\ldots,M-1\}$ and Paulis with $1 \leq \mathrm{wt}_X(P) \leq d_X - 1$. This follows from the distance of the code as before. Therefore, it is again sufficient to prove the non-deformation condition for diagonal Paulis. We need to find the subsets $C_1, C_2, \ldots, C_{M-1}$ such that

$$\langle 0_L|P|0_L\rangle = \langle 1_L|P|1_L\rangle = \cdots = \langle (M-1)_L|P|(M-1)_L\rangle. \tag{29}$$

Our method constructs the sets $C_0,\ldots,C_{M-1}$ such that they are disjoint and satisfy the foregoing equation. Unlike the qubit case, our proof technique will not be seeking a solution in the kernel of A anymore, rather we recursively build the logical quantum states.

An exciting open problem would be to see an alternative construction that uses the exponentially large kernel of the matrix A.

For every new logical state we need to call the following algorithm once:

Algorithm 2. Input: *A set of* $2V_q(d_Z-1)$ *columns of* A *and a vector* $\mathbf{b}$ *of size* $2V_q(d_Z-1)-1$.

- *Check that the augmented homogeneous linear system as described in Section 5 of [36] does not have a row that is all of the same sign.*
- *If no row has non-zero entries of the same sign, apply the algorithm of [36] to find a point in the feasible set, i.e., a solution* $\mathbf{x} \geq 0$. *End the algorithm.*
- *If there is a row that is all of same sign, augment the set of columns by one and repeat. If all the columns are exhausted, then output fail.*

Output: *If succeeded, output a solution* $\mathbf{x} \geq 0$ *in the feasible set.*

If recursively successful, then the algorithm can at least be called $m/2V_q(d_Z-1) = q^{n(1-2\mathrm{Ent}_q(d_Z/n))}$ times. The success is guaranteed if at any step of recursion no row of all the same sign is encountered.

We demonstrate the recursive construction of logical quantum states by first building a qu*trit* (three logical states). Recall that A has $2V_q(d_Z-1)-1$ rows whose first row is all ones, we now proceed to find a natural partitioning of the columns of A. To construct a logical qubit, we use the first $2V_q(d_Z-1)$ columns of A as follows. Let the matrix A_1' be defined by the first $2V_q(d_z-1)$ columns of A. Now solve for the solution $\boldsymbol{x_1}$ in $A_1'\boldsymbol{x} = \mathbf{0}$, where $\boldsymbol{x_1}$ has $2V_q(d_Z-1)$ components. This matrix equation certainly has a non-trivial kernel because it has more columns than rows. Just as in the one logical qubit construction in Alg. 1 we will find an $\boldsymbol{x} = \boldsymbol{x}^+ - \boldsymbol{x}^-$ where $\boldsymbol{x}^+ \geq 0$ and $\boldsymbol{x}^- \geq 0$, $\sum_i x_i^+ = \sum_i x_i^-$, and that $supp(\boldsymbol{x}^+) \cap supp(\boldsymbol{x}^-) = \emptyset$. We build the logical qubit exactly as in Eqs. (10) and (11).

We then rearrange the columns of A_1' according to the supports of $\boldsymbol{x}^+$ and $\boldsymbol{x}^-$ and write the concatenated matrix $[A_1 A_2]$, where A_1 has a set of columns

labeled by codewords c_s such that $s \in supp(\boldsymbol{x}^+)$ and A_2 has columns labeled by codewords c_s such that $s \in supp(\boldsymbol{x}^-)$. The new equation being satisfied is

$$[A_1 A_2] \begin{bmatrix} \boldsymbol{x_1^+} \\ -\boldsymbol{x_1^-} \end{bmatrix} = 0 \,,$$

where $\boldsymbol{x_1^+}, \boldsymbol{x_1^-} \geq 0$. To build the third logical state, we select a set of $2V_q(d_Z - 1)$ new columns out of A and solve

$$[A_2 A_3] \begin{bmatrix} -\boldsymbol{x_1^-} \\ \boldsymbol{x_2} \end{bmatrix} = 0 \,, \quad \boldsymbol{x_2} \geq \boldsymbol{0},$$

where $-\boldsymbol{x_1^-}$ is treated fixed from the previous step and we solve for a solution $\boldsymbol{x_2} \geq 0$. A solution exists as $A_3 \boldsymbol{x_2} = A_2 \boldsymbol{x_1^-}$ is under-constrained. Although this can be formally thought of as a linear programming problem, where the objective function is just zero and a point in the feasible set is sought, we proceed differently and give an explicit algorithm based on Dines' Annals of Math (1926) [36].

Once $\boldsymbol{x_2} \geq 0$ is found this way, we proceed to solve

$$[A_3 A_4] \begin{bmatrix} \boldsymbol{x_2} \\ -\boldsymbol{x_3} \end{bmatrix} = 0 \,, \quad \boldsymbol{x_3} \geq 0,$$

where now $\boldsymbol{x_3}$ is the unknown. Just as before this amounts to solving $A_4 \boldsymbol{x_3} = -A_3 \boldsymbol{x_2}$ where the right-hand side is a known vector. Continuing this way we can build $2 \leq M \leq q^{n(1-2\mathrm{Ent}_q(\frac{d_Z}{n}))}$ logical states.

The results of this section prove the following main theorem of part 1 of this work:

Theorem 1. *Take a random classical code C of length n on a q-ary alphabet with a minimum distance of d_X. Then almost surely with probability equal to 1 as n goes to infinity, we have $|C| \geq 2V_q(d_Z - 1)$. Moreover, using Alg. 1 and multiple calls to Alg. 2 explicitly, we will with probability 1 as n goes to infinity derive the M quantum logical states in (26) with bit- and phase-flip distances of d_X and d_Z respectively. The overall distance is $\min(d_X, d_Z)$.*

When the A matrix is wide (under-constrained) Alg. 1 always constructs two logical codewords (a logical qubit). The third and subsequent logical codewords are found recursively by calling Alg. 2 multiple times. Alg. 2 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. As shown in [36] this is the only way that the algorithm can fail. We define a random classical code as one whose codewords have entries over $\Sigma = \{0, 1, 2, \ldots, q-1\}$ such that each entry is independently and randomly drawn from the uniform distribution over Σ.

Lemma 3. *M quantum logical states can be constructed as long as in each step of the recursion, no row other than the first has entries that are all non-zero and with the same sign. When C is a random classical code, then with high probability, Alg. 2 succeeds in providing a quantum code with constant rate.*

Proof. The first part of the Lemma follows from the proof of Dines [36] applied to every step of the recursion. To prove the second part, first recall that at each step we are solving a linear system with $\rho \equiv 2V_q(d_Z - 1)$ columns and $\rho - 1$ rows. To find positive solutions of this linear system, we employ Dines algorithm which is itself recursive. Hence we will prove that at every step of Dines recursive algorithm, it fails with low probability. We prove this by induction, first starting with the base case.

Recall that $\omega \equiv \exp(2\pi i/q)$. For every diagonal P of weight at least one, $\langle c|P|c\rangle$ is a random variable that takes the values $\{1, \omega, \ldots \omega^{q-1}\}$ with a uniform probability. From Eq. (17) we know that each $\langle c|P|c\rangle$ is equal to a ω^j for some $j \in \{0, 1, \ldots, q-1\}$. That is, $\mathrm{Re}(\langle c|P|c\rangle)$ and $\mathrm{Im}(\langle c|P|c\rangle)$ are random variables that take values in $[-1, 1]$. Since the code words are random and uniformly distributed over the symbols, by symmetry the probability of an entry having a positive (or negative) sign is a half when q is even and is at most $2/3$ when q is odd. Moreover the entries are independent. Hence the probability that a given row has all the same sign is $(3/2)^{-\rho+1}$. And by a union bound, the probability that any of the $\rho - 1$ rows have entries whose all entries have the same sign is $O(\rho\,(3/2)^{-\rho})$.

