Aspects of Fault-Tolerant Quantum Computation

Thesis by

Joseph Kramer Iverson

In Partial Fulfillment of the Requirements for the
Degree of
Doctor of Philosophy

Caltech

CALIFORNIA INSTITUTE OF TECHNOLOGY
Pasadena, California

2020
Defended May 20, 2020

ACKNOWLEDGEMENTS

I would like to thank my academic advisor, John Preskill, for his insightful guidance. He planted the seeds of many of the ideas that appear in this thesis. I thank Oskar Painter and the members of his group, especially Eunjong Kim and Xueyue “Sherry” Zhang, for many interesting discussions and their different perspective on quantum information. I thank Fernando Brandão and Xie Chen for serving on my thesis defense committee alongside John and Oskar. I have greatly benefited from the many researchers at Caltech, those who have visited Caltech, and those I have met elsewhere too numerous to mention here, and I am grateful to each of them. I would like to mention in particular a few with whom I have spoken many times: Victor Albert, Michael Beverland, Thom Bohdanowicz, Aaron Chew, Richard Kueng, and especially Aleksander Kubica. I gratefully acknowledge funding from ARO-LPS (W911NF-18-1-0103) and NSF (PHY-1733907). I used the “vZome” software (https://vzome.com/home/) to create several of the figures in Chapter 4. Finally, I thank my family and friends for their constant support.

ABSTRACT

This thesis is concerned with fault-tolerant quantum information processing using quantum error-correcting codes. It contains two major pieces of work. The first is a study of coherent noise in the context of stabilizer error-correcting codes. The second is a proposed scheme for a universal set of fault-tolerant logical gates in a particular code family built out of the 3D toric code.

Chapter 1 provides an introduction to quantum computation and fault tolerance. Many basic concepts in error-correcting codes are defined. Special attention is paid to the set of code properties that are most likely to determine how easily a given fault-tolerant scheme might be implemented on a physical device. These include the fault-tolerant noise threshold and the overhead.

In Chapters 2 and 3 we study the effectiveness of quantum error correction against coherent noise. Coherent errors (for example, unitary noise) can interfere constructively, so that in some cases the average infidelity of a quantum circuit subjected to coherent errors may increase quadratically with the circuit size; in contrast, when errors are incoherent (for example, depolarizing noise), the average infidelity increases at worst linearly with circuit size. We consider the performance of quantum stabilizer codes against a noise model in which a unitary rotation is applied to each qubit, where the axes and angles of rotation are nearly the same for all qubits. In Chapter 2 we introduce coherent noise and incoherent noise and a number of methods that are useful for the study of coherent noise. We study the repetition code as a basic example, and we also study a correlated noise model. In Chapter 3 we show that for the toric code subject to such independent coherent noise, and for minimal-weight decoding, the logical channel after error correction becomes increasingly incoherent as the length of the code increases, provided the noise strength decays inversely with the code distance. A similar conclusion holds for weakly correlated coherent noise. Our methods can also be used for analyzing the performance of other codes and fault-tolerant protocols against coherent noise. However, our result does not show that the coherence of the logical channel is suppressed in the more physically relevant case where the noise strength is held constant as the code block grows, and we recount the difficulties that prevented us from extending the result to that case. Nevertheless our work supports the idea that fault-tolerant quantum computing schemes will work effectively against coherent noise, providing encouraging news for quantum hardware builders who worry about the damaging effects of control errors and coherent interactions with the environment.

Chapter 4 is connected to another aspect of fault tolerance, fault-tolerant logical gates. The toric code is a promising candidate for fault-tolerant quantum computation because of its high threshold and low-weight stabilizers. A universal gate set in the toric code generally requires magic state distillation, which can incur a significant qubit overhead. In this work we construct an error-correcting code in three dimensions based on the toric code that features a fault-tolerant T gate with no magic state distillation required. We further describe a subsystem version of our code which supports a universal set of fault-tolerant gates. This code can be converted into the stabilizer version using gauge-fixing. We also argue that our code can be converted to a (2+1)-D protocol, where a 2D lattice undergoes a measurement-based protocol over time. In this way, a fault-tolerant logical T gate can be realized in a 2D toric code structure.

PUBLISHED CONTENT AND CONTRIBUTIONS

[1] J. K. Iverson and J. Preskill. Coherence in logical quantum channels. *New Journal of Physics*, 2020. doi: https://doi.org/10.1088/1367-2630/ab8e5c. J.K.I was the primary contributor to this work.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

Chapter 1

INTRODUCTION

Quantum computing is still a relatively new field, but interest in the field has grown greatly in the last twenty years, driven by the promise that a properly controlled quantum system could perform computations beyond what can be achieved with classical computers. Some early ideas about quantum computing appeared in the 1980's [6, 58]. Feynman proposed a universal quantum simulator built out of quantum-mechanical elements that could simulate any quantum system in the same way that a universal classical computer can perform any computation that a classical Turing machine can [35]. Later, algorithms were discovered for quantum computers that performed certain tasks far more efficiently than any known algorithm on a classical computer. These include Shor's algorithm for factoring and Grover's search algorithm [38, 69]. There is not yet a rigorous proof that no classical algorithm can achieve the same speedups for these tasks. In other words, it has not yet been proven that quantum computation is more powerful than classical computation. However, the algorithms already discovered give us good reason to believe that an ideal, noiseless quantum computer would be able to solve problems that are intractable for classical digital computers.

In the real world, we do not have access to ideal, noiseless quantum computers. Any physical system has interactions with its surrounding environment. Also, in order to perform a computation, we must interact with the system, and any effort we make to control a physical system will introduce noise. There are many ways of building resilience to noise into physical devices, but some form of error-correcting code at the "software level" will very likely be required. The control pulses that implement all of our operations on the physical device cannot be calibrated to arbitrary precision. Further, there is a fundamental trade-off between isolating a system from its environment to insulate it against noise and at the same time being able to perform fast, well-controlled operations on the system. The coupling to the control introduces noise to the system from the environment on the other end of the control line. To have fast control, the coupling between control and system needs to be large, which means that the introduced noise is also fairly large. "Hardware level" protocols are useful to some extent, but they are not scalable in the sense that they do not offer a path to arbitrarily long and accurate computations. Also, many of the quantum algorithms that provide significant improvement over all known classical algorithms require a large problem size before the computation is beyond the best classical supercomputers. For example, with Shor's algorithm for factoring integers, a quantum computer would need to factor an integer of perhaps several thousand bits to beat the best classical computers. This would require a circuit with many thousands of qubits and gates and correspondingly low noise levels.

For these reasons, quantum error correction will be needed to overcome the noise and reliably operate a large-scale quantum computer that can solve difficult problems. Fortunately, the accuracy threshold theorem for quantum computation establishes that quantum computing is scalable, assuming that the noise is neither too strong nor too strongly correlated [1, 3, 36, 52, 67]. As long as the physical qubits satisfy a fixed condition on the noise, error-correcting codes can be used to perform arbitrarily long computations. However, in practice we do not have access to an unlimited number of qubits. Then the performance of different codes against the specific noise present in a given device becomes important. Also, we need to know how to perform the logical gates that make up the computation in a noise-resistant, fault-tolerant way. This thesis will discuss work on two major topics related to error-correcting codes: the performance of codes against specific noise models and the implementation of fault-tolerant logical gates.

1.1 Quantum Error-Correcting Codes

A quantum error-correcting code encodes a logical quantum state into a much larger quantum system, such that the logical observables are non-local. In this way, the logical state cannot be inferred from few local measurements. Equivalently, the environment cannot alter the logical state with weak, local interactions. The parameters of a code are often notated $[n, k, d]$, where n is the number of physical qubits, k is the number of logical qubits, and d is the code distance. The code distance is the weight of the minimal-weight operator that acts non-trivially on the encoded state. Quantum error-correcting codes can be defined for almost any quantum system, but for simplicity, both theoretically and in practice, a common choice is a system consisting of many small two-level systems called qubits. This choice is nicely analogous to the registers of bits used in classical computation and is also a convenient framework for describing quantum algorithms. In what follows, only the case of qubits will be considered.

Quantum error correcting codes for qubit systems is a well-studied subject. Stabilizer codes were the first family of such codes to be described [22, 36, 71] and they remain the best-studied class. These codes divide the Hilbert space of the physical system into eigenspaces of a mutually commuting set of operators, called stabilizers. The eigenspace that corresponds to +1 for all stabilizers is called the "code space," and it is here that the logical state is encoded. All other eigenspaces are called "error subspaces." The codes require active monitoring and correction. This consists of three steps: measuring a generating set of stabilizers, computing a correction predicated on the measurement outcomes, and finally applying the correction operator.

Depending on the implementation, the measurement step may require ancilla qubits in order to be fault-tolerant. The outcome of the stabilizer measurements is known as the "syndrome" and the process of measuring the stabilizer generators is known as "syndrome extraction." The task of computing a correction for a given syndrome is known as "decoding." The optimal decoding calculates the most likely class of error given the syndrome and some assumed noise model. This kind of decoding is inefficient. However, many efficient decoding algorithms are known to exist for certain classes of codes. The correction step undoes the error predicted by the decoder. This returns the system to the code space. If the decoder was successful, the correction matches the error that occurred up to stabilizer operators and the logical state is unchanged, and if the decoder is unsuccessful, after applying the correction the logical state has suffered an error.

The performance of error correcting codes is multi-faceted—it is a complicated interplay between the code, including the scheme for fault-tolerant syndrome extraction and decoding, the computation that will be performed, and the noise model. The noise present in a quantum device is difficult to characterize because a quantum channel acting on a D dimensional Hilbert space has $D^2(D^2 - 1)$ independent parameters in general. To fully characterize the noise channel acting on a quantum system, a number of experiments where a state is prepared and measured is required that is exponentially large in the number of qubits. Also, certain parameters of the noise channel can be efficiently extracted mostly independent of additional assumptions on the noise model [33, 53]. This approach offers a full characterization of the noise model only with strong assumptions on the noise model. Therefore, it is not particularly meaningful to study an overly specific noise model. In what follows, we will discuss general features of noise models, and when examples are necessary, we will consider simple noise models rather than try to match the noise in a complicated device. Similarly, the computation we may wish to perform on a quantum computer can be very complex. We will not focus on the specific computation; instead the focus will be on error correcting codes.

At the most basic level, there are two main aspects to the performance of a code: the "fault-tolerant threshold" and the "overhead." The fault-tolerant threshold for a given code and specified noise model is a level of noise strength ϵ_0 such that as long as the noise strength ϵ is below ϵ_0, then a logical computation can be carried out with a failure probability that is bounded above by $\left(\frac{\epsilon}{\epsilon_0}\right)^d$, where d is the code distance. In other words, by choosing a sufficiently large code, the failure probability for a logical computation can be made arbitrarily small. A sample threshold theorem has the form:

Theorem 1. *(Fault-Tolerant Threshold) Suppose that we have a particular family of error correcting codes combined with a decoding scheme. Let the noise model be the same single-qubit noise channel acting on each qubit with a noise strength bounded by ϵ. A fault-tolerant threshold ϵ_0 exists if the probability of a logical failure in a member of the code family with code distance d is $\leq c\left(\frac{\epsilon}{\epsilon_0}\right)^d$ for a constant c.*

Code thresholds have been proven for several code classes and local noise models [1, 36, 52, 67] as well as noise models with long-range correlations as long as these correlations are sufficiently small or decay sufficiently rapidly [3]. The overhead of a code is the number of qubits required to encode a logical state and operate on it. A code encodes a certain number of logical qubits into a certain number of physical qubits. One contribution to the overhead of a code is characterized by the ratio n/k, which is the number of physical qubits required for each logical qubit. Operating the code requires us to perform the error correction procedure that has already been described, measuring stabilizer generators, decoding the syndrome, and applying corrections. Measuring the syndrome fault-tolerantly requires ancilla qubits, which adds to the overhead. In addition, we also must be able to perform the operations that will implement a quantum computation. The set of fault-tolerant logical operations and their implementations will depend on the code and will often require additional ancilla qubits. These ancillas also contribute to the overhead of the code.

We have already used the term "fault-tolerant" without offering a definition. This term signifies roughly that the noise in all of the elements that go into the quantum information processing scheme are such that a threshold theorem applies. For example, if a syndrome measurement protocol is fault-tolerant, then the logical noise, or the cumulative effect of errors on the code qubits, the ancillas qubits, and in each measurement and gate, can be made arbitrarily small by choosing a code that is sufficiently large. This holds so long as the noise in each of the various elements is sufficiently small. Fault-tolerant syndrome extraction often requires ancilla qubits and many repeated measurements. Similarly, for a logical gate to be fault-tolerant, this means that all of the resulting noise can be corrected arbitrarily well.

Quantum algorithms can be implemented in different ways, but a popular model for quantum computation is the "gate model." Here an algorithm is implemented by a series of discrete gates acting on qubits. A gate is an elementary unitary operation that may involve one or more qubits. Because of the feature of error correcting codes that we will describe now, it is convenient to specify the gates in a computation from a discrete gate set. Then in some cases the discrete set of gates can be used to approximate any unitary operation to arbitrary accuracy. Such a set is called a "universal gate set." The idea of gates and universal gate sets is directly analogous to logic gates and universal sets of logic gates from classical computation. In the quantum case, we seek to implement logical gates within the encoded logical subspaces of error correcting codes. The implementation of logical gates in different codes is a rich field of study. The implementations we want are those that not only perform the correct logical operation, but are also fault-tolerant. Each code has a certain set of fault-tolerant logical gates. We would like a universal, fault-tolerant gate set, but this turns out to be impossible with unitary operations on a single code. The Eastin-Knill theorem [31] states:

Theorem 2. *(Eastin-Knill) For any nontrivial local-error-detecting quantum code, the set of logical unitary product operators is not universal.*

To avoid spreading errors and breaking the fault-tolerance of the code, gate implementations should be "locality-preserving." The noise present in the system will be transformed by the gate implementation, which will itself be noisy. The locality-preserving condition means that if the initial noise model is local, so that the noise is well-handled by the code, the residual noise after the imperfect gates are applied will remain local, and the code will be able to correct it. If the gate implementation requires gates coupling some qubits to many other qubits, errors will spread throughout the code in a long-range correlated way. This will likely not be corrected by the code. A stronger condition than locality-preserving is "constant depth," which means that the gate is implemented by a constant-depth circuit. If rounds of gates are applied such that no more than one gate acts on each qubit in each round, then the depth of a circuit is the minimum number of rounds required. A yet stronger condition is that the logical gate is "transversal." In this case each qubit is acted on at most once. Transversal gate implementations are best, but locality-preserving is a sufficient condition for fault-tolerance.

We have already defined universal sets of gates. There are many possible choices, but some are particularly popular. A useful concept for discussing gates is the "Clifford hierarchy." The Pauli group $\mathcal{P}$ forms the first level of the hierarchy. The second level of the hierarchy is called the "Clifford group," which is defined as the set of operators O such that for every Pauli operator $P \in \mathcal{P}$, $OPO^\dagger \in \mathcal{P}$. Then the i-th level of the hierarchy C_i is recursively defined as the set of operators O such that for every Pauli operator $P \in \mathcal{P}$, $OPO^\dagger \in C_{i-1}$. The level of the hierarchy to which a gate belongs is roughly a measure of how universal a gate is. Some gates are not contained in any level of the hierarchy. The second level of the hierarchy is not universal, but the second level supplemented by any gate outside the second level is a universal gate set. For many error correcting codes, some of the gates of the second level of the hierarchy, called the Clifford group, are relatively easy to implement fault-tolerantly. The Clifford group on any number of qubits (≥ 2) is generated by three gates, called S, H, and CNOT. In matrix form, these are given by

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{1.1}$$

If the Clifford group can be implemented transversally in a particular code, then the gate outside the first level poses a special challenge.

To realize a universal set of fault-tolerant logical gates, a more complicated protocol is necessary because of the Eastin-Knill theorem. A leading approach is magic state distillation [16]. In a protocol called "gate teleportation," logical gates can be performed using ancilla qubits in specific states. A CNOT gate is applied between ancilla and code qubit, and the ancilla is measured. Finally, a correction is applied to the code qubit conditioned on the measurement outcome from the ancilla. The idea of magic state distillation is to use a separate code to fault-tolerantly prepare the required magic states, which are then introduced into the original stabilizer code as needed to perform a universal set of gates. There are several types of protocols that can prepare magic states. Each of them contributes substantial overhead, and reducing this overhead has been a major focus of research for many years

[14, 42, 59]. Magic state distillation is not the only way to realize a universal set of gates. Other promising ideas include code switching and gauge-fixing. These methods are applicable to special classes of codes. We will discuss these ideas in more detail in Chapter 4.

There are many factors that determine whether a given scheme for fault-tolerant, universal quantum computation can be used to perform a given computation on a given physical device. We have already discussed the overhead, which is the number of qubits per logical qubit required to implement the protocol, and the noise threshold. The level of noise in the device must be below the threshold value for error correction to succeed. We also discussed logical gates. These gates require certain physical gates to be realized with good fidelity. In addition, the locality of the operations required is quite important. Certain codes require long range gates coupling qubits, while other codes require only local operations. Topological codes are an important example of this latter group. These codes have low-weight stabilizer generators that are local in some dimension. This locality makes these codes very promising for experimental implementation. In addition, these codes are connected to topological states of matter and topological field theories that are of independent interest. For topological codes, the dimension of the code is related to the realizable constant-depth logical gates by the Bravyi-König theorem [17], which states

Theorem 3. *(Bravyi-König) Let $D \geq 2$ and let L be the code space of a topological stabilizer code on a D-dimensional lattice. Suppose U is a constant-depth quantum circuit that maps L to itself. Then the restriction of U onto L implements an encoded gate from the D-th level of the Clifford hierarchy.*

Topological codes also have some of the highest known fault-tolerant thresholds.

1.2 Examples

To help illustrate the concepts we defined in the previous section, we now provide some examples.

The Five Qubit Code

The smallest error correcting code uses five physical qubits to encode one logical qubit [57]. It is often referred to as the five qubit code. We will use X and Z to denote Pauli X and Z operators and subscripts like X_1 to denote which qubit the operator acts upon. The stabilizer group is generated by the set of operators

$$\mathcal{S} = \langle\{X_1Z_2Z_3X_4,\ X_2Z_3Z_4X_5,\ X_3Z_4Z_5X_1,\ X_4Z_5Z_1X_2\}\rangle. \tag{1.2}$$

Five qubits and four independent stabilizer generators means that the code has one logical qubit. The code corrects all single-qubit errors. Here the word “corrects” means that the following condition (called the Knill-LaFlamme condition [51]) is satisfied:

$$\langle\psi|E_1E_2|\psi\rangle = 0 \quad \forall \text{ single-qubit operators } E_1, E_2. \tag{1.3}$$

This implies that the code distance d is 3. The five qubit code can be used to define a family of codes using concatenated codes. Here the physical qubits of one code are replaced by encoded qubits in another code. We can concatenate any number of five qubit codes to produce an infinite code family. This family has a noise threshold against local noise [3]. The value of the threshold depends on the decoder used. For a basic level-by-level decoder, the threshold error probability of storage with perfect syndrome extraction has been found to be 0.1376 [63]. More sophisticated decoders employing message passing give higher thresholds, for example 0.1885 [61]. The threshold will be significantly lower for circuit-level noise. In the five qubit code, the Pauli group is transversal. In addition, S is transversal. CNOT and H both require high-depth circuits.

The Toric Code

We mentioned topological codes as a particularly useful class. The most famous example of a topological code is the toric code [50]. This is a model originally in 2D, but can be extended to any dimension. It can be defined on many lattices, but the original and the simplest is the square lattice or its higher-dimensional generalizations.

We will now describe the 2D toric code, which is defined on a square lattice with qubits placed on edges. We choose a square patch of lattice with side length L and identify opposite edges. (The toric code can be constructed on a lattice with boundaries, but for simplicity, we choose periodic boundary conditions.) The stabilizer group for the toric code is generated by the X and Z generators shown in figure 1.1. The logical Pauli operators of the toric code are topologically non-trivial loops that wrap around the torus. Figure 1.2 shows two logical Pauli operators.

The toric code is parameterized by the linear dimensions of the lattice; when the side length is L, the code distance (the minimum weight of a nontrivial logical operator)

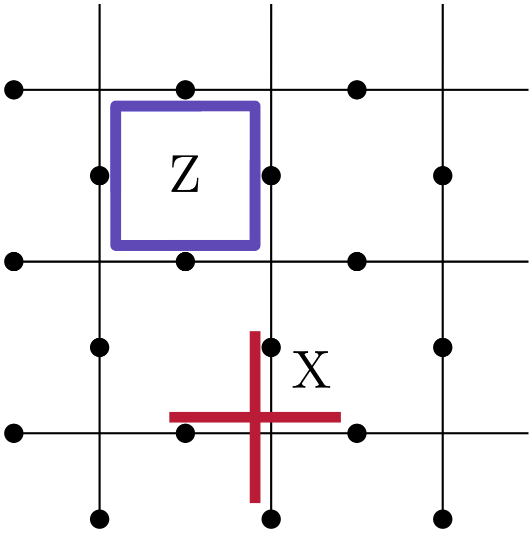


Figure 1.1: In blue is a Z-type stabilizer generator for the toric code. There are Z generators on every plaquette in the lattice. In red is an X-type stabilizer generator. There are X generators at every vertex of the lattice.

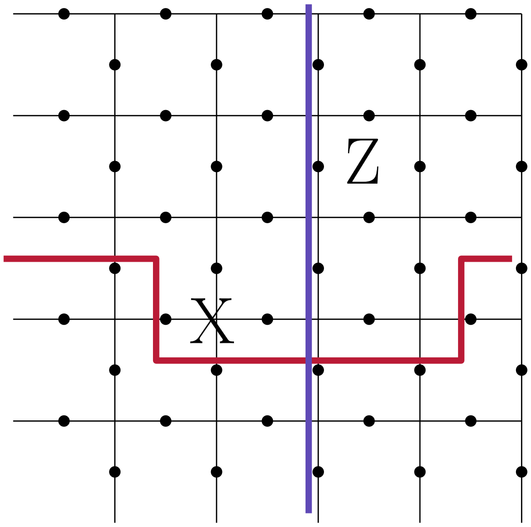


Figure 1.2: This figure illustrates two of the logical Pauli operators in the toric code. X and Z logical operators are shown for one of the two encoded qubits. Each logical operator is a topologically non-trivial loop that wraps around the torus. The logical operators for the other encoded qubit are similar, but rotated by 90 degrees.

is L. We will also sometimes refer to L as the code “size.” The number of physical qubits in the code block is $2L^2$, and there are two encoded logical qubits. To analyze the logical channel, we must choose a decoding procedure. Decoding the toric code is a well-studied problem and many good algorithms are known [18, 29, 30]. We will choose minimal-weight decoding, in which the applied recovery operation has the lowest possible weight consistent with the measured error syndrome. This recovery operation can be computed efficiently on a classical computer [32], and corrects the error with a success probability that is exponentially close to 1 when L is large and the noise is sufficiently weak.

Chapter 2

COHERENT NOISE IN ERROR-CORRECTING CODES[1]

2.1 Introduction

In Chapter 1 we emphasized how the noise model affects the performance of a code. The fault-tolerant noise threshold for the code depends sensitively on the noise model. A fault-tolerant threshold is defined for particular noise models and also only characterizes the residual logical noise channel by bounding the strength of the noise channel, or in other words, its distance from the identity channel. It does not specify what sort of channel describes the residual noise.

We have discussed the difficulty of characterizing the noise in a large, complicated experimental device. Until we try to build an error correcting code and perform fault-tolerant logical operations on a real device, we won't know for sure whether realistic noise is sufficiently benign for quantum error correction to work effectively. A general noise channel acting on n qubits is extremely complex when n is large, so it will not be practical to fully characterize the noise in a complex quantum device using any feasible experimental protocol. A commonly used metric for the performance of single-qubit and two-qubit quantum gates is the "average infidelity" $r = 1 - F$, where F is the fidelity of the output from the gate relative to the output of an ideal gate, averaged uniformly over all possible input states. This quantity r has the great virtue that it can be feasibly measured using randomized benchmarking [33, 53], but as a characterization of the noise strength, it has shortcomings. Assuming an uncorrelated noise model, threshold theorems guarantee scalability if a different metric, the diamond distance $D_\diamond$, is less than a critical value. Here $D_\diamond$ denotes the deviation of the noisy gate from the ideal gate as measured by the diamond norm. For an incoherent noise channel like a Pauli channel, the diamond distance $D_\diamond$ is equal to the average infidelity r; in contrast, for a highly coherent channel, $D_\diamond$ scales like the square root of r. If we know only r, and have no information about the coherence of the noise, we cannot estimate $D_\diamond$ accurately, and therefore cannot easily make sound predictions about how effectively any error-correcting code will combat the noise [56, 68, 74]. The situation is even worse for correlated noise models.

[1] The work in this chapter was carried out in collaboration with John Preskill.

The purpose of the next two chapters is to study further how well quantum error correction performs against coherent noise models. To make the analysis manageable, we will make some simplifying assumptions. For one, we will not actually consider quantum computation, but instead will focus on the easier task of operating a quantum memory. We envision encoding a quantum state in the memory using a quantum code; after the encoding step, the memory is subjected to noise, and then the quantum state is decoded. As a further simplification, we will assume that the encoding and decoding are noiseless. Therefore, the performance of the code against the noise is captured by a *logical channel*, the result of composing the encoding channel, noise channel, and decoding channel.

We will be interested in what happens to a quantum state which is stored in the memory for a long time, and undergoes many rounds of error correction — that is, we want to characterize the effect of applying the logical channel many times in succession. For this purpose, we will need to understand the coherence properties of the logical channel. If the logical channel is incoherent, then the diamond distance of the decoded state from the ideal state grows linearly with the number of channel repetitions, while for a highly coherent logical channel, it can grow quadratically. Our main conclusion is that, even if the physical noise acting on the quantum memory is highly coherent, the coherence of the logical channel becomes strongly suppressed as the block length of the quantum error-correcting code increases, assuming that the noise is sufficiently weak and sufficiently weakly correlated.

Although we can analyze the logical channel only in a simplified setting, and only for particular code families, we believe that the lessons learned apply more broadly. We expect, for example, that randomized benchmarking applied to *logical* gates will accurately characterize logical noise even when the physical noise is highly coherent, at least for large code blocks. This also suggests that for concatenated coding schemes, in which the “physical” qubits of a higher-level code are themselves the logical qubits of a lower-level code, the average infidelity of the lower-level code should be a good predictor for the performance of the higher-level code.

Our main conclusion is not unanticipated [3], as the suppression of coherence in the logical channel has an intuitive explanation. To decode, one measures the error syndrome, and then applies a recovery operation conditioned on the syndrome. For a large code, many different syndromes are possible, and only the errors which are projected onto the same syndrome value can interfere constructively, while errors projected onto different syndrome values add stochastically. The stochastic average over many syndrome sectors suppresses coherence, leaving only small residual coherent effects arising from summing coherently over errors which are projected onto a given syndrome sector. That said, carefully analyzing the residual coherence in the logical channel involves daunting combinatorics. It turns out that further cancellations occur, resulting in even stronger suppression of logical coherence than might be naively expected.

This discussion about averaging over all syndrome sectors highlights an important issue. We will consider the logical channel obtained by averaging over error syndromes, and then study the coherence of the resulting channel. One could make a case for an alternative procedure: define a metric that characterizes coherence, evaluate that metric for the logical channel conditioned on each syndrome, and then average the value of the metric over syndromes by weighting each syndrome with its probability. To argue in favor of this alternative procedure, one might note that the experimentalist who executes the error correction protocol could know the syndrome she measures in each run of the protocol, and might be interested in the properties of the logical channel conditioned on that knowledge [45]. Our view is that properties of logical channels conditioned on the syndrome are potentially of interest for near-term experiments using relatively small codes, particularly because it might be feasible to postselect by retaining favorable syndromes and rejecting unfavorable ones. In future experiments using larger codes, though, syndrome histories will be quite complex, and it will be impractical to make useful inferences about the logical channel conditioned on syndrome information. For long computations using large codes, properties of the logical channel averaged over syndromes will most likely provide more usable guidance regarding the features of the protected quantum computation.

We should also note that methods have been proposed to suppress the coherence of physical noise. One such method is randomized compiling, which, under certain assumptions, can transform any single-qubit noise channel into an incoherent depolarizing channel [75]. The assumptions include a Markovian noise model and gate independence of the noise for the “easy” gates in the scheme. These assumptions may hold to a good approximation for some realistic cases, but they will not hold exactly. We may then ask how the residual coherence is affected by error correction, an issue that can be addressed using the methods in this paper. Other schemes for mitigating coherent noise have been proposed in [21, 26–28]. These papers focus on the strength of the logical noise, whereas we study the character of the logical noise channel, specifically its degree of coherence.

Here we investigate the coherence of the logical channel in the case where the physical noise is fully coherent unitary noise, a problem that has been previously studied [5, 37, 44]. This chapter describes a number of basic concepts and methods concerning coherent noise channels and applies the methods to calculate the logical noise channel exactly in the case of the n qubit repetition code. The results in this chapter go beyond past work on unitary noise in the repetition code primarily in the way that the bounds on the coherence of the logical noise are stated and in the correlated unitary noise calculation in Section 2.5. The next chapter applies the methods to prove a bound on the coherence of the logical noise channel in the 2D toric code with minimal-weight decoding. This case will prove considerably more involved than that of the repetition code. However, in the end the form of the bound will closely match the calculation for the repetition code in this chapter.

In our analysis we make extensive use of the chi-matrix formalism for describing quantum channels. The chi matrix arises when the action of a channel on an input density operator is expanded in terms of Pauli operators (tensor products of 2×2 Pauli matrices) acting on the density operator from the left and from the right. A channel can be expressed as the sum of an "incoherent part" in which the Pauli operators on left and right are equal, and a "coherent part" in which the Pauli operators on left and right are distinct. Our main task will be to infer, in the case of stabilizer codes, how the logical chi matrix which describes the logical channel after error correction is related to the physical chi matrix which describes the noise acting on physical qubits.

A related conclusion holds for a broad class of correlated noise models. We provide a detailed analysis of correlated noise for the simpler case of the quantum repetition code, under the assumption that the noise Hamiltonian commutes with the Pauli operator X acting on each qubit, so that the repetition code provides effective protection against the noise model. In a model in which the rotations acting on pairs of qubits are strongly correlated, we find as expected that the correlations significantly enhance the probability of an uncorrectable logical error. However, the correlations enhance the coherent and incoherent parts of the logical chi matrix by comparable factors. Therefore, our conclusion that the coherence of the logical channel is heavily suppressed in the limit of large code length continues to apply despite the strong pairwise correlations in the noise.

The rest of this chapter is organized as follows. Section 2.2 is a self-contained review of quantum channels, emphasizing metrics for characterizing coherence and relations among them. We study the logical channel acting on the code's protected qubits by deriving the chi matrix of this logical channel from the chi matrix of the noise channel acting on the physical qubits. To interpret the meaning of the logical chi matrix, we find it convenient to relate the chi matrix to another formalism for describing quantum channels — the Pauli transfer matrix. We explain some properties of the Pauli transfer matrix N of a channel $\mathcal{N}$ in Section 2.2, relating N to the diamond distance $D_\diamond(\mathcal{N})$ in equation (2.50) and to the average infidelity r_m of the m-times repeated channel $(\mathcal{N})^m$ in equations (2.40) and (2.43). Using Lemma 1 these expressions for the diamond distance and the average infidelity in terms of the Pauli transfer matrix can be restated in terms of the chi matrix.

In Section 2.3 we study the performance of the quantum repetition code against coherent noise, and prove Theorem 4 using explicit computation of the logical channel combined with results derived in Section 2.2. This result shows that the logical channel is highly incoherent when the code block is large. An alternative proof of Theorem 4, making essential use of the chi matrix, is presented in Section 2.4, where we develop the key tools needed for the proof of Theorem 6. We also prove Lemma 2, which is used to show that, for independent unitary noise acting on the physical qubits, the coherence of the logical channel for the repetition code is maximized when all qubits are rotated by the same angle. A similar idea can be adapted for analyzing the coherence of the logical channel for the toric code.

In Section 2.5 we extend the analysis of the repetition code to the case of two-body correlated coherent noise, culminating in the proof of Theorem 5, showing that the coherence of the logical channel is heavily suppressed in this case as well. The proof is a computation of the logical channel for this case, achieved by a detailed combinatoric analysis. As expected, the noise correlations enhance the probability of a decoding error, but it turns out that both the coherent and incoherent parts of the logical channel are enhanced, so that the relationship between the two is not changed much compared to the case of uncorrelated coherent noise. The same reasoning used to prove Theorem 5 can also be applied to the toric code to show that, in that case as well, two-body correlations in the noise do not enhance the coherence of the logical channel.

2.2 Channel parameters

Pauli transfer matrix

We will use the *Pauli transfer matrix* representation to describe channels acting on n qubits. For this purpose we expand the density operator ρ in the Pauli operator basis $\{\sigma^i\}$:

$$\rho = \sum_{i=0}^{d^2-1} \rho_i \sigma^i, \tag{2.1}$$

where

$$\mathrm{Tr}\left(\sigma^i \sigma^j\right) = \frac{1}{d}\delta^{ij}, \tag{2.2}$$

and $\sigma^0 = (id)/d$. Here $d = 2^n$ is the Hilbert-space dimension, and id denotes the $d \times d$ identity matrix. Note that $\mathrm{Tr}(\rho) = \rho_0$. A linear map $\mathcal{N}$ acting on density operators defines a $d^2 \times d^2$ matrix (the Pauli transfer matrix associated with $\mathcal{N}$) according to

$$\mathcal{N}(\rho) = \sum_{i,j} \left(N_{ij}\rho_j\right) \sigma^i. \tag{2.3}$$

This matrix is real if $\mathcal{N}$ maps Hermitian operators to Hermitian operators. If the map $\mathcal{N}$ is trace preserving, then $\sum_i N_{0i}\rho_i = \rho_0$; hence $N_{0i} = \delta_{0i}$. If the map $\mathcal{N}$ is unital (that is, $\mathcal{N}(id) = id$), then $\sum_i N_{ij}\delta_{j0} = \delta_{i0}$; hence $N_{i0} = \delta_{i0}$. Thus the matrix representing the map $\mathcal{N}$ may be expressed as

$$N = \begin{pmatrix} 1 & 0 & 0 & \cdots \\ & & & \\ N_n & & N_u & \\ & & & \end{pmatrix}. \tag{2.4}$$

We say that the $(d^2-1) \times (d^2-1)$ matrix N_u is the unital part of $\mathcal{N}$ and that the length-(d^2-1) vector N_n is its nonunital part. Altogether the trace-preserving map $\mathcal{N}$ is specified by $d^2(d^2-1)$ parameters.

For a unitary map $\mathcal{N}(\rho) = U\rho U^\dagger$, we have $N_n = 0$ and (for $i \neq 0$)

$$U\sigma^i U^\dagger = \sum_{j=1}^{d^2-1} (N_u)_{ji}\sigma^j, \tag{2.5}$$

where

$$d\,\mathrm{Tr}\left(U\sigma^i U^\dagger U\sigma^k U^\dagger\right) = \delta^{ik} = d \sum_{j,l\neq 0} (N_u)_{ji}(N_u)_{lk}\mathrm{Tr}\left(\sigma^j\sigma^l\right) = \sum_{j\neq 0}(N_u)_{ji}(N_u)_{jk}; \tag{2.6}$$

hence N_u is an orthogonal matrix.

The matrix representing $\mathcal{N}$ is diagonal if and only if the map is a convex sum of Pauli operators

$$\mathcal{N}(\rho) = \sum_i p_i \sigma^i \rho \sigma^i, \tag{2.7}$$

in which case the diagonal entries are

$$N_{jj} = \sum_i p_i \xi_{ij}, \tag{2.8}$$

where $\sigma^i \sigma^j = \xi_{ij} \sigma^j \sigma^i$; that is, ξ_{ij} is the sign ±1 determined by whether the Pauli operators σ^i and σ^j commute or anticommute.

Average infidelity

The *fidelity* F of a channel $\mathcal{N}$ acting on a pure state $|\psi\rangle$ is defined by

$$F = \langle \psi | \mathcal{N}(\rho) | \psi \rangle, \tag{2.9}$$

and $1 - F$ is called the *infidelity*. The *average infidelity* r of $\mathcal{N}$ is

$$r = 1 - \int dU \, \mathrm{Tr} \left[U\rho U^\dagger \mathcal{N}(U\rho U^\dagger) \right], \tag{2.10}$$

where the integral is with respect to the normalized invariant Haar measure on the unitary group, and ρ is any pure state. Equivalently, r is the infidelity of the averaged channel

$$\bar{\mathcal{N}}(\rho) = \int dU \, U^\dagger \mathcal{N}(U\rho U^\dagger) U. \tag{2.11}$$

We may just as well define r as the infidelity of $\mathcal{N}$ averaged over a unitary 2-design. Hence r can be measured in randomized benchmarking experiments, in which U is chosen by sampling uniformly from the Clifford group, which is a unitary 2-design.

The $d \times d$ unitary matrix U defines an orthogonal $(d^2 - 1) \times (d^2 - 1)$ matrix $N_u = O$ according to

$$U\sigma^i U^\dagger = \sum_{j=1}^{d^2-1} O_{ji} \sigma^j, \quad U^\dagger \sigma^i U = \sum_{j=1}^{d^2-1} O^T_{ji} \sigma^j, \tag{2.12}$$

where O^T denotes the transpose of O; therefore

$$U^\dagger \mathcal{N}(U\sigma^i U^\dagger) U = \sum_{j=1}^{d^2-1} \left(O^T N_u O \right)_{ji} \sigma^j; \quad U^\dagger \mathcal{N}(U\sigma^0 U^\dagger) U = \sigma^0 + \sum_{i=1}^{d^2-1} (O^T N_n)_i \sigma^i. \tag{2.13}$$

The uniform average of U over the unitary group becomes a uniform average of O over the orthogonal group. The nonunital part of $\mathcal{N}$ averages to zero, and the average of the unital part can be evaluated using

$$\int dO\, O^T_{ij} O_{kl} = \frac{1}{d^2-1}\delta_{jk}\delta_{il}, \tag{2.14}$$

which yields

$$\left(\bar{N}_u\right)_{ij} = \frac{\mathrm{Tr}(N_u)}{d^2-1}\delta_{ij}. \tag{2.15}$$

Hence, the averaged channel is a completely depolarizing Pauli channel of the form

$$\bar{\mathcal{N}}(\rho) = p\rho + (1-p)\left(\frac{id}{d}\right), \tag{2.16}$$

where

$$p = \frac{1}{d^2-1}\mathrm{Tr}(N_u). \tag{2.17}$$

Note that if this averaged channel is applied m times in succession, we obtain

$$\bar{\mathcal{N}}^m(\rho) = p^m\rho + (1-p^m)\left(\frac{id}{d}\right); \tag{2.18}$$

thus p is called the *benchmarking parameter* because it determines the rate of exponential decay of fidelity in benchmarking experiments. The average infidelity r is given by

$$\begin{aligned} r &= 1 - \langle\psi|\bar{\mathcal{N}}(|\psi\rangle\langle\psi|)|\psi\rangle = 1 - \left(p + \frac{1-p}{d}\right) \\ &= \frac{d-1}{d}(1-p) = \frac{1}{d(d+1)}\mathrm{Tr}(I_{d^2-1} - N_u) \end{aligned} \tag{2.19}$$

for any pure state $|\psi\rangle$. Here I_{d^2-1} denotes the $(d^2-1)\times(d^2-1)$ identity matrix. Because $N_{00} = 1$, we may also express the infidelity as

$$r = \frac{1}{d(d+1)}\mathrm{Tr}\left(I_{d^2} - N\right), \tag{2.20}$$

where I_{d^2} denotes the $d^2 \times d^2$ identity.