Now we prove the induction step. We take q to be even for now, which ensure that a_{ij} are symmetric random variables with mean zero. Note that Dines algorithm takes a matrix with matrix elements a_{ij}, and constructs a new matrix $a_{r,ij} = a_{1i}a_{rj} - a_{1j}a_{ri}$. In the new matrix, the indices i and j belong to disjoint sets I and J. The number of columns in the new matrix is $|I||J|$. For the induction hypothesis, we assume that the matrix elements a_{ij} are identical and symmetric random variables with zero mean, which are furthermore independent with respect to the column index j. We will show that $a_{r,ij}$ will then also be a symmetric random variable with zero mean and also furthermore be independent with respect to the new column indices ij.

We now show that the $a_{r,ij}$ has zero mean. For that we see $\mathbb{E}(a_{r,ij}) = \mathbb{E}(a_{1i}a_{rj}) - \mathbb{E}(a_{1j}a_{ri})$ because the expectation is linear. Next the independence of i and j imply that $\mathbb{E}(a_{1i}a_{rj}) = \mathbb{E}(a_{1i})\mathbb{E}(a_{rj})$ and $\mathbb{E}(a_{1j}a_{ri}) = \mathbb{E}(a_{1j})\mathbb{E}(a_{ri})$. Substituting this shows that $\mathbb{E}(a_{r,ij}) = 0$ because a_{ij} are independent random variables with mean zero.

We now note that the random variables $a_{r,ij}$ are independent with respect to the column labels ij. This follows readily from the independence of a_{ij} with respect to j. For instance, treat i to be fixed and consider $a_{r,ij}$ and $a_{r,ij'}$ for $j \neq j'$.

We next show that the random variables $a_{r,ij}$ are

symmetric. For this, we use the fact that the product of non-degenerate symmetric random variables is a symmetric random variable [37].

In the base case, we have shown that a_{ij} satisfies the induction hypothesis with high probability. We have just shown that $a_{r,ij}$ is symmetric, independent, and has zero mean with respect to ij. This proves that its entries have equal probability of being positive or negative.

It remains to bound the probabilities of failure of our algorithm under our recursion and Dines recursion. With high probability, the product $|I||J|$ is going to be greater than the number of columns in a_{ij}. As shrinking the number of columns will only be due to at most one entry of a different sign, this happens with very low probability. The probability of this happening is at most $2\rho(1/2)^{\rho-1}$ for large ρ. The probability of a single row with all the same sign is at most $2(1/2)^{\rho}$. Hence the total probability of a given row being pathological is at most $2(1/2)^{\rho} + 2\rho(1/2)^{\rho-1} = O(\rho(1/2)^{\rho})$. The probability of a matrix at any step of Dines recursion to have a pathological row is therefore at most $O(\rho^2(1/2)^{\rho}))$. Since our algorithm has $O(m/\rho)$ steps, our algorithm's failure probability is at most $O(m\rho(1/2)^{\rho})$. The number of codewords in our q-random code is $m \leq q^n$, and therefore $m2^{-\rho}$ is at most $(q^n 2^{-2^{cn}})$ for some constant $c \in [0,1]$, our algorithm will succeed with overwhelming probability. Although this proof is specialized for the case where q is even, a similar argument will work for q odd. □

In the next section, we find that even if this happens we can always construct *Approximate* Quantum Error Correcting Codes (AQECC) [9] with linear distance and constant rate, provided that, the underlying classical code also has a linear distance and a sufficiently large rate.

1.4 AQECCs with designed rates

In the unlikely case, where building logical quantum states using Alg. 2 of the previous section fails, we can always build an AQECC as we now show. We introduce an algorithm that produces a quantum code with M logical codewords satisfying the KL criteria approximately. Here M can be strictly larger than 2 at the expense of an approximation error, which is equal to the infidelity of quantum code.

Suppose $C_1, \ldots, C_{M/2}$ are disjoint subsets of the classical code C whose minimum distance is d_X. Hence each C_j, $j \in [M/2]$ inherits the distance d_X, where we take M to be even for simplicity. Suppose that for every $j \in [M/2]$, it holds that

$$|C_j| \geq 2V_q(d_Z - 1)\ . \tag{30}$$

For each classical code C_j, we use Alg. 1 to construct a corresponding matrix A_j from which we derive logical codewords $|(2j)_L\rangle, |(2j-1)_L\rangle$ that satisfy the KL criteria for quantum codes with a bit-flip and phase-flip distance of d_X and d_Z respectively.

It is clear from our construction that for every diagonal Pauli P of weight at most $d_Z - 1$,

$$\langle (2j)_L | P | (2j)_L \rangle = \langle (2j-1)_L | P | (2j-1)_L \rangle = \gamma_{j,P} \tag{31}$$

where $\gamma_{j,P}$ is a complex number of norm at most one. Now for each $j \in [M/2]$, let $\Gamma_j = (\gamma_{j,P})$ be a row vector of length $V_q(d_Z - 1)$ with components that correspond to diagonal Paulis of weight at most $d_Z - 1$. Then it follows that each Γ_j lies in a $|V_q(d_Z - 1)|$-dimensional complex unit ball corresponding to a hyper-cube of length two centered at the origin with respect to the infinity norm.

Suppose $\max_{j,k \in [M/2]} \|\Gamma_j - \Gamma_k\|_\infty = \delta$. Then because of Eq. (31) we have

$$\max_{j,k=1,\ldots,M} \max_{P} |\langle j_L | P | j_L \rangle - \langle k_L | P | k_L \rangle| = \delta. \tag{32}$$

It remains to find a suitable upper bound for δ. To relate the error δ in satisfying the non-deformation to the size of the code $|C|$ and the number of logical qubits we can construct, we rely on the following fact.

Fact. *Consider the complex hyper-cube of side length two in N dimensions. Let x be the number of points distributed randomly inside it. Then there exists a ball of radius δ in the infinity norm that contains at least $x(\delta/2)^N$ points in expectation.*

The number of points inside the unit hyper-cube is $x = \lfloor |C|/(2V_q(d_Z - 1)) \rfloor$. The radius of the ball is δ. The dimension of the hyper-cube is $V_q(d_Z - 1)$. Hence from the above fact, we have that the expected number of logical codeword pairs is $\mathbb{E}M = 2x(\delta/2)^N$ which writes

$$\mathbb{E}M \geq 2 \left\lfloor \frac{|C|}{2V_q(d_Z - 1)} \right\rfloor \left(\frac{\delta}{2}\right)^{V_q(d_Z - 1)}. \tag{33}$$

The infidelity ϵ defined by one minus the worst case entanglement fidelity of the quantum code can be upper bounded as shown in [38], to be

$$\epsilon \leq O\left(\delta\ V_q^4(d_Z - 1)\right), \tag{34}$$

when the noisy quantum channel introduces bit-flip and phase-flip weights at most $d_X - 1$ and $d_Z - 1$ uniformly at random.

1.5 Illustrations

In this section we illustrate our framework through a series of examples. It is noteworthy that the first example is a one-to-one correspondence between the celebrated classical and quantum results of Hamming's and Steane's respectively.

1.5.1 C as a [7,4,3] Hamming code gives the Steane code

In classical coding theory, we use the notation (n, m, d) to denote a binary code with codewords of length n that has m codewords, a distance of d. We use $[n, \log_2 m, d]$ to denote a binary code with codewords of length n that has m codewords, a distance of d, and is furthermore a linear code. Consider the case when C is generated from the codewords 1000110, 0100101, 0010011, and 0001111. This classical code is the celebrated [7,4,3] Hamming code, and has been used previously by Steane to obtain the [[7,1,3]] Steane code. Applying our framework to C, we get the unique solution

$$\begin{aligned}|0_L\rangle =& \frac{1}{\sqrt{8}}\left(|0,0,0,0,0,0,0\rangle + |0,0,0,1,1,1,1\rangle\right.\\ &+|0,1,1,0,1,1,0\rangle + |0,1,1,1,0,0,1\rangle\\ &+|1,0,1,0,1,0,1\rangle + |1,0,1,1,0,1,0\rangle\\ &\left.+|1,1,0,0,0,1,1\rangle + |1,1,0,1,1,0,0\rangle\right) \quad (35)\\ |1_L\rangle =& \frac{1}{\sqrt{8}}\left(|0,0,1,0,0,1,1\rangle + |0,0,1,1,1,0,0\rangle\right.\\ &+|0,1,0,0,1,0,1\rangle + |0,1,0,1,0,1,0\rangle\\ &+|1,0,0,0,1,1,0\rangle + |1,0,0,1,0,0,1\rangle\\ &\left.+|1,1,1,0,0,0,0\rangle + |1,1,1,1,1,1,1\rangle\right). \quad (36)\end{aligned}$$

This is in fact equivalent to the Steane code.

1.5.2 C as a nonlinear cyclic code

We now give an example of a quantum code constructed from a non-linear classical code. Take the nonlinear $(4, 8, 2)$ code with codewords that are cyclic permutations of 0001 and 1110. The corresponding kernel of the matrix A has dimension 3, and one solution to this gives an error detecting quantum code with logical codewords

$$|0_L\rangle = \frac{1}{\sqrt{2}}(|0,0,0,1\rangle + |1,1,1,0\rangle) \quad (37)$$

$$|1_L\rangle = \frac{1}{\sqrt{2}}(|0,0,1,0\rangle + |1,1,0,1\rangle). \quad (38)$$

In fact, we can have the additional logical codewords

$$|2_L\rangle = \frac{1}{\sqrt{2}}(|0,1,0,0\rangle + |1,0,1,1\rangle) \quad (39)$$

$$|3_L\rangle = \frac{1}{\sqrt{2}}(|1,0,0,0\rangle + |0,1,1,1\rangle). \quad (40)$$

This gives a quantum code of dimension 4 and a minimum distance of 2. This quantum code is also an example of a CWS code. This is because for every $j = 0, 1, 2, 3$, there is a Pauli operator that takes the stabilizer state $\frac{1}{\sqrt{2}}(|0,0,0,0\rangle + |1,1,1,1\rangle)$ to $|j_L\rangle$. Since this quantum code is CWS, quantum error correction can proceed using formalism developed for CWS codes [5]. This quantum code also has some other attractive properties. First, by inducing cyclic shifts in the underlying qubits, we can move from one logical codeword to another. Second, this quantum code is stabilized by $X^{\otimes 4}$ and is affected uniformly by $Z^{\otimes 4}$. Together, this implies that the quantum code is invariant under transversal X and Y and Z operations.

1.5.3 Permutation-invariant quantum codes

Our quantum code construction formalism can also extend to quantum codes with logical codewords that are supported on non-product basis states. One example of such codes are permutation-invariant quantum codes, which are invariant under any permutation of the underlying particles. Permutation-invariant quantum codes have been explicitly constructed using a variety of different techniques [39, 40, 38, 41, 42, 43]. Recently, permutation-invariant quantum codes have been considered for applications such as for quantum storage [31], or for robust quantum meterology [44], and they can also be prepared in physically realistic scenarios [22].

When permutation-invariant quantum codes are constructed on n qubits, they must be superpositions over Dicke states

$$|D^n_w\rangle = \frac{1}{\sqrt{\binom{n}{w}}} \sum_{\substack{x_1,\ldots,x_N\in\{0,1\}\\ x_1+\cdots+x_n=w}} |x_1\rangle \otimes \cdots \otimes |x_n\rangle. \quad (41)$$

Here w is the weight of the Dicke state, and counts the Hamming weights of its constituent computation basis states' labels. The Dicke states for qubit states are labeled by only their weights, of which there are only $n+1$ possibilities. For our quantum code construction, we can choose the logical states to be supported on $|D^n_{w_1}\rangle, \ldots, |D^n_{w_m}\rangle$ where $w_{j+1} - w_j \geq d$ for any $j = 1, \ldots, m-1$, and d is the desired minimum distance of the quantum code.

When a quantum code is permutation-invariant, we only need to consider equivalence classes of Pauli operators up to a permutation. For Dicke states, $\langle D^n_w|P|D^n_w\rangle$ are not necessarily zero even when the Pauli P is non-diagonal [44], we need to count the number of all Paulis of weight at most $d-1$ up to a permutation. The number of unique qubit-Paulis up to a permutation having a weight of at most w is equal to the number of ways to order a w-tuple in $\{1, 2, 3\}^w$ in a non-decreasing sequence, and this number is just $\binom{n+w-1}{w}$. Hence to total number of Paulis that we need to consider for the non-deformation conditions is at most $\sum_{w=0}^{d-1} 3^w$.

Now we consider a variation of the A-matrix from Alg. 1 with the matrix elements

$$\langle D^n_{w_j}|P|D^n_{w_j}\rangle, \quad (42)$$

where P labels the rows and j labels the columns.

From this, we can get permutation-invariant quantum codes with a minimum distance of d whenever

$$(\lfloor n/d \rfloor + 1) \geq 1 + \sum_{w=0}^{d-1} 3^w. \tag{43}$$

For instance, when $d = 3$ this inequality becomes

$$\lfloor n/3 \rfloor \geq (1 + 13), \tag{44}$$

and this formalism show that we can get gives permutation-invariant codes with a distance of $d = 3$ when $n \geq 42$. This bound is however loose, because there are permutation-invariant quantum codes with $d = 3$ on 9 qubits [39, 38], and even on 7 qubits [40]. This suggests that rather than using loose bounds on the nullity of the A matrix in Alg. 1, we need to exploit additional structure about the kernel of A to realize the full potential of our formalism.

1.5.4 Remarks on optimality

If we take the metric of optimality to be maximization of the distance d for fixed length n and number of encoded qubits k, then our construction is not optimum. This is because the five-qubit code is the unique [[5,1,3]] code, and our framework does not encompass it. To see this, note that the classical codewords on which the [[5,1,3]] code is supported on comprise of a distance-1 classical code.

We demonstrate examples of optimal quantum codes using our framework which use the Hamming code and a nonlinear cyclic code in Sec. 1.5.1 and Sec. 1.5.2 respectively.

1.6 Recovery procedure

If a quantum code satisfies the KL criteria [6] exactly, we can use the KL procedure (Ref. [6]) to construct explicit recovery maps for the quantum code. We briefly review this recovery procedure.

Given an M-dimensional quantum code, the correctible subspaces reside within a space spanned by $W_1|k_L\rangle, \ldots, W_w|k_L\rangle$, where $k \in \{0, 1, \ldots, M-1\}$ and W_j are matrices that we call correctible errors. Using any Gram-Schmidt procedure on $W_1|k_L\rangle, \ldots, W_w|k_L\rangle$ for every $k \in \{0, 1, \ldots, M-1\}$, we obtain a set of orthonormal states

$$|F_{k,1}\rangle, \ldots, |F_{k,r}\rangle.$$

Here r is the dimension of the space spanned by $W_1|k_L\rangle, \ldots, W_w|k_L\rangle$, and is identical for every k. For any such Gram-Schmidt decomposition, and for any $j \in [r]$, we can form the projectors

$$P_j = \sum_{k=0}^{M-1} |F_{k,j}\rangle\langle F_{k,j}|. \tag{45}$$

From the KL criteria, these projectors are pair-wise orthogonal, and we can derive the corresponding unitary operators U_j so that the recovery operation with Kraus operators $U_j P_j$ will correct all errors spanned by the elements of the correctible set Ω. These Kraus operators correspond to the operational procedure of first performing projective measurements given by the projectors $\{P_1, \ldots, P_r\}$, obtaining an error syndrome j that corresponds to the projector P_j, and applying a conditional unitary operation U_j to complete the recovery procedure.