Examples

Depolarizing channel

We have seen that if $\mathcal{N}_p$ is the depolarizing channel with benchmarking parameter p, then $(\mathcal{N}_p)^m = \mathcal{N}_{p^m}$. Using the relation $r = \frac{d-1}{d}(1-p)$, we can express the infidelity r_m of $(\mathcal{N}_p)^m$ in terms of the infidelity r of $\mathcal{N}_p$, finding

$$r_m = \frac{d-1}{d}(1-p^m) = mr - \frac{d}{2(d-1)}m(m-1)r^2 + O(m^3r^3). \tag{2.21}$$

If mr is small, the infidelity accumulates linearly with m, the number of times the channel is applied. A similar remark applies to more general Pauli channels.

We say that a channel with this property is *incoherent*. The interpretation is that (up to a constant factor), the infidelity r may be regarded as a *probability* of error. If the channel is applied m times, where mr is small, any one of the m instances of the channel could be faulty, so that the total probability of error is mr + higher-order terms.

Qubit rotation

In contrast, consider the case of a unitary rotation of a single qubit about the X-axis

$$U^X(\theta) = \exp\left(-i\frac{\theta}{2}\sigma^X\right) \tag{2.22}$$

which rotates the Bloch sphere by θ. For this channel the Pauli transfer matrix is

$$N(\theta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\theta & \sin\theta \\ 0 & 0 & -\sin\theta & \cos\theta \end{pmatrix}; \tag{2.23}$$

therefore, the infidelity is

$$r = \frac{1}{6}\operatorname{Tr}\left(I - N_u\right) = \frac{1}{3}\left(1 - \cos\theta\right) = \frac{1}{6}\theta^2 - \frac{1}{72}\theta^4 + O(\theta^6). \tag{2.24}$$

Applying this channel m times, we obtain $N(\theta)^m = N(m\theta)$, a rotation by an angle m times larger. Therefore,

$$r_m = \frac{1}{3}(1 - \cos m\theta) = m^2 r - \frac{1}{2}m^2(m^2-1)r^2 + O(m^6 r^3). \tag{2.25}$$

Here, for $m^2 r$ small, the infidelity accumulates quadratically with m; it is the rotation angle, rather than the error probability, that increases linearly. We say that a channel like this one, for which the infidelity increases faster than linearly with m, is *coherent*.

Rotation/Dephasing channels

The distinction between a coherent and incoherent channel is not always clearcut, and we will need measures that quantify the degree of coherence. As an example, consider the case where a qubit either dephases in the X-basis (with probability q_D) or is rotated by angle θ about the X-axis (with probability q_R):

$$\mathcal{N}(\rho) = (1 - q_D - q_R)\rho + q_D\sigma^X\rho\sigma^X + q_R U^X(\theta)\rho U^X(\theta)^\dagger. \tag{2.26}$$

The Pauli transfer matrix is

$$N = \begin{pmatrix} I & 0 \\ 0 & M \end{pmatrix}, \tag{2.27}$$

where I is the 2×2 identity, and M is the 2×2 matrix

$$M = \begin{pmatrix} 1-\epsilon & \delta \\ -\delta & 1-\epsilon \end{pmatrix}, \tag{2.28}$$

with

$$\epsilon = 2q_D + q_R(1-\cos\theta), \quad \delta = q_R \sin\theta. \tag{2.29}$$

The infidelity is

$$r = \frac{1}{6}\operatorname{Tr}(I-M) = \frac{1}{3}\epsilon = \frac{2}{3}q_D + \frac{1}{3}q_R(1-\cos\theta). \tag{2.30}$$

The eigenvalues of M are

$$\lambda_\pm = 1 - \epsilon \pm i\delta, \tag{2.31}$$

and therefore the infidelity of $\mathcal{N}^m$ is

$$\begin{aligned} r_m &= \frac{1}{6}\operatorname{Tr}(I - M^m) = \frac{1}{6}\left[2 - (1-\epsilon+i\delta)^m - (1-\epsilon-i\delta)^m\right] \\ &= \frac{1}{3}m\epsilon - \frac{1}{6}m(m-1)\left(\epsilon^2 - \delta^2\right) + O(m^3\epsilon^3, m^3\epsilon\delta^2, m^4\delta^4). \end{aligned} \tag{2.32}$$

Here the degree of coherence depends on the relative value of ϵ and δ. In the case of a unitary rotation, we have $\epsilon = O(\delta^2)$, which means that the term growing quadratically with m can dominate. On the other hand, for $\epsilon \geq \delta$, there is no quadratically growing term at all.

A generalization of this channel will be useful in Section 2.3. Instead of a single rotation by θ occurring with probability q_R, we may consider an ensemble of possible rotations, where a rotation by θ_a occurs with probability q_a. In that case r_m is still given by equation (2.32), but now

$$\epsilon = 2q_D + \sum_a q_a(1-\cos\theta_a), \quad \delta = \sum_a q_a \sin\theta_a. \tag{2.33}$$

Unitarity and the coherence angle

We have seen that N_u is an orthogonal matrix if (and only if) the channel $\mathcal{N}$ is unitary. Hence a deviation from orthogonality of N_u indicates a deviation from unitarity of $\mathcal{N}$. With that in mind, following [74] we define the *unitarity* $u(\mathcal{N})$ of the channel $\mathcal{N}$ as

$$u(\mathcal{N}) = \frac{1}{d^2-1}\operatorname{Tr}\left(N_u^T N_u\right), \tag{2.34}$$

which is 1 for unitary channels and strictly less than 1 for nonunitary channels. For a fixed value of the infidelity r, the unitarity achieves its minimum for the depolarizing channel [76], where

$$u(\mathcal{N}) = \frac{1}{d^2-1}\left(\operatorname{Tr} N_u^2\right) = p^2 = \left(1 - \frac{dr}{d-1}\right)^2 . \tag{2.35}$$

The unitarity u and the benchmarking parameter p together provide a useful characterization of the coherence of a channel. We will be primarily interested in the case where the infidelity r is small, so that the diagonal elements $\{N_{ii}\}$ of the Pauli transfer matrix are close to one, and it makes sense to expand in the small quantity $1 - N_{ii}$. Writing

$$(N_u)_{ii}^2 = (1 - (1 - (N_u)_{ii}))^2 = 1 - 2\,(1 - (N_u)_{ii}) + (1 - (N_u)_{ii})^2 , \tag{2.36}$$

we see that

$$\begin{aligned} u(\mathcal{N}) = \frac{1}{d^2-1}\sum_{i,j}(N_u)_{ij}^2 = 1 - 2(1-p) + \frac{1}{d^2-1}\sum_{i,j|i\neq j}(N_u)_{ij}^2 \\ + \frac{1}{d^2-1}\sum_{i}(1-(N_u)_{ii})^2 . \end{aligned} \tag{2.37}$$

Expanding the square root of u, we find

$$\sqrt{u(\mathcal{N})} = p + \frac{1}{2(d^2-1)}\sum_{i,j|i\neq j}(N_u)_{ij}^2 + \cdots , \tag{2.38}$$

where the ellipsis indicates terms that are fourth order in the off-diagonal entries $(N_u)_{ij}$ and terms that are quadratic order in $(1 - (N_u)_{ii})$.

The *coherence angle* Θ is defined as

$$\Theta = \arccos\left(p/\sqrt{u}\right) , \tag{2.39}$$

which for p and u close to one, can be expressed as

$$\Theta^2 = 2\left(1 - \frac{p}{\sqrt{u}}\right) + \cdots = \frac{1}{d^2-1}\sum_{i,j|i\neq j}(N_u)_{ij}^2 + \cdots . \tag{2.40}$$

Apart from a normalization factor, and neglecting the higher-order terms, Θ^2 is the sum of squares of all off-diagonal terms in N_u. It quantifies the coherence in the channel.

For the qubit rotation channel in equation (2.23), the coherence angle is related to the rotation angle θ by

$$\Theta^2 \approx \frac{2}{3}\sin^2\theta \approx \frac{2}{3}\theta^2. \tag{2.41}$$

For the dephasing/rotation qubit channel in equation (2.28), our truncated power series expansion used to derive equation (2.40) is justified if ϵ is negligible compared to δ, in which case we find

$$\Theta^2 \approx \frac{2}{3}q_R^2\theta^2. \tag{2.42}$$

For the depolarizing channel, $u = p^2$ and hence $\Theta = 0$.

In [25] Carignan-Dugas *et al.* derived a bound on r_m, the infidelity when a *unital* channel $\mathcal{N}$ is applied m times in succession, in terms of the infidelity r and coherence angle Θ of $\mathcal{N}$:

$$r_m \leq mr + \frac{d-1}{2d}m(m-1)\Theta^2 + \cdots, \tag{2.43}$$

where the ellipsis indicates terms higher order in r and Θ^2. In this sense (for unital channels), the coherence angle controls the quadratic growth of r_m as a function of m, when r and Θ^2 are small.

Diamond distance

In some versions of the quantum accuracy threshold theorem, the strength of Markovian noise is characterized by the deviation of a noisy gate from the corresponding ideal gate in the *diamond norm* [49]. This diamond norm deviation is useful for quantifying the damage inflicted when the noisy gate acts on qubits which are entangled with other qubits in a quantum computer. The diamond norm $||\mathcal{E}||_\diamond$ of a linear map $\mathcal{E}$ is defined as the L^1 norm of the extended map $\mathcal{E}\otimes\mathcal{I}$:

$$||\mathcal{E}||_\diamond = \max_\rho ||\mathcal{E}\otimes\mathcal{I}(\rho)||_1. \tag{2.44}$$

If $\mathcal{E}$ acts on Hilbert space $\mathcal{H}$ with dimension d, then $\mathcal{I}$ denotes the identity acting on another Hilbert space $\mathcal{H}'$ with dimension d; the maximum is over all density operators on $\mathcal{H}\otimes\mathcal{H}'$. A measure of noise strength for a noisy channel $\mathcal{N}$ is the diamond distance of $\mathcal{N}$ from the identity channel,

$$D_\diamond(\mathcal{N}) := ||\mathcal{N}-\mathcal{I}||_\diamond. \tag{2.45}$$

If $\mathcal{N}$ is applied m times in succession, we have

$$D_\diamond(\mathcal{N}^m) \leq mD_\diamond(\mathcal{N}). \tag{2.46}$$

Upper and lower bounds on the diamond distance can be expressed in terms of the benchmarking parameter $p(\mathcal{N}) = 1 - r(\mathcal{N})d/(d-1)$ and the unitarity $u(\mathcal{N})$ [56]:

$$\frac{\sqrt{d^2-1}}{2d} f(p,u) \leq D_\diamond \leq \frac{d\sqrt{d^2-1}}{2} f(p,u), \tag{2.47}$$

where

$$f(p,u) = \sqrt{(1-2p+u)}. \tag{2.48}$$

For the depolarizing channel, we have $u = p^2$ and $f = 1 - p = rd/(d-1)$; the diamond distance scales linearly with the infidelity r. But for a unitary channel, we have $u = 1$ and $f = \sqrt{2(1-p)}$; then the diamond distance scales like $\sqrt{r}$.

From equation (2.37), we see that

$$f(p,u)^2 = 1 - 2p + u = \frac{1}{d^2-1}\left(\sum_{i,j|i\neq j} (N_u)_{ij}^2 + \sum_i (1-(N_u)_{ii})^2\right), \tag{2.49}$$

which, together with equation (2.47), provides upper and lower bounds on the diamond distance written in terms of Pauli transfer matrix elements:

$$\begin{aligned} D_\diamond(\mathcal{N}) &\geq \frac{1}{d}\left(\sum_{i,j|i\neq j} (N_u)_{ij}^2 + \sum_i (1-(N_u)_{ii})^2\right)^{1/2} \\ D_\diamond(\mathcal{N}) &\leq d\left(\sum_{i,j|i\neq j} (N_u)_{ij}^2 + \sum_i (1-(N_u)_{ii})^2\right)^{1/2}. \end{aligned} \tag{2.50}$$

We will be mostly interested in the upper bound on the diamond distance for a logical channel with a fixed number of encoded qubits; therefore, the unfavorable scaling of the upper bound with the dimension d need not cause us great concern.

Coherence in the chi-matrix representation

The Pauli transfer matrix representation is useful for proving the preceding relationships between channel components, the growth of average infidelity, and the dependence of the diamond distance from identity on the average infidelity. When we analyze error correction, we will make use of a different representation of the noise channel. Any channel $\mathcal{N}$ has an expansion in terms of Pauli operators. Consider a completely positive map $\mathcal{N}$ with Kraus operators $\{K_\alpha\}$, and expand each K_α as

$$K_\alpha = \sum_{i=0}^{d^2-1} c_{\alpha i}\sigma^i, \tag{2.51}$$

where all Pauli operators $\{\sigma^i\}$ are chosen to be Hermitian, and the $\{c_{\alpha i}\}$ are complex numbers. Then

$$\mathcal{N}(\rho) = \sum_\alpha K_\alpha \rho K_\alpha^\dagger = \sum_{i,j=0}^{d^2-1} \chi_{ij}\sigma^i \rho \sigma^j, \tag{2.52}$$

where

$$\chi_{ij} = \sum_\alpha c_{\alpha i} c_{\alpha j}^* = \chi_{ji}^*. \tag{2.53}$$

This is called the chi-matrix representation of the channel. The map $\mathcal{N}$ is trace preserving if

$$\sum_{ij} \chi_{ij}\sigma^j\sigma^i = id, \tag{2.54}$$

and unital if

$$\sum_{i,j} \chi_{ij}\sigma^i\sigma^j = id. \tag{2.55}$$

Note that $\sigma^i\sigma^k\sigma^j = \pm\sigma^k$ if and only if $i = j$; therefore, in the Pauli transfer matrix language, the terms in equation (2.52) with $i = j$ contribute to the diagonal entries in N_{ab}, while the terms with $i \neq j$ contribute to the off-diagonal entries.

To be more concrete, consider the single-qubit rotation about the X-axis $U^X(\theta) = \exp(\big(-i\theta\sigma^X/2\big)$, for which

$$\begin{aligned}\rho \rightarrow U^X(\theta)\rho U^X(\theta)^\dagger = {} & \cos^2(\theta/2)\rho + i\cos(\theta/2)\sin(\theta/2)\rho\sigma^X \\ & - i\cos(\theta/2)\sin(\theta/2)\sigma^X\rho + \sin^2(\theta/2)\sigma^X\rho\sigma^X;\end{aligned} \tag{2.56}$$

hence

$$\begin{pmatrix}\chi_{II} & \chi_{IX} \\ \chi_{XI} & \chi_{XX}\end{pmatrix} = \begin{pmatrix}\frac{1}{2}(1+\cos\theta) & \frac{i}{2}\sin\theta \\ -\frac{i}{2}\sin\theta & \frac{1}{2}(1-\cos\theta)\end{pmatrix}. \tag{2.57}$$

More generally, for the channel with Pauli transfer matrix

$$N = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1-\epsilon & \delta \\ 0 & 0 & -\delta & 1-\epsilon \end{pmatrix}, \tag{2.58}$$

as in equation (2.28), we have

$$\begin{pmatrix}\chi_{II} & \chi_{IX} \\ \chi_{XI} & \chi_{XX}\end{pmatrix} = \begin{pmatrix}1-\epsilon/2 & i\delta/2 \\ -i\delta/2 & \epsilon/2\end{pmatrix}. \tag{2.59}$$

There is a simple general relationship between the off-diagonal entries of the Pauli transfer matrix N_{ab} and the chi matrix χ_{ij}, namely:

Lemma 1. *The off-diagonal elements of the Pauli transfer matrix N_{ab} and the chi matrix χ_{ij} are related by*

$$\sum_{a,b|a\neq b} N_{ab}^2 = d^2 \sum_{i,j|i\neq j} |\chi_{ij}|^2, \tag{2.60}$$

where $d = 2^n$ is the Hilbert space dimension.

Because of this identity, we may quantify the coherence of a channel using the off-diagonal entries in either N_{ab} or χ_{ij}. The case $d = 2$ is explained explicitly in Appendix A.

Proof. To prove the claim, note that, for any Hermitian Pauli operators σ^i, σ^j, σ^a, we have

$$\sigma^i\sigma^a\sigma^j = \eta_{ij}^{ab}\sigma^b \tag{2.61}$$

for some Hermitian Pauli operator σ^b and some phase η_{ij}^{ab}. By taking Hermitian adjoints of both sides, we also have

$$\sigma^j\sigma^a\sigma^i = \eta_{ij}^{ab*}\sigma^b. \tag{2.62}$$

The phase is $\eta_{ij}^{ab} = \pm 1$ if $\sigma^i\sigma^a\sigma^j$ is Hermitian, and it is $\eta_{ij}^{ab} = \pm i$ if $\sigma^i\sigma^a\sigma^j$ is anti-Hermitian. Furthermore, for each fixed $i \neq j$, as σ^a ranges over the d^2 Hermitian Pauli operators, $\sigma^i\sigma^a\sigma^j$ is Hermitian for $d^2/2$ choices of σ^a, and anti-Hermitian for the remaining $d^2/2$ choices. (If σ^i and σ^j commute, then $\sigma^i\sigma^a\sigma^j$ is Hermitian if and only if σ^a commutes with $\sigma^j\sigma^i$. If σ^i and σ^j anticommute, then $\sigma^i\sigma^a\sigma^j$ is Hermitian if and only if σ^a anticommutes with $\sigma^j\sigma^i$.) Note that $b \neq a$ if $i \neq j$.

The entries in the Pauli transfer matrix are (for $a \neq b$).

$$N_{ab} = \sum_{i,j|i\neq j} \eta_{ij}^{ab}\chi_{ij} = \sum_{i,j|i<j} \left(\eta_{ij}^{ab}\chi_{ij} + \eta_{ij}^{ab*}\chi_{ji}\right), \tag{2.63}$$

where the sum is restricted to $\{i, j\}$ such that $\sigma^i\sigma^a\sigma^j \propto \sigma^b$. The summand is $(\pm 1)\left(\chi_{ij} + \chi_{ji}\right)$ if $\sigma^i\sigma^a\sigma^j$ is Hermitian, and it is $(\pm i)\left(\chi_{ij} - \chi_{ji}\right)$ if $\sigma^i\sigma^a\sigma^j$ is anti-Hermitian. Suppose now that, for fixed i, j, we collect all the terms in $\sum_{a\neq b} N_{ab}^2$ which are quadratic in $\{\chi_{ij}, \chi_{ji}\}$. Because $\sigma^i\sigma^a\sigma^j$ is Hermitian for half the choices of σ^a and anti-Hermitian for half the choices, we have

$$\frac{d^2}{2}\left(\chi_{ij} + \chi_{ji}\right)^2 - \frac{d^2}{2}\left(\chi_{ij} - \chi_{ji}\right)^2 = 2d^2\chi_{ij}\chi_{ji} = d^2\left(|\chi_{ij}|^2 + |\chi_{ji}|^2\right), \tag{2.64}$$

where we have used $\chi_{ij} = \chi_{ji}^*$, which is required by complete positivity.

To complete the proof of the claim, we must verify that all the multilinear terms of the form $\chi_{ij}\chi_{kl}$ (where $\{i,j\}$ and $\{k,l\}$ are disjoint) cancel in the sum $\sum_{a\neq b} N_{ab}^2$. Such a cross term of the form

$$\eta_{ij}^{ab}\eta_{kl}^{ab}\chi_{ij}\chi_{kl} \tag{2.65}$$

arises in N_{ab}^2 when we have

$$\begin{aligned} \sigma^i\sigma^a\sigma^j &= \eta_{ij}^{ab}\sigma^b, \\ \sigma^k\sigma^a\sigma^l &= \eta_{kl}^{ab}\sigma^b. \end{aligned} \tag{2.66}$$

We will consider all such terms with i,j,k,l fixed, as we vary σ^a and σ^b over the possible Hermitian Pauli operators. Multiplying both sides on the left by Hermitian Pauli operator σ^c, we obtain

$$\begin{aligned} \left(\sigma^c\sigma^i\sigma^c\right)\left(\sigma^c\sigma^a\right)\sigma^j &= \eta_{ij}^{ab}\left(\sigma^c\sigma^b\right), \\ \left(\sigma^c\sigma^k\sigma^c\right)\left(\sigma^c\sigma^a\right)\sigma^l &= \eta_{kl}^{ab}\left(\sigma^c\sigma^b\right). \end{aligned} \tag{2.67}$$

Given a standard sign choice for the d^2 Hermitian Pauli operators, we may write

$$\sigma^c\sigma^a = \phi_{ca}^{a'}\sigma^{a'}, \quad \sigma^c\sigma^b = \phi_{cb}^{b'}\sigma^{b'}; \tag{2.68}$$

here *e.g.* $\phi_{ca}^{a'}$ is a phase, which is ± 1 if σ^a and σ^c commute and $\pm i$ if σ^a and σ^c anticommute. We also have

$$\sigma^c\sigma^i\sigma^c = \xi_{ic}\sigma^i, \quad \sigma^c\sigma^k\sigma^c = \xi_{kc}\sigma^k; \tag{2.69}$$

here $\xi_{ic} = \pm 1$ is a sign indicating whether σ^c and σ^i commute or anticommute. Therefore

$$\begin{aligned} \sigma^i\sigma^{a'}\sigma^j &= \left(\xi_{ic}\phi_{ca}^{a'*}\phi_{cb}^{b'}\eta_{ij}^{ab}\right)\sigma^{b'}, \\ \sigma^k\sigma^{a'}\sigma^l &= \left(\xi_{kc}\phi_{ca}^{a'*}\phi_{cb}^{b'}\eta_{kl}^{ab}\right)\sigma^{b'}, \end{aligned} \tag{2.70}$$

and the corresponding cross term arising from $N_{a'b'}^2$ is

$$\xi_{ic}\xi_{kc}\left(\phi_{ca}^{a'*}\phi_{cb}^{b'}\right)^2\eta_{ij}^{ab}\eta_{kl}^{ab}\chi_{ij}\chi_{kl}. \tag{2.71}$$

Now suppose that either σ^c commutes with both σ^a and σ^b or anticommutes with both; in either case $\left(\phi_{ca}^{a'*}\phi_{cb}^{b'}\right)^2 = 1$. As we vary σ^c over the $d^2/2$ Pauli operators with this property, the sign $\xi_{ic}\xi_{kc}$ has the value $+1$ for the $d^2/4$ choices of σ^c such that σ^c commutes with both σ^i and σ^k or anticommutes with both, while $\xi_{ic}\xi_{kc}$ has the value -1 for the $d^2/4$ choices of σ^c such that σ^c commutes with one of σ^i and σ^k and anticommutes with the other. Therefore, as we vary a' and b' over these $d^2/2$ possible choices for σ^c, with i, j, k, l fixed, the cross terms cancel.

Alternatively, suppose that σ^c commutes with one of σ^a and σ^b and anticommutes with the other; then $\left(\phi^{a'*}_{ca}\phi^{b'}_{cb}\right)^2 = -1$. Again, as we vary a' and b' over the $d^2/2$ possible choices for σ^c, with i, j, k, l fixed, $\xi_{ic}\xi_{kc} = +1$ for half of the terms and $\xi_{ic}\xi_{kc} = -1$ for the other half; therefore, the cross terms cancel. This completes the proof. □

2.3 Logical channel for the repetition code

From now on we will use the streamlined notation for single-qubit Pauli operators:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.72}$$

Consider the repetition code, which protects one logical qubit against bit flip (X) errors, but provides no protection against phase (Z) errors. Let us analyze how well this code protects against coherent errors, in which each physical qubit in the code block rotates about the X-axis. Similar calculations were carried out in [37, 44]. Understanding this example will prepare us for an analysis of more general stabilizer codes.

To be as concrete as possible, we will start with the simplest interesting case, the 3-qubit repetition code spanned by $|000\rangle$ and $|111\rangle$. Our goal is to determine the logical channel that results when rotation errors applied to the physical qubits are followed by error correction. We will assume for now that the same rotation is applied to each of the three qubits; this will be generalized later.

Suppose that each physical qubit is subjected to the unitary rotation

$$U^X(\theta) = cI - isX, \quad c = \cos(\theta/2), \quad s = \sin(\theta/2); \tag{2.73}$$

thus the product unitary map applied to the three physical qubits is

$$\begin{aligned} U^X(\theta)^{\otimes 3} = c^3 III - ic^2 s\,(XII + IXI + IIX) \\ - cs^2\,(XXI + XIX + IXX) + is^3 XXX. \end{aligned} \tag{2.74}$$

To perform error correction we measure the operators ZZI and IZZ to obtain two syndrome bits. If the syndrome is trivial (both measurements yield +1), no further action is required. If the syndrome is nontrivial, X is applied to one of the three qubits, returning the state to the code space. Thus the terms in the expansion in equation (2.74) with weight 0 or 1 (where the weight is the number of X's) are error corrected to the logical operator $\bar{I} = III$, while terms with weight 2 or 3 are error corrected to the logical operator $\bar{X} = XXX$. We conclude that the logical channel $\mathcal{N}_L$ is a convex combination of two unitary transformations,

$$\mathcal{N}_L(\rho) = p_0 U^X(\theta_0)\rho U^X(\theta_0)^\dagger + p_1 U^X(\theta_1)\rho U^X(\theta_1)^\dagger, \tag{2.75}$$

where

$$\begin{aligned} p_0 &= c^6 + s^6, & \theta_0/2 &= \arctan(-s^3/c^3) \\ p_1 &= 3\left(c^4 s^2 + c^2 s^4\right), & \theta_1/2 &= \arctan(s/c) = \theta/2. \end{aligned} \tag{2.76}$$

A logical rotation by θ_0 is applied when the syndrome is trivial (weight 0), and a logical rotation by θ_1 is applied when the syndrome is nontrivial (weight 1).

The logical channel has the form specified in equation (2.28), where

$$\epsilon = p_0(1 - \cos\theta_0) + p_1(1 - \cos\theta_1), \quad \delta = p_0 \sin\theta_0 + p_1 \sin\theta_1. \tag{2.77}$$

These expressions for ϵ and δ can be simplified using trigonometric identities. In terms of $s/c = t = \tan\theta/2$, we have

$$\begin{aligned} p_0 &= c^6(1+t^6), & 1 - \cos\theta_0 &= \frac{2t^6}{1+t^6}, & \sin\theta_0 &= \frac{-2t^3}{1+t^6}, \\ p_1 &= 3c^6 t^2(1+t^2), & 1 - \cos\theta_1 &= \frac{2t^2}{1+t^2}, & \sin\theta_1 &= \frac{2t}{1+t^2}; \end{aligned} \tag{2.78}$$

therefore we find

$$\epsilon = 2s^6 + 6c^2 s^4, \quad \delta = -2s^3c^3 + 6s^3c^3 = 4s^3c^3. \tag{2.79}$$

Expanding to leading order for small θ, we have

$$\epsilon \approx \frac{3}{8}\theta^4, \quad \delta \approx \frac{1}{2}\theta^3. \tag{2.80}$$

Here, because ϵ is higher order in θ than δ, equation (2.40) applies, and therefore the coherence angle is

$$\Theta^2 \approx 2\delta^2/3 \approx \theta^6/6. \tag{2.81}$$

From equation (2.32), we see that if this logical channel $\mathcal{N}_L$ is applied m times, the infidelity becomes

$$r_m \approx \frac{1}{3}m\epsilon + \frac{1}{6}m(m-1)\delta^2 \approx \frac{1}{8}m\theta^4 + \frac{1}{24}m(m-1)\theta^6. \tag{2.82}$$

Note that the term quadratic in m actually matches the upper bound in equation (2.43). Equation (2.82) reveals that the coherence of the logical channel is somewhat suppressed, as it takes a number of repetitions $m = O(\theta^{-2})$ for the quadratically growing contribution to r to "catch up" with the dominant linear term.

Now let's do a similar analysis for the length-n repetition code (where n is odd), which corrects up to $(n-1)/2$ bit-flip errors. In this case the logical channel is a convex combination of $(n+1)/2$ unitary rotations,

$$\mathcal{N}_L(\rho) = \sum_{w=0}^{(n-1)/2} p_w U^X(\theta_w)\rho U^X(\theta_w)^\dagger \tag{2.83}$$

where w ranging from 0 to $(n-1)/2$ indicates the weight of a correctable X error occurring in the expansion of $(c - isX)^{\otimes n}$. When the $(n-1)$-bit syndrome is measured, syndromes pointing to a weight-w error occur with total probability

$$p_w = \binom{n}{w}\left[c^{2(n-w)}s^{2w} + c^{2w}s^{2(n-w)}\right] = \binom{n}{w}c^{2n}t^{2w}\left[1 + t^{2(n-2w)}\right], \tag{2.84}$$

and the logical rotation angle conditioned on a weight-w syndrome is

$$\begin{aligned} &\theta_w/2 = (-1)^{(n-1-2w)/2}\arctan\left[(s/c)^{n-2w}\right] \\ &\implies 1-\cos\theta_w = \frac{2t^{2(n-2w)}}{1+t^{2(n-2w)}}, \quad \sin\theta_w = (-1)^{(n-1)/2}(-1)^w\frac{2t^{n-2w}}{1+t^{2(n-2w)}}. \end{aligned} \tag{2.85}$$

Summing over the weight of the syndrome, we find

$$\begin{aligned} \epsilon &= \sum_{w=0}^{(n-1)/2} p_w\left(1-\cos\theta_w\right) = \sum_{w=0}^{(n-1)/2}\binom{n}{w}\left(c^2\right)^w\left(s^2\right)^{n-w}, \\ \delta &= \sum_{w=0}^{(n-1)/2} p_w\sin\theta_w = (-1)^{(n-1)/2}c^n s^n\sum_{w=0}^{(n-1)/2}(-1)^w\binom{n}{w} = 2\binom{n-1}{\frac{n-1}{2}}c^n s^n. \end{aligned} \tag{2.86}$$

In Appendix B we use Stirling's approximation to evaluate the sum in the expression for ϵ. Applying Stirling's approximation to our expression for δ as well, we have proven

Theorem 4. *Consider the length-n repetition code which protects against bit flip (X) errors, subject to the independent unitary noise map*

$$U = \left((\cos\theta/2)\,I - i\,(\sin\theta/2)\,X\right)^{\otimes n}, \tag{2.87}$$

where $\sin^2\theta/2 < 1/2$*. Let* $\mathcal{N}_L(\rho) = \mathcal{R}\left(U\rho U^\dagger\right)$ *be the logical map, where* ρ *is a code state and* $\mathcal{R}$ *decodes using majority voting. Then* $\mathcal{N}_L$ *has Pauli transfer matrix* N *of the form given in equations (2.27) and (2.28), with* ϵ *and* δ *given by*

$$\begin{aligned}\epsilon &= \sqrt{\frac{2}{\pi n}}\left(\frac{\sin^{n+1}\theta}{\cos\theta}\right)\left(1+O\left(\frac{1}{n}\right)\right),\\ \delta &= \sqrt{\frac{2}{\pi n}}\sin^n\theta\left(1+O\left(\frac{1}{n}\right)\right) = \left(\frac{\cos\theta}{\sin\theta}\right)\epsilon\left(1+O\left(\frac{1}{n}\right)\right).\end{aligned} \tag{2.88}$$

Therefore, using equation (2.32) and approximations that are well justified (according to Theorem 4) when n is large and $\sin^2\theta/2 < 1/2$, we can estimate the infidelity when the logical channel is applied m times is succession, finding

$$r_m \approx \frac{1}{3}m\epsilon + \frac{1}{6}m(m-1)\delta^2 \approx \frac{1}{3}\sqrt{\frac{2}{\pi n}}\left[m\left(\frac{\sin^{n+1}\theta}{\cos\theta}\right) + \frac{1}{\sqrt{2\pi n}}m(m-1)\sin^{2n}\theta\right]. \tag{2.89}$$

The scaling of the infidelity $r = O(\theta^{n+1})$ arises because a bit flip error must have weight at least $w = (n+1)/2$ to cause a logical error. The scaling $O(\theta^{2n})$ of the term quadratic in m indicates that the coherence of the logical channel is suppressed when θ is small. It takes $m \approx \sqrt{2\pi n}/\theta^{n-1}$ successive applications of the logical channel $\mathcal{N}_L$ for the quadratic term in r_m to become comparable to the linear term. This suppression arises because larger logical rotations occur with only smaller probability; for example a logical rotation by θ occurs with probability $O(\theta^{n-1})$.

Keeping only the leading-order terms in equation (2.86), we obtain

$$\epsilon \approx 2\binom{n}{\frac{n-1}{2}}\left(\frac{\theta}{2}\right)^{n+1}, \quad \delta \approx 2\binom{n-1}{\frac{n-1}{2}}\left(\frac{\theta}{2}\right)^{n} \implies \delta \approx \frac{n+1}{n}\theta^{-1}\epsilon, \tag{2.90}$$

generalizing equation (2.80). We derived the relationship

$$\epsilon \approx \frac{n}{n+1}(\theta\delta) \tag{2.91}$$

using the identity

$$\sum_{w=0}^{(n-1)/2}(-1)^w\binom{n}{w} = (-1)^{(n-1)/2}\binom{n-1}{\frac{n-1}{2}}, \tag{2.92}$$

which can be proved by induction. For drawing the conclusion that $\theta\delta/\epsilon$ is bounded above by an n-independent constant, the oscillating minus sign in this expression is important — if not for the oscillating sign, the sum would be 2^{n-1}, hence larger than equation (2.92) by a factor which scales like $\sqrt{n}$. This would mean that average infidelity r_m in equation (2.32) would have a large quadratic component relative to the linear component as the code length n becomes large. In other words, the logical noise channel would have significant coherence.

2.4 Repetition code revisited

In this section we will compute the logical channel for the repetition code using a different method than in Section 2.3. This new method can be extended more easily to general stabilizer codes.

Stabilizer formalism

We now briefly review the structure of stabilizer codes, as this will be used in our analysis. Let $\{g_\alpha, \alpha = 1, 2, \ldots, n-k\}$ denote the $n-k$ stabilizer generators for an $[[n, k, d]]$ stabilizer code. These generators are mutually commuting Hermitian Pauli operators such that $g_\alpha^2 = I$. The *syndrome* $s(\sigma^i)$ of Pauli operator σ^i is a length-$(n-k)$ binary vector such that $s(\sigma^i)_\alpha = s_\alpha^i$ where

$$g_\alpha \sigma^i = (-1)^{s_\alpha^i} \sigma^i g_\alpha. \tag{2.93}$$

Note that the syndrome of a product of Pauli operators is additive: $s(\sigma^i \sigma^j)_\alpha = \sigma_\alpha^i + \sigma_\alpha^j$, where the addition is modulo 2.

The code space is the simultaneous eigenstate with eigenvalue 1 of all the stabilizer generators. If $|\bar{\psi}\rangle$ is a pure state in the code space, then

$$g_\alpha \left(\sigma^i |\bar{\psi}\rangle\right) = (-1)^{s_\alpha^i} \sigma^i g_\alpha |\bar{\psi}\rangle = (-1)^{s_\alpha^i} \sigma^i |\bar{\psi}\rangle. \tag{2.94}$$

Therefore, the syndrome of σ^i can be identified by measuring all of the stabilizer generators. Hence we may say that $s\left(\sigma^i\right)$ is the syndrome of the state $\sigma^i|\bar{\psi}\rangle$. A Pauli operator that commutes with the stabilizer generators preserves the code space and is said to be *logical*. We may define a complete set of orthogonal projectors $\{\Pi_s\}$ on the n-qubit Hilbert space, where Π_s projects onto the subspace with syndrome s. Then

$$\Pi_s \Pi_t = \delta_{st} \Pi_s, \quad \sum_s \Pi_s = I. \tag{2.95}$$

An encoded density operator $\bar{\rho}$ (one supported on the code space) has the property

$$\Pi_s \bar{\rho} \Pi_t = \delta_{s0}, \delta_{t0} \bar{\rho}, \tag{2.96}$$

where $s = 0$ denotes the trivial syndrome.

To construct the error recovery map $\mathcal{R}$, we first perform an orthogonal measurement to identify the syndrome s. Then for each syndrome s, a particular Pauli operator $E_s^\dagger$ is applied, which returns the measured state to the code space; therefore,

$$\mathcal{R}(\rho) = \sum_s E_s^\dagger \Pi_s \rho \Pi_s E_s. \tag{2.97}$$

One says that E_s is the *standard error* associated with the syndrome s. In the case of *minimal-weight decoding*, E_s is chosen to be a minimal-weight Pauli operator with syndrome s. By the weight $w(\sigma)$ of the n-qubit Pauli operator σ, we mean the number of qubits to which a nontrivial Pauli matrix X, Y, or Z is applied, while I is applied to the remaining $n - w$ qubits.

By summing over all values of the syndromes s to construct the error recovery channel, we are averaging over all the possible outcomes of the syndrome measurement, with each syndrome weighted by its probability. We discussed in the introduction how to justify performing this average when computing the logical channel.

Recovery in the chi-matrix representation

For any such noise channel $\mathcal{N}$ acting on an encoded density operator $\bar{\rho}$, we would like to find the error corrected map $\mathcal{R} \circ \mathcal{N}(\bar{\rho})$. Using the chi representation of the noise channel, it evidently suffices to compute

$$\mathcal{R}\left(\sigma^i \bar{\sigma}^k \sigma^j\right) \tag{2.98}$$

for each pair of physical Pauli operators σ^i, σ^j and each logical Pauli operator $\bar{\sigma}^k$. Because the syndrome is additive, we have

$$\Pi_s P_t \Pi_s = \delta_{t0} P_0 \Pi_s \tag{2.99}$$

if P_t is any physical Pauli operator with syndrome t, and therefore

$$\begin{aligned} \mathcal{R}\left(\sigma^i \bar{\sigma}^k \sigma^j\right) &= \sum_s E_s^\dagger \Pi_s \sigma^i \bar{\sigma}^k \sigma^j \Pi_s E_s = 0 \\ \text{unless} \quad s\left(\sigma^i \bar{\sigma}^k \sigma^j\right) &= s\left(\sigma^i \sigma^j\right) = 0. \end{aligned} \tag{2.100}$$

That is, only the terms for which σ^i and σ^j have the same syndrome survive when the error recovery map is applied. This property will be crucial in our analysis of the logical channel.

Now let's understand the action of $\mathcal{R}$ in more detail. An $[[n, k, d]]$ stabilizer code has 4^k logical Pauli operators. The physical Pauli operator L representing a logical

Pauli operator is not unique, because L and LG act in the same way on the code space, where G is any element of the stabilizer group. But let us by convention choose standard physical operators $\{L_a, a = 0, 1, 2, \ldots 4^k - 1\}$ representing each of the logical Pauli operators. Since we have also assigned a standard error operator E_s to each syndrome s, any Hermitian Pauli operator has a unique decomposition of the form

$$\sigma(s, a, x) = \eta_{sax} E_s L_a G_x, \quad \eta_{sax} \in \{\pm 1, \pm i\}, \tag{2.101}$$

where G_x is an element of the stabilizer group, and η_{sax} is a phase. Since there are 2^{n-k} stabilizer group elements (up to phases), 2^{n-k} distinct syndromes, and 2^{2k} logical Pauli operators, we see that this decomposition accounts for all 4^n physical Pauli operators. We conclude that if $\bar{\rho}$ is an encoded density operator, then

$$\begin{aligned} \mathcal{R}\left(\sigma(s, a, x)\bar{\rho}\sigma(s', a', x')\right) &= \delta_{ss'} E_s^\dagger \left(\eta_{sax} E_s L_a G_x\right) \bar{\rho} \left(G_{x'}^\dagger L_{a'}^\dagger E_s^\dagger \eta_{s'a'x'}^*\right) E_s \\ &= \delta_{ss'}\, \eta_{sax} \eta_{s'a'x'}^*\, L_a \bar{\rho} L_{a'}^\dagger, \end{aligned} \tag{2.102}$$

where we have used the property that $\sigma(s', a', x')$ is Hermitian. In the logical channel, the terms with $L_a = L_{a'}$ are *incoherent* – they contribute to the on-diagonal elements of the logical Pauli transfer matrix. The terms with $L_a \neq L_{a'}$ are *coherent* – they contribute to the off-diagonal elements.

When the noise channel $\mathcal{N}$ is weak, the dominant terms in the chi-matrix expansion in equation (2.52) are those such that $\sigma^i \sigma^j$ has minimal weight, and we have also seen that the only terms that survive when the recovery map is applied are those such that $\sigma^i \sigma^j$ is a logical operator (has trivial syndrome). Now let's suppose that the code distance is d and that minimal-weight decoding is performed. This means that we choose E_s such that $L_a = I$ (up to multiplication by an element of the stabilizer) whenever $\sigma(s, a, x)$ has weight no larger than $(d-1)/2$, assuming d is odd.

To get a contribution to the incoherent part of the logical channel, we will need both σ^i and σ^j to have weight at least $(d+1)/2$, so that the total weight must be at least $d+1$. In that case it is possible for both σ^i and σ^j to be error corrected to a nontrivial logical operator. But there are also weight-d contributions to the coherent part of the logical channel, arising from the terms in which $w(\sigma^i) + w(\sigma^j) = d$, where $w(\sigma)$ denotes the weight of Pauli operator σ. In that case one of the two Pauli operators has weight less than or equal to $(d-1)/2$, hence is error corrected to the identity, while the other has weight greater than or equal to $(d+1)/2$, hence is corrected to a nontrivial logical operator L. The resulting term in the logical channel is either $L\bar{\rho}$ or $\bar{\rho}L$ (up to a phase), depending on whether σ^i or σ^j has higher weight.

If we choose the standard errors $\{E_s\}$ differently, then the action of the recovery operator may be modified. But it is evident from equation (2.102) that if we make the replacement $E_s \longrightarrow E'_s = \phi_s E_s G_y$, where G_y is an element of the stabilizer and ϕ_s is a phase, then $\mathcal{R}\left(\sigma\bar{\rho}\sigma'\right)$ is not changed. In particular, when we perform minimal-weight decoding, there may be more than one minimal-weight Pauli operator with syndrome s, so that the choice of E_s is ambiguous. However, as long as any two minimal-weight Pauli operators E_s and E'_s with syndrome s have the property that $E_s'^{\dagger}E_s$ is an element of the code stabilizer, then the logical channel will not depend on how the minimal-weight standard errors are chosen. This will certainly be the case if the code distance is d and the standard errors have weight not larger than $(d-1)/2$, since then $E_s'^{\dagger}E_s$ has weight at most $d-1$ and cannot be a nontrivial logical operator.

Analysis of repetition code using the chi-matrix formalism

To illustrate this method, we return to the length-3 repetition code, where the noise channel is as in equation (2.74). We write out the chi-matrix expansion of $\mathcal{N}(\rho)$ in equation (2.52), and then apply the recovery operator $\mathcal{R}$ to find the logical channel $\mathcal{N}_L = \mathcal{R}\circ\mathcal{N}$. The task of applying $\mathcal{R}$ is simplified by the observation that, if the state ρ is supported on the code space, then $\mathcal{R}$ annihilates all terms in which $\sigma^i\sigma^j$ is not logical. We may write

$$\mathcal{N}(\rho) = \mathcal{N}_{\text{incoh}}(\rho) + \mathcal{N}_{\text{coh}}(\rho) + \mathcal{N}_{\text{null}}(\rho), \tag{2.103}$$

where $\mathcal{N}_{\text{null}}$ is the sum of terms such that $\sigma^i\sigma^j$ is not logical (hence $\mathcal{R}\circ\mathcal{N}_{\text{null}} = 0$ acting on encoded density operators), $\mathcal{N}_{\text{incoh}}$ is the sum of terms such that $\sigma^i\sigma^j$ is the logical identity, and $\mathcal{N}_{\text{coh}}$ is the sum of terms such that $\sigma^i\sigma^j$ is a nontrivial logical operator. Then $\mathcal{R}\circ\mathcal{N}_{\text{incoh}}$ is the incoherent part of $\mathcal{N}_L$ and $\mathcal{R}\circ\mathcal{N}_{\text{coh}}$ is its coherent part. Explicitly,

$$\begin{aligned}\mathcal{N}_{\text{incoh}}(\rho) = c^6 III\rho III + c^4s^2\left(XII\rho XII + IXI\rho IXI + IIX\rho IIX\right)\\ + c^2s^4\left(XXI\rho XXI + XIX\rho XIX + IXX\rho IXX\right) + s^6 XXX\rho XXX,\end{aligned} \tag{2.104}$$

and

$$\begin{aligned}\mathcal{N}_{\text{coh}}(\rho) = ic^3s^3\left(XXX\rho III - III\rho XXX\right) + ic^3s^3\big(XII\rho IXX\\ + IXI\rho XIX + IIX\rho XXI - IXX\rho XII - XIX\rho IXI - XXI\rho IIX\big).\end{aligned} \tag{2.105}$$

The code has two syndrome bits, given by the measured values of ZZI and IZZ, and for a minimal-weight decoder we choose the standard errors to be

$$E_{00} = III, \quad E_{01} = IIX, \quad E_{10} = XII, \quad E_{11} = IXI, \tag{2.106}$$

while the nontrivial logical operator is $\bar{X} = XXX$. Each of the Pauli operators in equations (2.104) and (2.105) can be expressed as a product of a standard error and a logical operator which is either $\bar{I} = III$ or $\bar{X}$, so the logical map becomes

$$\begin{aligned} \mathcal{N}_{L,\text{incoh}}(\rho) &= \mathcal{R} \circ \mathcal{N}_{\text{incoh}}(\rho) = \left(c^6 + 3c^4 s^2\right) \rho + \left(3c^2 s^4 + s^6\right) \bar{X}\rho\bar{X}, \\ \mathcal{N}_{L,\text{coh}}(\rho) &= \mathcal{R} \circ \mathcal{N}_{\text{coh}}(\rho) = ic^3 s^3 \left([\bar{X},\rho] - 3[\bar{X},\rho]\right). \end{aligned} \tag{2.107}$$

To compare with our previous calculation of the logical channel, we note that

$$\begin{aligned} \mathcal{N}_{L,\text{incoh}}(\bar{I}) &= \left(c^2 + s^2\right)^3 \bar{I} = \bar{I}, \\ \mathcal{N}_{L,\text{incoh}}(\bar{X}) &= \left(c^2 + s^2\right)^3 \bar{X} = \bar{X}, \\ \mathcal{N}_{L,\text{incoh}}(\bar{Y}) &= \left[\left(c^2 + s^2\right)^3 - 6c^2 s^4 - 2s^6\right] \bar{Y} = \left(1 - 6c^2 s^4 - 2s^6\right) \bar{Y}, \\ \mathcal{N}_{L,\text{incoh}}(\bar{Z}) &= \left[\left(c^2 + s^2\right)^3 - 6c^2 s^4 - 2s^6\right] \bar{Z} = \left(1 - 6c^2 s^4 - 2s^6\right) \bar{Z}, \end{aligned} \tag{2.108}$$

and

$$\begin{aligned} \mathcal{N}_{L,\text{coh}}(\bar{I}) &= \mathcal{N}_{L,\text{coh}}(\bar{X}) = 0, \\ \mathcal{N}_{L,\text{coh}}(\bar{Y}) &= -2ic^3 s^3 [\bar{X},\bar{Y}] = 4c^3 s^3 \bar{Z}, \\ \mathcal{N}_{L,\text{coh}}(\bar{Z}) &= -2ic^3 s^3 [\bar{X},\bar{Z}] = -4c^3 s^3 \bar{Y}. \end{aligned} \tag{2.109}$$

In the notation of equation (2.28), we have found that the logical channel is parameterized by

$$\epsilon = 6c^2 s^4 + 2s^6, \quad \delta = 4c^3 s^3, \tag{2.110}$$

in agreement with the result found in equation (2.79).

Now consider the length-n repetition code, for n odd, where the noise is the product unitary transformation $U^X(\theta)^{\otimes n}$. The incoherent part $\mathcal{N}_{L,\text{incoh}}$ of the logical channel arises from the diagonal terms $\{\sigma^i \rho \sigma^i\}$ in the chi-matrix expansion of $\mathcal{N}(\rho)$. Here σ^i can be any one of the 2^n Pauli operators contained in $\{I, \sigma^X\}^{\otimes n}$. The code can correct $t = (n-1)/2$ σ^X errors, so σ^i is error corrected to $\bar{I}$ if its weight $w(\sigma^i)$ is t

or less, and is error corrected to $\bar{X}$ if its weight is $t+1$ or more. Therefore, if ρ is an encoded density operator, then

$$\mathcal{N}_{L,\mathrm{incoh}}(\rho) = \left(\sum_{w=0}^{t} \binom{n}{w} c^{2(n-w)} s^{2w}\right) \rho + \left(\sum_{w=t+1}^{n} \binom{n}{w} c^{2(n-w)} s^{2w}\right) \bar{X}\rho\bar{X}, \tag{2.111}$$

where the binomial coefficient $\binom{n}{w}$ counts the number of weight-w (or weight-$(n-w)$) operators. Using

$$\sum_{w=0}^{n} \binom{n}{w} c^{2(n-w)} s^{2w} = \left(c^2+s^2\right)^n = 1, \tag{2.112}$$

we see that $\mathcal{N}_{L,\mathrm{incoh}}(\bar{I}) = \bar{I}$ and $\mathcal{N}_{L,\mathrm{incoh}}(\bar{X}) = \bar{X}$, and furthermore

$$\mathcal{N}_{L,\mathrm{incoh}}(\bar{Y}) = \left(1 - 2\sum_{w=t+1}^{n} \binom{n}{w} c^{2(n-w)} s^{2w}\right) \bar{Y}; \tag{2.113}$$

hence

$$\epsilon = 2\sum_{w=(n+1)/2}^{n} \binom{n}{w} c^{2(n-w)} s^{2w} \tag{2.114}$$

in agreement with equation (2.86). To leading order in $s \approx \theta/2$, this becomes

$$\epsilon \approx 2\binom{n}{\frac{n+1}{2}} \left(\frac{\theta}{2}\right)^{n+1}, \tag{2.115}$$

as in equation (2.90).

The coherent part $\mathcal{N}_{L,\mathrm{coh}}$ of the logical channel arises from the terms in the Pauli operator expansion of $\mathcal{N}(\rho)$ such that $\sigma^i\sigma^j = \bar{X}$. There are 2^n such terms — σ^i can be any operator among $\{I, X\}^{\otimes n}$, and σ^j is then the complementary operator with X and I interchanged. If σ^i has weight $\le t$, and so is error corrected to $\bar{I}$, then σ^j has weight $\ge (t+1)$, and so is error corrected to $\bar{X}$. We obtain

$$\begin{aligned}\mathcal{N}_{L,\mathrm{coh}}(\rho) &= \left(\sum_{w=0}^{t} \binom{n}{w} c^{w}(-is)^{n-w} c^{n-w}(is)^{w}\right) \bar{X}\rho \\ &\quad + \left(\sum_{w=0}^{t} \binom{n}{w} c^{n-w}(-is)^{w} c^{w}(is)^{n-w}\right) \rho\bar{X} \\ &= (-i)^n c^n s^n \left(\sum_{w=0}^{t} (-1)^w \binom{n}{w}\right) [\bar{X}, \rho]. \end{aligned} \tag{2.116}$$

Therefore,

$$\mathcal{N}_{L,\mathrm{coh}}(\bar{Y}) = 2(-i)^{n-1}(cs)^n \left(\sum_{w=0}^{t} (-1)^w \binom{n}{w}\right) \bar{Z}; \tag{2.117}$$

hence

$$\delta = 2(-i)^{n-1}\left(\sum_{w=0}^{(n-1)/2}(-1)^w\binom{n}{w}\right)(cs)^n \approx 2\binom{n-1}{\frac{n-1}{2}}\left(\frac{\theta}{2}\right)^n, \tag{2.118}$$

in agreement with equation (2.90).

Inhomogeneous X-axis rotations

Now let's consider the logical channel obtained by decoding the length-n repetition code, in the case where the rotation angle varies from qubit to qubit. That is, the unitary noise channel is

$$U^X(\theta_1,\theta_2,\ldots\theta_n) = \bigotimes_{\alpha=1}^{n}\left(c_\alpha - is_\alpha\sigma^X\right), \tag{2.119}$$

where $c_\alpha = \cos\theta_\alpha/2$ and $s_\alpha = \sin\theta_\alpha/2$. As in our previous derivation for the case where all angles are equal, we can calculate the incoherent and coherent parts of the logical channel by expanding this tensor product and isolating the terms in $\mathcal{N}(\rho)$ of the form $\sigma^i\rho\sigma^j$ where $\sigma^i\sigma^j$ is either a trivial logical operator (for the incoherent part) or a nontrivial logical operator (for the coherent part). The only difference from the previous calculation is that, while previously all terms in the expansion of U^X with the same weight occurred with equal amplitudes, now operators of the same weight may have different amplitudes.

Still, the derivation goes through in much the same way as before. Let S denote a subset of the n qubits, let $|S|$ denote the size of S, and let $\bar{S}$ denote the subset complementary to S. Extending our previous argument to the case of unequal angles yields

$$\begin{aligned}\epsilon &= 2\sum_{S,|S|\geq t+1}\prod_{\alpha\in S}\prod_{\bar\alpha\in\bar S}c_{\bar\alpha}^2 s_\alpha^2,\\ \delta &= (-2i)\sum_{S,|S|\leq t}\prod_{\alpha\in S}\prod_{\bar\alpha\in\bar S}c_{\bar\alpha}(-is_\alpha)c_\alpha(is_{\bar\alpha})\\ &= (-2i)\prod_{\alpha=1}^{n}(ic_\alpha s_\alpha)\sum_{S,|S|\leq t}(-1)^{|S|}.\end{aligned} \tag{2.120}$$

Note that the sum in the expression for δ does not depend on the angles. To leading order in the small $\{s_\alpha\}$, we find

$$\begin{aligned}\epsilon &= 2\sum_{S,|S|=(n+1)/2}\prod_{\alpha\in S}s_\alpha^2+\cdots,\\ \delta &= 2\binom{n-1}{\frac{n-1}{2}}\prod_{\alpha=1}^{n}s_\alpha,\end{aligned} \tag{2.121}$$

where we have used the identity

$$\sum_{S,|S|\leq\frac{n-1}{2}}(-1)^{|S|}=\sum_{w=0}^{(n-1)/2}(-1)^w\binom{n}{w}=(-1)^{(n-1)/2}\binom{n-1}{\frac{n-1}{2}}. \tag{2.122}$$

As before we find $\epsilon = O(s^{n+1})$ and $\delta = O(s^n)$. Furthermore, the expression for δ is very simple — the same as our previous formula, but with s^n replaced by $\prod_\alpha s_\alpha$.

The formula for ϵ depends in a more complicated way on the set of angles $\{\theta_\alpha\}$. But we can show that for fixed δ, ϵ is minimized when all the s_α are equal. Therefore, we have a lower bound on ϵ, namely

$$\epsilon \geq 2\binom{n}{\frac{n+1}{2}}s^{n+1}+\cdots \tag{2.123}$$

where the ellipsis indicates terms higher order in s, and we have defined

$$s^n=\prod_{\alpha=1}^{n}s_\alpha. \tag{2.124}$$

Correspondingly, using

$$\binom{n}{\frac{n+1}{2}}=\frac{2n}{n+1}\binom{n-1}{\frac{n-1}{2}}, \tag{2.125}$$

we have the upper bound on δ:

$$\delta\leq\frac{n+1}{2n}\left(\frac{\epsilon}{s}\right)+\cdots . \tag{2.126}$$

Therefore, for inhomogeneous as well as homogeneous rotations, we conclude that the coherent part of the logical channel is suppressed. In fact, the case where all rotation angles are equal is the worst case, where equation (2.126) is saturated.

Now let's prove that ϵ is minimized (for fixed δ), when all $\{s_\alpha\}$ are equal.

Lemma 2. *Consider minimizing the function*

$$f_m(x_1,x_2,\ldots,x_n)=\sum_{S,|S|=m}\prod_{\alpha\in S}x_\alpha \tag{2.127}$$

subject to the constraint $\prod_{\alpha=1}^n x_\alpha = c > 0$, where all x_α are nonnegative. Here S denotes a subset of the n variables, and $|S|$ is the size of S. The minimum occurs for $x_1 = x_2 = \cdots = x_n = c^{1/n}$.

Proof. Note that f_m is a symmetric function, invariant under permutations of its n arguments, and can be decomposed as

$$\begin{aligned} f_m(x_1, x_2, \ldots, x_n) = f_m(x_3, \ldots x_n) + x_1 f_{m-1}(x_3, \ldots x_n) \\ + x_2 f_{m-1}(x_3, \ldots x_n) + x_1 x_2 f_{m-2}(x_3, \ldots x_n). \end{aligned} \tag{2.128}$$

Using the constraint we write

$$x_1 = \frac{c}{x_2 x_3 \ldots x_n}, \tag{2.129}$$

and regard f_m as a function of the $n-1$ independent variables $x_2, x_3, \ldots, x_n$; then

$$\frac{\partial}{\partial x_2}(x_1 x_2) = 0, \quad \frac{\partial}{\partial x_2}(x_1) = \frac{-x_1}{x_2}. \tag{2.130}$$

Therefore, setting the gradient of f_m equal to zero, we find

$$\frac{\partial}{\partial x_2} f_m(x_1, x_2, \ldots, x_n) = \left(1 - \frac{x_1}{x_2}\right) f_{m-1}(x_3, \ldots, x_n) = 0. \tag{2.131}$$

The constraint requires that all x_α are positive; therefore $f_{m-1}(x_3, \ldots x_n)$ is positive and we find that $x_1 = x_2$. From the symmetry of f_m, we conclude that $x_1 = x_\alpha = c^{1/n}$ for $\alpha = 2, 3, \ldots, n$, when f_m is stationary. This is the unique stationary point of $f_m(x_1, x_2, \ldots x_n)$ when all x_α are positive; furthermore f_m is smooth and bounded below. Therefore it must be the minimum of f_m. □

2.5 Correlated unitary noise

Now let's consider unitary noise acting on n qubits which does not factorize into a product of single-qubit unitaries. Since we still wish to consider noise that can be corrected by the repetition code, assume that the n-qubit unitary U has an expansion in terms of X-type Pauli operators:

$$U = \sum_S \psi(S) X(S), \tag{2.132}$$

where S denotes a subset of the n qubits and $X(S) = \otimes_{\alpha \in S} X_\alpha$ is the X-type operator supported on S. (X_α means X acting on the αth qubit, and it is implicit that I acts on qubit α for $\alpha \notin S$.) Unitarity of U implies

$$\sum_S |\psi(S)|^2 = 1, \tag{2.133}$$

and

$$\sum_S \psi(S)^* \psi(S + S') = 0, \tag{2.134}$$

where S' is a nonempty set and $S + S' = S \cup S' \setminus S \cap S'$ is the disjoint union of S and S'. To make the analysis of the noise more tractable, let's also suppose the noise is invariant under permutations of the n qubits. In that case $\psi(S) = \psi(|S|)$; that is, the amplitude ψ depends only on the weight $w = |S|$ of the error operator $X(S)$. A tensor product of n identical unitary X rotations, $U = (cI - isX)^{\otimes n}$, is the special case where

$$\psi(w) = c^n \left(\frac{-is}{c}\right)^w , \tag{2.135}$$

an exponential function of the weight w.

The symmetric unitary transformation may also be expressed as $U = e^{-iH}$ where H is a symmetric n-qubit Hamiltonian of the form

$$H = \sum_{w=0}^{n} h_w \left(\sum_{S,|S|=w} X(S) \right). \tag{2.136}$$

We are assuming that there is no geometric locality constraint on the interactions among the qubits — the strength of a weight-w term in the Hamiltonian depends only on the weight, not on which set S of w qubits are interacting. Since h_w is the coefficient of a sum of $\binom{n}{w}$ terms, it is implicit that h_w decays as a function of w. It is natural to assume that $\binom{n}{w} h_w = O(n)$, as only in that case do we expect (for h_w sufficiently small) the probability of a logical error to drop rapidly as n gets large. For example, if $h_2 = O(1)$, then each qubit has $O(1)$ coupling strength with $n-1$ other qubits, so the strength of the noise acting on each qubit grows linearly in n, and error correction fails for n sufficiently large. We will elaborate on this point in the discussion below of two-body correlated noise. In a more realistic noise model, the higher-weight terms in the Hamiltonian would have $O(1)$ strength (independent of system size) but would decay sufficiently rapidly as the distance between qubits increases so that the effective single-qubit noise strength is also $O(1)$ [2, 62].

The structure of the noise correlations is determined by how h_w falls off as the weight w increases. In particular, if $n^{w-1} h_w = O\left(h_1^w\right)$, then $\psi(w)$ in equation (2.132) is a sum of $O\left(h_1^w\right)$ terms; in that case the parameters of the logical channel will be $\epsilon = O(h_1^{n+1})$ and $\delta = O(h_1^n)$, so the coherent and incoherent parts of the logical channel qualitatively resemble what we found for uncorrelated noise. On the other hand, in the extreme case where $h_n \neq 0$ and $h_w = 0$ for $0 \le w \le n-1$, the code provides no protection against logical errors and there is no suppression of coherence. Instead we find $\delta = O(h_n)$ and $\epsilon = O(h_n^2)$ so that $\epsilon = O(\delta^2)$ just as in equation (2.23).

To be concrete, consider the 3-qubit repetition code and noise Hamiltonian

$$H = h_1 \left(X_1 + X_2 + X_3\right) + h_2 \left(X_1X_2 + X_2X_3 + X_3X_1\right) + h_3 \left(X_1X_2X_3\right). \tag{2.137}$$

The unitary noise has the expansion

$$\begin{aligned} U = e^{-iH} &= (1 + \cdots) I + (-ih_1 + \cdots) (X_1 + X_2 + X_3) \\ &+ \left(-ih_2 - h_1^2 + \cdots\right) (X_1X_2 + X_2X_3 + X_3X_1) \\ &+ \left(ih_1^3 - 3h_1h_2 - ih_3 + \cdots\right) X_1X_2X_3, \end{aligned} \tag{2.138}$$

where only the leading terms are shown in the coefficient of each Pauli operator. Repeating the analysis of the logical channel as in Section 2.4, but now using this modified unitary noise operator, we find

$$\begin{aligned} \mathcal{N}_{L,\text{incoh}}(\rho) &= \rho + \left(3h_1^4 + 3h_2^2 + h_3^2 + \cdots\right) \bar{X}\rho\bar{X}, \\ \mathcal{N}_{L,\text{coh}}(\rho) &= \left(ih_1^3 - ih_3\right) [\bar{X}, \rho] - 3h_1h_2 \left(\bar{X}\rho + \rho\bar{X}\right) \\ &\quad - 3ih_1^3[\bar{X}, \rho] + 3h_1h_2 \left(\bar{X}\rho + \rho\bar{X}\right) + \cdots \\ &= -i(2h_1^3 + h_3)[\bar{X}, \rho], \end{aligned} \tag{2.139}$$

(showing only the leading terms), which yields

$$\tilde{\chi}_{XX} = \epsilon/2 = 3h_1^4 + 3h_2^2 + h_3^2 + \cdots, \quad \tilde{\chi}_{XI} = -i\delta/2 = -i\left(2h_1^3 + h_3 + \cdots\right), \tag{2.140}$$

where $\tilde{\chi}$ denotes the logical chi matrix after error correction. (We don't find any contribution to the coherent part of the logical channel depending only on h_2, because the h_2 term in the Hamiltonian has even X parity, while the logical operator $\bar{X}$ has odd parity.) Now whether coherence is suppressed hinges on the strength of the h_3 term in the Hamiltonian. In particular, if h_3 is large compared to h_1^2 and h_2, then highly correlated noise dominates, and coherence of the logical channel is unsuppressed.

As another instructive example, consider the length-n repetition code, where the Hamiltonian contains only single-qubit and two-qubit terms. We will compute the coherent and incoherent parts of the logical channel following the same reasoning as in Section 2.4. Again, we'll need to sum over all the possible values of the syndrome weight, which we'll now denote by k. For each value of k, we'll find a contribution to the chi matrix for the error-corrected logical channel, with logical operators acting on the encoded density operator ρ from the left and from the right.

Each such operator can be obtained in many ways as a product of one-body and two-body terms in the Hamiltonian, and we'll have to do some combinatorics to sum up those contributions. By computing the logical chi matrix, and comparing its coherent and incoherent parts, we can prove the following:

Theorem 5. *Consider the bit flip code with n qubits, and let the noise model be given by the n-qubit unitary map*

$$U = \exp(-iH), \quad \text{where} \qquad H = \sum_i h_1 X_i + \sum_{i<j} h_2 X_i X_j. \tag{2.141}$$

After error correction, the logical noise channel satisfies the following bound relating the coherent and incoherent components:

$$\tilde{\chi}_{XX} \geq \frac{2n}{n+1}(\tan h_1)|\tilde{\chi}_{XI}|, \tag{2.142}$$

where $\tilde{\chi}$ denotes the logical chi matrix. Equation (2.142) holds for any odd n, and for any h_1, but we have made the approximation $nh_2 \ll 1$, neglecting a multiplicative $(1 + O(nh_2))$ correction on the right-hand side.

Theorem 5 implies that, even for this correlated unitary noise model, the coherence of the logical noise channel is heavily suppressed for large n. In fact, the ratio of the coherent to incoherent components of the logical noise channel is similar to what we found for the uncorrelated case, where $h_1 \approx \theta/2$, *c.f.* equation (2.91).

Proof. To prove the lemma, we'll compute first the coherent component of the logical channel, then the incoherent component, and finally we'll compare the two to obtain equation (2.142).

The unitary operator $U = e^{-iH}$ can be expressed as

$$\begin{aligned} U &= \prod_i (c_1 - is_1 X_i) \prod_{i<j} (c_2 - is_2 X_i X_j) \\ &= c_1^n c_2^{n(n-1)/2} \prod_i (1 - it_1 X_i) \prod_{i<j} (1 - it_2 X_i X_j), \end{aligned} \tag{2.143}$$

where $s_1 = \sin h_1, c_1 = \cos h_1, t_1 = \tan h_1$, and likewise for h_2. In our computations, we will suppress the prefactor $c_1^n c_2^{n(n-1)/2}$, which is implicit in all formulas, and we will expand U in a *collisionless approximation*. That is, we will neglect terms in the expansion in which operators such as X_i and $X_i X_j$ or $X_k X_i$ and $X_i X_j$ act on a qubit in common. The terms we are neglecting are systematically suppressed by powers of nh_2 compared to the terms we are keeping. More precisely, these corrections can be absorbed into a multiplicative renormalization of h_1 and h_2 by a factor $(1 + O(nh_2))$.

Coherent component

Let us look first at the coherent component $\tilde{\chi}_{XI}$ of the logical chi matrix. For each syndrome of weight k, the physical error contributing to this logical component consists of an uncorrectable X error of weight $n-k$ on the left of ρ and a correctable X error of weight k on the right, where k ranges from 0 to $(n-1)/2$. The operators on the left and right are supported on disjoint sets of qubits. When we write these operators as products of one-body and two-body terms we will need to count the number of ways of dividing a set of $2p$ X errors into distinct combinations of p two-body terms. We denote this number by κ_p where

$$\kappa_p = \frac{(2p)!}{2^p p!}. \tag{2.144}$$

Let us count the terms with k_L factors of t_2 on the left and k_R factors of t_2 on the right. In addition, there will be some number w of factors of t_1 on the right and $n-2k_L-2k_R-w$ factors of t_1 on the left to fill out the coherent term. First we choose the $2k_L$ qubits on the left where the t_2 terms act; these qubits can be chosen in $\binom{n}{2k_L}$ ways. Once these $2k_L$ qubits have been chosen, there are κ_{k_L} ways to divide up the qubits into pairs where the two-body terms act. Next we choose the $2k_R$ qubits on the right where the t_2 terms act. Because the operators on the left and right are supported on disjoint sets of qubits, these $2k_R$ qubits can be chosen in $\binom{n-2k_L}{2k_R}$ ways. Once these $2k_R$ qubits have been chosen, there are κ_{k_R} ways to divide up the qubits into pairs where the two-body terms act. Of the remaining $n-2k_L-2k_R$ qubits where no two-body terms act, we choose w qubits on the left where the one-body terms acts; these can be chosen in $\binom{n-2k_L-2k_R}{w}$ ways. As usual, this contribution to the logical channel has a phase, which is determined by including a factor of $-i$ for each term in the Hamiltonian which acts from the left and a factor of i for each term in the Hamiltonian which acts from the right. By combining all these factors, we find a contribution to $\tilde{\chi}_{XI}$

$$(i)^{n-w-2k_R-k_L}\,(-i)^{w+k_R} t_1^{n-2k_L-2k_R} t_2^{k_L+k_R} \binom{n}{2k_L}\binom{n-2k_L}{2k_R}\binom{n-2k_L-2k_R}{w} \kappa_{k_L}\kappa_{k_R}. \tag{2.145}$$

Next we sum over w, taking care to note the w-dependent phase in equation (2.145). Fortunately, this sum can be evaluated explicitly using an identity satisfied by binomial coefficients, just as we saw in Section 2.3. The sum ranges from $w = 0$ to $w = (n-1)/2 - k_R$, so we have

$$\sum_{w=0}^{(n-1)/2-2k_R} (-1)^w \binom{n-2k_L-2k_R}{w} = (-1)^{(n-1)/2-2k_R} \binom{n-2k_L-2k_R-1}{(n-1)/2-2k_R}. \tag{2.146}$$

To complete the evaluation of $\tilde{\chi}_{XI}$, it remains to sum over k_L and k_R in

$$\tilde{\chi}_{XI} = \sum_{k_L,k_R} \Omega(k_L,k_R) t_2^{k_L+k_R} t_1^{n-2k_L-2k_R}, \tag{2.147}$$

where from equations (2.145) and (2.146) we have

$$\begin{aligned}\Omega(k_L,k_R) = {} & (i)^{n-k_L-k_R}(-1)^{k_R}(-1)^{(n-1)/2} \\ & \times \binom{n}{2k_L}\binom{n-2k_L}{2k_R}\binom{n-2k_L-2k_R-1}{(n-1)/2-2k_R}\kappa_{k_L}\kappa_{k_R}.\end{aligned} \tag{2.148}$$

In the sum in equation (2.147), $2k_R$ can be any nonnegative integer less than or equal to $(n-1)/2$, and $2(k_R+k_L)$ can be any nonnegative integer less than or equal to $n-1$.

Our goal is to compare this coherent component with the incoherent component, which can also be expressed as a sum. Instead of performing an unrestricted sum over k_L and k_R, we will consider the sum over k_L where $k_L + k_R = q$ is fixed. This collects all the terms in $\tilde{\chi}_{XI}$ of order t_2^q. Then we will follow a similar path to compute the incoherent component $\tilde{\chi}_{XX}$ to order t_2^q, so that we can compare the coherent and incoherent components in each order.

Let us isolate the parts of $\Omega(k_L, q-k_L)$ that depend on q only (not on k_R), and let us introduce the shorthand $m = (n-1)/2$, finding

$$\Omega(q-k_R,k_R) = \frac{(i)^{n-q}(-1)^m(m+1)}{(n-2q)2^q}\binom{n}{m}\frac{(m!)^2}{(2m-2q)!q!} \times (-1)^{k_R}\binom{2m-2q}{m-2k_R}\binom{q}{k_R}, \tag{2.149}$$

where we have used equation (2.144). Now we need to sum k_R from $k_R = 0$ to $k_R = q$, and then sum q from $q = 0$ to $q = (n-1)/2$.

We observe that, due to the oscillating sign $(-1)^{k_R}$, the sum over k_R vanishes when q is odd. This cancellation occurs because if we replace k_R by $q - k_R$, the summand remains the same except for a change in phase $(-1)^q$. What's happening is that for each term contributing to $\tilde{\chi}_{XI}$ with l factors of it_2 on the right and $q-l$ factors of $-it_2$ on the left, there is a corresponding term with $q-l$ factors of it_2 on the right and l factors of $-it_2$ on the left. These two terms have equal magnitude but opposite sign, if q is odd. Similar cancellations occur in the computation of the incoherent component $\tilde{\chi}_{XX}$.

Incoherent component

Now we can use similar reasoning to compute the incoherent component $\tilde{\chi}_{XX}$ of the logical channel. In this case, though, we will not perform a sum over all syndromes; instead we will keep only the contribution of lowest order in t_1 and t_2, arising from the syndrome of highest weight. This will suffice for deriving the lower bound in equation (2.142), because the contributions to $\tilde{\chi}_{XX}$ higher order in t_1 and t_2 are nonnegative. Furthermore, keeping only the lowest-order term is a good approximation when t_1 and t_2 are sufficiently small.

For n odd, this leading-order contribution arises from terms with X acting $(n+1)/2$ times from both the left and the right. In a term with k_L factors of t_2 on the left and k_R factors of t_2 on the right, there will also be $(n+1)/2 - 2k_L$ factors of t_1 on the left, and $(n+1)/2 - 2k_R$ factors of t_1 on the right. Summing over k_L and k_R, and arguing as in our discussion of the coherent contribution, we find

$$\tilde{\chi}_{XX} = \sum_{k_L, k_R} \Delta(k_L, k_R) t_2^{k_L+k_R} t_1^{n+1-2k_L-2k_R} + \cdots . \tag{2.150}$$

Here

$$\Delta(k_L, k_R) = (i)^{m+1-k_L}(-i)^{m+1-k_R}\binom{n}{m}\binom{m+1}{2k_L}\binom{m+1}{2k_R}\kappa_{k_L}\kappa_{k_R}, \tag{2.151}$$

we have defined $m = (n-1)/2$, and the ellipsis indicates nonnegative higher-order corrections. We can again introduce $q = k_L + k_R$ and isolate the portion of $\Delta(q-k_R, k_R)$ that depends only on q:

$$\Delta(q-k_R, k_R) = \frac{(i)^q}{2^q}\binom{n}{m}\frac{((m+1)!)^2}{(2m-2q+2)!q!}\times(-1)^{k_R}\binom{2m-2q+2}{m-2k_R+1}\binom{q}{k_R}; \tag{2.152}$$

here k_R is to be summed from 0 to q, followed by a sum over q from 0 to $(n+1)/2$. As for the coherent component, the sum over k_R with q fixed vanishes when q is odd, due to the oscillating minus sign $(-1)^{k_R}$.

Comparing the coherent and incoherent components

Now we are ready to compare $\tilde{\chi}_{XI}$ and $\tilde{\chi}_{XX}$. In both cases there is a sum over k_R to perform for each even value of q, and by inspecting (2.149) and (2.152) we see that the k_R-dependent factors in $\Omega(q, k_R)$ and $\Delta(q, k_R)$ are nearly the same; the factor in Δ is obtained from the factor in Ω if we replace m by $m+1$. Because this factor grows rapidly with m, we see that the factor in Δ is larger than the factor in Ω for each value of q and k_R, but that by itself does not suffice for comparing $\tilde{\chi}_{XI}$ and $\tilde{\chi}_{XX}$, due to the alternating sign $(-1)^{k_R}$ in the sum over k_R.

To compare the coherent and incoherent logical noise components properly, we must perform the sum over k_R. We will make use of the generalized hypergeometric function ${}_3F_2$. This function is defined

$$ {}_3F_2\left[\begin{matrix} a, & b, & c \\ & d, & e \end{matrix};\ z\right] = \sum_{k=0}^{\infty} \frac{(a)_k(b)_k(c)_k z^k}{(d)_k(e)_k k!}, \tag{2.153}$$

where $(a)_k$ denotes the Pochhammer function or the rising factorial

$$ (a)_k = a(a+1)(a+2)(a+3)\ldots(a+k-1). \tag{2.154}$$

If a is a negative integer, then

$$ \frac{(a)_k}{k!} = (-1)^k \binom{-a}{k}, \tag{2.155}$$

and the sum over k in equation (2.153) terminates — instead of 0 to ∞, the sum runs from 0 to $-a$. The same is true if b or c is a negative integer.

Using this definition of ${}_3F_2$, we can write the sum over k_R of Ω or Δ in terms of ${}_3F_2$. We will have to distinguish the two cases $2q < m$ and $2q \geq m$, although we will see at the end that the final expressions will coincide for the two cases. Take the second term in equation (2.149). Supposing that $2q < m$, we can write

$$ \begin{aligned} \sum_{k_R} (-1)^{k_R} \binom{2m-2q}{m-2k_R}\binom{q}{k_R} &= \binom{2m-2q}{m} \sum_{k_R} \binom{q}{k_R} \frac{m(m-1)\ldots(m-2k_R+1)}{(m-2q+2k_R)\ldots(m-2q+1)} \\ &= {}_3F_2\left[\begin{matrix} -q, & \frac{1-m}{2}, & \frac{-m}{2} \\ & \frac{m+1}{2}-q, & \frac{m}{2}-q+1 \end{matrix};\ 1\right] \binom{2m-2q}{m}. \end{aligned} \tag{2.156}$$

Then we can apply Dixon's identity for the hypergeometric function ${}_3F_2$. This reads

$$ \begin{aligned} &{}_3F_2\left[\begin{matrix} a, & b, & -c \\ & 1+a-b, & 1+a+c \end{matrix};\ 1\right] \\ &\quad = \frac{\Gamma(1+\frac{a}{2})\Gamma(1+\frac{a}{2}-b-c)\Gamma(1+a-b)\Gamma(1+a-c)}{\Gamma(1+a)\Gamma(1+a-b-c)\Gamma(1+\frac{a}{2}-b)\Gamma(1+\frac{a}{2}-c)}; \end{aligned} \tag{2.157}$$

c.f. equation (2.3.3.5) in [70]. Applying this formula to equation (2.156), we get

$$\begin{aligned}&\sum_{k_R}(-1)^{k_R}\binom{2m-2q}{m-2k_R}\binom{q}{k_R}\\&\quad=\frac{(-q/2)!}{(-q)!}\frac{\Gamma(m-q/2-1/2)\Gamma(m/2-q-1/2)\Gamma(m/2-q)}{\Gamma(m-q-1/2)\Gamma(m/2-q/2-1/2)\Gamma(m/2-q/2)}\times\binom{2m-2q}{m}.\end{aligned}\tag{2.158}$$

We need to do something about the first factor on the right hand side $(-q/2)!/(-q)!$ because the gamma function has poles at each negative integer. However, this ratio can still be defined:

$$\frac{(-q/2)!}{(-q)!}=\lim_{q/2\to\text{Integer}}\frac{\Gamma(-q/2+1)}{\Gamma(-q+1)}=(-q)_{q/2}=(-1)^{q/2}\frac{q!}{(q/2)!}.\tag{2.159}$$

We can substitute this into equation (2.158) and we find that we can simplify the expression

$$\sum_{k_R}(-1)^{k_R}\binom{2m-2q}{m-2k_R}\binom{q}{k_R}=\frac{(-1)^{q/2}(2m-q)!q!}{(m-q/2)!(q/2)!m!}.\tag{2.160}$$

Up until now we have assumed $2q < m$. If we instead assume $2q \leq m$, we find that the intermediate steps look different, but we arrive at the same final answer as in equation (2.160).