This KL recovery procedure does not guarantee a priori efficient implementations of these recovery maps. Indeed, the complexity of these projective measurements and conditional unitary operations when decomposed into individual experimentally accessible operations or quantum-gate sequences remains to be elucidated. We believe that a constructing a systematic and efficient decoding scheme that is compatible with our quantum coding framework is an important milestone to be achieved in bringing our quantum codes closer toward implementation.

2 Part 2: Linear distance codes in ground space of local Hamiltonians

2.1 Local Hamiltonian and its ground space

Let us consider a spin chain of length n with open boundary conditions and the local Hilbert space dimension of $2s + 1$, where $s \geq 1$ is a positive integer. We take a representation in which $|j\rangle$ denotes the $s_z = j$ state of a spin-s particle:

$$\hat{S}_z|j\rangle = j\ |j\rangle, \qquad j \in \Sigma \quad .$$

The local Hamiltonian whose ground space will be shown to contain a nontrivial quantum error correcting code is

$$H_n = H_n^J + H_n^s \tag{46}$$

where $H_n^J = J \sum_{k=1}^n (|0\rangle\langle 0|)_k$. Recall that the Hamiltonian H_n^s, is defined by

$$H_n^s = \sum_{k=1}^{n-1} \left\{ \sum_{m=-s}^{s} P_{k,k+1}^m + \sum_{m=1}^{s} Q_{k,k+1}^m \right\}, \tag{47}$$

and the local terms are projectors acting on two neighboring spins $k, k+1$ defined by

$$\begin{aligned} P^m &= |0 \leftrightarrow m\rangle\langle 0 \leftrightarrow m| \\ Q^m &= |00 \leftrightarrow \pm m\rangle\langle 00 \leftrightarrow \pm m|; \end{aligned} \tag{48}$$

where

$$|0 \leftrightarrow m\rangle \equiv \frac{1}{\sqrt{2}} [|0, m\rangle - |m, 0\rangle] \tag{49}$$

$$|00 \leftrightarrow \pm m\rangle \equiv \frac{1}{\sqrt{2}} [|0, 0\rangle - |m, -m\rangle], \tag{50}$$

and we denoted by $|j,k\rangle$ the spin state $|s^z_k = j, s^z_{k+1} = k\rangle$. There are $3s$ local projectors as $P^0_{k,k+1}$ automatically vanishes. See Fig. 4.

In the simplest form $s = 1$, and we have

$$H^1_n = \frac{1}{2}\sum_{k=1}^{n-1} \{|0 \leftrightarrow 1\rangle\langle 0 \leftrightarrow 1| + |0 \leftrightarrow -1\rangle\langle 0 \leftrightarrow -1| + |00 \leftrightarrow \pm 1\rangle\langle 00 \leftrightarrow \pm 1|\} ,$$

where $|1 \leftrightarrow 0\rangle \propto |0,1\rangle - |1,0\rangle$, $|-1 \leftrightarrow 0\rangle \propto |0,-1\rangle - |-1,0\rangle$, and $|\pm 1 \leftrightarrow 00\rangle \propto |0,0\rangle - |1,-1\rangle$. Below we will be mostly interested in $s > 1$, because the case of $s = 1$ has a ground space of dimension too small for us to construct non-trivial QEC codes, and the case of $s > 1$ offers a ground space of large enough dimension for us to construct non-trivial QEC codes.

Lemma 4. *Suppose $H_1 \geq 0$ and $H_2 \geq 0$, and $H_1 + H_2$ is a frustration free (FF) Hamiltonian with zero energy ground state. Then the ground space of $H_1 + H_2$ coincides with the intersection of the ground spaces of H_1 and H_2.*

Proof. Any state in the intersection of the kernels of H_1 and H_2 automatically vanishes on $H_1 + H_2$. Conversely, a state $|\psi\rangle$ that is in the kernel of the sum $H_1 + H_2$ obeys $\langle\psi|(H_1 + H_2)|\psi\rangle = 0$. Since each summand is a positive operator, so is their sum, and for $|\psi\rangle$ to be a zero energy ground state of $H_1 + H_2$ it has to vanish on each summand $\langle\psi|H_i|\psi\rangle = 0$ for $i = 1, 2$. Therefore $|\psi\rangle$ is a FF ground state of each H_i as well. □

It is clear that

$$\mathrm{spec}(H^J_n) = J\{0, 1, 2, \ldots, n\} \tag{51}$$

whose gap we denote by $\Delta(H^J_n) = J$. The kernel of H^J_n is the span of all product states $|\mathbf{t}\rangle$ of weight n, where $\mathbf{t} \in \Sigma^n_*$; note that the letter 0 is excluded in these strings.

We will obtain the ground space of H_n by taking the intersection of the ground space of H^J_n with H^s_n. We proceed to analytically derive the ground space of H^s_n after preliminary definitions. From now we assume that m is a positive integer unless stated otherwise.

Since H^s_n is free of the sign problem (i.e., stoquastic), the local projectors define an effective Markov chain, which have the correspondence shown in Table 1.

We say two strings $\mathbf{t}, \mathbf{z}$ are equivalent, denoted by $\mathbf{t} \sim \mathbf{z}$ if $\mathbf{z}$ can be reached from $\mathbf{t}$ by applying a sequence of the local moves defined in the table. We define a set of equivalence classes as follows. Let k denote the number of nonzero letters in a product state (Eq. (52)). Using a consecutive set of the local moves stated above, we can take any state $\ldots m0\ldots0(-m)\cdots \rightarrow \ldots0\ldots0m(-m)0\ldots0\cdots \rightarrow \ldots0000\ldots$. We then move all the zeros to the rightmost end and ensure that all strings are of the form

$$c_{x_1,\ldots,x_k} = x_1\ldots x_k \underbrace{0\ldots0}_{n-k} \tag{52}$$

where $x_i \in \Sigma_*$. By assumption the string $x_1\ldots x_k$ cannot be further reduced and $n-k$ is the maximum number of zeros. Then it follows that if $x_i = m$ then it must *not* have to its immediate right an $x_{i+1} = -m$ for otherwise the annihilation rule $(m, -m) \rightarrow 00$ would further reduce it.

Lemma 5. *Any string $\mathbf{t} \in \Sigma^n$ is equivalent to one and only one $c_{x_1,\ldots,x_k}$ (Eq. (52)).*

Proof. By applying the local moves in the table above to any string $\mathbf{t}$, one can make sure that there are no substrings $m(-m)$ or $m0\cdots0(-m)$ for any $m \in [s]$, where $[s] = \{1, 2, \ldots, s\}$. Now suppose we apply these moves to $\mathbf{t}$ as much as possible to bring it as close as possible to the state of all zeros. Then if $\mathbf{t}$ contains a single m, then the first non-zero letter to its right cannot be $-m$. Similarly if $\mathbf{t}$ contains at least one $-m$ then the first non-zero letter to its left must not be m. By applying $0(-m) \rightarrow (-m)0$ and $0m \rightarrow m0$ we move all the zeros to the right to obtain a string of the form given by Eq. (52). To prove that the set of all strings equivalent to $c_{x_1,\ldots,x_k}$ is indeed an equivalence class, we need to prove that the classes are distinct. It is clear that any string is equivalent to itself (reflexive). If $\mathbf{x} \sim \mathbf{y}$ and $\mathbf{y} \sim c_{x_1,\ldots,x_k}$ then $\mathbf{x} \sim c_{x_1,\ldots,x_k}$ (transitive). Lastly if $\mathbf{x} \sim \mathbf{y}$, then $\mathbf{y} \sim \mathbf{x}$ because of the reversibility of the local moves (symmetric). Therefore indeed the set of strings equivalent to $c_{x_1,\ldots,x_k}$ form an equivalence class and it is an elementary fact that equivalence classes are distinct and partition the state space (i.e., the set of all strings) into disjoint subsets. □

Lemma 6. *The uniform superposition of all strings in an equivalence class (i.e., equivalent to the irreducible string in Eq. (52)) is a (frustration free) zero energy ground state of H^s_n.*

Proof. The Hamiltonian H^s_n in Eq. (47) is a sum of local projectors (Eq. (48)). If a ground state ψ vanishes on each local projector, then for any $m \in [s]$ it must obey $\langle\psi|0m\rangle = \langle\psi|m0\rangle$, $\langle\psi|0(-m)\rangle = \langle\psi|(-m)0\rangle$ and $\langle\psi|00\rangle = \langle\psi|m(-m)\rangle$. It follows that ψ has the same amplitude on a pair of equivalent strings $\mathbf{s} \sim \mathbf{t}$, which means $\langle\psi|\mathbf{s}\rangle = \langle\psi|\mathbf{t}\rangle$. It follows that the ground subspace of H^s_n is frustration free and is spanned by the pairwise orthogonal states

$$|c_{\mathbf{x_k}}\rangle \propto \sum_{\mathbf{s}\sim c_{\mathbf{x_k}}} |\mathbf{s}\rangle \tag{53}$$

where to simplify the notation, we denoted $\mathbf{x_k} = (x_1, \ldots, x_k)$. Clearly each distinct $\mathbf{x_k}$ results in a distinct ground state $|c_{\mathbf{x_k}}\rangle$. □

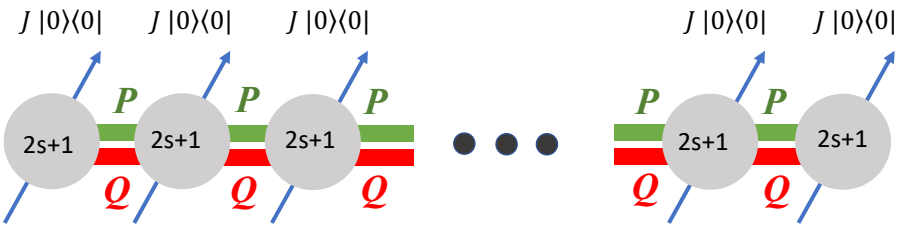

Figure 4: The new local integer spin-s Hamiltonian H_n.

The ground states can be highly entangled. However, among the many ground states there is a substantial subset that are all product states, i.e., $k = n$. We will use these to construct quantum error correcting codes. Before doing so let us answer: How many product state ground states are there?

Let T_n be the set of all *allowed* $2s$-ary strings $\mathbf{t} = t_1 t_2 \dots t_n$ of length n defined by

$$T_n \equiv \{\mathbf{t} \in \Sigma_*^n \mid \text{if } t_j = m, m \in [s], \text{ then } t_{j+1} \neq -m\}\,. \tag{54}$$

Let $|T_n|$ be the size of this set. Since $T_0 = \emptyset$ and $T_1 = \Sigma_*$, we have that $|T_0| = 1$ and $|T_1| = 2s$.

Lemma 7. *$|T_{n+2}| = 2s|T_{n+1}| - s|T_n|$, with $|T_0| = 1$ and $|T_1| = 2s$. We have*

$$|T_n| = \frac{s^n \left\{(1+\bar{s})^{n+1} - (1-\bar{s})^{n+1}\right\}}{2\sqrt{1-1/s}}, \tag{55}$$

where $\bar{s} = \sqrt{1-1/s}$. Asymptotically, for $n \gg 1$, it holds that

$$|T_n| \approx \frac{1+\sqrt{1-1/s}}{2\sqrt{1-1/s}} \left[s(1+\sqrt{1-1/s})\right]^n. \tag{56}$$

Proof. We prove this by induction, any $\mathbf{t} \in T_n$ is $\mathbf{t} = t_1 \dots t_n$, where $t_j \in \Sigma_*$. Since t_1 can be either a m or $-m$ for some $m \in [s]$, $\mathbf{t}$ is either $\mathbf{t} = (-m)\mathbf{t}'$, where the string $\mathbf{t}' \in T_{n-1}$ or $\mathbf{t} = m\mathbf{t}'$ where $\mathbf{t}'$ denotes the subset of strings in T_{n-1} that do not start with the letter $-m$, i.e., $t_1' \neq -m$. The number of strings $\mathbf{t} = (-m)\mathbf{t}'$ with $\mathbf{t}' \in T_{n-1}$ is clearly $s|T_{n-1}|$. Now the set of all string $\mathbf{t} = m\mathbf{t}'$ with $t_1' \neq -m$ coincides with the set that excludes the strings $\mathbf{t} = m(-m)\mathbf{t}''$ where $\mathbf{t}'' \in T_{n-2}$. Since m takes on s different values, we have that the number of strings $\mathbf{t} = m\mathbf{t}'$ with $t_1' \neq (-m)$ is $s\,(|T_{n-1}| - |T_{n-2}|)$.

The total size of the set is then $|T_n| = 2s|T_{n-1}| - s|T_{n-2}|$, which is a linear recursion of second order with initial conditions $|T_0| = 1$ and $|T_1| = 2s$. Shifting the indices to reflect $|T_0|$ and $|T_2|$ as the starting values, we have

$$|T_{n+2}| = 2s|T_{n+1}| - s|T_n|.$$

The solution is elementary and of the form $|T_n| = Ar_+^n + Br_-^n$, where the two roots $r_\pm$ are $r_\pm = s(1 \pm \sqrt{1-1/s})$ and $A = \frac{1+\sqrt{1-1/s}}{2\sqrt{1-1/s}}$, $B = \frac{-1+\sqrt{1-1/s}}{2\sqrt{1-1/s}}$ are obtained from the initial conditions $|T_0| = 1$ and $|T_1| = 2s$. This proves Eq. (55) and the observation $(1 - \sqrt{1-1/s}) < 1$ proves the asymptotic formula Eq. (56). □

In the limit we have $\lim_{s\to 1} |T_n| = n+1$, which is the number of distinct product ground states $|(-)_1 \dots (-)_p (+)_{p+1} \dots (+)_n\rangle$ where $p \in \{0, 1, \dots, n\}$ with $p = 0$ corresponding to $|+ + \cdots +\rangle$.

Corollary 1. *The dimension of the kernel of H_n^s is $\sum_{k=0}^n |T_k| = \frac{\left(-2+r_+^{n+1}+r_-^{n+1}\right)}{2(s-1)}$, where $r_\pm \equiv s(1 \pm \sqrt{1-1/s})$. Asymptotically we have $\dim(\ker(H_n^s)) \approx r_+^{n+1}/[2(s-1)]$.*

Proof. The total number of equivalent classes is the dimension of the kernel. For each $k \in [n]$ there are $|T_k|$ equivalent classes and we have

$$\dim(\ker(H_n^s)) = \sum_{k=0}^n |T_k| = \frac{r_+^{n+1} + r_-^{n+1} - 2}{2(s-1)}.$$

□

Remark 3. *The fraction of product state ground states is a constant independent of n*

$$\frac{|T_n|}{\sum_{k=0}^n |T_k|} = \sqrt{\frac{s-1}{s}} \left[\frac{1 - (r_-/r_+)^{n+1}}{1 + (r_-/r_+)^{n+1} - 2r_+^{-n-1}}\right] \approx \sqrt{\frac{s-1}{s}} \quad , \quad s > 1 \quad ;$$

whereas for $s = 1$, $\lim_{s\to 1} \dim(\ker(H_n^s)) = \frac{1}{2}(n+1)(n+2)$ and the fraction vanishes with the system's size as $2/(n+2) \approx 2/n$.