Now we can compute the sum of equation (2.149) as k_R goes from 0 to q using what we found in equation (2.160). We can also apply our result to perform the sum over k_R for equation (2.152). This gives:

$$\begin{aligned}\Omega(q)&\equiv\sum_{k_R}\Omega(q-k_R,k_R)=\frac{(2m-q)!(m+1)!}{(m-q/2)!(q/2)!(2m+1-2q)!2^q}\binom{n}{m},\\\Delta(q)&\equiv\sum_{k_R}\Delta(q-k_R,k_R)=\frac{(2m+2-q)!(m+1)!}{(m-q/2+1)!(q/2)!(2m+2-2q)!2^q}\binom{n}{m}.\end{aligned}\tag{2.161}$$

The ratio of these quantities is

$$\frac{\Omega(q)}{\Delta(q)}=\frac{(2m+2-2q)(m-q/2+1)}{(2m-q+2)(2m-q+1)}=\frac{n+1-2q}{2n-2q}\leq\frac{n+1}{2n}.\tag{2.162}$$

Now we can sum over q; because all terms are nonnegative and the bound holds for every q, we conclude

$$\tilde{\chi}_{XX}>\frac{2n}{n+1}t_1\tilde{\chi}_{XI},\tag{2.163}$$

thus proving the lemma. □

Summary

By setting $q = 0$, we can check that the result in equation (2.161) matches what we found in Section 2.3 for the uncorrelated case. It is also instructive to consider the expansion of $\tilde{\chi}_{XI}$ in powers of t_2, under the assumption $q \ll m$. From equation (2.161) we see that

$$\Omega(q) = \left(\frac{m^{q/2}(2m)^{2q}}{2^q(q/2)!(2m)^q} + \cdots\right)\Omega(0) = \left(\frac{m^{3q/2}}{(q/2)!} + \cdots\right)\Omega(0), \tag{2.164}$$

where the ellipsis indicates $O(q/m)$ corrections.

Restoring the factors of t_1 and t_2 from equation (2.147), we see that this expansion in t_2 generates a multiplicative correction to $\tilde{\chi}_{XI}$ which exponentiates:

$$\sum_{q\,\text{even}} \frac{1}{(q/2)!}\left(\frac{m^3 t_2^2}{t_1^4} + \cdots\right)^{q/2} \approx \exp\left(m^3 t_2^2/t_1^4\right). \tag{2.165}$$

Since the sum over q is dominated by terms with $m^3 t_2^2/t_1^4 \sim q$, this exponential series should be a good approximation for $m^3 t_2^2 t_1^4 \ll m$, or $mt_2 \ll t_1^2$, since in that case neglecting the terms higher order in q/m can be justified. Under this condition, the two-body terms in the Hamiltonian in equation (2.162) make a small contribution to the total energy, suppressed by $O(t_1)$ compared to the one-body terms. Recall that we also needed $mt_2 \ll 1$ to justify the collisionless approximation used in the proof of Theorem 5; this condition is subsumed by $mt_2 \ll t_1^2$ if $t_1 = O(1)$.

We see that there is a regime

$$\frac{1}{m} \gg \frac{t_2}{t_1^2} \gg \frac{1}{m^{3/2}} \tag{2.166}$$

in which our approximations are reliable, yet the multiplicative corrections to $\tilde{\chi}_{XI}$ are large. That large corrections occur, even when the two-body terms make a small contribution to the total energy, is not a surprise; we have found as expected that the noise correlations can substantially enhance the probability of a logical error. The important point established by Theorem 5 (at least for the simple noise model we have analyzed) is that even when the correlated noise produces large corrections to the logical channel, the corrections occur in both the coherent part and the incoherent part of the channel, so that our conclusion that the coherence is strongly suppressed for large n continues to apply.

It is not immediately obvious why the leading power of m in equation (2.164) should be $m^{3q/2}$, because higher powers of m occur in $\Omega(q - k_R, k_R)$ and $\Delta(q - k_R, k_R)$

for each fixed k_R and q. It turns out that these higher powers of m all cancel when we do the sum over k_R. In Appendix C we explain why these cancellations occur, providing a useful check on our results.

2.6 Conclusions

Noise channels on n qubits are in general parameterized by $2^n(2^n - 1)$ independent real parameters. This very large space of possibilities makes it impractical to fully characterize the noise in a large experimental device and also hard to determine the performance of error-correcting codes against completely general noise channels. It is common to study the performance of error-correcting codes against simplified noise models like depolarizing noise. Many of these simple noise models are incoherent noise models, where an error operator is applied with a given probability. In the Pauli transfer matrix representation and the chi matrix representation, these noise channels are diagonal. In this work we have studied a broader class of noise models—unitary noise models and convex combinations of unitary noise models. Unitary noise models are maximally coherent. Fault-tolerant threshold theorems do apply to local coherent noise; however, we set out to answer a different question that is also closely related to the practicality of error correction. Rather than asking about the strength of the residual logical noise, we ask how the coherence of the logical noise channel is suppressed relative to the coherence of the physical noise channel.

We have described coherent and incoherent quantum noise channels in the Pauli transfer matrix and chi matrix representations. The coherence of a noise channel can be characterized by studying the growth of the average infidelity r of the cumulative channel while the noise is applied repeatedly. For incoherent noise channels, r grows linearly with the number of channel applications. For highly coherent channels, r grows quadratically. We also discussed a second diagonostic for coherence. The diamond distance from the identity of an incoherent noise channel scales with r, while for the most coherent noise channels it scales with $\sqrt{r}$. We described how error correction transforms the noise channel to produce the logical noise channel, and we calculated the logical noise channel in the repetition code subject to unitary noise.

The repetition code provided a simple example of a code for which it is not too difficult to exactly calculate the logical noise channel. This direct calculation approach can be applied to any fixed code, although the number of terms in the sum scales with the number of independent stabilizer generators in the code. When the repetition code is subject to unitary single-qubit rotations, the logical noise channel is less coherent than the physical noise channel. As the size of the repetition code grows, the logical noise channel is increasingly incoherent. The basic calculation in the proof of Theorem 4 is similar to calculations in, for example, [37] and [44]. We go beyond the previous calculations for the repetition code by stating our bounds on the coherence of the logical channel in terms of the growth of average infidelity and the relation between diamond distance from identity and average infidelity and additionally by considering a correlated unitary noise model. In Theorem 5 we assumed that a repetition code was subject to a unitary noise model generated by a Hamiltonian consisting of one-body terms and all-to-all two-body terms. We found that even in this case, the coherence of the logical noise is suppressed relative to that of the physical noise, and moreover, this suppression increases with the size of the repetition code.

While it does provide a useful example calculation, the repetition code is not a quantum error-correcting code because it only corrects one type of Pauli error. For quantum computation, families of quantum error-correcting with fault-tolerant thresholds are required. This is the context in which the question of the suppression of logical coherence is most important. In the next chapter, we shift our focus from the toy model of the repetition code to the case of the 2D toric code. This code family represents the first class of topological error-correcting codes to be described [50] and remains among the best studied.

Chapter 3

THE TORIC CODE AGAINST COHERENT NOISE[1]

3.1 Introduction

We now analyze the logical channel for the two-dimensional toric code on an $L \times L$ square lattice, where L is odd. We will continue in the same vein as in the previous chapter, making use of our characterizations of the coherence of a noise channel as well as our technique for calculating the logical noise channel. We'll consider uncorrelated unitary noise acting on the $2L^2$ qubits, and suppose that error correction is performed using minimal-weight decoding. Our goal is to show that, when the noise is sufficiently weak, the coherence of the logical noise channel is highly suppressed for large L.

In the introduction to the previous chapter, we mentioned that the coherence of the logical noise channel in the presence of unitary noise has been previously studied [5, 37, 44]. Our work in this chapter improves on these past results in that we consider a family of codes with an accuracy threshold (toric codes without boundaries) and prove bounds on the logical coherence which apply in the limit of a large code block. By specializing to a particular code family, we also find better bounds on the logical coherence for finite code length. Other authors have obtained numerical results for sufficiently small codes in the case where all physical qubits are rotated about a fixed axis [19, 39, 72], including analyses of logical channels conditioned on particular error syndromes [45]. We focus instead on investigating asymptotic properties for large codes, using analytic methods. Some asymptotic statements about the performance of concatenated codes were proven in [34].

In Chapter 2 the repetition code calculation was exact. Now in the case of the toric code, we estimate the coherent component of the logical chi matrix up to order $L+2\zeta$ in the rotation angle θ, where is any L-independent constant, and relate this coherent component to the incoherent component of the logical channel. Our main theorem states that the strength of the coherent part of the logical channel is bounded above by strength of the incoherent part times a factor of $1/\theta$. (Here θ is the rotation angle applied to each of the physical qubits — our result also holds for rotation angles and axes that vary somewhat from qubit to qubit.) From this statement, we may infer

[1] The work in this chapter was carried out in collaboration with John Preskill.

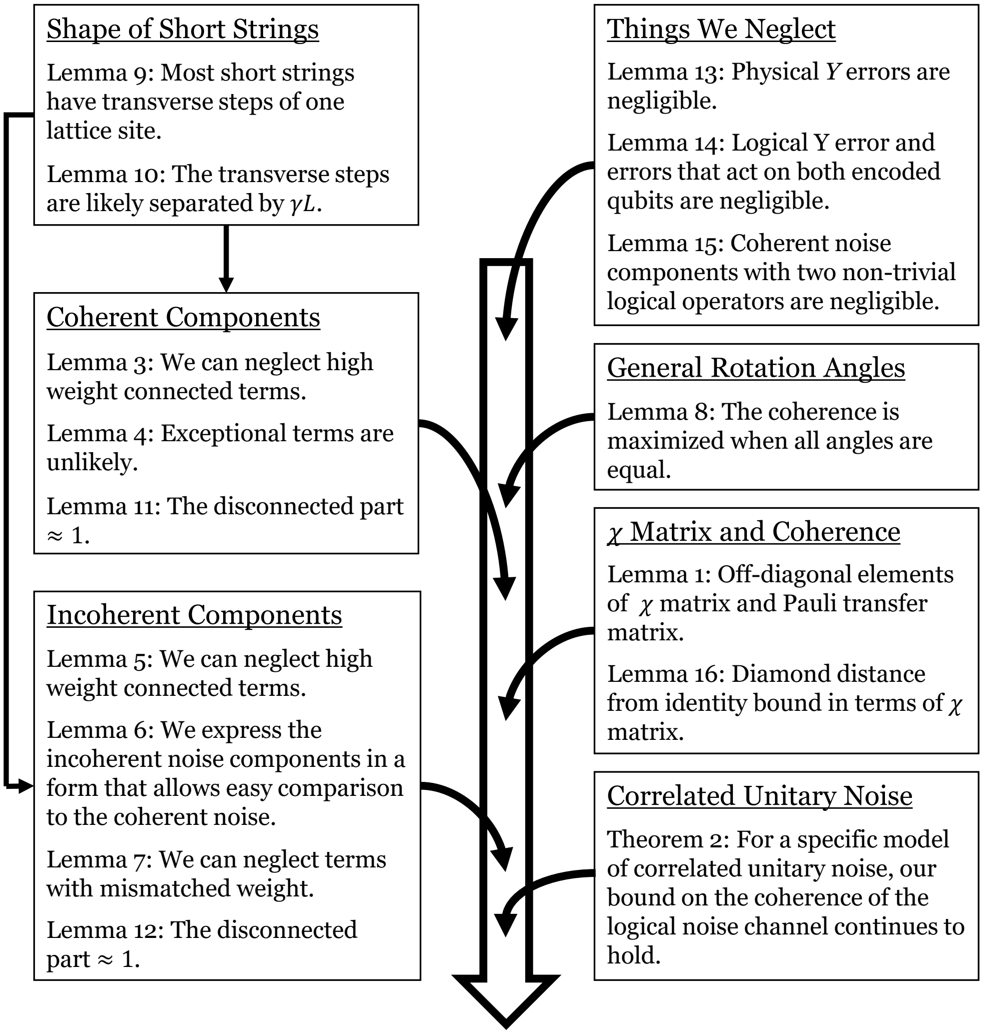
that when the logical channel is applied m times in succession, the average infidelity grows linearly with m. (There is a small contribution to the infidelity that grows quadratically with m, but this contribution is highly suppressed by a factor that scales as L^{-L}.) Stated differently, our result says that after m applications of the logical channel, the accumulated distance from the identity channel, as measured by the diamond norm, grows linearly with m, apart from a correction which is negligible for large L. To reach this conclusion it is necessary to assume that the rotation angle θ scales with the block size as $1/L$. Therefore, unfortunately, we are not able to make a definitive statement about the coherence of the logical channel in the more physically relevant case where L becomes large with θ fixed; the combinatoric task required exceeds our ability.

In this chapter, we build on lessons learned from the analysis of the repetition code to prove our main result, which asserts that, for an independent unitary noise model, the coherence of the logical channel is strongly suppressed by the toric code when the code block is large, assuming that the noise strength scales like $1/L$. The proof mainly consists of a combinatoric analysis which allows us to bound the coherent and incoherent components of the logical chi matrix. We have divided the proof into a series of lemmas; figure 3.1 indicates how these lemmas fit together to build our main theorem. The appendices provide various supplementary details to accompany this chapter. Furthermore, our analysis of two-body correlated noise in the repetition code can be extended to the toric code assuming the noise is sufficiently weak for error correction to succeed with high probability; therefore we conclude that the coherence of the logical channel is highly suppressed even in the case of strongly correlated two-body noise. Section 3.13 contains our conclusions. There we recount some of the obstacles that prevented us from extending our main theorem to the more physically relevant case where the noise strength is a constant independent of L.

Overview of the proof of Theorem 6

Here we provide some additional guidance regarding how the different parts of this chapter fit together to build our main result, Theorem 6 in Section 3.11. The structure of our argument is also summarized in figure 3.1. To prove the theorem we compute first the coherent part of the logical channel and then the incoherent part, after which we can make an inference about how the two are related. For this purpose, upper bounds on the logical noise strength would not suffice. Instead, we compute both the coherent and incoherent part of the logical channel up to an error which we show is small if the physical noise is sufficiently weak.

A Guide to the Proof



Shape of Short Strings

Lemma 9: Most short strings have transverse steps of one lattice site.

Lemma 10: The transverse steps are likely separated by γL.

Coherent Components

Lemma 3: We can neglect high weight connected terms.

Lemma 4: Exceptional terms are unlikely.

Lemma 11: The disconnected part ≈ 1.

Incoherent Components

Lemma 5: We can neglect high weight connected terms.

Lemma 6: We express the incoherent noise components in a form that allows easy comparison to the coherent noise.

Lemma 7: We can neglect terms with mismatched weight.

Lemma 12: The disconnected part ≈ 1.

Things We Neglect

Lemma 13: Physical Y errors are negligible.

Lemma 14: Logical Y error and errors that act on both encoded qubits are negligible.

Lemma 15: Coherent noise components with two non-trivial logical operators are negligible.

General Rotation Angles

Lemma 8: The coherence is maximized when all angles are equal.

χ Matrix and Coherence

Lemma 1: Off-diagonal elements of χ matrix and Pauli transfer matrix.

Lemma 16: Diamond distance from identity bound in terms of χ matrix.

Correlated Unitary Noise

Theorem 2: For a specific model of correlated unitary noise, our bound on the coherence of the logical noise channel continues to hold.

Theorem 3: Coherence is suppressed in the toric code.

Figure 3.1

Our arguments in this chapter make use of observations, discussed in Section 2.4, which apply to any stabilizer code. We may assign a "standard error" E_s to each error syndrome s, and define a decoder which returns the damaged state to the code space by applying $E_s^\dagger$ when the syndrome is measured to be s. This E_s is a Pauli operator acting on the code block. Furthermore, each logical Pauli operator $\tilde{L}_a$ acting on the code may by convention be associated with a particular standard physical Pauli operator L_a — the choice of L_a is not unique, and therefore must be fixed by convention, because we have the freedom to multiply L_a by an element of the code's stabilizer group without changing its logical action. Once the standard error for each syndrome, and the physical Pauli operator corresponding to each logical Pauli operator, are determined, any physical Pauli operator acting on the code block has a unique decomposition of the form (up to a phase factor) $\sigma(s, a, x) = E_s L_a G_x$, where E_s is a standard error, L_a is a standard logical Pauli operator, and G_x is an element of the code stabilizer.

In the chi matrix formalism, the result $\mathcal{N}(\rho)$ of applying noisy channel $\mathcal{N}$ to density operator ρ is expanded as a sum of terms of the form $\sigma(s, a, x)\, \rho\, \sigma(s', b, y)^\dagger$. As explained in Section 2.4, if ρ is a logical density operator, then a term of this form is annihilated by the error recovery operation for $s \neq s'$, and for $s = s'$ is mapped to $L_a \rho L_b^\dagger$, up to a phase. (That phase is important, and we will need to keep track of it carefully.) Recovery is successful if L_a and L_b are both logical identity operators. The terms in the logical channel with $L_a = L_b$ are said to be incoherent, and the terms with $L_a \neq L_b$ are said to be coherent.

The key point is that we have a conceptually simple algorithm for computing the chi matrix for the logical channel, and for identifying its coherent and incoherent parts. To find the coefficient of $L_a \rho L_b^\dagger$ in the logical channel, we just need to sum up the coefficients of all terms in the physical chi matrix of the form $\sigma(s, a, x)\, \rho\, \sigma(s, b, y)^\dagger$, being mindful of phase factors, for all possible values of s, x, y. Unfortunately, in general this algorithm is too complex to carry out in practice, but under suitable conditions we can estimate logical chi matrix with sufficient accuracy for our purposes.

For the case of the toric code, we can begin by noting some helpful simplifications. We choose standard errors defined by minimal-weight decoding. Because of the code's CSS structure, we can analyze the logical X and logical Z errors separately, and in fact a single analysis applies to errors of both types. We don't need to worry about logical Y errors or about logical errors acting nontrivially on more than one of the code's logical qubits (Lemma 14 in Appendix H) because these are so highly suppressed; the same goes for coherent errors in which both L_a and $L_{a'}$ are nontrivial (Lemma 15 in Appendix I). We can assume that the coherent noise rotates physical qubits about an axis in the $X-Z$ plane (Lemma 13 in Appendix G); otherwise the logical noise would be even less coherent. We are left with the task of estimating two nontrivial elements of the logical chi matrix — the coherent term $\tilde{Z}_1\rho\tilde{I}$ term and the incoherent term $\tilde{Z}_1\rho\tilde{Z}_1$, where $\tilde{Z}_1$ denotes the logical Z operator acting on one of the code's two encoded qubits. In the proof of Theorem 6, we estimate both quantities using a series of approximations, and verify that these approximations are trustworthy when the physical noise is sufficiently weak.

First consider the coherent part of the logical chi matrix. We need to sum up all the terms in the physical chi matrix which contribute to $\tilde{Z}_1\rho\tilde{I}$ after the action of the decoding map. Each such term has the form $E_s Z_1 G_x \rho\, G_y^\dagger E_s^\dagger$, where E_s denotes a standard correctable Pauli error, G_x and G_y are Pauli operators in the code stabilizer, and Z_1 is the standard physical Pauli operator whose logical action matches $\tilde{Z}_1$. For the purpose of our computation, we may assume that all the Pauli operators are of the Z type — that is, each applies Z to a subset of the qubits and applies I to the complementary set. For the purpose of enumerating all such contributions, it is convenient to note that the product $G_y^\dagger Z_1 G_x$ of the Pauli operators acting on the density operator from the right and from the left is a logical operator, one commuting with the code stabilizer. This logical operator can be decomposed into a connected path that winds once around on the periodically identified square lattice — what we call a "logical string" — and a collection of homologically trivial closed loops on the lattice — what we call the "disconnected part" of the logical Pauli operator.

We can therefore enumerate all the contributions to $\tilde{Z}_1\rho\tilde{I}$ by this procedure:

1. Consider all possible logical strings.
2. For each logical string, consider all possible "partitions" of that string into an uncorrectable error acting from the left and a correctable error acting from the right.
3. For each logical string and partition, consider all possible choices for the disconnected part. We compute $\tilde{Z}_1\rho\tilde{I}$ by summing all these contributions. Though we can't perform this sum exactly, we can approximate the sum and estimate the resulting errors.

It is for the purpose of approximating this sum that we need the assumption that the rotation angle θ scales like $1/L$, where L is the linear system size. Under this assumption, we show that we make a small error by truncating the sum to include only relatively short logical strings (Lemma 3 in Section 3.4) which have a typical shape (Lemmas 9 and 10 in Appendix D). Summing over all partitions of a fixed logical string is similar to the computation we performed for the repetition code, but with a few new subtleties. Specifically, there are some "exceptional" partitions such that the uncorrectable error acting from the left actually has lower weight than the correctable error acting from the right. Fortunately, we can show that we make a small error by ignoring this effect (Lemma 4 in Section 3.5), simplifying the sum over partitions.

For a fixed connected logical string and partition of that string, we need to sum over disconnected closed loops and partitions of those loops. Performing this sum is almost equivalent to adding up all possible error patterns weighted by their probabilities, which trivially sums to unity. The only complication is that, for some closed loops that closely approach the logical string, and for some special partitions, the additional loop can flip how the error is decoded. It turns out, though, that we make only a small error by ignoring this effect (Lemma 11 in Appendix E).

With all the above simplifications in hand, we can estimate the coherent part of the logical chi matrix. In particular, the sum over partitions for a fixed logical string can be evaluated much as in the proof of Theorem 4 for the repetition code. It then remains to estimate the incoherent part and compare the two.

In the incoherent part, $\tilde{Z}_1$ acts from both the left and the right; therefore, there are two logical strings to keep track of, one on each side. These two logical strings have segments in common, determined by the intersection of the string with the standard error, but are free to fluctuate independently away from those segments (figure 3.8 of Section 3.7). To approximate the sum over contributions from these logical strings to the incoherent part of the logical chi matrix, we may truncate the sum as in the computation of the coherent part, limiting our attention to relatively short strings with a typical shape (Lemma 5 in Section 3.7 and Lemma 6 in Section 3.8), and ignoring complications arising from the disconnected part of the error (Lemma 12 in Appendix F). Furthermore, we may also ignore contributions with "mismatched weight," confining our attention to minimal-weight uncorrectable errors on the logical string acting from both the left and the right (Lemma 7 in Section 3.9). With these approximations, the incoherent part of the logical chi matrix may be expressed in a form which can be conveniently compared with the coherent part.

As for the repetition code, we can justify considering unitary noise such that all physical qubits are rotated by the same angle — rotating different qubits by different angles only makes the logical channel less coherent (Lemma 8 in Section 3.10). For such a coherent noise model with uniform rotation angles, we compare the coherent and incoherent parts of the logical chi matrix, proving Theorem 6 (Section 3.11). Using the findings from Section 2.2, these results can be translated into statements about the diamond distance of the logical channel and about the average infidelity of the m-times repeated logical channel. We also observe (Section 3.11), that our analysis of the performance of the repetition code against two-body correlated coherent noise (Theorem 5) is applicable with few modifications to the toric code as well.

Our conclusion that the coherence of the logical channel is heavily suppressed applies in the limit of large code size L, and under the assumption that the physical qubits are rotated by an angle θ scaling like $1/L$. In Section 3.13 we discuss the difficulties that have prevented us from extending the result to larger values of θ.

Related work

The performance of stabilizer codes against fully coherent unitary noise has been previously studied in [5, 37, 44]. Huang, Doherty, and Flammia [44] derived an inequality which relates the diamond distance $D_\diamond$ of the logical channel from the identity to the rotation angle θ for independent unitary noise, finding

$$D_\diamond \leq c_{n,k} |\sin\theta|^d; \tag{3.1}$$

here d is the code distance, n is the code length, and k is the number of encoded qubits. Their result applies to any stabilizer code, but $c_{n,k}$ grows exponentially with n (it is bounded above by 2^{3n+k+1}), so their result is not very informative for large codes. In contrast, we derive a bound relating the coherent and incoherent components of the logical channel which does not involve any exponentially large factors. We achieve this improved result by specializing to the toric code, and by assuming $\sin\theta < 1/L$. Furthermore, to obtain equation (3.1) the authors of [44] bounded a sum of contributions to the logical channel using the triangle inequality, hence obtaining a bound that would apply even if all the terms in the sum had a common phase. Instead, we sum the contributions with the appropriate phases; the resulting cancellations among terms yield a much smaller result than we would have obtained by merely invoking the triangle inequality. We are able to carry out this more detailed analysis because our assumption $\sin\theta < 1/L$ allows us to restrict our attention to short logical strings, for which approximating the sum becomes a manageable task.

Beale, Wallman, Guttiérrez, Brown, and Laflamme [5] also studied the performance of stabilizer codes against independent unitary noise, and they concluded that the coherence of the logical channel is suppressed. For a fixed code length, they study the limit of small rotation angle θ. If the logical channel is expanded in powers of θ, then for sufficiently small θ the leading term in this expansion dominates, and they draw their conclusions by analyzing this leading term. In effect, they (like us) investigate the case in which the noise strength deceases as the code length increases, but their assumption about the noise strength is much stronger than ours. We (unlike them) include all corrections to the logical channel higher order in θ that are needed to accurately approximate the logical channels for $\sin\theta < 1/L$, albeit only for the special case of the toric code.

Bravyi, Engelbrecht, König, and Peard [19] have studied the performance of the toric code against independent unitary noise numerically, using a clever mapping from qubits to Majorana fermions, for code distance up to $d = 37$, and they found that the coherence of the logical channel becomes negligible as the code length increases, provided that the rotation angle θ is smaller than a nonzero constant threshold value θ_0. Their numerical method applies to a noise model in which all qubits are rotated about the Z axis, which according to our analysis is the worst case that maximizes the coherence of the logical channel. The numerical results support a value of θ_0 greater than 0.25 and less than 0.32, while for the largest code sizes they consider our analytic results apply only for θ less than about 0.027. They characterize the coherence of the logical channel by sampling from the distribution governing the logical rotation angle θ_{logical} conditioned on the measured error syndrome, finding that this distribution becomes strongly peaked around $\theta_{\text{logical}} = 0$ for large code length when θ_{physical} is smaller than θ_0. They also consider, as we do, the logical channel averaged over syndromes, and show that the "twirled" logical channel has an error probability close to the error probability of the untwirled logical channel for large code length, a further indication of suppressed logical coherence. Their numerical findings appear to be at least notionally consistent with our analytic results, though it is difficult to make a quantitative comparison because our formulas are accurate only for asymptotically large L and for $L\sin\theta$ sufficiently small compared to 1.

3.2 Notation

Our analysis will draw heavily on the tools we developed in our study of the repetition code in Chapter 2. Before proceeding further, we will review some notation. We will use the chi matrix to describe the physical noise channel $\mathcal{N}$ acting on the $2L^2$ qubits in the code block:

$$\mathcal{N}(\rho) = \sum_{i,j} \chi_{ij} \sigma^i \rho \sigma^j, \tag{3.2}$$

where $\{\sigma^i\}$ is a basis of Pauli operators.

Definition 1. *When we speak of a "noise term," we will mean a component of the chi matrix for the physical noise channel acting on the qubits in the code block. We will find it convenient to use the notation $(\sigma^i \rho \sigma^j)$ for the number χ_{ij}, the coefficient of $\sigma^i \rho \sigma^j$ in the chi-matrix expansion in equation (3.2).*

We may choose the index that labels a Pauli operator to be (s, a, x), where $\sigma(s, a, x) = E_s L_a G_x$; here s denotes the error syndrome, E_s is the standard error associated with the syndrome s, L_a is a standard choice for the physical Pauli operator that acts as the logical Pauli operator $\tilde{L}_a$, and G_x is an element of the code stabilizer. To compute the logical chi matrix, we sum over the syndrome s and the stabilizer elements, observing that the standard error E_s is removed by the recovery procedure. Hence we find that a term in the logical chi matrix can be expressed in our notation as

$$\tilde{\chi}_{ab} \equiv (\tilde{L}_a \tilde{\rho} \tilde{L}_b^\dagger) = \sum_{s,x,y} (E_s L_a G_x \rho \, G_y^\dagger L_b^\dagger E_s^\dagger). \tag{3.3}$$

We say that the diagonal components of the logical chi matrix $\tilde{\chi}_{ab}$ with $a = b$ are "incoherent" noise terms. and that the off-diagonal terms with $a \neq b$ are "coherent."

3.3 Coherent and Incoherent Logical Components

We are going to analyze the coherent and incoherent sums separately at first. Using path counting and assuming the noise is sufficiently weak, we will prove that in both cases the logical chi matrix is dominated by "short logical strings" (logical Pauli operators of relatively low weight), those with length $\leq L + 2\zeta$ for a constant ζ. Then by summing up the contributions due to these short logical strings, we will derive an inequality relating the coherent and incoherent components of the logical channel.

Our argument will use equation (3.3), where we have expressed the logical chi matrix as a sum of terms in the physical chi matrix. In the next several sections we will analyze the sums contributing to coherent and incoherent components of $\tilde{\chi}_{ab}$. We will make a series of approximations to simplify the sums by neglecting certain terms. In the end we will demonstrate that the two sums are related by a constant factor.

3.4 The Coherent Sum

First, consider the coherent sum. The coherent components of the logical noise channel are sums of terms from the physical noise channel. We want to upper bound the magnitude of these coherent logical components. Before we go any further, we will make some simplifications. For one, we will neglect certain coherent logical noise components. We focus on the components of the logical noise $\tilde{\chi}_{ab}$, where exactly one of the operators L_a and L_b is identity and the other is either an X or a Z error on one of the two encoded qubits. These components of the logical noise channel can be expressed as a sum over physical noise terms:

$$\tilde{\chi}_{aI} = \sum_{s,x,y} (E_s L_a G_x \rho \, G_y^\dagger E_s^\dagger), \tag{3.4}$$

where L_a is either an X or Z logical error on one of the two encoded qubits of the toric code. In Appendix I we prove that we can neglect the coherent terms with non-trivial logical operators on both sides of ρ, and in Appendix H we prove that we can neglect Y logical operators and operators that act non-trivially on both encoded qubits. The proof comes down to showing that terms with a non-trivial error on both sides of ρ, that act on both encoded qubits, or that apply a Y to one of the logical qubits, have high weight relative to the terms we keep. A further simplification concerns the structure of the noise model. Our result applies to a noise model in which the single-qubit unitary operator acting on each qubit has an axis of rotation and angle of rotation that varies somewhat from qubit to qubit. However, we will prove that the most coherent logical channel is one in which the same unitary operator is applied to each qubit, so we may confine our attention to that case for the purpose of deriving a bound on the relative strength of the coherent and incoherent parts of the logical channel.

We will make use of another way of writing the coherent sum. Each coherent term in the form of equation (3.4) can be unambiguously associated with a logical string. The product of the Pauli operators acting on the left-hand and right-hand sides is the logical operator $L_a G_x G_y$, which in general consists of a connected logical string wrapping around the code block, accompanied by some number of closed loops. To be concrete, if L_a is a logical X error, then the logical string contains only physical

X errors, the closed loops are either loops of X errors which are disjoint from the logical string, or closed loops of Z errors which may or may not intersect with the logical string or with the closed loops of X errors (the intersections are the Y errors).

Definition 2. *For a given noise term $(E_s L_a G_x \rho\, G_y^\dagger E_s^\dagger)$, we can extract a connected logical string by removing the topologically trivial loops from $L_a G_x G_y$. Call this logical string $\mathcal{L}$. We define the "connected part" of the noise term as the restriction to the qubits in $\mathcal{L}$. The connected part of $(E_s L_a G_x \rho\, G_y^\dagger E_s^\dagger)$ is a noise term given by*

$$((E_s L_a G_x)|_{\mathcal{L}}\, \rho\, (G_y^\dagger E_s^\dagger)|_{\mathcal{L}}), \tag{3.5}$$

where the symbol $|_{\mathcal{L}}$ denotes the restriction of an operator to the support of $\mathcal{L}$.

Definition 3. *For a noise term $(E_s L_a G_x \rho\, G_y^\dagger E_s^\dagger)$ the "disconnected part" is the part of the noise term not in the connected part. Once again, we can define a continuous logical string $\mathcal{L}$ by removing all topologically trivial closed loops from $L_a G_x G_y$. The disconnected part of $(E_s L_a G_x \rho\, G_y^\dagger E_s^\dagger)$ is given by*

$$((E_s L_a G_x)|_{\mathcal{L}^C}\, \rho\, (G_y^\dagger E_s^\dagger)|_{\mathcal{L}^C}), \tag{3.6}$$

where the symbol $|_{\mathcal{L}^C}$ denotes the restriction of an operator to the qubits in the complement of the support of $\mathcal{L}$.

Furthermore, we will be able to assume that all of the physical single-qubit errors in the connected part are X or Z type. For example, in the case of a logical X-type error, we may neglect terms in which a closed loop of Z errors intersects with the logical string. To justify this assumption, we show in Appendix G that allowing Y errors along the logical string will only make the logical noise channel less coherent.

A coherent term contributing to the logical chi matrix element $\tilde{\chi}_{Z_1 I}$, which includes disconnected errors, is illustrated in figure 3.2. The disconnected part includes identity on the qubits without errors in addition to the the disconnected errors. Z errors acting on the density operator from the left are shown in red, and Z errors acting from the right are shown in blue. Because the errors acting from the left and right have the same syndrome s, the product of the left and right logical operators is logical. The connected logical string crosses the code block near the bottom of the figure. Associated with the syndrome s is the corresponding standard error E_s, the Z error of minimal weight with that syndrome. (If the minimal-weight error is not unique, we arbitrarily choose E_s to be one of the errors of minimal weight by

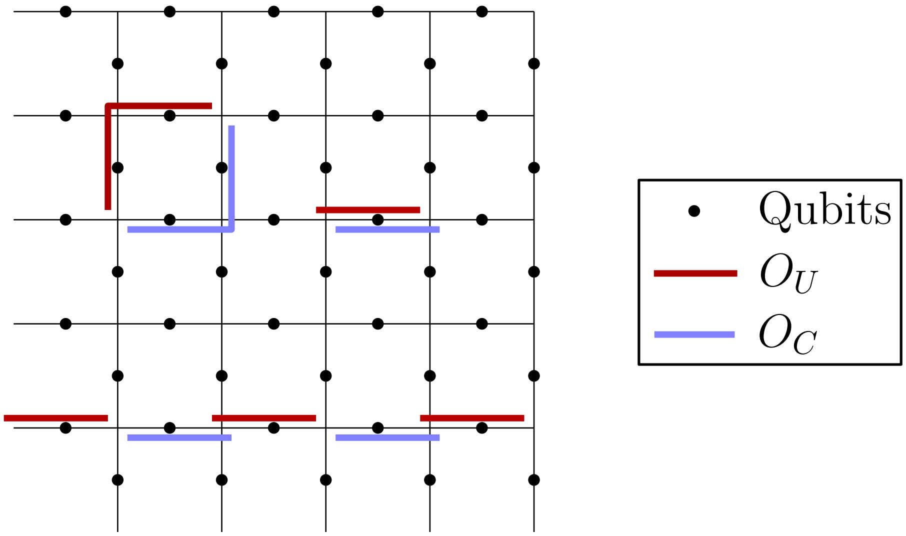


Figure 3.2: In this coherent term, the uncorrectable error O_U (acting on the density operator from the left) is in red, while the correctable error O_C (acting from the right) is in blue. Only Z errors are shown. The connected logical string consists of the five qubits near the bottom that are split between red and blue. In addition, there are disconnected errors in the form of the closed loop containing two red edges and two blue edges and the pair of cancelling single-qubit errors acting on the left (in red) and right (in blue).

convention.) To evaluate the logical chi matrix element $\tilde{\chi}_{Z_1 I}$ as in equation (3.3), we need to sum over the syndrome s and the stabilizer elements G_x and G_y. To facilitate estimating the sum, it will be helpful to organize it in an appropriate way.

To this end, we introduce the following definition:

Definition 4. *For a logical string $\mathcal{L}$ with no topologically trivial closed loops, the word "partition" denotes a connected noise term $(O_1 \rho O_2)$ such that $O_1 O_2 = \mathcal{L}$ and O_1 and O_2 are disjoint. In other words, each partition is a way of dividing the single-qubit errors in $\mathcal{L}$ into two subsets, O_1 and O_2. By definition O_1 and O_2 share the same syndrome. Because the code size L is odd, exactly one of O_1 and O_2 will be corrected to a logical operator with the same action as $\mathcal{L}$ and the other will be corrected to the logical identity.*

For each fixed logical string, the sum over all partitions of the logical string will produce the full set of connected terms derived from that logical string. The sum over partitions, for a fixed logical string, is directly analogous to the sum over syndromes we encountered in our analysis of the repetition code in Section 2.4. In the case of the toric code, we compute the coherent part $\tilde{\chi}_{Z_1 I}$ of the logical channel by summing over all possible logical strings, and for each choice of logical string we sum over all partitions of the logical string. In addition, for each chosen logical string, we sum over the possible disconnected pieces, the additional closed loops of Z errors which are disjoint from the logical string.

Schematically, the coherent component of the logical chi matrix is

$$\tilde{\chi}_{Z_1 I} = \sum_{\text{strings}} \sum_{\text{partitions}} (\text{Connected Part})\,(\text{Disconnected Sum})\,. \tag{3.7}$$

This form will allow us to approximate the coherent sum. Assuming that the noise is sufficiently weak, we will prove that we can truncate the sum over logical strings, including only short strings. Furthermore, most of the short logical strings have a particular shape. To complete the argument, we will show that the disconnected sum is approximately the same for each short logical string and for each partition of the logical string.

Counting of Logical Strings

We want to find an upper bound on the magnitude of the coherent component of the logical noise channel. We have already put the sum over physical noise terms into a convenient form by factoring out the disconnected piece of each term. Next we will simplify the sum by restricting the set of connected pieces we need to consider; we will neglect the long logical strings in favor of those strings with length no larger than than $L + 2\zeta$, where ζ is an L-independent constant. To justify this truncation we will require a strong assumption on how the physical noise strength scales with L; namely, the single-qubit rotation angles must scale as $1/L$.

In equation (3.7), we wrote the contribution of a given logical string to the coherent logical noise as a product of a connected and disconnected part as described in Definitions 2 and 3. The connected part summed over partitions as defined in Definition 4. The sum over partitions contains 2^{w-1} terms for a weight-w logical string (one containing w lattice edges). Suppose that the unitary rotation $U^Z(\theta) = \exp\left(-i\frac{\theta}{2}Z\right)$ is applied to each physical qubit in the toric code block. We can upper bound the sum using the number of terms times the magnitude of each term. Then the contribution of each logical string is upper bounded by $2^{w-1}(|\sin(\theta/2)|\cos(\theta/2))^w$ times the factor from the disconnected part. We will prove in Section 3.6 and Appendix E that the disconnected piece is 1 plus a higher weight correction that we can neglect for short logical strings.

There is a regime where we can upper bound the number of logical strings as a function of the string's length. Asymptotically, the number c_w of self-avoiding random walks with length w was proven in [43] to satisfy

$$c_w = \mu^{w+o(w)}, \tag{3.8}$$

where $\mu \approx 2.64$ for the 2D square lattice. We can start a walk from a fixed point along one edge of the toric code. Logical strings will be the self-avoiding walks that wrap around the torus and end at the starting point. We can use equation (3.8) to show that the contribution to the coherent logical noise from logical strings of length ℓ is exponentially decaying with ℓ as long as $|\theta| < \arcsin 1/\mu \approx 0.39$. This statement applies only for logical strings with length much greater than the minimum of L, the code distance. We do not have a precise estimate indicating at what length above L the number of logical strings begins to scale like equation (3.8). This means we do not know at what string length ℓ the contribution will begin to decay exponentially, and therefore we do not know where to truncate the sum if we wish to use equation (3.8) to bound the terms we are neglecting. In any case, in our subsequent analysis we will truncate the sum over the string length ℓ at $L + 2\zeta$ for some constant ζ. In this regime the asymptotic estimate in equation (3.8) is not helpful and we will not make use of it. Instead, we will assume that $|\theta|$ is sufficiently small that we can use the following lemma to bound the terms we neglect.

Lemma 3. *Suppose that $|\sin\theta| < 1/L$. In equation (3.7), we wrote $\tilde{\chi}_{Z_1 I}$ as a sum over logical strings. If we truncate the sum to include only logical strings of length $w \leq L + 2\zeta$, then magnitude of the difference between the truncated sum and the complete sum is*

$$\leq \alpha L^{2\zeta+1} |\sin\theta|^{L+2\zeta}, \tag{3.9}$$

where $\alpha = (1 - L|\sin\theta|)^{-1}$.

Proof. We begin by fixing a point along one edge of the code block, which can be chosen in L ways. We will count the number of logical strings that wrap around the torus and pass through that fixed point on the edge. Let ℓ denote the logical string length. At minimum length $\ell = L$, there is only one logical string. At length $\ell = L + 2$, if the logical string runs left to right across the code, then the string features one step up and one step down. There are $L(L-1)$ such logical strings. At longer string lengths, there are many steps up and down. We can upper bound the number of such logical strings by supposing we choose any of the L positions to place each of the steps up and steps down. We divide by $((\ell - L)/2)!$ to capture the fact that the $(\ell - L)/2$ steps up are all identical, and the same for the steps down. This encompasses all possible combinations of steps up and down including cases where the several steps up are placed at the same point creating a step up of more than one. It does not encompass strings that backtrack, but in Lemma 9 we show that among strings of length $L + 2\zeta$, those that feature backtracking are suppressed by $O(1/L)$. Also, the number of strings grows most quickly near minimum and eventually approaches the asymptotic value, where the number of strings grows like μ^L. In the asymptotic regime, the number of strings grows much slower than $L^{\ell-L}$. We conclude that

$$\text{number of logical strings of length } \ell \leq LL^{\ell-L}. \tag{3.10}$$

In equation (3.7), for each logical string in the sum, the contribution to the logical noise is a sum over partitions of the connected part times a disconnected part. We will discuss the sum over partitions in detail in Section 3.5, but for now it is enough that we know that the sum over partitions contains $2^{\ell-1}$ terms for each connected logical string of length ℓ. These terms have different phases and in general the sum can be complicated. We can obtain a simple bound by multiplying the number of terms by the magnitude of each term, in other words treating all the phases as if they are the same. For each weight w string,

$$\sum_{\text{partitions}} (\text{Connected Part}) \leq 2^{\ell}(|\sin\theta/2|\cos\theta/2)^{\ell}. \tag{3.11}$$

We still have to handle the disconnected piece. In Section 3.6 we will argue that the disconnected sum decreases as the length of the logical string increases. Furthermore, the disconnected part equals 1 up to corrections which are small for logical strings with length $\leq L + 2\zeta$ for a constant ζ. This means that we can upper bound the coherent logical noise component $\tilde{\chi}_{Z_1 I}$ by

$$\sum_{\ell=L}^{\ell_{\max}} L^{\ell-L+1}|\sin\theta|^{\ell}, \tag{3.12}$$

where $\ell_{\max}$ is the longest Z_1 logical string supported on the code. If $|\sin\theta| < 1/L$, the contribution from logical strings of length ℓ decreases exponentially with ℓ.

If we truncate the sum over logical strings to those with weight $w \leq L + 2\zeta$, the error we make is equal to the total contribution of strings with weight $w > L + 2\zeta$.

The contribution at weight w is exponentially decreasing with w, so we can bound the sum over the long logical strings using

$$\sum_{\ell=c}^{\infty} \beta^{\ell} = \frac{\beta^c}{1-\beta} = \alpha\beta^c \quad 0 < \beta < 1, \tag{3.13}$$

where $\alpha = \frac{1}{1-\beta}$. We conclude that the absolute error we make by truncating the series is

$$\leq \alpha L^{2\zeta+1} |\sin\theta|^{L+2\zeta} \tag{3.14}$$

where $\alpha = (1 - L|\sin\theta|)^{-1}$. Therefore, the error due to truncation is exponentially small in both L and ζ.

□

In Lemma 3 we proved an upper bound on the absolute magnitude of the error due to truncation in the coherent sum. However, so far we have not described any lower bound on the terms that we have kept, arising from the logical strings with length $\leq L+2\zeta$. Therefore, we have not yet justified that the error we have neglected is small relative to the coherent noise contributions that we kept. However, we will prove in Section 3.9 that the *incoherent* logical noise component is at least $L\binom{L}{\frac{L+1}{2}}(\frac{\sin\theta}{2})^{L+1}$; compared to this incoherent component the contribution in equation (3.14) to the coherent component due to strings of length $> L + 2\zeta$ is suppressed by a factor $(L\sin\theta)^{2\zeta}$. This means that the error we make in truncating the sum in Lemma 3 is negligible compared to the incoherent component, an observation which will be helpful for showing that the coherence of the logical channel is suppressed. For now, we will restrict our attention to connected logical strings with length $\leq L + 2\zeta$ for a constant ζ. We will refer to these as "short logical strings."

Definition 5. *A "short logical string" is a nontrivial logical Pauli operator with no topologically trivial closed loops and length $\leq L + 2\zeta$, where L is the code size and ζ is our chosen cutoff constant.*

3.5 Sum Over Partitions

In the previous section we restricted our attention to short logical strings, which have length $\leq L + 2\zeta$ where L is the code size and ζ is a constant. We can go further by characterizing the shape of a logical string, and arguing that logical strings with shape meeting certain criteria give a dominant contribution to the logical channel.

Definition 6. *Among short logical strings, we will speak of those with "typical shape." This means two things. First, supposing that the logical string in question runs left to right across the code block, then the steps up and down along the string are by one lattice spacing at a time. Furthermore, the string contains no backtracking steps that move from right to left. Second, the individual steps up and down are separated from each other by at least $\gamma\sqrt{L}$, where γ is a small constant we may choose. This constant γ will appear in the error term in many of our subsequent estimates.*

In Lemmas 9 and 10 in Appendix D, we prove that most short strings have a typical shape. Among short strings with length $\leq L + 2\zeta$, the fraction of atypical strings relative to the total number of logical strings of the same length is

$$\frac{\text{Atypical strings}}{\text{Total strings}} = \frac{8\gamma\zeta^2}{\sqrt{L}} + O\left(\frac{1}{L}\right). \tag{3.15}$$

Figure 3.3 illustrates a string with typical shape for some small γ. Short logical strings with typical shape are simple, which makes our analysis easier, particularly when we discuss the sum over partitions.

Let's revisit the sum over partitions for a fixed connected logical string. That is, for a given logical string contributing to $\tilde{\chi}_{Z_1 I}$, we wish to enumerate all the ways to divide the Z errors along the string into an uncorrectable error acting on the density operator from the left and a correctable error acting from the right. This sum over partitions of a fixed logical string is analogous to the sum we encountered when we summed over syndromes in our analysis of the repetition code. In the case of the repetition code of length n, there is just one length-n "logical string" to consider, and summing over syndromes is equivalent to summing over all ways of choosing a (correctable) error acting on the right that has weight at most $(n-1)/2$ (where n is odd).

In the toric code, although the sum over partitions is similar to the sum over syndromes in the repetition code, there is a complication.

Definition 7. *An "exceptional term" is a partition of a connected logical string $\mathcal{L}$ such that the uncorrectable error has lower weight than the correctable error.*

In some cases, depending on the geometry of the logical string, we will have some number of exceptional terms. These exceptional terms complicate our analysis of the logical channel. Fortunately, because we need only consider contributions to the logical channel arising from short logical strings when the noise is weak enough, we will be able to fully characterize the exceptional terms and show they are negligible.

How exceptional terms can occur is illustrated in figure 3.4. Here, for the toric code with $L = 9$, we consider the logical string of length 15 shown in figure 3.3, and we have chosen a partition such that the uncorrectable error shown in red has weight 7, while the correctable error shown in blue has weight 8. Note that the minimal-weight standard error associated with the error syndrome on the logical string has weight 6 — it follows nearly the same path as the correctable error, but achieves a lower weight than the correctable error by taking a "shortcut" across the blue notch on the logical string. Another example of an exceptional term for this same logical string is shown in figure 3.5, where this time the weight of the uncorrectable error is 6, and the minimal-weight error has weight 5. Again, the minimal-weight error takes a shortcut, avoiding the excursions up and down followed by the correctable error.

For all these examples, the correctable error contains the qubits along the logical string that make the furthest excursions up and down. This turns out to be a universal rule, at least among the typical short logical strings — for exceptional terms, the uncorrectable error has no support on the outermost steps along the string. In the next lemma we count the number of exceptional terms and find that relative to the total number of partitions of a typical short logical string, these exceptional terms are exponentially unlikely in L.

Lemma 4. *Fix a logical string of length $\ell \leq L + 2\zeta$, where ζ is a specified L-independent constant, with a typical shape according to Definition 7. This means that if the string runs left to right across the code block, it has steps up and down by one lattice spacing at a time and the steps are separated by at least $\gamma\sqrt{L}$ for some constant γ. To keep the fraction of atypical strings small in equation (3.15), we will choose γ to be a sufficiently small constant. Now consider all the ways of partitioning this typical logical string into a correctable error and an uncorrectable error. Then the fraction of exceptional partitions relative to all partitions of this string is bounded by*

$$\frac{\text{Exceptional}}{\text{Total}} < (\zeta + 1)\exp(\gamma^2)\,(2)^{-\gamma\sqrt{L}}\,(1 + O(1/L))\,. \tag{3.16}$$

Exceptional terms are exponentially rare for typical short logical strings and large L.

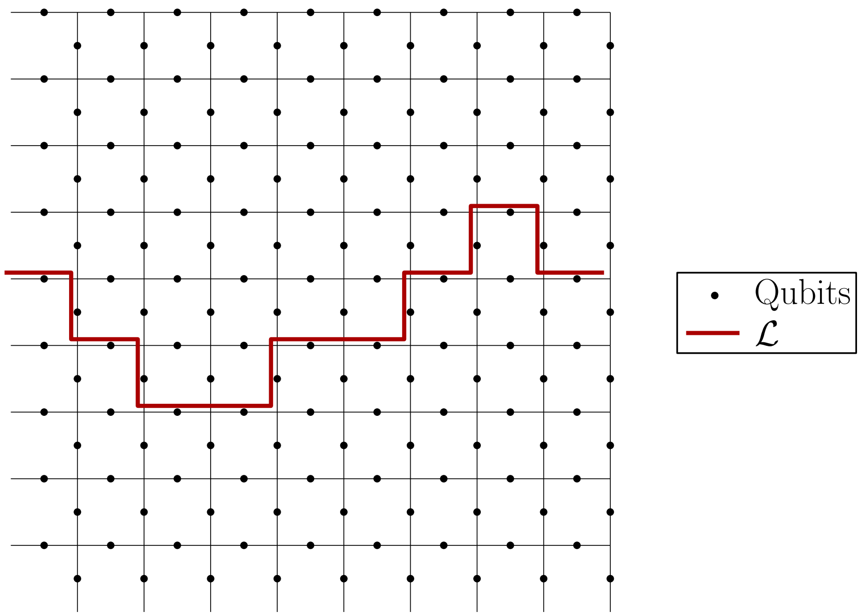


Figure 3.3: Here we have one logical string $\mathcal{L}$ of length 15 in an $L = 9$ toric code. Imagine the code size growing while ζ remains fixed. The likely strings will be those where the steps up and down are widely separated.

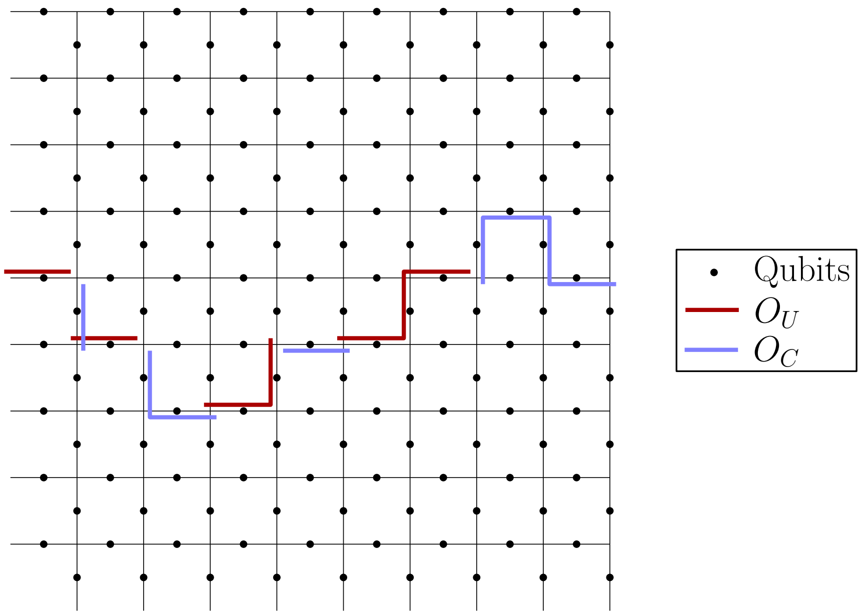


Figure 3.4: Now we choose a subset of 7 of the errors in the logical string in figure 3.3. The uncorrectable error O_U is in red and the correctable error O_C is in blue. All three errors along the "cap" in the top right appear on the correctable side. For this reason, the correctable error has weight 8, which is higher than the uncorrectable error with weight 7. We call this a weight-7 exceptional term.

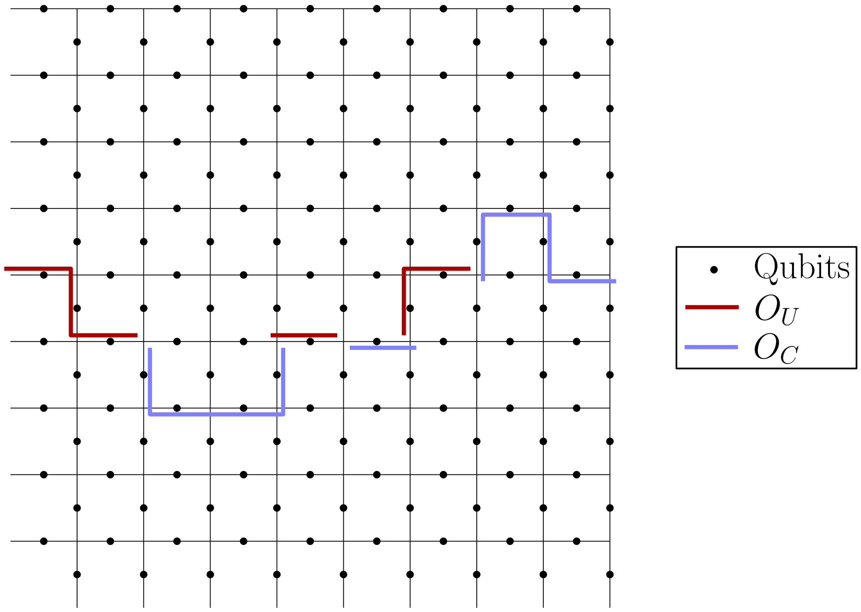


Figure 3.5: Again, one possible partition of the logical string in figure 3.3 is illustrated. The uncorrectable error O_U is in red, and the correctable error O_C is in blue. The correctable error includes all the errors along both the cap in the top right and the bottommost cap of the logical string. For this reason, the correctable error has weight 9, while the uncorrectable error has weight 6. Therefore, we call this partition a weight-6 exceptional term.

Proof. Take a logical string of length $\ell \leq L + 2\zeta$ with typical shape. Each step is separated from the others by at least $\gamma\sqrt{L}$ for some γ. Now, consider taking a subset of $\frac{\ell-1}{2}$ of the qubits in the logical string. We would expect such a subset to be correctable. If not, this partition is exceptional.

Choose a partition of a connected logical string and let O_U be the uncorrectable error and O_C be the correctable error. O_U and O_C share a syndrome by definition. Denote that syndrome by s. The decoding algorithm, which in our case is minimal-weight decoding, applies some correction to this syndrome to return it to the code space. Call this correction E_s. E_s is by definition a correctable error in the code, and therefore, because we are using minimal-weight decoding, E_s must have lower weight than O_U. The fact that we chose our code size L to be odd ruled out the case where the two might be equal. Now if the partition we are considering happens to be exceptional, this means by definition that O_C has higher weight than O_U, and we have

$$\text{Exceptional Term } (O_U \rho\, O_C) \implies \qquad |O_C| > |O_U| > |E_s|. \tag{3.17}$$

We will use this condition to bound the number of exceptional terms for a given connected logical string.

What does it mean for O_C to have higher weight than E_s? For connected logical strings of typical shape as in Definition 6, this happens only if on some subset or subsets of the logical string, the correctable error O_C contains errors on qubits arranged in a "cap." By this we mean a configuration of errors where the errors form three edges of a rectangle. The minimal-weight decoder will choose the fourth edge of the rectangle as part of the correction E_s. This is illustrated in figure 3.4 and figure 3.5. If the connected logical string has length greater than L, then it has steps up and down if it crosses the code block left to right. In every exceptional term, the correctable error O_C will contain the outermost qubits around some of the steps, forming a cap.

Now that we have a simple necessary condition for an exceptional term, we will bound the number of exceptional terms for each short logical string with a typical shape according to Definition 6. Start with a logical string of length ℓ. Consider first the partitions into $\frac{\ell+1}{2}$ and $\frac{\ell-1}{2}$. Of course, those partitions for which the weight-$\frac{\ell+1}{2}$ error is correctable will be exceptional. Every exceptional term like this will have the property that the correctable error contains some number of "caps" where all of the qubits around three sides of a rectangle are part of the correctable error. To bound the number of exceptional terms, we will count the number of partitions with this property.

Each partition of a weight-ℓ connected logical string into weight-$\frac{\ell+1}{2}$ and $\frac{\ell-1}{2}$ errors is formed by choosing $\frac{\ell-1}{2}$ out of the ℓ errors in the logical string. This is what we mean by a partition. We want to count the number of ways of choosing these errors such that the correctable error (of weight $\frac{\ell+1}{2}$ because we are counting exceptional terms) contains all the errors along a "cap." This means that the subset of $\frac{\ell-1}{2}$ errors contains no errors along one or more of the "caps." A typical short logical string running left to right across the code consists of horizontal segments separated by single steps up and down. The outermost of these steps form "caps." The number of such "caps" depends on the particular pattern of steps in the logical string. However, we can bound the number of exceptional terms by counting the number of ways of choosing no qubits along one of the horizontal segments of length $\gamma\sqrt{L}$. This is because every "cap" consists of an outermost horizontal segment combined with the up and down steps on either side. This counting gives

$$\binom{(\ell - \gamma\sqrt{L})}{\frac{\ell-1}{2}} \tag{3.18}$$

ways of choosing no qubits along a horizontal segment of length $\gamma\sqrt{L}$. We want the number of ways of choosing no qubits along at least one of the horizontal segments. There are $\leq 2\zeta$ steps up and down along the logical string. Therefore, there are $\leq 2\zeta$ horizontal segments. We can use a union bound to write

$$\text{Number of weight-}\left(\frac{\ell+1}{2}, \frac{\ell-1}{2}\right)\text{ exceptional terms} \leq 2\zeta\binom{\ell-\gamma\sqrt{L}}{\frac{\ell-1}{2}}. \tag{3.19}$$

This is relative to the total number of $\left(\frac{\ell+1}{2}, \frac{\ell-1}{2}\right)$ partitions for our logical string of length ℓ, which is

$$\text{Total number of }\left(\frac{\ell+1}{2}, \frac{\ell-1}{2}\right)\text{ partitions} = \binom{\ell}{\frac{\ell-1}{2}}. \tag{3.20}$$

We can expand the ratio of exceptional terms to the total using Stirling's approximation. This gives

$$\begin{aligned}2\zeta\binom{\ell-\gamma\sqrt{L}}{\frac{\ell-1}{2}}\Big/\binom{\ell}{\frac{\ell-1}{2}} &= \frac{2\zeta\left(\ell-\gamma\sqrt{L}\right)!\frac{\ell+1}{2}!}{\ell!\left(\frac{\ell+1}{2}-\gamma\sqrt{L}\right)!}\\ &\approx 2\zeta\sqrt{\frac{(\ell+1)(\ell-\gamma\sqrt{L})}{2\ell\left(\frac{\ell+1}{2}-\gamma\sqrt{L}\right)}}\frac{(\ell-\gamma\sqrt{L})^{\ell-\gamma\sqrt{L}}\left(\frac{\ell+1}{2}\right)^{\frac{\ell+1}{2}}}{\ell^{\ell}\left(\frac{\ell+1}{2}-\gamma\sqrt{L}\right)^{\frac{\ell+1}{2}-\gamma\sqrt{L}}}.\end{aligned} \tag{3.21}$$

This approximation holds up to corrections $O(1/\ell)$. We can rewrite this as

$$= 2\zeta\sqrt{\frac{(\ell+1)(\ell-\gamma\sqrt{L})}{\ell(\ell+1-2\gamma\sqrt{L})}}\left(1-\frac{\gamma\sqrt{L}}{\ell}\right)^{\ell}\left(1-\frac{2\gamma\sqrt{L}}{\ell+1}\right)^{-\frac{\ell+1}{2}}\left(\frac{\ell-\gamma\sqrt{L}}{\frac{\ell+1}{2}-\gamma\sqrt{L}}\right)^{-\gamma\sqrt{L}}. \tag{3.22}$$

Next we square the $(1-\frac{\gamma\sqrt{L}}{\ell})$ term in order to combine terms:

$$= 2\zeta\sqrt{\frac{(\ell-\gamma\sqrt{L})}{\ell}}\left(\frac{1-\frac{2\gamma\sqrt{L}}{\ell}+\left(\frac{\gamma\sqrt{L}}{\ell}\right)^2}{1-\frac{2\gamma\sqrt{L}}{\ell+1}}\right)^{\ell/2}\left(\frac{\ell-\gamma\sqrt{L}}{\frac{\ell+1}{2}-\gamma\sqrt{L}}\right)^{-\gamma\sqrt{L}}. \tag{3.23}$$

We upper bound the term inside the radical and also the term raised the power $\ell/2$:

$$< 2\zeta\left(1+\frac{\gamma^2}{\ell-2\gamma\sqrt{\ell}}\right)^{\ell/2}\left(\frac{\ell-\gamma\sqrt{L}}{\frac{\ell+1}{2}-\gamma\sqrt{L}}\right)^{-\gamma\sqrt{L}}. \tag{3.24}$$

The second of the three terms is exponentially decaying to $\exp(\gamma^2/2)$. As long as $\ell \geq 4$, we can bound it by

$$\left(1+\frac{\gamma^2}{\ell-2\gamma\sqrt{\ell}}\right)^{\ell/2} < \exp\gamma^2. \tag{3.25}$$

Now, we bound $\frac{\ell-\gamma L}{(\ell+1)/2-\gamma L} > 2$ and assemble one term raised to the power L and another to the power $(\ell - L)/2$:

$$< 2\zeta \exp(\gamma^2) 2^{-\gamma\sqrt{L}}. \tag{3.26}$$

We chose some small value for γ in Lemma 10, and then the number of exceptional terms with a weight-$\frac{\ell-1}{2}$ logical error on one side and a weight-$\frac{\ell+1}{2}$ correctable error on the other is exponentially small in L.

For the chosen connected logical string of weight ℓ, we have calculated the fraction of exceptional terms among the partitions into $\frac{\ell-1}{2}$ and $\frac{\ell+1}{2}$. We will also have exceptional terms among the partitions into other weights, possibly all the way down to partitions into weight $\frac{L+1}{2}$ and $\ell - \frac{L+1}{2}$. Above, we applied the condition in equation (3.17) that for every exceptional term the correctable error must have higher weight than the minimal-weight correction. If we apply this same method to bound the number of exceptional terms among partitions into $\frac{\ell-3}{2}$ and $\frac{\ell+3}{2}$, we find that the correctable error must be at least 4 longer than the minimal-weight correction. This means we want to count the number of configurations where at least two of the "caps" are contained in the correctable error. This is clearly far fewer than the number of configurations where one "cap" is contained. Therefore, the ratio of exceptional terms to total partitions is bounded by the ratio we found for partitions into $\frac{\ell-1}{2}$ and $\frac{\ell+1}{2}$.

In the end we see that number of weight-$\frac{\ell-1}{2}$ exceptional terms is exponentially small in L for fixed ζ and further that the weight-$\frac{\ell-3}{2}$ exceptional terms are exponentially small in L relative to the higher-weight exceptional terms, and so on. Then for large L, exceptional terms are negligible. □

Lemma 4 allows us to approximate the sum over partitions for a typical, short logical string $\mathcal{L}$. Neglecting exceptional terms, the sum over partitions resembles the calculation of what we called δ in the repetition code in equations (2.86) and (2.118). Let $\mathcal{L}$ have length ℓ. Each partition contributes $\left(\frac{\sin\theta}{2}\right)^\ell$ with a phase. The sum over partitions is given by

$$\begin{aligned}\sum_{\text{partitions}} (\text{Connected Part}) &= \left(\sum_{j=0}^{\frac{\ell-1}{2}} i^\ell (-1)^j \binom{\ell}{j} \left(\frac{\sin\theta}{2}\right)^\ell\right)(1+\epsilon) \\ &= \left(i\binom{\ell-1}{\frac{\ell-1}{2}}\left(\frac{\sin\theta}{2}\right)^\ell\right)(1+\epsilon),\end{aligned} \tag{3.27}$$

where ϵ is the error from exceptional terms, which is upper bounded

$$|\epsilon| < 4\zeta \exp(\gamma^2) 2^{-\gamma\sqrt{L}}. \tag{3.28}$$

This is two times the expression in equation (3.26), because each exceptional term contributes to the sum over partitions with the opposite sign relative to a non-exceptional term.

3.6 The Disconnected Part

In the preceding subsections, we analyzed the coherent component of the logical noise channel, expressed as a sum over many physical noise terms. So far we have only considered the connected logical string associated with each coherent term. In this subsection, we will analyze the disconnected errors in more detail, and describe more rigorously how they affect the evaluation of the coherent terms in the logical channel. In Section 3.4 we described how to decompose a contribution to $\tilde{\chi}_{Z_1 I}$ into a connected piece and some number of disconnected pieces. The left and right hand side of each coherent term can be expanded as the product of the errors contained in the connected logical string and the errors outside of it; schematically,

$$(\mathrm{Conn}_L \mathrm{Disc}_L \, \rho \, \mathrm{Conn}_R \mathrm{Disc}_R) = (\mathrm{Conn}_L \, \rho \, \mathrm{Conn}_R) \text{ Disconnected}. \tag{3.29}$$

The factor "Disconnected" means the contribution to the coherent term from disconnected components that appeared in equation (3.7). The product of the two (disjoint) factors Conn_L and Conn_R yields the connected logical string, with no additional disjoint loops included. The connected factor includes $\sin\theta/2 \cos\theta/2$ for each qubit along the connected logical string. The disconnected factor includes $(\cos\theta/2)^2$ on every qubit not in the connected logical string in addition to a sum over all possible disconnected errors.

Fix a partition $(O_U \rho \, O_C)$ of a short, typical logical string, and consider dressing it with disconnected errors. We can distinguish two types of added errors: incoherent and coherent. If the disconnected error is D_L acting on the density operator from the left, and D_R acting from the right, then if a particular qubit is hit by the same error contained in both D_L and D_R, we say that the disconnected error acting on that qubit is incoherent. If a particular qubit is hit by distinct errors contained in D_L and D_R, then the error is coherent. The product $D_L D_R$ of the errors added on right and left must be a non-identity stabilizer operator, i.e. a closed loop or a set of disjoint closed loops. (Here, because we are investigating the encoded Z errors in the logical channel, only the Z-type physical errors are considered.) The two types

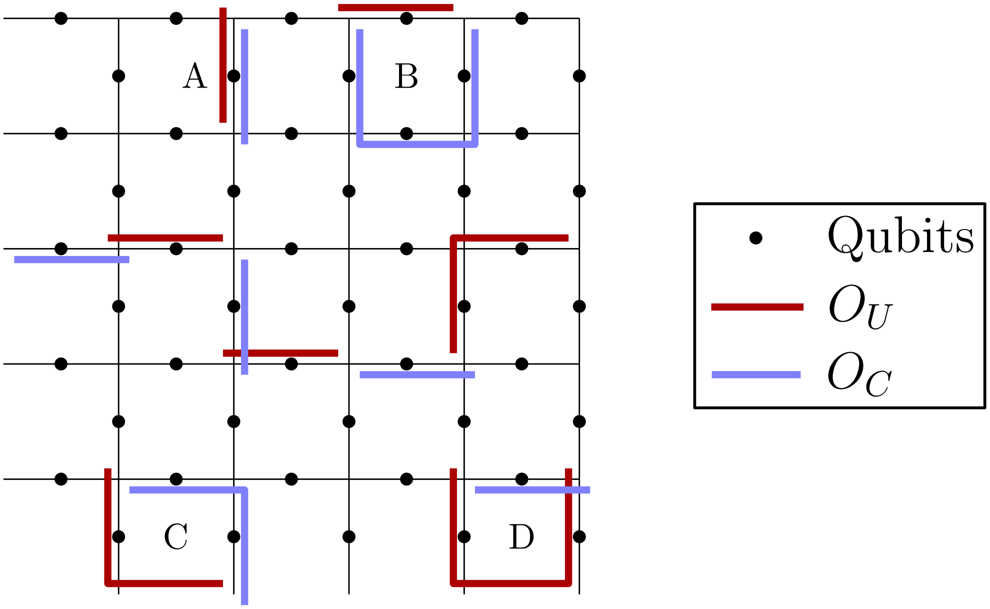


Figure 3.6: Here we have a partition $(O_U \rho\, O_C)$ of a connected logical string adorned in four different ways by added errors. The errors in red are the uncorrectable part, O_U, of the partition, while the errors in blue form the correctable part, O_C. The four added errors are labelled A, B, C, and D. In A, the same error has been added to both O_U and O_C. In B and D, three errors are added to one side of the partition and one to the other. This produces a minus sign. In C, two errors are added to each side.

of added error — incoherent and coherent — are shown in figure 3.6, where (A) is an incoherent-type added error and (B)-(D) are coherent-type.

Let us first treat the case of incoherent-type added errors, where $D_L = D_R \equiv D$. These are the ones with the same disconnected error added to both operators in the partition, for example (A) from figure 3.6. These terms do not change the phase of the original partition, and they multiply the magnitude by $(\sin\theta/2)^{2m}$ if m is the weight of the error added on each side. The disconnected part contains $\cos^2\theta/2$ on each qubit corresponding to no disconnected errors plus many configurations of disconnected errors. The incoherent-type added errors on each qubit in the disconnected part supply the $\sin^2\theta/2$ term to give 1 on the qubits not contained in the connected logical string. This reasoning applies to each incoherent-type added error that does not change how the operators O_U and O_C are decoded. In other words, if D is the disconnected error we add to O_U and O_C, we require that DO_U is an uncorrectable error.

We must be careful because in some cases the added incoherent-type errors can change how the correctable and uncorrectable errors in the partition are decoded. The added error can "flip" the uncorrectable error to a correctable one. This means that the noise term that contributes to the logical $\tilde{\chi}_{Z_1 I}$ component is not $(DO_U\rho DO_C)$ as we would have expected but is instead $(DO_C\rho DO_U)$. This term has the opposite sign relative to the expected term. This is only possible when the added error D is located very near the connected logical string and only for special partitions. We prove in Lemma 11 in Appendix E that the contribution from these disconnected terms is negligible.

What of the coherent-type added errors? Again, fix a partition of a connected logical string. Let O_U and O_C be the correctable and uncorrectable errors. Now consider choosing a stabilizer operator or a closed loop, ℓ that is disjoint from the connected logical string. Let the length of the loop be $|\ell|$. Now choose a subset of p of the qubits in the loop, and let the disconnected error D_L act on these p qubits from the left, while the disconnected error D_R acts on the remaining $|\ell| - p$ qubits from the right. Suppose further that the qubits in the loop and the partition are such that the uncorrectable error O_U plus the additional error D_L remains uncorrectable. This need not always be true; we will consider the case where the $O_U D_L$ is correctable in a moment.

Supposing that the disconnected error D_L does not change the decoding, we can perform a sum over all the ways of choosing the p errors in D_L from among the $|\ell|$ errors in the loop. The number of ways of choosing p errors is given by a binomial coefficient, and the magnitude of each term is suppressed by $(\sin\theta/2)^{|\ell|}$ relative to the original partition of the connected logical string without any additional disconnected errors added. The phase of each term depends, as always, on the relative weight of the errors on the right and the left. The disconnected part contributes a phase of $(i)^p(-i)^{|\ell|-p}$, and ℓ is a closed loop so $|\ell|$ is even. The sum yields

$$\text{(connected part)} \sum_{p=0}^{|\ell|} (-1)^p (-1)^{|\ell|/2} \binom{|\ell|}{p} (\sin\theta/2)^{|\ell|} = 0. \tag{3.30}$$

When we sum over all ways of forming disconnected terms out of the original loop ℓ, the sum is 0. This holds for any loop such that the disconnected part does not change how the connected part is decoded.

In the examples we considered in figure 3.6, the additional disconnected errors did not change how the connected part was decoded. This is the same condition we encountered in the discussion of incoherent-type added errors. In certain cases the error D_L that we add to the O_U side of the partition can be such that $D_L O_U$ is a correctable operator. This means the partition is "flipped" by the disconnected error. We account for this case in Lemma 11 and prove that the contribution to the logical noise from these special disconnected terms is negligible for short logical strings.

Using Lemma 11 we can neglect the added errors that change how the partition is decoded. Then we can conclude that the net contribution from coherent-type added errors is 0 and the incoherent-type added errors contribute a $\sin^2\theta/2$ factor on each qubit not in the connected logical string. This implies that the "Disconnected Sum" term in equation (3.7) is equal to 1 plus a small correction. This implies that

$$\tilde{\chi}_{Z_1 I} = \left[\sum_{\mathcal{L}} \sum_{\text{partitions}} (O_U \rho \, O_C)\right] (1 + \mathcal{E}) + \text{High Weight}, \tag{3.31}$$

where $\mathcal{L}$ is a connected, short, typical logical string, partitions refers to the partitions of $\mathcal{L}$ denoted $(O_U \rho \, O_C)$, and $\mathcal{E}$ is a noise term. The error term satisfies

$$\mathcal{E} \leq \frac{16\gamma\zeta^2}{\sqrt{L}} + O(1/L). \tag{3.32}$$

This error term is from Lemma 11 and comes from the added errors that change how the partition is decoded. The term "High Weight" in equation (3.31) is the error from Lemma 3 corresponding to the contributions of logical strings with length $> L + 2\zeta$. We have not yet justified that this error is small relative to the short strings. This is because we do not have a lower bound on the short strings. The justification comes from our subsequent discussion of the incoherent logical noise components.

3.7 Incoherent Sum

Now that we have simplified the sum for the coherent components of the logical noise channel, factored out the disconnected pieces, and performed the sum over syndromes for the connected pieces, we turn our attention to the incoherent logical noise components. We start by making several of the same simplifications we made in the coherent sum. Of the incoherent logical components $(\tilde{L}_a \tilde{\rho} \tilde{L}_a^\dagger)$, we neglect all the terms where L_a is a logical Y operator or acts non-trivially on both encoded qubits. We retain only the terms where L_a is a logical X or Z on one of the two encoded qubits. The reason is the same as for the coherent sum. The neglected terms are much higher weight, such that the path counting excludes them. Then we have the sum

$$\left(\tilde{L}_a \tilde{\rho} \tilde{L}_a^\dagger\right) = \sum_{s,x,y} \left(E_s L_a G_x \rho \, G_y^\dagger L_a^\dagger E_s^\dagger\right), \tag{3.33}$$

where L_a is an X or Z logical operator on one of the encoded qubits and identity on the other. Again, we suppose that all the angles are equal to some fixed θ for each single-qubit rotation. We will extend to general rotations in Lemma 8.

Again, we will divide each term into connected and disconnected pieces. In this discussion of the incoherent logical noise components, Definition 2 must be modified. The noise terms that enter into the incoherent logical noise contain an uncorrectable error on both sides of ρ. We will need to consider two logical strings in our definition.

Definition 8. *The "connected part" of a noise term $(E_s L_a G_x \rho\, G_y L_a E_S)$ is a noise term defined in the following way: let $\mathcal{L}_1$ equal $L_a G_x$ with all topologically trivial closed loops removed and $\mathcal{L}_2$ equal $L_a G_y$ with all trivial closed loops removed. Then let A denote the set of qubits $\subset \mathcal{L}_1 \cup \mathcal{L}_2$ where either $E_s L_a G_x$ or $E_s L_a G_y$, or both, act non-trivially. The connected part of $(E_s L_a G_x \rho\, G_y^\dagger L_a^\dagger E_S^\dagger)$ is given by*

$$((E_s L_a G_x)|_A\, \rho\, (G_y^\dagger L_a^\dagger E_S^\dagger)|_A), \tag{3.34}$$

where $|_A$ denotes the restriction of an operator to the set of qubits A.

If the incoherent term is $(O_U \rho\, O'_U)$, then this definition captures the set of qubits in the support of O_U or O'_U that lie along the two logical strings formed by O_U and E_s and O'_U and E_s pruned of all trivial closed loops. Figure 3.7 illustrates the connected and disconnected part of a noise term that enters into the incoherent logical noise. The connected part of the noise term in the figure features factors of $\sin\theta/2 \cos\theta/2$ for the qubits that appear in exactly one of O_U or O'_U and $\sin^2\theta/2$ for the qubits that appear in both O_U and O'_U. We can lower bound the connected part of each incoherent noise term by $(\sin\theta/2\cos\theta/2)^{|O_U|+|O'_U|}$. This will be useful later on when we sum over many possible choices for the operators O_U and O'_U.

Definition 9. *The "disconnected part" of a noise term $(E_s L_a G_x \rho\, G_y^\dagger L_a^\dagger E_s^\dagger)$ is the restriction of the noise term to the qubits not in the connected part. In Definition 8 we constructed the set A, which contained the qubits in the connected part. The disconnected part is given by*

$$((E_s L_a G_x)|_{A^C}\, \rho\, (G_y^\dagger L_a^\dagger E_s^\dagger)|_{A^C}), \tag{3.35}$$

where $|_{A^C}$ denotes the restriction of an operator to the complement of the set A.

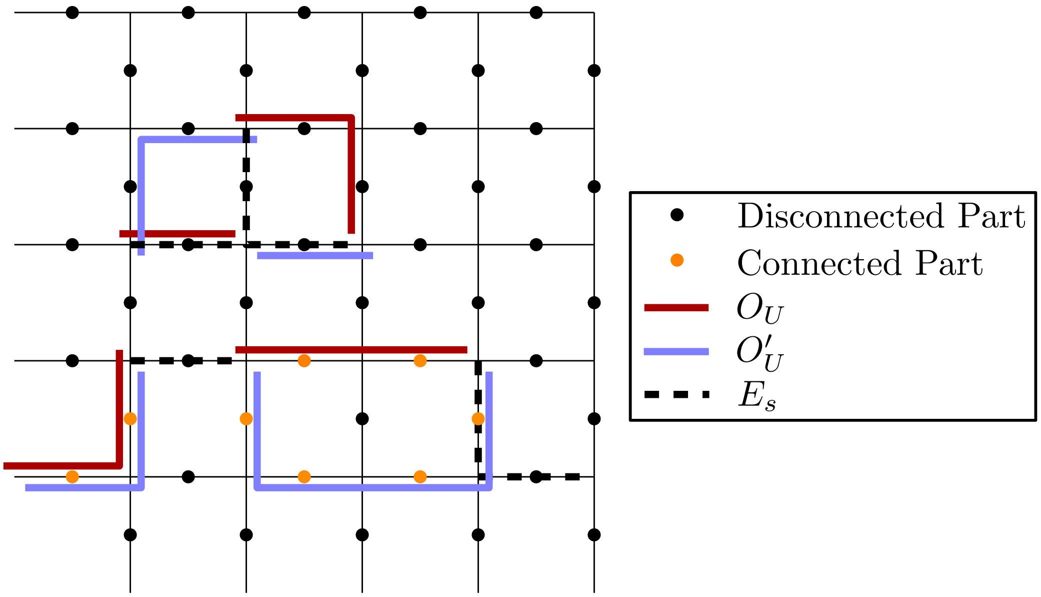


Figure 3.7: A noise terms $(O_U \rho\, O'_U)$ is shown with O_U in red and O'_U in blue. The standard correction E_s chosen by the minimal-weight decoder is drawn as a dotted black line. The connected part of this noise term is signified by the orange qubits, while the disconnected part contains the black qubits.