We now return to the ground space of H_n.

Lemma 8. *Ground space of $H = H_n^s + H_n^J$ with $J > 0$ coincides with the span of the equivalent classes $|c_{\mathbf{x_n}}\rangle$, which are all product states. The ground space dimension is $|T_n|$.*

Proof. The set of FF ground states of H_n^s is given by Eq. (53) in Lemma 6. The kernel of $J\sum_{k=1}^n (|0\rangle\langle 0|)_k$ is the span of all product states of weight n, i.e., states $|\mathbf{t}\rangle$ where $\mathbf{t} \in \Sigma_*^n$. By Lemma 4 the intersection of the two is $|c_{\mathbf{x_n}}\rangle$, which we recall are the product states of the irreducible strings of weight n and there are $|T_n|$ of them (Eqs. (55) and (56)). □

2.2 Constructing good quantum codes in the ground space

In this section we construct quantum codes that are supported on a selected subset of computational basis states that lie within the kernel of our 2-local Hamiltonian. We show that these quantum codes that encode a single logical qubit can have a linear distance.

Recall that the standard local spin states are $|j\rangle$, with $j \in \Sigma = \{-s, \ldots, +s\}$. We also define the non-zero alphabet $\Sigma_* \equiv \{-s, \ldots, -1, +1, \ldots, s\}$. Clearly $|\Sigma| = 2s+1$ and $|\Sigma_*| = 2s$. Define the generalized (non-Hermitian) Pauli operators in terms of these basis states as

$$X = \sum_{j \in \Sigma_c} |j\rangle\langle j+1| \,, \qquad Z = \sum_{j \in \Sigma_c} \omega^j |j\rangle\langle j| \quad ,$$

where $\omega = \exp(2\pi i/(2s+1))$ is a root of unity, and by Σ_c, we mean the set Σ with the cyclic property that $s+1 = -s$ and $-s-1 = +s$. We denote by X_k and Z_k the generalized Pauli operators that act on the k^{th} spin (qudit) and act trivially on the rest.

Recall that $\ker(H_n)$ is spanned by certain product states of weight n. We denote the basis of $\ker(H_n)$ by $\mathcal{T}_n$ where

$$\mathcal{T}_n = \{|\mathbf{t}\rangle \ : \ \mathbf{t} \in T_n\}$$

and T_n is defined in Eq. (54).

The quantum code that we construct will be a two-dimensional subspace of $\mathcal{T}_n$. In general, the logical codewords can be supported on an exponential number of basis states in $\mathcal{T}_n$. However, we select a subset of computational basis states labels $C \subset T_n$ such that the minimum Hamming distance of C is at least $2t+1$, where t is the designed maximum number of correctable errors. The set of labels C has the interpretation as a classical code, and we denote its distance by $\mathrm{dist}(C)$:

$$\mathrm{dist}(C) \equiv \min\{\mathrm{dist}(\mathbf{t}, \mathbf{t}') \mid \mathbf{t}, \mathbf{t}' \in T_n \ , \ \mathbf{t} \neq \mathbf{t}'\} \ ,$$

and

$$\mathrm{dist}(\mathbf{t}, \mathbf{t}') = |\{t'_i \neq t_i \ : \ i \in [n]\}|$$

is the usual Hamming distance between codewords $\mathbf{t}, \mathbf{t}' \in \Sigma_*^n$. The logical codewords of our quantum code will be supported only on the set of basis sets labeled by the classical code C.

Since the basis are product states, finding the subset C with the desired distance can be seen as a problem in classical coding theory. For example, when $s = 2$ one can map the elements of T_n to $\mathbb{F}_4^n$ and use the properties of quartenary codes over $\mathbb{F}_4^n$ to derive a classical code with the prescribed distance. For instance, one can apply the mapping

$$\varphi(1) = 0 \,, \quad \varphi(-1) = 1 \,, \quad \varphi(2) = a \,, \quad \varphi(-2) = b \,, \tag{57}$$

where $\mathbb{F}_4 = \{0, 1, a, b\}$, $b = a+1$ and $a^3 - 1 = 0$, and for every $\mathbf{t} = t_1 \ldots t_n \in T_n$, define $\varphi(t_1 \ldots t_n) = (\varphi(t_1), \ldots, \varphi(t_n))$.

Our strategy is to construct a code C over $\mathbb{F}_4^n$ that has a guaranteed minimum distance and delete all codewords in it that have the forbidden substrings (01) and (ab) to obtain a code C'. Then we let $C = \varphi^{-1}(C')$, which will be the strings that define the computational (product) basis states.

Here, we prove that there are quantum codes within $\ker(H_n)$ that have linear distance in n. We leverage on the existence of good binary codes. The relative distance of a code is the ratio of its distance to its length. Good binary codes are defined as binary codes with positive relative distance. To use the results from binary codes, we define a map β from the binary symbols 0 and 1 to 2 and 1 respectively. It is then easy to see that given any binary code C, $\beta(C)$ is guaranteed to be a feasible subset of T_n, and hence we may use $\beta(C)$ to construct our quantum code.

Our main theorem is:

Theorem 2. *Let $0 < \tau \leq 1/4$ be a real and positive constant. There exist quantum codes in $\ker(H_n)$ that encode one logical qubit and have the distance of $2\tau n$ whenever*

$$\mathrm{Ent}_2(2\tau) + \mathrm{Ent}_{2s+1}(2\tau)\log_2(2s+1) + o(1) \leq 1. \tag{58}$$

Second, there are explicit quantum codes which encode one logical qubit with a distance of $2\tau n$ whenever

$$1/2 - \tau/0.11 \geq \log_2(2s+1)\mathrm{Ent}_{2s+1}(2\tau). \tag{59}$$

Remark 4. *We call the constructions given by optimizing (58) and (59) as the Gilbert-Varshamov (GV) [16, Chpt. 1] and Justesen construct [16, Chpt. 10, Thm. 11] respectively. The GV construct arises from choosing a random C, while the Justesen construct uses the classical Justesen code to define C.*

Proof. To prove the first result, we use random coding arguments. Namely, we turn our attention to random binary codes. By the Gilbert-Varshamov bound [16, Chapter 1], we know that such binary codes are almost surely good binary codes. Moreover we know that for any positive integer t, there exists a classical binary code C that corrects $2t+1$ errors where

$$|C| \geq 2^n / V_2(2t). \tag{60}$$

Using Lemma 2, by setting $C = \beta(C)$, this implies that if

$$2^n / V_2(2t) \geq 2V_{2s+1}(2t), \tag{61}$$

then there exists some quantum code encoding a single qubit in $\ker(H_n)$ that also corrects $t = \tau n$ errors. Since the inequality (61) is equivalent to the (58), the first result of our theorem follows.

The second result follows from using Justesen's concatenated construction, which gives binary codes of with asymptotically linear distance and positive

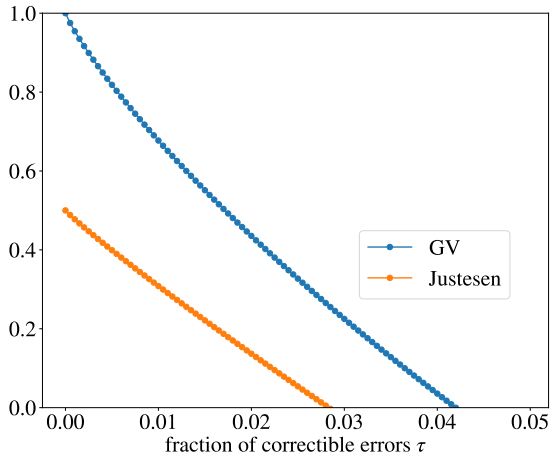

Figure 5: The vertical axis is equal to $\dim(\ker(\log_n(|A|)))$, which gives a lower bound on the size of the kernel of the A matrix in log-scale. The horizontal axis is $\tau = t/n$, where t denotes the number of correctable errors for our quantum code in the ground space of $\ker(H_n)$. The length n is taken to be asymptotically large. This demonstrates that there are linear distance quantum codes in the ground space of the frustration-free 2-local Hamiltonian H_n.