For the example in figure 3.7, the disconnected part features factors of $\sin\theta/2\cos\theta/2$ for the six qubits along the trivial closed loop near the top of the figure and $\cos^2\theta/2$ for the rest of the qubits. For a given connected part, we can imagine adding disconnected errors to form many different noise terms. The connected part contains factors of $\sin\theta/2\cos\theta/2$ for each qubit that appears in one of the uncorrectable errors and $\sin^2\theta/2$ for each qubit that appears in both errors. The disconnected term includes $\cos^2\theta/2$ for each qubit not in the connected part plus a sum over all possible coherent and incoherent-type disconnected error. Just as in Section 3.6, when the disconnected errors do not change how the connected term is decoded, the incoherent-type errors give $\cos^2\theta/2 + \sin^2\theta/2 = 1$ on qubits not in the connected part. The coherent-type disconnected errors, which form loops split between left and right, sum to zero because of the alternating signs.

Just as in the case of the coherent logical noise components, some disconnected errors will not be allowed because they change how the connected term is decoded. We will set the disconnected part equal to 1 plus an error term that comes from these disallowed disconnected errors. In Lemma 12 we justify this by proving that the error term is small. This is analogous to Lemma 11, where we prove that the disconnected part of the coherent logical noise components is equal to 1 up to small corrections.

We want to continue to follow a similar argument to the one for the coherent terms. The next step is restricting the set of connected terms we consider. We will break up each error into connected and disconnected pieces and restrict ourselves to noise terms with low-weight connected part, where the total weight of the connected part is bounded by $L+2\zeta+1$; here ζ is the same L-independent cutoff as in the coherent sum. Just as for the analysis of the coherent logical noise in Section 3.4, we will require θ to scale like $1/L$ to justify this truncation of the noise terms contributing to the connected part.

Lemma 5. *Consider an incoherent logical noise component, say $\tilde{\chi}_{Z_1Z_1}$. We write this logical noise component as a sum over physical noise terms $(O_U\rho\, O'_U)$. Then if $|\sin\theta| < 1/L$, we can truncate the sum to include only those noise terms where $|O_U| + |O'_U| \le L + 2\zeta + 1$, where ζ is the same cutoff constant as in Lemma 3. In other words,*

$$\tilde{\chi}_{Z_1Z_1} = \sum_{O_U,O'_U:\ |O_U|+|O'_U|\le L+2\zeta+1} (O_U\rho\, O'_U) \times \text{Disconnected} \times \left(1 + O\left((L\sin\theta)^{2\zeta}\right)\right). \tag{3.36}$$

Proof. We split each noise term into connected and disconnected parts. We show in Lemma 12 that the disconnected part is decreasing as the weight of the connected part increases. Moreover, the disconnected part is approximately equal to 1 for connected terms with total weight $\le L + 2\zeta + 1$. Therefore, we need only consider the connected part as we proceed to truncate the sum and upper bound the error.

Let us denote the connected part of a noise terms that enter into the logical $\tilde{\chi}_{Z_1Z_1}$ component by $(O_U\rho\, O'_U)$. All such noise terms have the shape drawn in figure 3.8. The connected part is supported on a series of loops. The loops are joined by the minimal-weight correction. Denote the minimal-weight correction of O_U and of O'_U by E_s. Let w be the weight of O_U and w' the weight of O'_U. Suppose $w \le w'$. If not, then swap O_U and O'_U in what follows. Let $E_sO_U = \mathcal{L}$. Then $\mathcal{L}$ is a connected Z_1 logical string with length at most $2w - 1$. The number of such logical strings is upper bounded by L^{2w-L} using our bound on the number of logical strings in equation (3.10).

The number of ways of choosing a weight w operator O_U as a subset of $\mathcal{L}$ is upper bounded by 2^{2w-2}. Now that O_U is fixed, the number of ways of choosing the operator

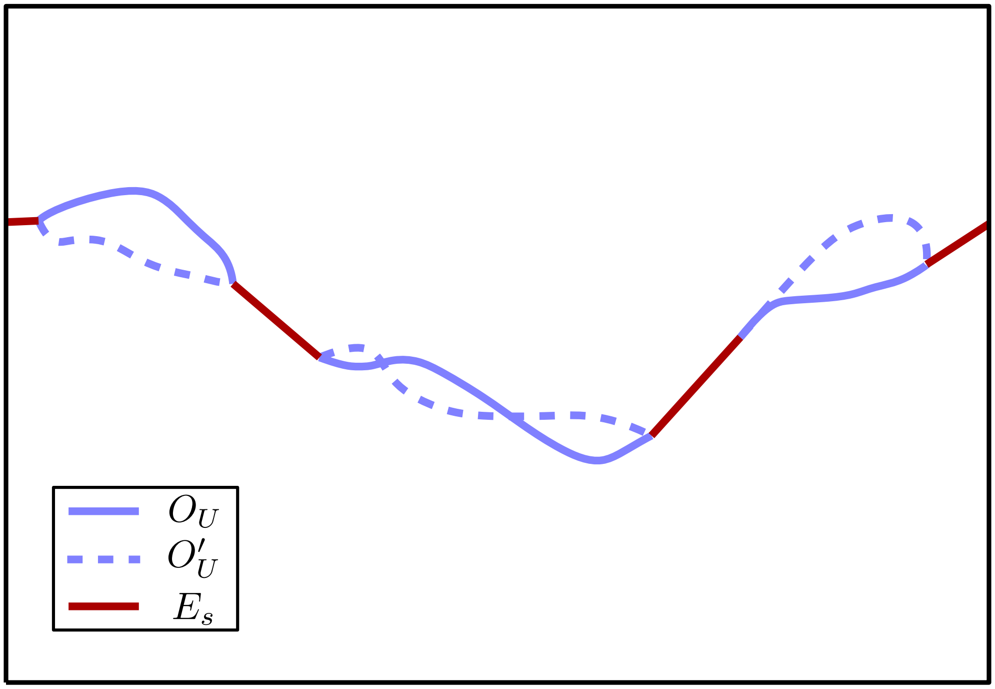


Figure 3.8: This is a connected incoherent noise term, $(O_U \rho\, O'_U)$. The operator O_U is drawn with the solid blue line. The operator O'_U is drawn with the dashed blue line. The standard correction E_s for the syndrome shared by O_U and O'_U is drawn with the solid red line. Each connected incoherent term is a configuration of loops where each loop is formed by two segments with shared endpoints, one segment from O_U and one from O'_U. The operator E_s links together the loops like beads on a string, so that $O_U E_s$ and $O'_U E_s$ are both continuous logical strings spanning the code.

O'_U is upper bounded by $O(L^{w'-w})$. This is because the lowest-weight operator with the same syndrome and logical action has weight $\leq w$. Then O'_U consists of this lowest-weight operator combined with a number of additional deviations like we considered to derive equation (3.10). (Here we are neglecting a factor which is polynomial in w and w'; bounding the exponential dependence on $w' - w$ will suffice for what follows.) All together we have the following upper bound on the number of noise terms with fixed w and w':

$$\leq 2^{2w-2} L^{2w-L} L^{w'-w}. \tag{3.37}$$

Each of these terms has magnitude at most $(\sin\theta/2)^{w+w'}$, which is positive because $w + w'$ is even. As in Lemma 3, we will truncate the sum and keep only those connected noise terms with $w + w' \leq L + 2\zeta + 1$. If we let $w + w' = w_{\text{total}}$, for each w_{total} there are several combinations of w and w' with the same total. Because w and w' must be $> (L+1)/2$, there are less than $w_{\text{total}} - L$ combinations. We perform a sum over w_{total} from $L + 2\zeta + 1$ up to the maximum weight. Therefore, if we let ϵ denote the contribution from the higher weight connected terms to $\tilde{\chi}_{Z_1 Z_1}$, then ϵ is bounded by

$$\epsilon \leq O((2\sin(\theta/2))^{L+2\zeta+1} L^{2\zeta+2}). \tag{3.38}$$

Here we have estimated the sum over w_{total} using the same method as in the derivation of equation (3.14). We will compare this error ϵ to the contribution from the lowest weight noise terms. These terms have $w = w' = (L+1)/2$, and contribute at least ξ, where

$$\xi = L(\sin\theta)^{L+1}. \tag{3.39}$$

Then the relative error associated with our truncation is given by

$$\frac{\epsilon}{\xi} \leq O((L\sin\theta)^{2\zeta}). \tag{3.40}$$

We have neglected a polynomial factor in L in our counting of noise terms. Nevertheless, as long as $L|\sin\theta| < 1$, the relative error is exponentially small in k, and the higher-weight connected terms are negligible.

□

3.8 The Incoherent Sum Over Strings

The connected part of the incoherent components is not as simply expressed as a sum over strings as the coherent components because each uncorrectable error $E_s L_a G_x$ can generally be completed to many different logical strings by multiplying by different correctable errors. Nevertheless, we can rewrite the sum in a similar way. This will form our primary tool for comparing coherent and incoherent logical noise components. We will write a sum over each logical string with logical action L_a. For each string, we will sum over different ways of choosing the uncorrectable subset O_U. We will restrict the subsets we consider for each logical string in order to control the over-counting factor that we will describe shortly. Then for each operator O_U, we will sum over all possible uncorrectable operators O'_U with the same syndrome and logical action. Fix a connected logical string $\mathcal{L}$ with length ℓ and choose an uncorrectable subset of the logical string O_U with weight w. We impose two constraints on O_U: first that $w \geq (\ell+1)/2$ and second that the complement of O_U has the same weight as the minimal-weight correction E_s. The complement of O_U is $O_U\mathcal{L}$, which we will denote O_C. Note that the name O_C is chosen in analogy to the way the errors were labelled in the coherent noise terms, but O_C is not a part of the incoherent noise term, which is notated $(O_U \rho\, O'_U)$. Now that O_U is fixed, choose a second uncorrectable error O'_U with the same syndrome and with weight w'. This will produce every incoherent connected term $(O_U \rho\, O'_U)$. However, each uncorrectable error O_U will appear many times as a subset of many different logical strings. This is the over-counting we mentioned above.

Each operator O_U can be completed to a logical string in many ways. Because of the constraints we imposed on the subset O_U, the complement, which we called O_C, must have the same weight as the minimal-weight correction to O_U, denoted E_s. Let $\{O'_C\}$ be the set of possible complements. Then each possible complement $O'_C \in \{O'_C\}$ defines a logical string $O_U O'_C$, which will appear in the sum over strings. For each operator O_U in the sum over strings, we need to divide by the number of complements O'_C with weight $|E_s|$. Each incoherent logical noise component can be written as a sum over connected logical strings $\mathcal{L}$ times a disconnected factor. This form of the sum will allow us to compare with equation (3.7). We sum over logical strings, and for each logical string we sum over possible choices of O_U and O'_U. We divide by the over-counting factor for each O_U. This gives

$$\tilde{\chi}_{Z_1 Z_1} = \sum_{\mathcal{L}} \sum_{O_U \subset \mathcal{L}} \frac{1}{|\{O'_C\}|} \sum_{O'_U} (O_U \rho\, O'_U) \times \text{Disconnected} \times \left(1 + O\left((L \sin\theta)^{2\zeta}\right)\right), \tag{3.41}$$

where

$$|\mathcal{L}| = \ell,\ |O_U| \geq \frac{\ell+1}{2},\ |O'_C| = |E_s|. \tag{3.42}$$

To reiterate, equation (3.41) expresses an incoherent logical noise component as a sum over connected logical strings. For each string $\mathcal{L}$ with weight ℓ, we sum over all uncorrectable subsets O_U of weight $\geq (\ell+1)/2$ such that the complement O_C has weight equal to the minimal-weight correction of O_U, namely E_s. For each O_U we must divide by the number of correctable errors O'_C with the same syndrome and weight as O_C in order to cancel the over-counting. $\{O'_C\}$ is the set of such operators, and $|\{O'_C\}|$ is its cardinality. Finally, we sum over all uncorrectable operators O'_U with the same syndrome to produce the complete set of incoherent terms. We will prove the following lemma, which provides a lower bound on the contribution of each logical string to the incoherent logical noise component. We will apply this lemma to lower bound the incoherent logical noise strength in terms of the coherent logical noise strength.

Lemma 6. *As long as $|\sin\theta| < 1/L$, we can apply Lemma 5. This means that in equation (3.41) we can restrict to the case where $|O_U| + |O'_U| \leq L + 2\zeta + 1$. Let us also suppose that $|O_U| = |O'_U|$. This assumption will be justified by Lemma 7. Then* *we can pick a connected logical string $\mathcal{L}$ with $|\mathcal{L}| = \ell$ such that $\ell \leq L + 2\zeta$. $\mathcal{L}$ is a Z_1 logical string if we are calculating the $\tilde{\chi}_{Z_1 Z_1}$ logical noise component. O_U is subset of $\mathcal{L}$ such that O_U is corrected to a logical Z_1 operator and $|O_U| = (\ell + 1)/2$. O'_U is an operator with the same weight, syndrome, and logical action as O_U. For each fixed $\mathcal{L}$ with length $\ell \leq L + 2\zeta$, the following holds:*

$$\sum_{O_U} \frac{1}{|\{O'_C\}|} \sum_{O'_U} 1 \geq \sum_{O_U} 1. \tag{3.43}$$

Proof. For each short logical string $\mathcal{L}$ with length ℓ, we partition it into an uncorrectable operator O_U of weight $w = (\ell + 1)/2$ and a correctable operator O_C of length $|O_C| = |E_s|$. Then we consider the alternative uncorrectable and correctable paths, O'_U and O'_C, with weight w and $|E_s|$, respectively. The logical string $\mathcal{L}$ is short, so we can use Lemmas 9 and 10. Say the logical string runs right to left across the code. We observe by studying figure 3.10 that we have multiple possible strings of the same weight exactly when both a vertical error and some number of adjacent horizontal errors are contained in either the correctable or uncorrectable part.

Suppose that for some partition consisting of an uncorrectable operator $O_U^{(1)}$ and a correctable operator $O_C^{(1)}$, denote the operators with the same weight, syndrome, and logical action by $O'^{(1)}_U$ and $O'^{(1)}_C$. Suppose $|\{O'^{(1)}_C\}| > |\{O'^{(1)}_U\}|$. We construct a new operator $O_U^{(2)}$ by exchanging all but one of the errors in $O_U^{(1)}$ with the errors in $O_C^{(1)}$, so that $O_U^{(2)}$ is equal $O_C^{(1)}$ plus one additional error. This is shown in figure 3.9, where we have kept the error on the farthest left vertical segment fixed and flipped the rest relative to the term in figure 3.10. For every O_U there are w possible mappings, one for each of the w choices of the single-qubit error that remains fixed. In the same way, every O_U is mapped onto by w different mappings acting on w other operators with the same logical action as O_U. Then there exists a convention that selects exactly one partner for each O_U.

We assumed that for the original $O_U^{(1)}$

$$|\{O'^{(1)}_C\}| > |\{O'^{(1)}_U\}|. \tag{3.44}$$

The mapping we described constructs a partner $O_U^{(2)}$ such that

$$|\{O'^{(2)}_U\}| \geq |\{O'^{(1)}_C\}| > |\{O'^{(1)}_U\}| \geq |\{O'^{(2)}_C\}|. \tag{3.45}$$

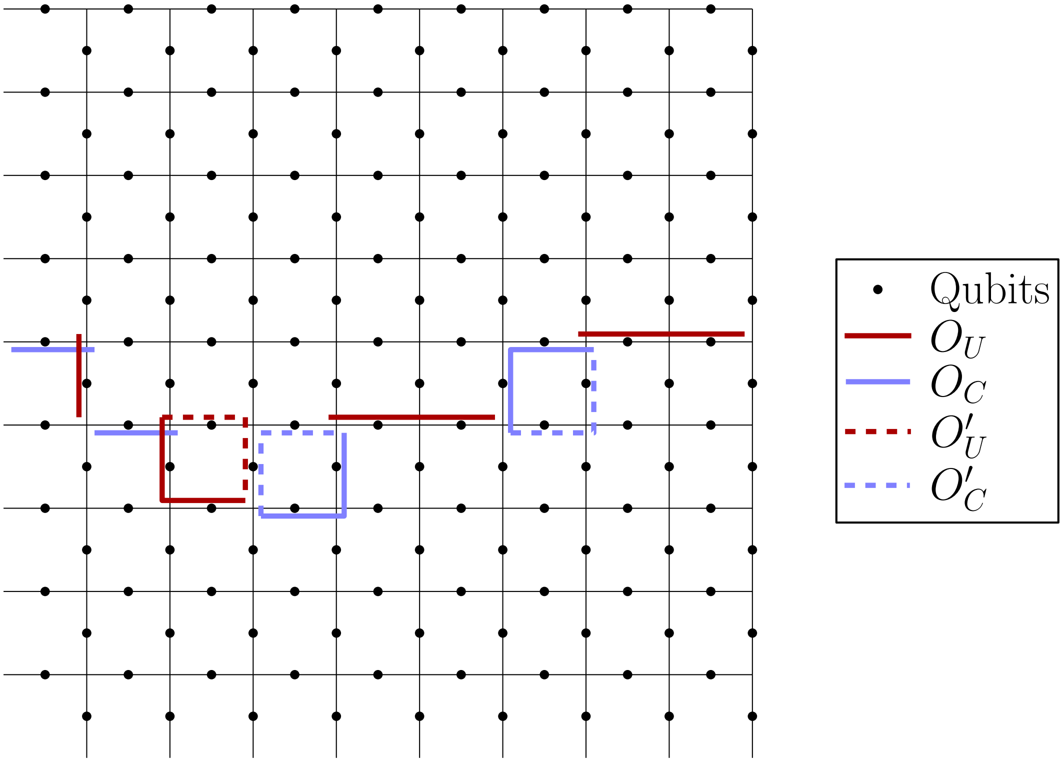


Figure 3.9: A partition of a length-13 logical string is shown in a toric code with $L = 9$. The operator O_U is shown in solid red. The operator O_C is shown in solid blue. The alternative operators with the same weight, syndrome, and logical action, which we denoted O'_U and O'_C, are drawn with dotted lines. For this partition $|\{O'_U\}| = 2$ and $|\{O'_C\}| = 4$.

Then for each pair $O_U^{(1)}$ and $O_U^{(2)}$, we can lower bound the contribution to the incoherent logical noise using

$$\begin{aligned}
&\frac{|\{O'^{(1)}_U\}|}{|\{O'^{(1)}_C\}|} + \frac{|\{O'^{(2)}_U\}|}{|\{O'^{(2)}_C\}|} \\
&\geq \frac{|\{O'^{(1)}_U\}|}{|\{O'^{(1)}_C\}|} + \frac{|\{O'^{(1)}_C\}|}{|\{O'^{(1)}_U\}|} \\
&= \frac{|\{O'^{(1)}_U\}|^2 + |\{O'^{(1)}_C\}|^2}{|\{O'^{(1)}_U\}||\{O'^{(1)}_C\}|} \\
&\geq 2.
\end{aligned} \tag{3.46}$$

Finally, we apply the lower bound to the entire sum over O_U to conclude

$$\sum_{O_U} \frac{|\{O'_U\}|}{|\{O'_C\}|} \geq \sum_{O_U} 1. \tag{3.47}$$

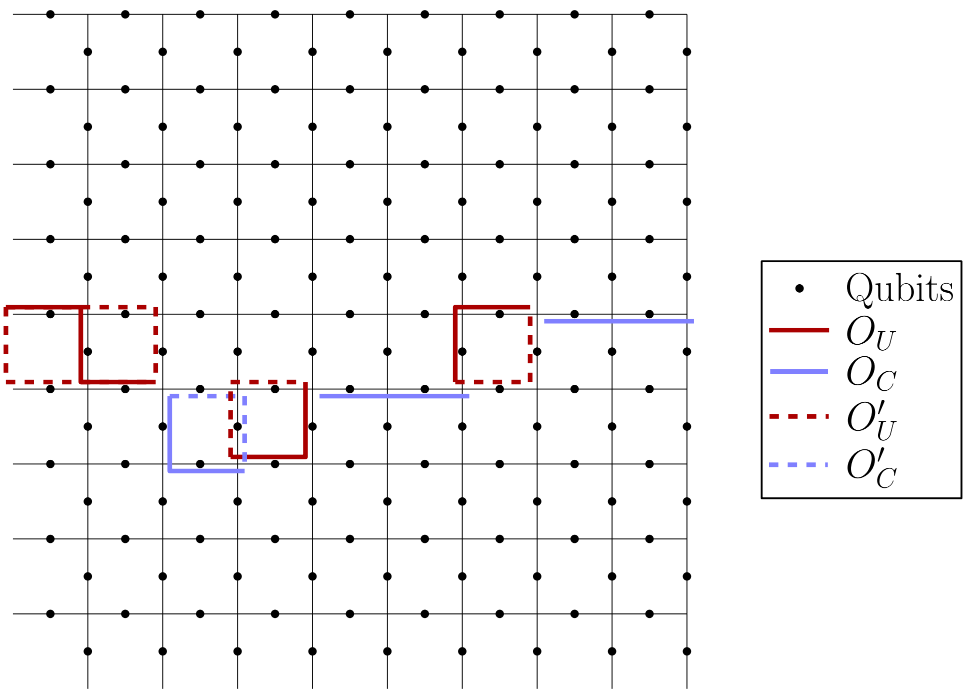


Figure 3.10: This is a partner of the partition shown in figure 3.9. It is another partition of the same logical string, and the errors in O_U and O_C are interchanged except for one qubit. In this case that qubit is the one that lies on the farthest left vertical segment. The error on that qubit is part of O_U in both partitions. Once again, the operator O_U is in red and the operator O_C is in blue. The alternative operators with the same weight, syndrome, and logical action are given by the dashed lines. For this partition $|\{O'_U\}| = 12$ and $|\{O'_C\}| = 2$.

The number of terms in the sum over O_U is at most $\binom{\ell}{w}$, where ℓ is the length of the logical string $\mathcal{L}$. For typical, short logical strings the binomial coefficient will be the number of terms in the sum over O_U up to a small correction.

□

3.9 Noise Terms with Mismatched Weight

We have already shown that we can neglect the high-weight noise terms in the incoherent logical noise components, and we can also write the incoherent logical noise components as a sum over logical strings. Next we will show that among the low-weight noise terms, we may neglect the terms with different weight errors on each side of ρ. This is crucial to our proof that the coherence of the logical noise is suppressed. We will construct a lower bound on the incoherent logical noise components and an upper bound on the coherent logical noise components. The noise terms with mismatched weight enter with a phase of -1 whenever the difference between the weights on left and right = 2 mod 4. A large contribution from noise terms with mismatched weight could spoil our lower bound on the incoherent logical noise. Fortunately, no such contribution occurs.

Lemma 7. *If $|\sin\theta| < 1/L$, then the incoherent logical noise component $\tilde{\chi}_{Z_1 Z_1}$ can be written*

$$\tilde{\chi}_{Z_1 Z_1} \geq \sum_{\mathcal{L}} \sum_{O_U} \frac{1}{|\{O'_C\}|} \sum_{O'_U} (O_U \rho \, O'_U) \times Disconnected \times \left(1 + O\left(L \sin\theta\right)^{2\zeta}\right)\right). \tag{3.48}$$

The sum over $\mathcal{L}$ includes all typical, short logical strings with length ℓ such that $\ell \leq L + 2\zeta$. The sum over O_U includes uncorrectable subsets of $\mathcal{L}$ with weight $(\ell + 1)/2$ such that the complement O_C has minimal weight. The sum over O'_U has the same syndrome and the same weight as O_U. The error term comes from the high weight terms we neglected in Lemma 5.

Proof. Using Lemma 5 we can truncate the sum over noise terms in the incoherent logical noise component $\tilde{\chi}_{Z_1 Z_1}$ to include only those noise terms with total weight $\leq L + 2\zeta + 1$. In doing so we make an error that is exponentially small in the cutoff ζ, assuming that the single-qubit angle of rotation θ satisfies $|\sin\theta| < 1/L$. We will use equation (3.41) to express the incoherent logical noise components as a sum over strings. We will begin by reviewing how we construct that form of the sum.

We denote the weight of O_U by w and O'_U by w'. We upper bound the mismatched-weight terms where $w \neq w'$ by letting $w > w'$ and multiplying by two. As in equation (3.41), we can generate the complete set of connected incoherent terms with fixed w and w' by summing over connected logical strings $\mathcal{L}$. Denote the length of the logical string by $|\mathcal{L}| = \ell$. To produce the incoherent terms with fixed $w + w'$, it will suffice to sum over logical strings with $\ell < w + w'$. We already restricted to low-weight terms, so $w + w' \leq L + 2\zeta + 1$. For each logical string, we sum over the uncorrectable subsets O_U with weight w. We will also require that the complement of O_U, which we denoted O_C, has minimal weight. This is to control the over-counting of each incoherent term $(O_U \rho \, O'_U)$. Then for each O_U, we sum over the operators O'_U with weight w' that have the same syndrome and logical action as O_U. As discussed in Section 3.8, we must also divide by an over-counting factor $1/|\{O_C\}|$ that is a function of O_U and equals one over the number of times O_U appears in the sum over $\mathcal{L}$. The contribution to the incoherent logical noise is lower bounded by

$$\text{Contribution from string } \mathcal{L} \geq \sum_{O_U} \frac{|\{O'_U\}|}{|\{O'_C\}|} \left(\frac{\sin\theta}{2}\right)^{w+w'} . \tag{3.49}$$

The inequality comes from the cosine factors. If the operators O_U and O'_U act on the same set of qubits, then we have $(\sin\theta/2)^{2w}$ with no cosine factors in the connected part. The lower bound corresponds to the case where O_U and O'_U act on disjoint sets of qubits, and we pick up a cosine factor on each qubit in the connected part. We also have an upper bound:

$$\text{Contribution from string } \mathcal{L} \leq \sum_{O_U} \frac{|\{O'_U\}|}{|\{O'_C\}|} \left(\sin(\theta/2)\right)^{w+w'} . \tag{3.50}$$

In this bound, we have $(\sin(\theta/2))^{w+w'}$. This corresponds to the case when O_U and O'_U act on the same qubits, yielding no cosine terms.

Consider first the terms with $w = w'$. These are generated from logical strings of length $\ell \leq 2w - 1$. Some strings $\mathcal{L}$ with length ℓ such that $L \leq \ell \leq L + 2\zeta$ have typical shape and some do not. We will prove first that the contribution from a given string of atypical shape is no greater than that of a string of typical shape, in fact it will be less. We will conclude that we can safely neglect the contribution from strings of atypical shape (because there are fewer such strings). This is the same simplification we made in our discussion of the coherent logical noise components in Section 3.5.

We require that O_U is an uncorrectable error, so we cannot choose any subset of w qubits in $\mathcal{L}$. We ignore the subsets that correspond to exceptional partitions like we discussed in Section 3.5. Now, if we have two connected logical strings of the same length, one with a typical shape and one with an atypical shape, we want to compare the terms with $w = w'$. The first thing we notice is that exceptional terms are exponentially unlikely for the string with typical shape, while for the atypical string, exceptional terms may be a significant fraction of the total partitions. This tells us that in the sum over O_U there are many more terms for the typical string than for the atypical string. We have argued about the number of terms in the sum in equations (3.49) and (3.50), but we must also consider the magnitude of each term, which is given by the ratio of $|\{O'_U\}|$ over $|\{O'_C\}|$.

We must argue that after summing the ratio of $\{O'_U\}$ and $\{O'_U\}$ over O_U, the result is less for an atypical string than for a typical string. $\{O'_U\}$ here is the set of uncorrectable operators with the same weight and syndrome as O_U and $\{O'_C\}$ is the set of correctable weight-$\ell - w$ operators with the same syndrome. Suppose the logical string runs left to right across the code. The set $\{O'_U\}$ contains more than one element whenever O_U contains a set of contiguous qubits around one or more of the vertical steps in the logical string. This was discussed in detail in Section 3.8. $|\{O'_U\}|$ and $|\{O'_C\}|$ are large when either O_U or O_C contain contiguous sets of qubits around the vertical steps. The typical logical string has at least $\gamma\sqrt{L}$ horizontal steps around each of the vertical steps. The atypical string does not. This means that the typical string has more possible sets of qubits around each vertical step that make $|\{O'_U\}|$ or $|\{O'_C\}|$ large. Therefore, $|\{O'_U\}|$ and $|\{O'_C\}|$ will tend to be larger for the typical string. The ratio of $|\{O'_U\}|$ to $|\{O'_C\}|$ is what determines the contribution to the incoherent logical noise. In Lemma 6 we showed how we can match up terms such that for each O_U satisfying $|\{O'_U\}|/|\{O'_C\}| = c$, the partner has $|\{O'_U\}|/|\{O'_C\}| \geq 1/c$. If c is large, then $c + \frac{1}{c} \gg 2$. It follows that because the typical string has more operators O_U in the sum and the $|\{O'_U\}|/|\{O'_C\}|$ factors tend to be larger, the contribution to the incoherent logical noise is smaller for an atypical string than the contribution from a typical string. When we combine this fact with the fact that the atypical strings represent an small minority, this means we can neglect the atypical strings among the $w = w'$ terms in the incoherent logical noise. The error is given by Lemma 10.

Now, consider the mismatched-weight terms that are the subject of this lemma. Fix $w + w'$ and suppose $w > w'$. For each $\mathcal{L}$ we can construct a number of incoherent terms with mismatched weight depending on the length and shape of $\mathcal{L}$. Let $|\mathcal{L}| = \ell$. Once again O_U is an uncorrectable subset of the logical string $\mathcal{L}$ with weight w. Then for each O_U we have the possibility that there may exist an operator O'_U with the same syndrome as O_U and lower weight. We sum over the set of O_U such that for each O_U there exists an O'_U with weight w'. If we sum over all logical strings of length $< w + w'$, we produce every connected incoherent term with $|O_U| = w$ and $|O'_U| = w'$. We will proceed by fixing a logical string and upper bounding the sum over w of the noise terms derived from this logical string with $w + w'$ fixed. In this sum the terms will alternate sign as w increases. The terms with $w = w'$ have a positive sign. As we seek to bound the contribution of these mismatched-weight terms to the incoherent logical noise, there are two things we need to bound. First, we must understand the combinatorics that govern the number of operators O_U that permit lower-weight O'_U. Second, we must bound the factor $|\{O'_U\}|/|\{O'_C\}|$ for each such O_U.

Suppose that the logical string $\mathcal{L}$ has a typical shape. To be concrete, consider the set of operators O_U with weight $w = (\ell + 3)/2$. If there exist lower-weight O'_U, then O_U must contain all of the qubits around a "cap," which is similar condition to the one we discussed in Section 3.5. Each cap has width at least $\gamma\sqrt{L}$ because the string is typical. This means that such O_U are exponentially few relative to the total set of uncorrectable O_U with weight w. This is the same calculation as in Lemma 4. We compare these terms to the terms with $|O_U| = (\ell + 1)/2 = |O'_U|$. There are exponentially more of these terms where $|O_U| = |O'_U|$. This means that in equations (3.49) and (3.50) the sum over O_U contains exponentially more terms when $w = w'$ for a typical logical string. The summand also tends to be less for the $w > w'$ terms. The argument is similar to the one we used earlier when we were discussing the $w = w'$ terms from typical and atypical strings. $|\{O'_U\}|$ is large when O_U contains many qubits around several of the different steps up and down along the logical string. In this case the terms with $w > w'$ feature operators O_U that contain at least one of the "caps" along the logical string. This removes at least two of the vertical steps. These steps cannot contribute to $|\{O'_U\}|$. Then by the argument we used above, the ratio $|\{O'_U\}|/|\{O'_C\}|$ tends to be less for the $w > w'$ terms relative to the $w = w'$. We chose $w = (\ell + 3)/2$, but we could have chosen any $w > (\ell + 1)/2$ and any $w' < w$. We would find that there are $2^{\gamma\sqrt{L}(w-w')}$ fewer of the mismatched weight terms. We have a factor of $2^{\gamma\sqrt{L}}$ for each cap contained in O_U. We conclude that the mismatched-weight terms are negligible for strings of typical shape.

Finally, consider a logical string $\mathcal{L}$ with an atypical shape. Fix $w + w'$. We already neglected the contribution of atypical strings to the $w = w'$ terms. We seek a bound on the contribution from the terms with $w > w'$ for atypical strings. We will compare two sets of terms for fixed $\mathcal{L}$ with length ℓ. On the one hand, take the terms with $w = w_1$ for some $w_1 > (\ell - 1)/2$ and $w' = w_2 < w_1$. On the other hand, take the terms with $w = w_1 + 1$ and $w' = w_2 - 1$. We will show that the latter set of terms contribute less than the former. This will tell us that the sum over mismatched-weight terms for the fixed string $\mathcal{L}$ is bounded by the contribution from terms with $|O_U| = |O'_U|$.

When O'_U has lower weight than O_U, O_U must contain all the qubits along a cap. If $O_U - O'_U = 2j$, then O_U must contain at caps with total height at least j. Because the logical string $\mathcal{L}$ has an atypical shape, these caps may have width one or height greater than one. It will not be exponentially unlikely that all qubits around a small cap are contained in O_U. For the terms with $w = w_1$ and $w' = w_2$, relative to O'_U,

O_U contains all the qubits around $w_1 - w_2$ of the caps. These terms will be a fraction of the $\binom{\ell}{w_1}$ subsets of w_1 qubits in the logical string $\mathcal{L}$. We compare these terms to the ones with $w = w_1 + 1$ and $w' = w_2 - 1$ keeping our logical string $\mathcal{L}$ fixed. These terms include all the qubits around an additional cap. On one of the caps, instead of containing at least one and less than all of the qubits, O_U contains all of the qubits around that cap. This stricter condition of O_U means that the fraction of the total $\binom{\ell}{w_1+1}$ weight w_1 subsets of $\mathcal{L}$ that feature an O'_U operator with weight $w_2 - 1$ is smaller than the fraction of the total $\binom{\ell}{w_1}$ weight w_1 subsets of $\mathcal{L}$ that feature an O'_U operator with weight w_2. This means that in equations (3.49) and (3.50) in the sum over O_U for our fixed logical string, the number of possible O_U at a given weight $w > (\ell + 1)/2$ is given by a binomial coefficient times a function that decreases monotonically as w increases. As for the summand $|\{O'_U\}|/|\{O'_U\}|$, we apply the same reasoning as above. For each cap contained in O_U, there are fewer vertical steps to create many operators O'_U. This implies that the summand will tend to be smaller as w increases. The sum over the different values of w has the form

$$\sum_{w=c}^{\ell}(-1)^w f(w)\binom{\ell}{w} < \binom{\ell}{c}, \tag{3.51}$$

where $c \geq (l + 1)/2$ and f is a monotonically decreasing function. The inequality in equation (3.51) is proven by pairing the adjacent terms in the sum, positive and negative, to produce small positive contributions bounded by the contributions in the case where $f(w) = 1$ for all w. It follows that the sum over the mismatched-weight terms derived from the logical string $\mathcal{L}$ is positive, and moreover is bounded by the $w = w'$ terms. We already argued that the $w = w'$ terms from atypical strings are negligible relative to those terms from typical strings. Finally, we can lower bound the incoherent logical noise component by neglecting the atypical strings and for the typical strings, neglecting the mismatched-weight terms. This yields equation (3.48). □

We are left with only the incoherent terms that have the same weight of uncorrectable error on each side and the weight is $\leq \frac{L+2\zeta+1}{2}$. These terms all have the same phase +1, so the incoherent terms with different weights will add constructively. This gives us lower bounds on the logical incoherent noise strength. Each logical string with length $\ell \leq L + 2\zeta$ contributes at least $\binom{\ell}{\frac{\ell+1}{2}}\left(\frac{\sin\theta}{2}\right)^{\ell+1}$. When ℓ is much larger than the minimum logical string length, L, the number of logical strings is given by equation (3.8).

In particular, the incoherent logical noise components must be larger than the lowest order term. This at last completes the argument begun in Section 3.4 about neglecting the contribution to the coherent logical noise from connected logical strings with length $> L + 2\zeta$ for a cut-off constant ζ. In Lemma 3 we proved that the contribution from long logical strings is upper bounded by $\alpha L^{2\zeta+1}|\sin\theta|^{L+2\zeta}$, where α is $(1 - L|\sin\theta|)^{-1}$. This bound is exponentially small in ζ relative to the lowest order incoherent logical noise component, $L\binom{L}{\frac{L+1}{2}}\left(\frac{\sin\theta}{2}\right)^{L+1}$. Our aim is to compare the logical coherent and incoherent noise components, and we have shown that the contribution to the coherent logical noise from long strings is small relative to the incoherent logical noise components. Therefore, we can safely neglect the long connected logical strings. The same applies for the truncation error in Lemma 5. The truncation error is negligible relative to the lowest order incoherent terms for large enough ζ.

3.10 More General Rotation Angles

In Sections 3.4 and 3.7, we simplified the problem by assuming that all qubits are rotated by the same single-qubit unitary rotation. Now we want to extend our result to more general single-qubit rotations. We will allow the magnitude of the rotation angle to vary from qubit to qubit and will also allow different axes of rotation for different qubits. Here we will assume that each rotation axis is contained in the X-Z plane. Physical Y errors are treated in Appendix G, where we prove that rotations partly along the Y-axis produce less coherent logical noise channels than those arising from rotations along axes in the X-Z plane.

The idea of the proof is the same as that of Lemma 2. We will consider the coherent and incoherent logical noise components as functions of individual qubit rotation angles and prove that the coherent component is maximized relative to the incoherent component when all rotation angles are equal.

Lemma 8. *Consider the toric code with qubits subject to single-qubit rotations, where each rotation axis lies in the X-Z plane, and both the rotation axis and angle of rotation may vary from qubit to qubit. The bound on the coherence of the logical noise channel proved in Theorem 6 continues to apply if the rotations are sufficiently close to uniform; that is, provided that each rotation axis and angle deviates from a fixed constant value within a bounded region.*

Proof. Suppose at first that all rotations are about the Z-axis and denote the rotation angle for the ith qubit by θ_i. Each logical coherent or incoherent component is a sum of physical noise terms, which are functions of all the angles θ_i. We will refer to the coherent or incoherent logical noise strength; by this we mean the sum of norms squared of the off-diagonal or diagonal components of the chi matrix for the logical noise channel. We are interested in the coherence of the logical noise channel, that is, the relative magnitude of the coherent and incoherent logical noise strength. Our approach will be to fix the coherent logical noise strength and calculate how the incoherent logical noise strength varies as we change rotation angles while remaining in the submanifold with constant coherent logical noise strength.

We begin at a point where all single-qubit rotation angles are equal. Suppose that this rotation angle is > 0. The proof will be similar if the angle is < 0. We will perturb away from this point, moving along the submanifold with fixed coherent logical noise strength. These perturbations can be built out of small elementary steps, in which two qubits, i and j, are selected. We require that $\theta_i \geq \theta_j$. Then the elementary step consists of increasing θ_i by some amount and decreasing θ_j such that we remain on the submanifold with constant coherent logical noise strength. We will prove that such elementary steps increase the incoherent logical noise strength. Therefore, we will conclude that the coherence of the logical noise is maximized when all single-qubit rotation angles are equal. Our calculation will be limited to configurations of angles not too far from the point where all angles are equal.

In Lemmas 3 and 5, we proved that when all the rotation angles are equal and satisfy $|\sin\theta| < 1/L$, the logical noise is dominated by the contributions of the low-weight connected terms. We bounded the absolute magnitude of the sum over high-weight connected terms. These high-weight terms were negligible relative to the low-weight connected terms in the incoherent logical noise. If the rotation angles are allowed to differ, so long as all the angles θ_i satisfy $|\sin\theta_i| < 1/L$, our upper bound on the absolute magnitude of the error from the high-weight terms continues to hold. We require that this error is negligible relative to the low-weight terms we keep in the incoherent logical noise components. This was true when all angles were equal and will continue to be true for a wide range of configurations; only certain edge cases will violate this condition. For instance, one such edge case arises if all the rotation angles are 0 except for the qubits along a long logical string with a shape such that it contains no low-weight uncorrectable subsets.

We previously defined the connected and disconnected parts of a noise term (Definitions 2, 3, 8, and 9). As we described in Section 3.6 and Lemmas 11 and 12, the disconnected part has a value of 1 up to corrections. These corrections are small for low-weight connected terms when all rotation angles are equal. If the angles are different, we can still apply our analysis, so long as the absolute error from the corrections is small relative to the low-weight connected terms in the incoherent logical noise components. This holds in a region around the point where all angles are equal. Hence, in this proof we will compare only the connected terms in the coherent and incoherent logical noise components with the understanding that the error terms we are neglecting are small relative to the low-weight connected terms we have kept.

We can build any general perturbation out of an elementary (non-infinitesimal) perturbation where we increase one rotation angle θ_i and decrease a second angle, θ_j, such that the connected contribution to the coherent logical noise strength is unchanged. The perturbation will look different depending on how the two qubits are positioned. If the qubits i and j are adjacent to each other and aligned in the correct direction, they will appear together in many short logical strings. Otherwise, i and j will not appear together in short logical strings. Throughout this section, we will approximate $\sin \theta_i/2 \approx \theta_i/2$ to simplify the equations. We will incur a relative error of $\theta_i^2/4$, that will always be small, since we have assumed that $|\sin \theta_i| < 1/L$ for every i. Then the contribution to the coherent logical noise strength from the low-weight connected terms as a function of θ_i and θ_j is

$$\text{coherent} = \gamma_0 + \gamma_1(\theta_i + \theta_j) + \gamma_2\theta_i\theta_j. \tag{3.52}$$

The coherent logical noise strength is a sum of norms squared and is therefore positive. This implies that $\gamma_0 > 0$. Moreover, the sum over partitions has the same phase for every short logical string as in equation (3.27). This means that each logical string makes a positive contribution to the noise strength. Therefore, γ_1 and γ_2 are both non-negative. The relative size of γ_1 and γ_2 depends on how close the two chosen qubits i and j are. When i and j are both along the same horizontal or vertical line, many low-weight logical strings will contain both qubits. These strings contribute to γ_2, so that the γ_2 term may be comparable to the γ_1 term. On the other hand, if qubits i and j are not along a horizontal or vertical line, then none of the minimal-weight logical strings contain both qubits. Also, for any fixed length $\ell \leq L + 2\zeta$, the number of logical strings of length ℓ that contain both qubits i and j is negligible relative to the number of length ℓ logical strings that contain qubit i and not qubit j. In this case the γ_2 term is negligible relative to the γ_1 term. In either case, we can write down the perturbation that leaves the coherent logical noise strength unchanged. Let $\theta_i = c_i\theta$ and $\theta_j = c_j\theta$ for some θ, and then we will solve for c_j such that the connected coherent sum is constant. This yields

$$c_j = \frac{(2 - c_i)\gamma_1 + \gamma_2\theta}{\gamma_1 + c_i\gamma_2\theta}, \tag{3.53}$$

so that when $\gamma_2 = 0$, we have $c_j = 2 - c_i$.

We can expand the incoherent logical noise strength in the same way. The noise terms that enter into the incoherent logical noise have the form $(O_U\rho\, O'_U)$. As we expand in the angles θ_i and θ_j, we have cases where the qubits i and j are contained in neither, one of, or both O_U and O'_U:

$$\text{incoherent} = \delta_0+\delta_1(\theta_i^2+\theta_j^2)+\delta_2\theta_i^2\theta_j^2+\delta_3(\theta_i+\theta_j)+\delta_4\theta_i\theta_j+\delta_5(\theta_i^2\theta_j+\theta_i\theta_j^2). \tag{3.54}$$

By Lemma 5 the contributions of high-weight logical strings to the logical incoherent noise components are negligible. The contributions for each short logical string are positive due to Lemma 7. If we fix a short logical string that contains both qubit i and qubit j and require that O_U and O'_U both contain i and j or one of i and j, then the same proof as in Lemma 7 implies that these contributions are positive. Therefore, the coefficients δ_1 and δ_2 are positive when all rotation angles are equal. We can now substitute the perturbation from equation (3.53) into each of the terms in equation (3.54). We compute the perturbed value of the incoherent logical noise strength and subtract the initial value when all the angles of rotation are equal. Let incoherent(a) denote the value of the incoherent term in equation (3.54) with $c_i = a$. The difference between the perturbed and initial values is

$$\begin{aligned}
&\text{incoherent}(c_i) - \text{incoherent}(1)\\
&\quad= \delta_1\frac{(c_i-1)^2(2\gamma_1^2\theta^2 + 2(2+c_i)\gamma_1\gamma_2\theta^3 + (c_i^2+2c_i+1)\gamma_2^2\theta^4)}{(\gamma_1+c_i\gamma_2\theta)^2}\\
&\quad- \delta_2\frac{(c_i-1)^2\left(\gamma_1^2\theta^4(2-(c_i-1)^2) + 2c_i\gamma_1\gamma_2\theta^5\right)}{(\gamma_1+c_i\gamma_2\theta)^2}\\
&\quad+ \delta_3\frac{(c_i-1)^2(\gamma_1\gamma_2\theta^2 + c_i\gamma_2^2\theta^3)}{(\gamma_1+c_i\gamma_2\theta)^2}\\
&\quad- \delta_4\frac{(c_i-1)^2(\gamma_1^2\theta^2 + c_i\gamma_1\gamma_2\theta^3)}{(\gamma_1+c_i\gamma_2\theta)^2}\\
&\quad- \delta_5\frac{(c_i-1)^2(2\gamma_1^2\theta^3 + c_i^2\gamma_1\gamma_2\theta^4 - c_i\gamma_2^2\theta^5)}{(\gamma_1+c_i\gamma_2\theta)^2}.
\end{aligned} \tag{3.55}$$

We see that the δ_1 term is positive for all $c_i > 1$. We will show that the positive terms are larger than the other terms for all $c_i > 1$. Each term has the same denominator and contains a factor of $(c_i - 1)^2$ in the numerator. This means immediately that the first derivative with respect to c_i vanishes at the point $c_i = 1$. We pull out the shared factors of $\frac{(c_i-1)^2}{(\gamma_1+c_i\gamma_2\theta)^2}$ and rearrange terms in equation (3.55):

$$\begin{aligned}
&= \frac{(c_i - 1)^2}{(\gamma_1 + c_i\gamma_2\theta)^2}\times \\
&\Big(\gamma_1^2(2\theta^2\delta_1 - 2\theta^4\delta_2 - \theta^2\delta_4 - 2\theta^3\delta_5) \\
&\quad + \gamma_1\gamma_2(4\theta^3\delta_1 + \theta^2\delta_3) \\
&\quad + \gamma_1\gamma_2(2c_i\theta^3\delta_1 - 2c_i\theta^5\delta_2 - c_i\theta^3\delta_4) \\
&\quad + \gamma_2^2(2c_i\theta^4\delta_1 + c_i\theta^3\delta_3 + c_i\theta^5\delta_5) \\
&\quad + \gamma_1^2(c_i - 1)^2\theta^4\delta_2 + \gamma_2^2(c_i^2 + 1)\theta^4\delta_1 - \gamma_1\gamma_2 c_i^2\theta^4\delta_5\Big)\,. \qquad (3.56)
\end{aligned}$$

If the conditions,

$$\begin{aligned}
2\theta^2\delta_1 &> 2\theta^4\delta_2 + \theta^2|\delta_4| + 2\theta^3|\delta_5|, \\
4\theta^3\delta_1 &> \theta^2|\delta_3|, \\
\theta^4\delta_1 &> \theta^3|\delta_3| + \theta^5|\delta_5|, \\
\text{and}\quad \gamma_2^2(c_i^2 + 1)\theta^4\delta_1 + \gamma_1^2(c_i - 1)^2\theta^4\delta_2 &> \gamma_1\gamma_2 c_i^2\theta^4|\delta_5|, \qquad (3.57)
\end{aligned}$$

are satisfied, then each line of equation (3.56) is greater than 0. Recall that γ_1, γ_2, δ_1, and δ_2 are non-negative. Each elementary perturbation increases the value of c_i. Therefore, if the conditions in equation (3.57) are satisfied, then each elementary step along the submanifold with constant coherent noise strength increases the incoherent logical noise strength. It remains for us to argue that these conditions are satisfied when the rotation angles are close to equal.

Consider two cases for the relative positions of qubits i and j. In the first case, suppose qubits i and j are positioned so that no short logical strings contain both. Then the strings that contribute to γ_2 as well as δ_2, δ_4, and δ_5 are all long. Such strings do not appear in the sum over low-weight connected terms, so $\gamma_2 = 0$ in equation (3.56). Therefore, the only condition is the first line of equation (3.57). In this inequality δ_2, δ_4 and δ_5 are 0, and the condition is satisfied.

In the other case, qubits i and j are in a horizontal or vertical line so that both qubits are contained in several short logical strings. In this case $\theta\gamma_2$ is comparable to γ_1. Now consider the incoherent contribution from the strings that contain both qubits i and j. For each weight-$(2w - 1)$ logical string containing both qubits i and j, the errors O_U are weight-w subsets of the logical string. Nearly half will contain exactly one of qubits i and j and one quarter will contain both qubits i and j. This means that more terms contribute to $\theta^2\delta_1$ and $\theta\delta_3$ than to $\theta^4\delta_2$, $\theta^2\delta_4$, and $\theta^3\delta_5$. In particular, $\theta^2\delta_1 > 2\theta^4\delta_2$. For each O_U, the set $\{O'_U\}$ contains operators with the same syndrome, logical action and weight. O'_U differs from O_U only near certain transverse steps along the logical string as we described in Section 3.8. For most logical strings, if O_U does not contain qubit i, then most of the operators O'_U also will not. If O_U contains qubit i, most operators O'_U will as well. This implies that

$$\begin{aligned} \theta^2\delta_1 &\gg \theta|\delta_3|, \\ \theta^4\delta_2 &\gg \theta^2|\delta_4|, \\ \theta^4\delta_2 &\gg \theta^3|\delta_5|, \\ \text{and} \quad \theta^2\delta_1 &\gg \theta^3|\delta_5|. \end{aligned} \tag{3.58}$$

Together with our earlier statement that $\theta^2\delta_1 > 2\theta^4\delta_2$, this implies that even when i and j are near to each other, the conditions in equation (3.57) are satisfied.

We have proven that each of the elementary perturbations starting from uniform angles increases the incoherent logical noise strength. However, we must also consider elementary perturbations that are applied after a different elementary perturbation has taken us away from uniform angles. In that case in equations (3.52) and (3.54) we would no longer have exact symmetry between θ_i and θ_j. In other words, equation (3.52) would read

$$\text{coherent} = \gamma_0 + \gamma_1^{(i)}\theta_i + \gamma_1^{(j)}\theta_j + \gamma_2\theta_i\theta_j, \tag{3.59}$$

where $\gamma_1^{(i)}$ and $\gamma_1^{(j)}$ are different coefficients. However, as long as we are not too far from uniform angles, $\gamma_1^{(i)} \approx \gamma_1^{(j)}$, and the change in the incoherent logical noise strength will be almost the same as in equation (3.55). We have argued that the conditions in equation (3.57) are satisfied by a large margin. Therefore, there exists a region around the point with uniform angles where every elementary perturbation on the submanifold with fixed coherent logical noise strength increases the incoherent logical noise strength. We conclude that in a region around the symmetric point where every single-qubit rotation is by the same angle θ, this symmetric point gives the largest coherent logical noise strength relative to the incoherent logical noise strength. This means that the connected contribution to the incoherent logical noise strength has a local minimum at the point with uniform rotations within the submanifold with constant connected contribution to the coherent logical noise strength. This implies that the upper bound on logical coherence we derive in

Theorem 6 for the case where all angles are equal also upper bounds the logical coherence in a region around the point where all angles are equal.

Now consider changing the axes of rotation while keeping the total rotation angle the same. Let the noise model be a rotation in the X-Z plane such that the rotation angles are θ_X and θ_Z for every qubit. We show that Y rotations on the qubits will produce less coherent logical noise in Lemma 13. The X and Z rotations contribute to independent components of the logical noise channel. Then each noise term that enters into the X-type logical noise components depend on at least L powers of θ_X. Similarly, the Z-type logical noise depends on at least L powers of θ_Z. Therefore, if the total rotation angle for each qubit, $\sqrt{\theta_X^2 + \theta_Z^2}$, is fixed, the logical noise strength is greatest when either θ_X or θ_Z is 0. Also, because the X- and Z-type errors contribute to different logical noise components, we can apply our analysis of coherent and incoherent logical noise components to the two types of errors separately. If both $|\sin\theta_X|$ and $|\sin\theta_Z|$ are $< 1/L$, then Lemmas 3 and 5 imply that the logical coherent and incoherent X and Z noise is dominated by the contributions of short logical strings. With this noise model, we will in general expect logical Y noise, but Lemma 14 implies that logical Y-type errors are negligible relative to X- and Z-type errors. The θ_X rotations contribute to the X_1 and X_2 logical noise, while the θ_Z rotations contribute to the Z_1 and Z_2 logical noise. The bounds we proved for coherent and incoherent logical noise components apply equally well to the X- and Z-type noise separately in this noise model. □

Lemma 8 states that among noise models consisting of single-qubit rotations where each rotation is close to the same, the coherence of the logical channel is greatest for the noise model consisting of Z-axis rotations on every qubit by the same angle. The same does not necessarily hold for noise models consisting of single-qubit rotations with wildly different angles of rotation on each qubit. This is not surprising because if we allow for wildly different rotation angles, we encounter the case where all the rotation angles are 0 except for the qubits along some very long logical string. This kind of high-weight connected term is beyond the scope of the present work, *cf.* Lemmas 3 and 5.

3.11 Correlations

We can apply Theorem 5 to study the toric code with minimal-weight decoding subject to correlated unitary noise. In the repetition code, we found that adding two-body correlations did not change the relation between coherent and incoherent components of the logical noise when the code size n is large. We can transfer that to the toric code using what we have already proven. Consider a single logical string. We can sum over its partitions. With correlated unitary noise, instead of $\sin\theta/2\cos\theta/2$ for each qubit in the logical string, we have a sum over the one- and two-body couplings in the Hamiltonian, h_1 and h_2. The model of correlated noise that we considered in Theorem 5 included two-body coupling terms between every pair of qubits in the code. Therefore, the magnitude of each multi-qubit error is a function only of its weight. We found that the coherent and incoherent logical noise in the toric code is dominated by the contributions from short logical strings with typical shape. In Theorem 6 we will finish proving a relation between the coherent and incoherent terms that is based on the number of terms and their magnitudes, which we always assumed to be $\sin\theta/2$ raised to the weight of the terms. In the correlated case we alter the magnitude of each term, but Theorem 5 tells us that string by string we can bound the coherent logical noise contribution in terms of the incoherent logical noise contribution.

Main Theorem

Theorem 6. *Consider the $L\times L$ toric code without boundaries subject to single-qubit unitary noise acting on each qubit. We chose minimal-weight decoding and assume that syndrome extraction is perfect. Suppose that each qubit is rotated by an angle θ about some axis and that $|\sin\theta| < 1/L$. Our conclusion will also hold for angles and axes that differ among the qubits, so long as the deviation is small as discussed in Lemma 8. Let $\tilde{\mathcal{N}}$ be the logical noise channel produced by encoding into the toric code, acting with single-qubit unitary noise, and then decoding. Denote by $\tilde{\chi}$ the chi matrix for the logical noise channel $\tilde{\mathcal{N}}$. Then the coherent and incoherent components of the logical channel are related by*

$$\sum_{i,j|i\neq j} \left|\tilde{\chi}_{i,j}\right|^2 < \frac{2}{(\sin\theta)^2}\left(\sum_{l|l\neq 0}\tilde{\chi}_{l,l}\right)^2 (1+\mathcal{E}), \tag{3.60}$$

where

$$|\mathcal{E}| \leq \frac{24\gamma\zeta^2}{\sqrt{L}} + O\left(\frac{1}{L}\right) + O\left((L\sin\theta)^{2\zeta}\right), \tag{3.61}$$

and ζ is an arbitrary L-independent constant. We denote the diamond norm distance of $\tilde{\mathcal{N}}$ from the identity channel by $D_\diamondsuit(\tilde{\mathcal{N}})$. It follows that

$$D_\diamondsuit(\tilde{\mathcal{N}}) \leq c\tilde{r}, \tag{3.62}$$

for a constant c given by

$$c^2 = \frac{(d_L+1)^2}{2}\left(1 + \frac{1}{(\sin\theta)^2}\right)(1+\mathcal{E}), \tag{3.63}$$

where d_L is the dimension of the code space ($d_L = 4$ for the 2D toric code without boundaries). Here $\tilde{r}$ is the average infidelity of the logical noise channel $\tilde{\mathcal{N}}$, and $\mathcal{E}$ is the error term bounded in equation (3.61). (If the logical noise channel $\tilde{\mathcal{N}}$ were unitary, then $D_\diamondsuit(\tilde{\mathcal{N}})$ would be proportional to $\sqrt{\tilde{r}}$.) We can also consider the growth of the average infidelity as we apply the logical noise channel many times in succession. Let $\tilde{r}_m$ be the average infidelity after m applications of $\tilde{\mathcal{N}}$; then using equation (3.60), we can write

$$\tilde{r}_m = m\tilde{r}\left(1 + \frac{d_L}{(d_L+1)\sin^2\theta}(m-1)\tilde{r}(1+\mathcal{E})\right), \tag{3.64}$$

where $d_L = 4$ for the 2D toric code without boundaries, $\mathcal{E}$ is the error term that is upper bounded in equation (3.61), and $\tilde{r}$ is the average infidelity for a single application of the logical noise channel. As long as the physical noise strength is below the fault-tolerant threshold, $\tilde{r}$ will be exponentially small in the code distance L. Therefore, equation (3.64) states that the term growing quadratically in m is exponentially small in L relative to the term growing linearly with m. In this sense, the coherence of the logical channel is heavily suppressed.

Proof. We start with a noise model consisting of Z rotations by angle θ on every qubit in the $L \times L$ block of toric code. We seek to approximate the coherent logical noise component $\tilde{\chi}_{Z_1 I}$ and relate it to the incoherent logical noise component $\tilde{\chi}_{Z_1 Z_1}$. First, let us calculate the coherent component. We write $\tilde{\chi}_{Z_1 I}$ as a sum over strings and partitions with a connected and disconnected part as in equation (3.7). Applying Lemma 3 to the connected part, we neglect high-weight terms, leaving only the logical strings with length $\leq L + 2\zeta$ for a fixed ζ, and making an error which is exponentially small in ζ. For this step, the magnitudes of the sines of the single-qubit rotation angles are required to be below a threshold value $1/L$. We apply Lemma 11 to argue that the disconnected part is equal to 1 up to a small correction. Lemmas 9 and 10 tell us that we can treat all short logical strings $\mathcal{L}$ as typical and make another small error. Now that we have only short typical logical strings, we apply Lemma 4 to perform the sum over partitions. We conclude that

$$\tilde{\chi}_{Z_1 I} = \sum_{\mathcal{L}} i^\ell \binom{\ell-1}{\frac{\ell-1}{2}}\left(\frac{\sin\theta}{2}\right)^\ell \left(1 + \mathcal{E}_{Shape}\right) + \mathcal{E}_{Long}, \tag{3.65}$$

where the sum is over all connected logical Z_1 strings $\mathcal{L}$ with length ℓ such that $\ell \leq L+2\zeta$. The error from logical strings with length greater than $L+2\zeta$ is bounded

$$\left|\mathcal{E}_{Long}\right| \leq \alpha L^{2\zeta+1}(\sin\theta)^{L+2\zeta}, \tag{3.66}$$

where $\alpha = (1 - L\sin\theta)^{-1}$. This error is from Lemma 3. The other error term from Lemmas 10 and 11 is bounded

$$\left|\mathcal{E}_{Shape}\right| \leq \frac{16\gamma\zeta^2}{\sqrt{L}} + O(1/L). \tag{3.67}$$

A further error due to neglecting exceptional partitions is subdominant according to Lemma 4, and is not shown in equation (3.65).

Now, we will lower bound the incoherent logical noise component $\tilde{\chi}_{Z_1Z_1}$. Lemma 5 implies that we can neglect the contributions of noise terms $(O_U\rho\, O'_U)$ such that $|O_U| + |O'_U| > L+2\zeta+1$. The error we make by truncating the sum is exponentially small in ζ, so long as the rotation angle θ satisfies $|\theta| < 1/L$. The incoherent logical noise component can be put in the form of a sum over logical strings as in equation (3.41). Using Lemma 7 we restrict to the connected terms where the logical string $\mathcal{L}$ is short and has typical shape and $|O_U| = |O'_U|$. We can also keep only the terms with $|O_U| = (\ell+1)/2$, because just as in the repetition code, these higher-weight partitions are suppressed by factors of $\sin\theta^2$ and the binomial coefficients are decreasing as we consider higher-weight O_U. The disconnected part is equal to 1 up to small correction according to Lemma 12. Finally, Lemma 6 gives a lower bound on the contribution of each logical string to the incoherent logical noise. All together, we have the following lower bound on $\tilde{\chi}_{Z_1Z_1}$:

$$\tilde{\chi}_{Z_1Z_1} \geq \sum_{\mathcal{L}} \binom{\ell}{\frac{\ell+1}{2}} \left(\frac{\sin\theta}{2}\right)^{\ell+1} \left(1 - \frac{8\gamma\zeta^2}{\sqrt{L}} + O(1/L) + O\left((L\sin\theta)^{2\zeta}\right)\right). \tag{3.68}$$

The error terms come from Lemmas 10, 5, and 12. A subdominant error term from Lemma 4 is suppressed in equation (3.68).

Putting together equation (3.65) and equation (3.68), we conclude the following about how the coherent and incoherent terms in the logical chi matrix are related:

$$\frac{|(\tilde{L}_a\tilde{\rho})|}{|(\tilde{L}_a\tilde{\rho}\tilde{L}_a)|} \leq \frac{1}{|\sin\theta|}(1+\mathcal{E}), \tag{3.69}$$

where

$$|\mathcal{E}| \leq \left(\frac{24\gamma\zeta^2}{\sqrt{L}}\right) + O\left(\frac{1}{L}\right) + O\left((L\sin\theta)^{2\zeta}\right). \tag{3.70}$$

We used

$$\binom{\ell}{\frac{\ell-1}{2}} \approx 2\binom{\ell-1}{\frac{\ell-1}{2}} \tag{3.71}$$

to arrive at equation (3.69).

We have restricted our attention to the coherent logical component $(\tilde{L}_a\tilde{\rho})$ and the corresponding incoherent component $(\tilde{L}_a\tilde{\rho}\tilde{L}_a)$, where L_a was either X or Z on one of the two encoded qubits. We did this because these are the largest components in the logical noise. This is proven in appendices H and I. In Lemma 14 we prove that we can neglect the logical noise components $(\tilde{L}_a\tilde{\rho})$ where L_a is a logical Y or a non-trivial operator on both encoded qubits. In Lemma 15 we prove that we can neglect coherent terms of the form $(\tilde{L}_a\tilde{\rho}\tilde{L}_b)$ with $a \neq b$. Using these results, we can bound the sum of all coherent logical terms relative to the sum of all incoherent logical terms. There are two off-diagonal terms for each diagonal term, e.g. $\tilde{\chi}_{Z_1 I}$ and $\tilde{\chi}_{I Z_1}$ are matched with $\tilde{\chi}_{Z_1 Z_1}$, so we have

$$\sum_{i,j|i\neq j} \left|\tilde{\chi}_{i,j}\right|^2 < \frac{2}{(\sin\theta)^2}\left(\sum_{k|k\neq 0} \tilde{\chi}_{k,k}\right)^2 (1+\mathcal{E}). \tag{3.72}$$

We have proven equation (3.60). The term on the right hand side is proportional to the infidelity by equation (K.9). Going back to Lemma 1 and equation (2.43), we can write

$$\tilde{r}_m \leq m\tilde{r} + m(m-1)\frac{d_L}{2(d_L+1)}\sum_{i,j|i\neq j} \tilde{\chi}_{i,j}^2, \tag{3.73}$$

where d_L is the dimension of the physical Hilbert space, which is 4 for the toric code without boundaries. We can combine this with equation (3.72).

$$\tilde{r}_m \leq m\tilde{r}\left(1 + \frac{d_L}{(d_L+1)\sin^2\theta}(m-1)\tilde{r}(1+\mathcal{E})\right). \tag{3.74}$$

Finally, we can use Lemma 16 with equation (3.72) to derive equation (3.62).

So far we have considered a noise model consisting of the same Z rotation by angle θ on every qubit in the code block. We can use Lemma 8 and Lemma 13 to prove that this noise channel produces maximally coherent logical noise in a region around uniform rotations. The single-qubit rotation angles are allowed to differ so long as the deviation is not too great. Therefore, the relation we found between coherent and incoherent logical noise components for the Z rotation noise model bounds the coherence of the logical noise channel for small rotations about any axis, so long as the rotations are close to uniform across the qubits. □

There are some subtleties in the interpretation of Theorem 6. We address these in the next subsection, but first we will make a remark about the error bound in equation (3.61). This error bound is satisfactory for finite code size L; however, we will need make a small modification before the bound is suitable for the $L \to \infty$ limit. This is because the term $O\left((L \sin\theta)^{2\zeta}\right)$ in equation (3.61) contains a factor polynomial in L. If the single qubit rotation angle θ satisfies $|\sin\theta| \propto 1/L$, then this polynomial factor would make the truncation error large as $L \to \infty$. The polynomial factor comes partly from the fact that the truncation error in equation (3.65) has a factor of 2^L relative to the factor of $\binom{L}{\frac{L+1}{2}}$ that appears in the lowest-weight incoherent noise terms. The ratio is proportional to $\sqrt{L}$. The other contribution to this polynomial factor comes from the path counting in Lemma 5, where we neglected a factor polynomial in $w + w'$ in equation (3.37). We can cancel the polynomial factor by slightly modifying our truncation procedure. Denote this polynomial factor $p(L)$. Instead of neglecting noise terms with weight $> L + 2\zeta$ in the coherent logical noise components, we neglect noise terms with weight $> L + 2\lceil \zeta' \log(L) \rceil$ for a constant ζ'. We perform a similar truncation for the incoherent logical noise components. Then we can choose ζ' large enough that $(L \sin\theta)^{2\zeta'} p(L)$ is decreasing with L. The minimum value for ζ' such that this is decreasing depends on the degree of $p(L)$ and the magnitude of $L \sin\theta$. If ζ' is greater than this minimum value, then $(L \sin\theta)^{2\zeta'} p(L)$ is bounded above by $a|L \sin\theta|^{\lambda\zeta' \log(L)}$, where a is a constant that is determined by the coefficients in the polynomial $p(L)$, and λ is a constant that depends on ζ', the degree of $p(L)$, and the magnitude of $L \sin\theta$. Our new truncation rule slightly alters the other error terms in equation (3.70). The new error term is

$$|\mathcal{E}| \leq \frac{24\gamma\zeta'^2(\log L)^2}{\sqrt{L}} + O\left(\frac{1}{L}\right) + a|L \sin\theta|^{\lambda\zeta' \log(L)}, \tag{3.75}$$

where a, ζ', and λ are constants. a and λ are determined as we described above. We are free to choose ζ', so long as it is greater than a minimum value. Now, if we take the limit $L \to \infty$, we find that the error term in equation (3.75) remains small. Therefore, we may apply Theorem 6 in the limit of $L \to \infty$ with equation (3.75) replacing equation (3.61).

3.12 Interpreting Bounds on Coherence

We have proved a relation between the diagonal and off-diagonal components of the chi matrix of the logical noise channel. The interpretation is a bit subtle, so it is worth commenting on here. We upper bounded the off-diagonal components by $1/|\sin\theta|$ times the diagonal components, and we were forced to assume that

$|\sin\theta| < 1/L$ because our analysis only applies to logical strings with length $\leq L + 2\zeta$ where ζ is a constant. With this assumption, the factor of $1/|\sin\theta|$ implies that the coherent component of the logical channel may be L times larger than the incoherent component. This might seem to indicate that the coherence of the logical channel is not suppressed for large L, but that is not the best way to think about the comparison.

In equation (3.64), the term quadratic in m has a coefficient proportional to $\tilde{r}/(\sin\theta)^2$ relative to the linear term. But the average infidelity $\tilde{r}$ is exponentially small in L. Thus the coefficient of the quadratic term is really exponentially smaller in L relative to the coefficient of the linear term. In equation (3.62), the constant c^2 is not really a constant, since it scales like L^2 if θ scales like $1/L$. The point is that if the logical noise channel were fully coherent, i.e. unitary, then c would scale like $1/\sqrt{\tilde{r}}$, but we find that $1/\sqrt{\tilde{r}}$ scales like $L^{L/2}$, which is vastly greater than L^2. We conclude that, although the logical noise channel is not exactly incoherent, it is quite close to an incoherent channel as measured by our statements about the growth of average infidelity and the relation between diamond distance and average infidelity.

We could also consider writing our logical noise channel as a product of a unitary rotation and a Pauli channel. We can solve for the single parameter in each of these two channels. In the limit of low logical noise strength, the angle of rotation of the unitary channel approximately equals one of the off-diagonal chi matrix elements, and the probability of error in the Pauli channel is comparable to one of the diagonal components of the chi matrix. Theorem 6 implies that the logical channel can be written as a product of a unitary channel and a Pauli channel where the angle of rotation of the unitary is larger than the error probability of the Pauli channel by a factor which is approximately $1/|\sin\theta|$, and therefore enhanced by a factor of L if θ scales like $1/L$. Again, this might make it seem like the coherence is not suppressed; however, the coherent channel makes a contribution to the average infidelity proportional to the rotation angle squared. This is why we find that the growth of average infidelity becomes nearly linear in m as the code size L increases. As the code block becomes large, the diamond distance for the logical noise channel is much smaller than what one would expect for a coherent channel based on the value of the average infidelity r. This is another way of making the same point as in the previous paragraph.

One might wonder whether a tighter upper bound than Theorem 6 can be derived on the strength of the coherent part of the logical channel relative to the incoherent part.

In fact, a substantially tighter upper bound is not possible, if we want this bound to hold for arbitrary small rotation angles. For instance, we could choose to set every rotation angle equal to zero except for the qubits along a single length L logical string. For this case, the computation of the logical channel is similar to our computation for the repetition code, where we were able to compute the logical channel quite precisely. Alternatively, for a fixed code size we could choose sufficiently small uniform rotation angles θ such that the lowest-weight terms dominate in the logical noise. In this case the computation of the logical channel is again similar to that of the repetition code. Since the bound we proved for the toric code nearly matches what we found for the repetition code, we know that our result is optimal in this special case. Of course, for some other particular set of single-qubit rotations, the logical noise channel may be less coherent than our upper bound predicts.

3.13 Conclusions

We have studied characterizations of coherence in quantum channels. One useful method for diagnosing the coherence of a channel $\mathcal{N}$ is to consider applying $\mathcal{N}$ m times in succession, and to investigate how the average infidelity r of the composite channel $\mathcal{N}^m$ increases with m. For incoherent channels r is linear in m, while for highly coherent channels it can grow quadratically with m. Another useful diagnostic is provided by the relationship between r and $D_\diamond(\mathcal{N})$, the distance between $\mathcal{N}$ and identity channel as measured by the diamond norm. For incoherent channels this distance scales linearly with r, while for highly coherent channels it scales like $\sqrt{r}$.

Using these criteria we have investigated the coherence properties of *logical* channels. To define a logical channel, we choose a particular quantum error-correcting code and decoding method; then we consider encoding an initial input state, subjecting the physical qubits to a noise model, and finally applying the decoder to obtain the channel's output. Our main conclusion is that, for the code families we examined, even if the physical noise model is highly coherent, the coherence of the logical channel is heavily suppressed in the limit of a large code block.

For the case of the quantum repetition code, we can compute the logical channel precisely, and verify that the logical channel is highly incoherent for large block size. Most of this paper was devoted to the analysis of a more challenging case, the $L \times L$ two-dimensional toric code subject to independent unitary noise. Our main conclusion about this case is encompassed by Theorem 6. Regrettably, for the case of the toric code we were able to prove that the coherence of the logical channel is suppressed only under an unrealistic assumption: that as the size L of the code block increases, the rotation angle θ applied to each qubit scales like $1/L$.

Under this assumption, we can estimate the logical channel well enough for our purposes by expanding it to a constant (L-independent) order in θ, and argue that the higher-order terms we ignore make a contribution that can be safely neglected. A key step in our argument is the observation, backed up by Lemmas 9 and 10, that for $L|\sin\theta| < 1$, the logical channel is dominated by logical strings with an easily characterized typical shape. For the logical strings of this typical shape, Lemmas 4, 7, 11, and 12 provide a sufficiently accurate estimate of the logical channel to prove Theorem 6.

Our main conclusion, that the coherence of the logical coherence is heavily suppressed, applies to unitary physical noise such that each qubit is rotated independently, even if the rotation axis and rotation angle vary from qubit to qubit, as long as the rotations are close to the same and sufficiently small. It also applies for some highly correlated noise models. The result also extends to physical noise channels which are convex combinations of unitary channels, or convex combinations of unitary channels and depolarizing channels. (Depolarizing physical noise is mapped to an incoherent depolarizing logical channel under error correction.)

We emphasize that our result is an asymptotic statement in the limit of large code size L, albeit under the assumption that the noise strength scales like $1/L$. For codes of fixed size, our results may not be tight; the coherence of logical channels for finite code blocks has been studied elsewhere [19, 37, 45]. Our goal was to study a family of codes with an accuracy threshold instead. When the noise is below threshold, the logical channel approaches the identity as the code block increases in size. In addition, under conditions where Theorem 6 applies, the coherent component of the logical channel vanishes much more rapidly than the incoherent component.

It is reasonable to expect that our conclusion — that the logical channel becomes increasingly incoherent as L grows — continues to hold even if we allow L to increase while the rotation angle θ has a fixed constant value. But proving this will be challenging. For one thing, if θ is a constant, we cannot accurately estimate the logical channel by expanding to a constant order in θ. Instead, logical strings with length $\leq L(1+\beta)$ need to be included for some constant β. These logical strings are not easy to count. A logical string can be regarded as a self-avoiding walk on the square lattice whose endpoints are a distance L apart, but previously derived upper bounds on the number of self-avoiding walks with specified length [40, 41, 43] do not treat the case where the distance between the endpoints differs from the length of the walk by an $O(1)$ multiplicative factor. And even if we could count the logical strings accurately, we would still need to overcome some additional obstacles to prove that the coherence of the logical channel is suppressed.

First, to prove Theorem 6, we disposed of the “exceptional” terms (Definition 7), those in which the uncorrectable error on a logical string has lower weight than the correctable error, by arguing that these terms are sufficiently rare as to make a negligible contribution to the coherent part of the logical channel. But for logical strings with length $L(1+\beta)$, exceptional terms will be far more common.

Second, when we calculated the contribution to the coherent or incoherent logical noise, we separated the computation into a sum over a connected part and a disconnected part, and argued in Lemmas 11 and 12 that the disconnected part contributes a multiplicative factor close to 1. But the proofs of these lemmas required the logical strings to be short, of length $L+2\zeta$ for constant ζ; these proofs don’t apply for longer logical strings of length $L(1+\beta)$.

Third, and even more dauntingly, our proof of Theorem 6 made use of a relationship between the physical noise terms that contribute to the coherent and incoherent logical noise. But as the logical string length increases, the contributions to the coherent and incoherent component of the logical channel become less and less alike. Each contribution to the coherent logical noise is associated with a logical string. In contrast, each contribution to the incoherent logical noise is associated with a pair of logical strings; these strings have segments in common, but they fluctuate relative to one another apart from those shared segments. For short logical strings, these fluctuations are relatively mild, and did not prevent us from relating the incoherent and coherent logical noise, as described in Section 3.8. For longer logical strings, the combinatorics become much harder to handle.

Unable to overcome these obstacles ourselves, we settled for proving a weaker result that applies for $L|\sin\theta| < 1$ rather than constant θ. Perhaps a more ambitious combinatoric analysis can push the proof through even for constant θ. Or perhaps a completely different approach will be more successful. Conceivably, it’s not true that the coherence of the logical channel becomes heavily suppressed for large L and sufficiently small constant θ, though we consider that possibility unlikely.

Further numerical studies of logical coherence may also prove to be instructive. The problem has already been studied numerically [19, 39, 45, 72]; however, our methods for organizing the estimate of the logical channel suggest different approaches to numerically simulating the logical channel. Numerics could help to resolve the issues that prevented us from extending Theorem 6 to the case where θ is an L-independent constant.

In our analysis of the toric code subject to single-qubit unitary rotations, we used minimal-weight decoding because it can be systematically analyzed. However, we don't expect our conclusion about suppression of logical coherence to be very sensitive to the choice of decoding method. The suppression arises from averaging over many error syndromes, and therefore should occur for other families of stabilizer codes with good decoders. Many of the elements from which we built the proof of Theorem 6 can be applied to more general stabilizer codes, including "logical strings," "partitions," "exceptional terms," and the decomposition into connected and disconnected parts.

We analyzed the toric code because it has an accuracy threshold, and we aspired to study the coherence of the logical channel for a fixed nonzero value of θ as the linear size L of the code block gets large. That aspiration eluded us, so we settled for investigating the logical coherence in the regime $L|\sin\theta| < 1$. In that regime, asymptotic results similar to ours, derived using similar methods, may be applicable to other code families that do not have an accuracy threshold. For example, for the Bacon-Shor code family subjected to depolarizing noise with error probability p, the optimal logical failure probability, computed analytically in [60], is achieved by the code with distance $d = O(1/p)$. We anticipate that, for unitary noise, decoding the optimal Bacon-Shor yields a logical channel with strongly suppressed coherence, though we have not done a careful analysis.

It has long been suspected that error correction suppresses the coherence of noise. Such suppression had been observed numerically for the toric code [19], but no rigorous argument supporting this conclusion had been previously known for any code family with an accuracy threshold. Our goal in this project was to prove that, for the toric code subject to sufficiently weak independent or weakly correlated unitary noise, the logical channel after decoding is highly incoherent in the limit of a large code block. We fell short of this goal, settling for a proof that coherence is suppressed in the case where the noise strength decreases as the code block grows. Nevertheless, we hope and expect that the tools we have developed will prove to be useful in future studies of quantum error correction.