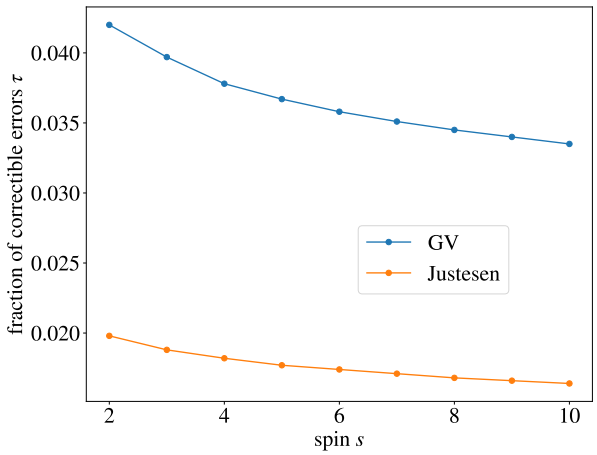

Figure 6: The vertical axis is $\tau = t/n$, where t denotes the number of correctable errors for our quantum code in the ground space of $\ker(H_n)$. The horizontal axis is the spin number our spin-chain.

rate [16][Chapter 10, Theorem 11]. More specifically, a binary Justesen code C_{Justesen} is a concatenated code, with a Reed-Solomon outer code on the finite field of dimension 2^m as the outer code, and distinct inner codes each encoding m bits into $2m$ bits. When C_{Justesen} has a length of n, the length of the Reed-Solomon outer code is $n/(2m)$. Each inner code is a binary code and has rate 1, and is a distinct mapping from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2^{2m}$. The relative distance $\delta = d/n$ of this family of Justesen codes is given by

$$\delta \geq 0.110(1 - 2\log_2 |C_{\text{Justesen}}|/n) + o(1). \tag{62}$$

Rearranging this inequality and using $\tau = \delta/2$, we get

$$\log_2 |C_{\text{Justesen}}| \geq n(1/2 - \tau/0.11 + o(1)). \tag{63}$$

Hence the number of codewords of a Justesen code with distance $2t + 1$ is asymptotically at least $2^{n(1/2-9.1\tau+o(1))}$. Now we set $C = \beta(C_{\text{Justesen}})$, and use Lemma 2 to find that a quantum code in the ground space of $\ker(H_n)$ that corrects asymptotically τn errors exists whenever $\tau < (2s)/(2s+1)$ and the inequality (59) holds. □

Using (59) and (63), we plot the attainable values of τ for different values of spins in Fig. 5.

In the next two sections we illustrate explicit quantum codes on 8 and 6 qudits respectively. These quantum code were obtained from punctured variants of the classical ternary Golay code, where by punctured we mean that the first three symbols of the code were ignored for the 8 qudit code, and five symbols were ignored for the 6 qudit code.

We furthermore use (59) and (63) to plot the fraction of correctible errors attainable for spin chains of different spin if we use QEC codes constructed using either random classical codes or Justesen codes.

2.2.1 A ground subspace Steane code that corrects a single error

By slightly modifying the 7-qubit Steane code, we can embed it in the ground space of H_7. Namely, on the set of computational basis vectors, we can apply the map $|0\rangle \to |1\rangle$ and $|1\rangle \to |2\rangle$. This also corresponds to the quantum code with logical codewords

$$\begin{aligned}|0_L\rangle =& \frac{1}{\sqrt{8}}(|1,1,1,1,1,1,1\rangle + |1,1,1,2,2,2,2\rangle \\ &+|1,2,2,1,2,2,1\rangle + |1,2,2,2,1,1,2\rangle \\ &+|2,1,2,1,2,1,2\rangle + |2,1,2,2,1,2,1\rangle \\ &+|2,2,1,1,1,2,2\rangle + |2,2,1,2,2,1,1\rangle)\end{aligned} \tag{64}$$

and

$$\begin{aligned}|1_L\rangle =& \frac{1}{\sqrt{8}}(|1,1,2,1,1,2,2\rangle + |1,1,2,2,2,1,1\rangle \\ &+|1,2,1,1,2,1,2\rangle + |1,2,1,2,1,2,1\rangle \\ &+|2,1,1,1,2,2,1\rangle + |2,1,1,2,1,1,2\rangle \\ &+|2,2,2,1,1,1,1\rangle + |2,2,2,2,2,2,2\rangle).\end{aligned} \tag{65}$$

Using the KL criteria, we can verify that this quantum code corrects any single error.

2.2.2 A ground subspace code on eight spins that corrects a single error

Here, we give an example of a quantum code that lies in the kernel of H_n^s for $n = 8$ and $s = 2$. This quantum code encodes a single logical qubit, corrects an

arbitrary one-qubit error, and has logical codewords

$$\begin{aligned}|0_L\rangle =&(|\phi_0\rangle|\theta_0\rangle + |\phi_1\rangle|\theta_1\rangle + |\phi_2\rangle|\theta_2\rangle \\ &+ |\phi_3\rangle|\theta_3\rangle + |\phi_4\rangle|\theta_4\rangle + |\phi_5\rangle|\theta_5\rangle)/\sqrt{6} \\ |1_L\rangle =&(|\phi_1\rangle|\theta_4\rangle + |\phi_0\rangle|\theta_3\rangle + |\phi_3\rangle|\theta_0\rangle \\ &+ |\phi_2\rangle|\theta_5\rangle + |\phi_5\rangle|\theta_2\rangle + |\phi_4\rangle|\theta_1\rangle)/\sqrt{6}, \end{aligned} \tag{66}$$

where

$$\begin{aligned}|\phi_0\rangle &= |1,1,1,-2\rangle, \\ |\phi_1\rangle &= |1,-2,-1,-1\rangle, \\ |\phi_2\rangle &= |-1,-2,-2,-1\rangle, \\ |\phi_3\rangle &= |-1,-1,1,1\rangle, \\ |\phi_4\rangle &= |2,-1,-1,1\rangle, \\ |\phi_5\rangle &= |2,1,-2,-2\rangle, \end{aligned} \tag{67}$$

and

$$\begin{aligned}|\theta_0\rangle &= |-2,2,2,1\rangle, \\ |\theta_1\rangle &= |1,-2,-2,-2\rangle, \\ |\theta_2\rangle &= |-1,2,2,1\rangle, \\ |\theta_3\rangle &= |-2,-2,-2,-2\rangle, \\ |\theta_4\rangle &= |1,2,2,1\rangle, \\ |\theta_5\rangle &= |-1,-2,-2,-2\rangle. \end{aligned} \tag{68}$$

The KL criteria for correcting a single error using this quantum code are satisfied. Also this code is not a CWS code. To see this, note that for any stabilizer state made using qudits of dimension 5 (a prime number), the number of computational basis states over which they are superposition over must be a power of 5. However the logical codewords the 8-qudit code are superpositions over 6 computational basis states, and 6 is not a power of 5. Hence there does not exist any Pauli that takes either of logical codewords to a stabilizer state. Hence, the 8-qudit code is not a CWS code. Therefore, we have an example of a quantum code that falls outside of the CWS, stabilizer and CSS quantum coding formalisms.

Next we point out that the quantum code in (66) has a concatenated structure. The logical codewords of the outer code, given in (66) are simply maximally entangled states on two six-level systems.

From the structure of the inner codes, it is clear that to perform a logical bit-flip on our quantum code, it suffices to induce the transition $|-2,-2,-2\rangle \leftrightarrow |2,2,1\rangle$ on the last three spins. Performing other logical computation operations is significantly more complicated and we leave this for future work.

2.2.3 A ground subspace code that detects a single error

We also construct an error detecting quantum code (distance equal to 2) on six spins with $s = 2$ using the logical operators

$$|0_L\rangle = \frac{|1,1,2,1,-2,1\rangle \ + \ |-2,1,-2,-2,2,2\rangle}{\sqrt{2}} \tag{69}$$

$$|1_L\rangle = \frac{|1,1,-2,-2,2,1\rangle \ + \ |-2,1,2,1,-2,2\rangle}{\sqrt{2}}. \tag{70}$$

Such a construction is not unique, and we have many other error detecting codes on six spins.

Acknowledgement

RM acknowledges funding from the MIT-IBM Watson AI Lab under the project *Machine Learning in Hilbert space*. The research was supported by the IBM Research Frontiers Institute. YO acknowledges support from the EPSRC (Grant No. EP/M024261/1) and the QCDA project (Grant No. EP/R043825/1) which has received funding from the QuantERA ERANET Cofund in Quantum Technologies implemented within the European Union's Horizon 2020 Programme. YO also acknowledges support from EPSRC (Grant No. EP/W028115/1).

References

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

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

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

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

[5] 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. (2008).

[6] Emanuel Knill and Raymond Laflamme. "Theory of quantum error-correcting codes". Phys. Rev. A **55**, 900–911 (1997).

[7] Yingkai Ouyang. "Avoiding coherent errors with rotated concatenated stabilizer codes". npj Quantum Information **7**, 1–7 (2021).

[8] Jingzhen Hu, Qingzhong Liang, Narayanan Rengaswamy, and Robert Calderbank. "Mitigating coherent noise by balancing weight-2 z-stabilizers". IEEE Transactions on Information Theory **68**, 1795–1808 (2021).

[9] Debbie W Leung, M A Nielsen, I L Chuang, and Y Yamamoto. "Approximate quantum error correction can lead to better codes". Phys. Rev. A **56**, 2567 (1997).

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

[11] Alexei Kitaev. "Anyons in an exactly solved model and beyond". Annals of Physics **321**, 2 – 111 (2006).

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

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

[14] 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 (2019).

[15] Thomas C Bohdanowicz, Elizabeth Crosson, Chinmay Nirkhe, and Henry Yuen. "Good approximate quantum ldpc codes from spacetime circuit hamiltonians". In Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing. Pages 481–490. (2019).

[16] F J MacWilliams and N J A Sloane. "The Theory of Error-Correcting Codes". North-Holland publishing company. (1977). First edition.

[17] 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**, 43029 (2009). url: http://stacks.iop.org/1367-2630/11/i=4/a=043029.

[18] Martina Gschwendtner, Robert König, Burak Şahinoğlu, and Eugene Tang. "Quantum error-detection at low energies". Journal of High Energy Physics **2019**, 1–81 (2019).

[19] 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**, 13278–13282 (2016).

[20] P O Boykin, T Mor, M Pulver, V Roychowdhury, and F Vatan. "On universal and fault-tolerant quantum computing: a novel basis and a new constructive proof of universality for Shor's basis". In Foundations of Computer Science, 1999. 40th Annual Symposium on. Pages 486–494. (1999).

[21] Andreas Bärtschi and Stephan Eidenbenz. "Deterministic preparation of Dicke states". In International Symposium on Fundamentals of Computation Theory. Pages 126–139. Springer (2019).

[22] Chunfeng Wu, Yimin Wang, Chu Guo, Yingkai Ouyang, Gangcheng Wang, and Xun-Li Feng. "Initializing a permutation-invariant quantum error-correction code". Phys. Rev. A **99**, 012335 (2019).

[23] Mattias T Johnsson, Nabomita Roy Mukty, Daniel Burgarth, Thomas Volz, and Gavin K Brennen. "Geometric pathway to scalable quantum sensing". Physical Review Letters **125**, 190403 (2020).

[24] Yingkai Ouyang and Gavin K Brennen. "Quantum error correction on symmetric quantum sensors" (2022).

[25] P. Zanardi and M. Rasetti. "Noiseless quantum codes". Phys. Rev. Lett. **79**, 3306–3309 (1997).

[26] G Alber, Th Beth, Ch Charnes, A Delgado, M Grassl, and M Mussinger. "Stabilizing distinguishable qubits against spontaneous decay by detected-jump correcting quantum codes". Physical Review Letters **86**, 4402 (2001).

[27] Gernot Alber, Th Beth, Ch Charnes, Aldo Delgado, Markus Grassl, and Michael Mussinger. "Detected-jump-error-correcting quantum codes, quantum error designs, and quantum computation". Physical Review A **68**, 012316 (2003).

[28] Dave Bacon, Julia Kempe, Daniel A Lidar, and K Birgitta Whaley. "Universal fault-tolerant quantum computation on decoherence-free subspaces". Physical Review Letters **85**, 1758 (2000).

[29] Anatoly Dymarsky and Alfred Shapere. "Quantum stabilizer codes, lattices, and cfts". Journal of High Energy Physics **2021**, 1–84 (2021).

[30] Iman Marvian and Daniel A. Lidar. "Quantum error suppression with commuting hamiltonians: Two local is too local". Phys. Rev. Lett. **113**, 260504 (2014).

[31] Yingkai Ouyang. "Quantum storage in quantum ferromagnets". Phys. Rev. B **103**, 144417 (2021).

[32] Sergey Bravyi and Matthew B Hastings. "A short proof of stability of topological order under local perturbations". Communications in mathematical physics **307**, 609 (2011).

[33] Ramis Movassagh, Gilbert Strang, Yuta Tsuji, and Roald Hoffmann. "The Green's function for the Hückel (tight binding) model". Journal of Mathematical Physics **58**, 033505 (2017).

[34] E Knill, R Laflamme, and G J Milburn. "A scheme for efficient quantum computation with linear optics". Nature **409**, 46–52 (2001). url: http://dx.doi.org/10.1038/35051009.

[35] Ron Graham and Neil Sloane. "Lower bounds for constant weight codes". IEEE Transactions on Information Theory **26**, 37–43 (1980).

[36] Lloyd L Dines. "On positive solutions of a system of linear equations". Annals of MathematicsPages 386–392 (1926).

[37] GG Hamedani and GG Walter. "On the product of symmetric random variables". Statistics & probability letters **3**, 251–253 (1985).

[38] Yingkai Ouyang. "Permutation-invariant quantum codes". Phys. Rev. A **90**, 062317 (2014). arXiv:1302.3247.

[39] Mary Beth Ruskai. "Pauli Exchange Errors in Quantum Computation". Phys. Rev. Lett. **85**, 194–197 (2000).

[40] Harriet Pollatsek and Mary Beth Ruskai. "Permutationally invariant codes for quantum error correction". Linear Algebra and its Applications **392**, 255–288 (2004).

[41] Yingkai Ouyang and Joseph Fitzsimons. "Permutation-invariant codes encoding more than one qubit". Phys. Rev. A **93**, 042340 (2016).

[42] Yingkai Ouyang. "Permutation-invariant qudit codes from polynomials". Linear Algebra and its Applications **532**, 43 – 59 (2017).

[43] Yingkai Ouyang and Rui Chao. "Permutation-invariant constant-excitation quantum codes for amplitude damping". IEEE Transactions on Information Theory (2019).

[44] Yingkai Ouyang, Nathan Shettell, and Damian Markham. "Robust quantum metrology with explicit symmetric states". IEEE Transactions on Information Theory **68**, 1809–1821 (2022).