Chapter 4

FAULT-TOLERANT UNIVERSAL COMPUTATION IN THE 3D TORIC CODE[1]

4.1 Introduction

As discussed in the general introduction in Chapter 1, finding a fault-tolerant implementation of a set of logical gates that allows for universal quantum computation is one of the primary challenges in the study of quantum error-correcting codes. According to the Eastin-Knill theorem [31], an error-correcting code cannot support a universal set of gates implemented with unitary, transversal operations. This means that in order to perform a universal encoded computation, some additional protocol is required. One possibility is to use magic state distillation [16]. This is when a separate code block is used to prepare high-fidelity encoded versions of special states known as magic states. With gate teleportation these states can be used to perform particular logical gates on the original error-correcting code. This technique can be used to implement a T gate in the 2D toric code, for example. At the same time, this approach incurs a significant overhead cost. Over the last several years many alternative approaches have been proposed.

One is to combine two different codes with different fault-tolerant gate sets in such a way that it is possible to perform a universal set of gates. This is possible by concatenating a pair of codes [47]. This has the significant drawbacks that even if both codes are topological, the resulting code has non-local, high-weight stabilizer generators. Also, the scheme sacrifices much of the code distance in an ordinary concatenated code. The number of qubits is the product of the number of qubits in the two codes. This means that for a given code distance, a relatively large number of qubits is required.

Another way of combining two codes is to construct a protocol to allow an encoded state in one code to be transformed into an encoded state of the other code. This is called code-switching, and it can be used to achieve a universal set of fault-tolerant gates [4]. The color codes [11] provide a convenient family of topological codes for this purpose. 2D and 3D color codes can be combined into a single code structure that exhibits a universal set of fault-tolerant, logical gates [9, 12, 46]. These schemes

[1] The work in this chapter was carried out in collaboration with Aleksander Kubica.

often include high-weight stabilizer generators.

A universal set of fault-tolerant gates can also be realized in a small fixed stabilizer code by performing the logical gates in many steps with interspersed error correction [77]. This idea is called "pieceable fault-tolerance." The primary disadvantages of this approach are that it is not clear how widely applicable it is and that it is slow, requiring a number of error correction steps that increases with the code size.

Another idea that in a sense also combines different error-correcting codes to achieve universal fault-tolerant computation is gauge-fixing in subsystem topological codes. These codes are similar to stabilizer codes, but some number of the logical operators have been demoted to gauge operators, the values of which are no longer considered to contain logical information. For each fixed state of the gauge qubits, the code is a stabilizer code, and by changing the state of the gauge, different stabilizer codes can be reached. The gauge group $\mathcal{G}$ is a set of Pauli operators that are not required to commute with each other. The stabilizer group $\mathcal{S}$ is contained in $\mathcal{G}$ and is defined as the center of the gauge group $\mathcal{G}$. Just as for a stabilizer code, error correction consists of measuring a set of generators for the stabilizer group, decoding the syndrome, and applying the calculated correction. Subsystem codes support a gauge-fixing procedure, where a subset of gauge generators is measured, fixing the value of the gauge qubits. Certain logical gates may be realized fault-tolerantly in the subsystem code with the gauge unfixed, while different logical gates may be realized fault-tolerantly after the code is fixed to a particular gauge. This can be used with the 3D gauge color codes to achieve universal computation without ever involving a 2D code [7].

Many of these approaches for a universal gate set require 3D codes. This is because the Bravyi-König theorem [17] implies that only the Clifford group of logical gates can be realized with constant depth circuits in 2D topological codes. A way of realizing a 3D topological code as a 2D lattice of qubits that undergoes a protocol over time was recently proposed [10]. This is a type of "measurement-based" quantum computation protocol. The measurement-based model of computation is another framework like the gate model, and it is equivalent to the gate model [64–66]. In the measurement-based model computations are carried by a series of single-qubit measurement performed on a large resource state. A 3D topological code can be realized as measurements performed on a resource state of which only a single 2D layer is present at any given time step.

The toric code (or the surface code) offers some advantages over the color codes.

For one, the weight of the stabilizer generators tends to be lower in the toric code, which means that the fault-tolerant threshold tends to be higher than for the color codes [24, 55]. The two codes are, however, closely related. It has been shown that every color code is equivalent up to local unitary operations to a number of folded copies of the toric code [54]. This connection means that some of the things that can be done in the color code may be translated to the toric code. For example, the 2D color code has a transversal implementation of the S logical gate, while the 2D toric code does not. However, it is possible to construct a fault-tolerant implementation of the S gate in the 2D toric code by braiding twist defects. In this work we present a family of 3D topological stabilizer codes built out of the 3D toric code that feature a fault-tolerant implementation of the logical T gate. Then we show how to construct a subsystem version of this code that can be gauge-fixed to recover the original stabilizer code. This subsystem code allows for universal fault-tolerant computation. Further, our code is compatible with a (2+1)-D measurement-based scheme, in which the logical operations happen on a 2D array of qubits that goes through a protocol in time.

4.2 The Stabilizer Code

The Lattice

We will begin by constructing the lattice on which our code will be defined. We begin with the 2D example of the toric code on the square lattice. This code is traditionally defined with qubits along edges of the square lattice [50]. The rotated toric code is defined on a different lattice formed by connecting each qubit to its four neighbors. This new lattice is a 2D square lattice rotated by 45 degrees. Now the qubits are located at vertices and the X and Z stabilizer operators are generated by alternating X and Z plaquettes in a checkerboard pattern. We can perform the same transformation in the 3D toric code defined on the cubic lattice. The resulting lattice is called the “rectified” lattice [73]. If we put qubits on the edges of the 3D cubic lattice, and then we join the midpoints of the edges, this gives us the cells shown in figure 4.2.

There are three different choices we can make for the stabilizer group of the 3D toric code on the rectified lattice. These are illustrated in figure 4.3. One choice is to put weight-6 X stabilizer generators on the octahedrons. In this case there are weight-4 Z generators on faces of the cubic lattice. This corresponds to X stabilizer generators on vertices and Z stabilizer generators on faces in the original cubic lattice. We could also choose weight-12 X operators on every other 12 vertex volume of the

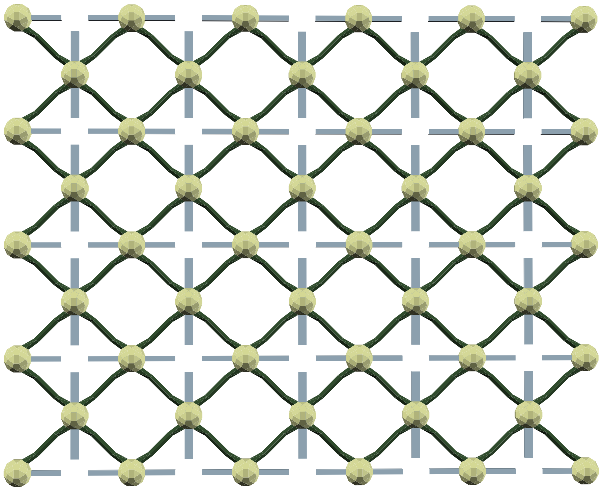


Figure 4.1: The 2D toric code on the square lattice is drawn with the original lattice in blue and the rotated lattice in green. In the original lattice, the qubits were on edges, whereas in the rotated lattice, the qubits are at vertices.

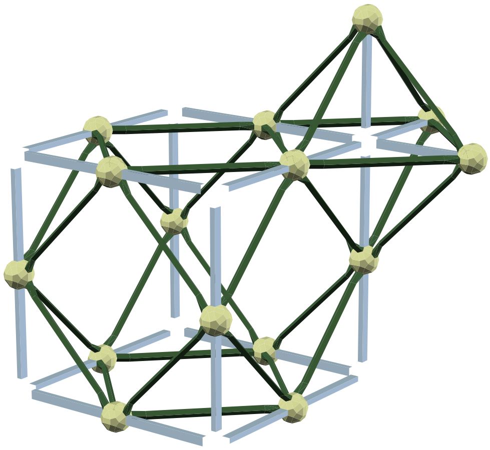


Figure 4.2: Pictured is the 3D cubic lattice with qubits on edges. Connecting the qubits forms the rectified 3D cubic lattice.

lattice and weight-3 Z operators around the faces of the alternate volumes. We could choose either set of volumes for our X generators in a checkerboard fashion. In total we have three independent choices of stabilizer group for a given cubic lattice. The conditions we require from a lattice so that we can construct a 3D toric code can be summarized as follows.

Definition 10. *Fix a 3D lattice $\mathcal{L}$ and choose a subset of the volumes B. This choice of lattice and subset of volumes supports a 3D toric code if both of the following*

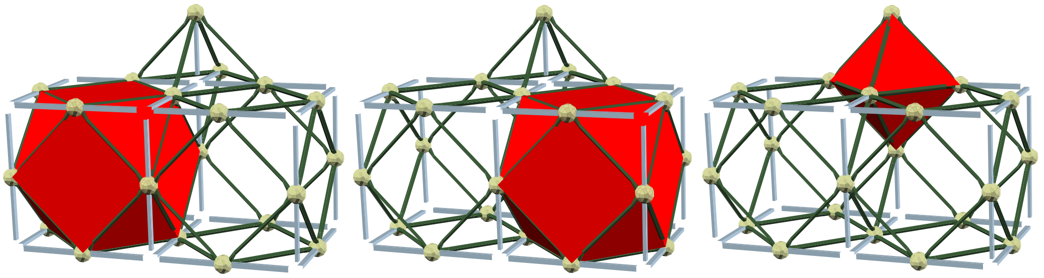


Figure 4.3: In the rectified 3D cubic lattice, there are three choices of stabilizer group to form the toric code. Here the red volume represents an X operator on every qubit in the volume. We can choose either the A, B, or C volumes to form the X part of the stabilizer group. The Z generators will be the faces not contained in the X volumes.

hold:

a) Every vertex $v \in \mathcal{L}$ is contained in exactly two different volumes, $b_1, b_2 \in B$.

b) For every $b \in B$ and face f not contained in b, the intersection $f \cap b$ is either empty or an edge in $\mathcal{L}$.

In the 3D cubic lattice, the sets of stabilizer operators described above are three possible choices that satisfy these conditions.

We will build our 3D toric code on the rectified lattice using one copy of toric code for each of the three possible choices of stabilizer group. These three copies of toric code are each defined on an identical piece of rectified lattice. Start with a block of cubic lattice and slice it along the $x = 0$ plane, the $y = 0$ plane, the $z = 0$ plane, and the $x + y + z = L$ plane, where L characterizes the code size. This gives us a tetrahedron of cubic lattice like the one in figure 4.4. Our lattice will consist of one copy of the tetrahedron of cubic lattice for each of the three possible toric codes on the rectified lattice. Let's call these A, B, and C. These three copies of toric code are joined at the base, or in other words, each qubit in the base of the A lattice is identified with the matching qubits in the bases of the B and C lattices. We can view this as one tetrahedron of cubic lattice with three qubits at each vertex except in the base. The qubits from the A code are coupled to the qubits in the B or C codes only via the base. Now, we modify the lattice at the base, so that this layer becomes a 2D color code. To do this we need to double the qubits in the base, so that the original square lattice becomes a square-octagonal lattice. This is illustrated in figure 4.5. The lattice above the base remains unchanged. The 2D square octagonal lattice and the 3D cubic lattice are compatible with each other in a way that will

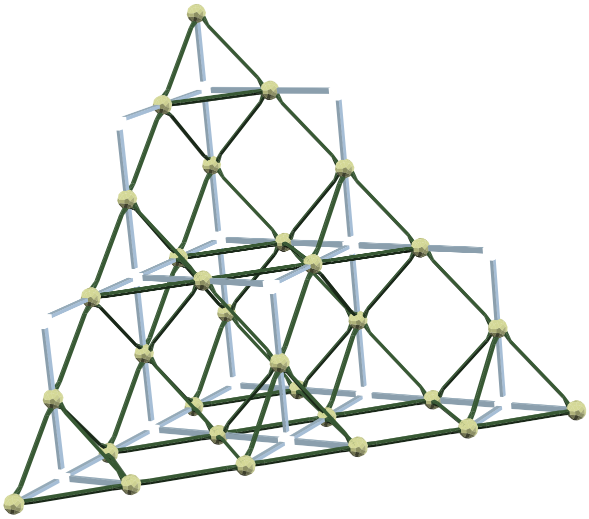


Figure 4.4: This tetrahedron of 3D toric code on the cubic lattice is bounded by the planes $x = 0$, $y = 0$, $z = 0$, and $x + y + z = L$. The (1,1,1) plane cuts through the lattice such that the boundary is made up of triangles and hexagons.

allow a simple implementation of a fault-tolerant T gate. The C lattice volumes in the base no longer intersect with each other after doubling the qubits in the base. We characterize the size of the code using L, the number of C volumes (octahedrons) along each of its linear dimensions.

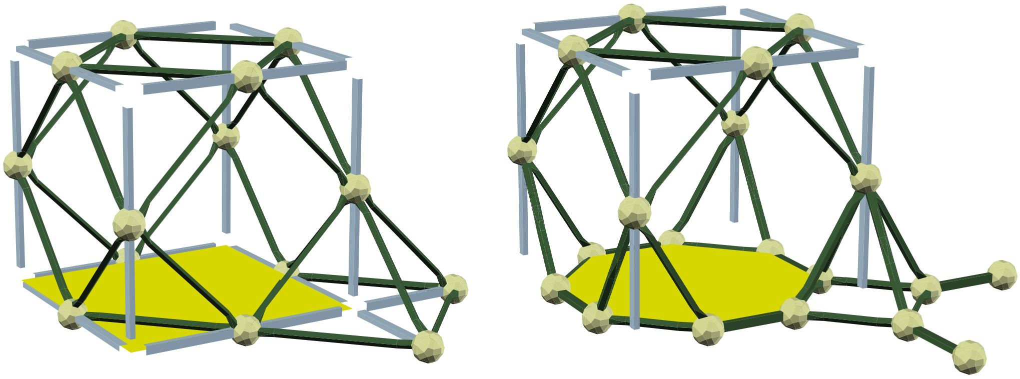


Figure 4.5: On the left, we have the toric code on the cubic lattice that we have cut along the $z = 0$ plane marked by the yellow square. This will be the base facet of the lattice. We modify the lattice at the base as shown on the right. Where the original lattice had one qubit, we place two so that the original square is inflated into an octagon. At the base we now have the square-octagonal color code lattice.

The 3D stabilizer toric code is supported on the lattice in figure 4.6, where each vertex above the base represents 3 qubits, A, B, and C. The stabilizer generators for the code are depicted for a version with size $L = 3$ in figures 4.7a, 4.7b, and 4.7c. The X stabilizer generators on the C lattice consist of X on the six qubits of each octahedron. Half of the weight-12 volumes in alternating, checkerboard fashion will be the X generators for the A, and the other half will be X generators for the B lattice. The Z generators for each lattice are the faces formed from the intersection of the X volumes for the other two lattices. This yields weight-4 Z generators for the C lattice and weight-3 Z generators in the A and B lattices. The stabilizer generators near the base are modified along with the lattice. The A and B X volumes that have weight-12 in the bulk are expanded to weight-16 along the base. The Z operators along the base in the A and B lattices remain weight-3, with two of the qubits in the base, but in the C lattice the weight-4 Z operators become weight-5 with two qubits in the base. There are also boundary stabilizer generators. These are discussed in the next section.

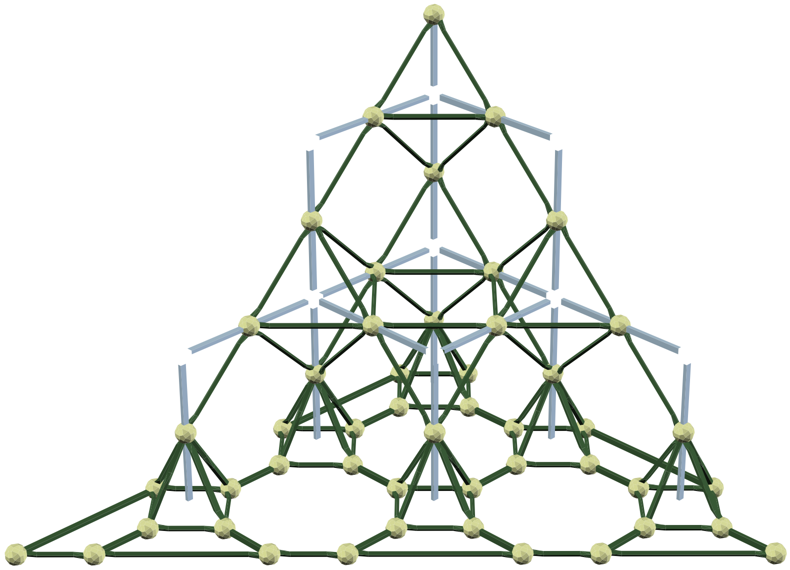
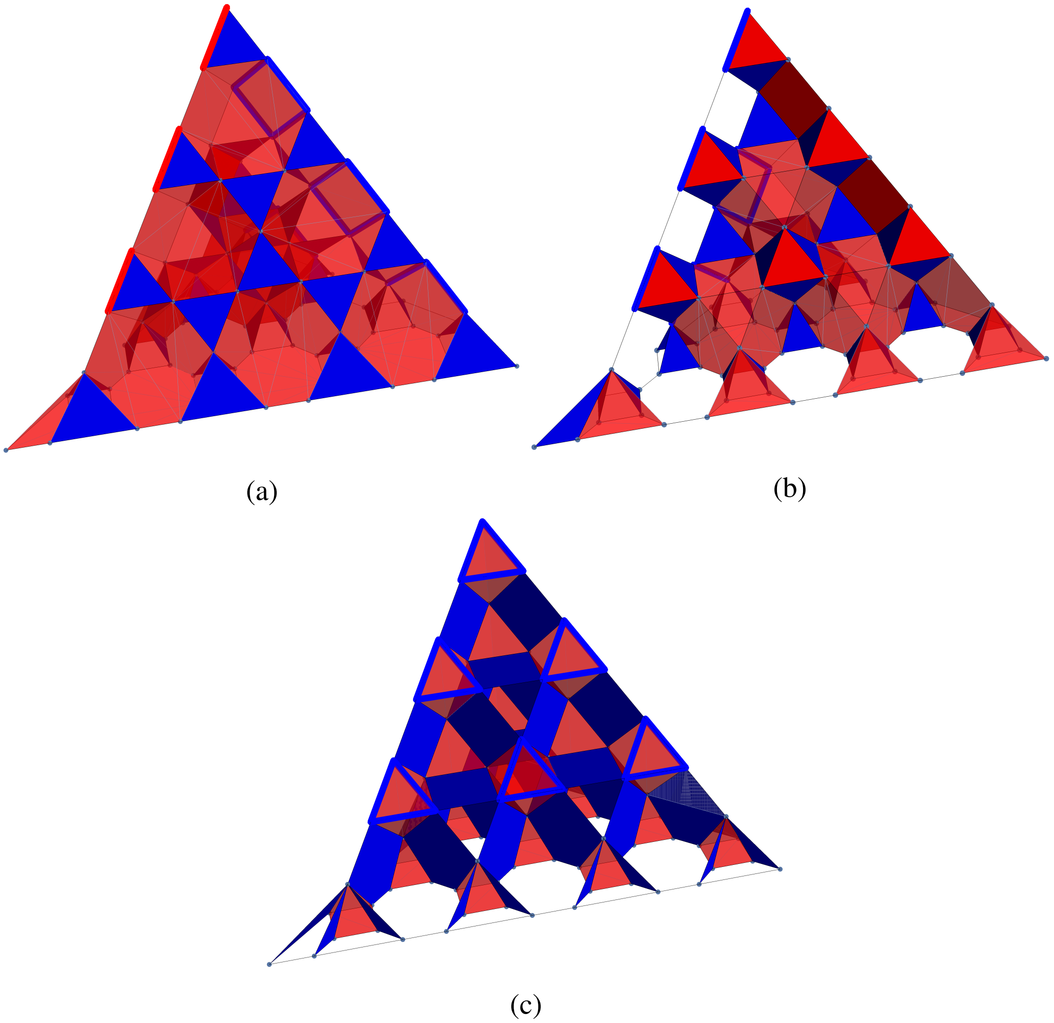


Figure 4.6: This is the lattice we use to construct a fault-tolerant T gate in the 3D toric code. The base is a 2D square-octagonal color code lattice. Three pieces of the 3D toric code are fused at the base, so that the qubits in the base are shared between three toric codes. The qubits not in the base represent three physical qubits, one for each toric code.

Boundary Conditions

Each copy of the toric code has three boundaries corresponding to the three facets at $x = 0$, $y = 0$, and $x + y + z = L$ in addition to the base at $z = 0$ where the three copies coincide. Of the three boundaries for each code one will be rough and the other two smooth. At each boundary we retain all the faces that are contained in



(a)

(b)

(c)

Figure 4.7: The stabilizer generators for the A, B, and C codes are shown in (a), (b), and (c), respectively. The X volumes are in red, and the Z faces are in blue. This includes boundary stabilizers of weight 2, 3, or 4.

the boundary. In addition, at the smooth boundaries we add the intersection of the boundary with the X volumes that would lie outside the boundary if the lattice were extended. At the rough boundaries we do the same for Z faces. Along the edges of the tetrahedron where rough and smooth meet, we apply the rough boundary condition. At the base, we add no additional stabilizers. In figure 4.7 we chose the rough boundary to be the facet on the left in the A lattice, the right facet in B, and the front facet in C.

Logical Pauli Gates and Code Distance

The logical Z operators in the code are string-like, and they must terminate on rough boundaries. The logical X operators are membrane-like and intersect two smooth boundaries in each copy of the code. Both types of operators can be supported entirely on the base. There are logical Z operators that run along each of the three sides of the triangular base. X acting on every qubit of the base is logical. Moreover, the logical Pauli group can also be represented on any of other three facets of the tetrahedron. Each of the three codes has one rough boundary. We have already said that there is a logical Z operator supported on each of the three edges of the base. There is also a logical X operator consisting of X on every qubit of the rough boundary for each of the codes. Except for these extreme cases, each logical operator will be supported in all three lattices as well as the base. A representative Z logical operator is illustrated in figure 4.8. A representative X logical operator consists of a plane or set of planes in each lattice defining a region of X operators in the base, for example see figure 4.9.

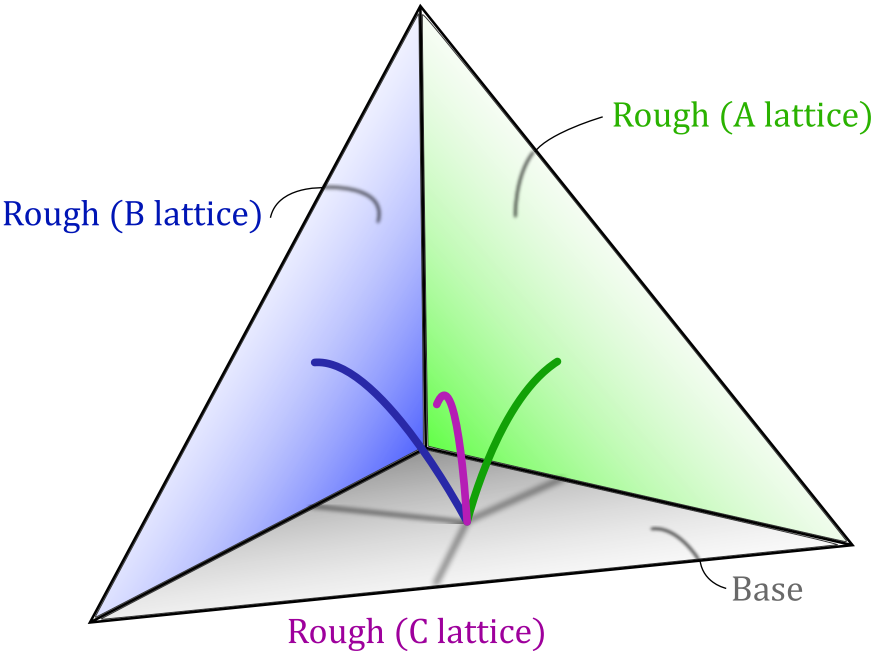


Figure 4.8: This logical Z operator contains a single qubit in the base and a string of qubits in each lattice connecting the qubit in the base to the rough boundary of each lattice.

The minimal-weight logical operator is of Z type. Notice that the three qubits at each of the three corners of the base are checked by only one X-type stabilizer generator. Therefore, there exist Z-type logical strings that start from one of these three base corner qubits and pass through only one of the three lattices. For instance, we could start at the qubit at the back corner of the base which is checked only by an X stabilizer generator from the C lattice and draw a line of Z errors up the “spine”

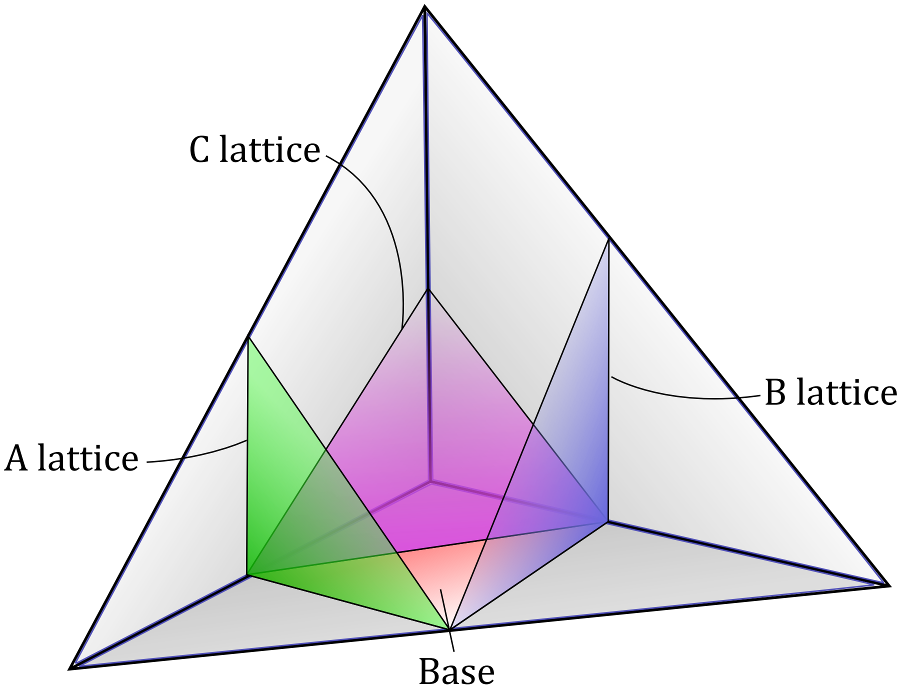


Figure 4.9: This logical X operator consists of a vertical plane in the A and B lattices, perpendicular to each other and intersecting at the front edge of the base. In the C code the operator contains a plane with normal (1,1,1). Together the three planes define a triangle of qubits in the base. The X logical operator includes X acting on each of the qubits in this triangle.

of the tetrahedron. In figure 4.6 this string has weight 4. The length of this logical string is equal to the code distance. In general, if we measure the lattice by how many C volumes are along one linear dimension, so that the lattice in figure 4.6 has size $L = 3$, then the code distance is $L + 1 = 4$.

Logical CZ and CNOT gates

Two copies of stabilizer toric code on the tetrahedron support a transversal CZ gate along the facets of the tetrahedra. Suppose we have two tetrahedra of our 3D toric stabilizer code. If we apply CZ gates between corresponding pairs of qubits in the bases of the two tetrahedra, this is a transversal logical CZ gate. Also, there are transversal logical CZ gates supported on many pairs of non-base facets. In figure 4.6 the three non-base facets appear at the front (the equilateral triangle facet) and at the back on the left and right (the two right triangle facets). There exists a transversal CZ gate between each pair of corresponding facets. On the front facets, the logical CZ gate consists of CZ on each pair of corresponding qubits in the front facet of the C lattice only. For the back left facet, the CZ gates are applied between the qubits in the A and C lattices only. On the back right facet, the transversal CZ gate acts only on qubits in the B and C lattices.

Proposition 1. *For two copies of stabilizer 3D toric code on the tetrahedron, there exist transversal logical CZ gates supported on the bases of the two tetrahedra as well as on any of the following pairs of corresponding facets*

Tetrahedron 1	*Tetrahedron 2*	*Number of CZ gates*
base	*base*	$2L^2 + 4L + 1$
front C lattice	*front C lattice*	$\frac{3}{2}(L^2 + L) + 1$
back left C lattice	*back left A lattice*	$2L^2 + 2L + 1$
and		
back left A lattice	*back left C lattice*	
back right C lattice	*back right B lattice*	$2L^2 + 2L + 1$
and		
back right B lattice	*back right C lattice*	
back right C lattice	*back left A lattice*	$2L^2 + 2L + 1$
and		
back right B lattice	*back left C lattice*	
back left C lattice	*back right B lattice*	$2L^2 + 2L + 1$
and		
back left A lattice	*back right C lattice*	

The facets are named front or back and left or right based on figure 4.6. CZ gates act between the sets of qubits listed in the same horizontal line. For example, in the first case each qubit in the base of tetrahedron 1 is acted on by a CZ gate with the corresponding qubit in the base of tetrahedron 2. Notice that logical CZ is supported on each facet of the tetrahedron. The number of physical CZ gates required differs depending on the facet, but for a large code the number of gates is small compared to the total number of qubits in the code, which is given by $\frac{3}{2}L^3 + \frac{7}{2}L^2 + 4L + 1$.

Proof. We will argue first that the stabilizer group is preserved by the CZ gates acting transversally on each pair of facets. Then we will show that a representative of each logical Pauli gate is mapped correctly.

We check the base first. The intersection of each X stabilizer and the base is equal to the support of a Z stabilizer, so CZ acting transversally on the bases of the two tetrahedra maps stabilizers to stabilizers. On the other facets we note that along the rough boundaries of each lattice, if we take the intersection of the facet with the X stabilizer generators, the intersection is contained in the boundary Z generators for that lattice. This means that CZ applied transversally along any facet preserves the stabilizer group. Let $\mathcal{S}$ denote the stabilizer group. Then

$$\mathrm{CZ}^{1,2}_{\mathrm{facet}}\, S_i\, \mathrm{CZ}^{1,2}_{\mathrm{facet}} \in \mathcal{S} \quad \forall S_i \in \mathcal{S}. \tag{4.1}$$

$\mathrm{CZ}^{1,2}_{\mathrm{facet}}$ denotes CZ acting between corresponding qubits in tetrahedra 1 and 2 on a given facet.

Next we check the action on logical Pauli operators. X on every qubit in the base is a logical X operator. If we act transversally with CZ gates along the base, this is mapped to Z on every qubit in the base of the other tetrahedron, which is a logical Z operator. Alternatively, if we act transversally with CZ along one of the non-base facets of the tetrahdron, the X logical operator is mapped to a line of Z operators in the second tetrahedron. These Z operators run along the intersection of the chosen facet and the base. This line of Z operators is a logical Z. Therefore, we conclude that CZ applied transversally to the sets of facets in the table has the correct commutation with logical operators. □

The stabilizer 3D toric code on the tetrahedron is a CSS code, meaning that the stabilizer generators can be divided into a set of X operators and a set of Z operators. This means that we also have a transversal CNOT acting on every pair of corresponding qubits in the two tetrahedra.

Fault-tolerant T gate

The stabilizer 3D toric code we have constructed supports a fault-tolerant logical T gate that is given by alternating T and T† gates on the qubits in the base combined with CCZ between the triple of qubits at each site away from the base. The square-octagonal base is a bipartite graph, so we can partition the qubits into sets α and β such that every neighbor of each qubit in α is in β and vice versa. There are an odd number of qubits in the base, so let the set α contain one more qubit than set β. We apply T to the α qubits and T† to the β qubits. That way when the logical gate acts on the all 0 or all 1 states, the net phase from the T and T† is correct.

An operation on the physical qubits is a logical gate if each logical state of the code remains in the logical space and moreover is mapped to the correct logical state. We will make use of a simple condition to check that our proposed T gate is, in fact, correct.

Theorem 7. *The base of the 3D lattice is a 2D square octagonal lattice. This is bipartite, so let us partition it into α and β such that each qubit in α shares an edge only with qubits in β and vice versa. The total number of qubits in the base is odd, so let the set α be one larger than β. Then the gate given by*

$$U = \mathrm{T}_\alpha \mathrm{T}^\dagger_\beta \mathrm{CCZ}_{\mathrm{Bulk}} \tag{4.2}$$

is a logical T gate. Here we have used a shorthand notation where T_α means a tensor product of T gates acting on each qubit in the set α and identity on qubits not in α.

Proof. We will make use of a condition on the commutators of our gate with the stabilizer generators of our code to show that our gate is a logical T. Here we use the group commutator $[A, B] = ABA^\dagger B^\dagger$. T commutes with Z, and for X there is a simple formula for all Z rotations:

$$[\mathrm{T}, X] = \mathrm{S} \quad [\mathrm{S}, X] = Z \quad [\mathrm{R}(\theta), X] = \mathrm{R}(2\theta), \tag{4.3}$$

where

$$\mathrm{R}(\theta) = \begin{pmatrix} \exp(-i\theta) & 0 \\ 0 & \exp(i\theta) \end{pmatrix}. \tag{4.4}$$

The logical state $|\tilde{0}\rangle$ is constructed by projecting the product state $|0\rangle^{\otimes n}$ onto the code space. The projector onto the code space is a uniform sum over all stabilizer operators. We can write this sum as a sum over all products of stabilizer generators:

$$U|\tilde{0}\rangle = U \sum_{i_1,\ldots,i_m \in \{0,1\}} S_{i_1} \ldots S_{i_m} |0\rangle^{\otimes n}. \tag{4.5}$$

The Z-type stabilizer generators acting on the state $|0\rangle^{\otimes n}$ give 1, so we may remove them leaving only the X-type stabilizer generators. Now we begin to commute the operator U towards the right:

$$= \sum_{i_1,\ldots,i_m \in \{0,1\}} S_{i_1} \left[S_{i_1}, U\right] U S_{i_2} \ldots S_{i_m} |0\rangle^{\otimes n}. \tag{4.6}$$

We continue to move U to the right and we also commute $[S_{i_1}, U]$ to the right:

$$= \sum_{i_1,\ldots,i_m \in \{0,1\}} S_{i_1} S_{i_2} \left[S_{i_2}, \left[S_{i_1}, U\right]\right] \left[S_{i_1}, U\right] \left[S_{i_2}, U\right] U S_{i_3} \ldots S_{i_m} |0\rangle^{\otimes n}. \tag{4.7}$$

We continue until U and all commutators are all the way to the right. We are left with

$$= \sum_{i_1,\ldots,i_m \in \{0,1\}} S_{i_1} \ldots S_{i_m} * \text{ Commutators } * U|0\rangle^{\otimes n}, \tag{4.8}$$

where the term called "Commutators" consists of products of the single commutators of U with each stabilizer generator and multiple commutators of U with all strings of stabilizer generators in ascending order. Now we must apply what we know about the commutators of our gate and the stabilizer generators.

Let us compute the commutator $[U, S_i]$. If S_i is a Z-type stabilizer generator, then it commutes with U. Next suppose it is an X-type generator. Let us rename the generator S_i^X as a reminder that it is X-type. We can decompose S_i^X into base sites Q and bulk sites R. The bulk sites will lie in one of the three lattices A, B, and C. Suppose that

$$S_i^X = X_{Q \cup R_A} \quad Q \subset \text{Base} \quad R \subset \text{Bulk} \quad R_A = \text{A lattice qubits in } R. \tag{4.9}$$

Then the T and T† gates along the base in U will give S and $S^\dagger$ gates in the commutator on qubits in Q. On the qubits in R_A, the inner commutator is between CCZ on corresponding qubits in the A, B, and C lattices with X operators on the qubits in R_A. This will give CZ between the corresponding qubits in the B and C lattices, specifically the qubits in R_B and R_C. In total the single commutator gives

$$\left[U, S_i^X\right] = \mathrm{S}_{Q\cap\alpha} \mathrm{S}^\dagger_{Q\cap\beta} \mathrm{CZ}_{(R_B, R_C)}. \tag{4.10}$$

Recall that α and β were our bipartite decomposition of the base. The base is such that every stabilizer generator that intersects the base has even weight on the base. Moreover, the qubits in each stabilizer that lie on the base are connected by edges, so that the intersection of each stabilizer consists of the same number of qubits in α and β. When this commutator acts on the all 0 state, it yields a net phase of 1 because of the equal number of S and S† gates.

Next the double commutators $\left[\left[U, S_i^X\right], S_j^X\right]$ will be non-identity only if S_j^X intersects Q, R_A, or R_B. Suppose that the support of S_j^X can be decomposed into Q' in the base and R'_B in the B lattice. The commutator of S and X gives Z, while the commutator of X on one qubit with CZ gives Z on the other qubit. Then the double commutator can be written

$$\left[\left[U, S_i^X\right], S_j^X\right] = Z_{Q' \cap Q} Z_{R'_C \cap R_C} = Z_{\left(\operatorname{supp} S_i^X \cap \operatorname{supp} S_j^X\right)}. \tag{4.11}$$

This is a Z operator in the C lattice along the intersection of the two X stabilizer S_i^X in the A lattice and S_j^X in the B lattice. The stabilizers in our lattice were defined such that the Z stabilizers in the C lattice are supported on the intersections of X stabilizers in the A and B lattice. The same holds if we permute A, B, and C. In equation (4.8) the single commutators all give 1 and the double commutators are all stabilizer group elements. This means that all the higher commutators vanish. The stabilizer elements from the double commutators are all Z-type and give 1 when acting on the all 0 state. Finally, we conclude:

$$U|\tilde{0}\rangle = U\text{Proj}\,|0\rangle^{\otimes n} = e^{i\pi/8}\text{Proj}\,|0\rangle^{\otimes n} = e^{i\pi/8}|\tilde{0}\rangle. \tag{4.12}$$

For the $|\tilde{1}\rangle$ state, we can multiply by an X logical operator consisting of X acting on every qubit in the base:

$$U|\tilde{1}\rangle = U\tilde{X}|\tilde{0}\rangle = \tilde{X}[\tilde{X},U]U|\tilde{0}\rangle = \tilde{X}[\tilde{X},U]U|\tilde{0}\rangle. \tag{4.13}$$

The commutator is given by

$$[\tilde{X},U] = [X,\mathrm{T}]_\alpha[X,\mathrm{T}^\dagger]_\beta = \mathrm{S}_\alpha^\dagger\mathrm{S}_\beta. \tag{4.14}$$

Then we have

$$U|\tilde{1}\rangle = \tilde{X}e^{-i\pi/4}e^{i\pi/8}|\tilde{0}\rangle = e^{-i\pi/8}|\tilde{1}\rangle. \tag{4.15}$$

□

Disjointness

We can use the disjointness to bound the accessible levels of the Clifford hierarchy [48]. We find that the disjointness bound matches the bound from the Bravyi-König theorem [17]. We do this by constructing a set of logical operators with limited intersections.

Proposition 2. *In the 3D stabilizer code we have constructed that features a fault-tolerant T gate, no logical gate beyond the third level of the Clifford hierarchy can be realized by a constant-depth circuit.*

Proof. To make use of the disjointness bound [48], we will construct families of logical Pauli operators.

Z **Operators:** For the Z operators, we choose a family of operators with support on exactly one qubit in the base. We define the family of Z operators by picking one of the qubits from each of the C volumes in the base. Then the string rises vertically in the C lattice. In the A and B lattice, the string angles upwards towards the one rough boundary. There are $\frac{1}{2}(L^2 + L)$ non-intersecting operators in this family.

X **Operators:** For X logical operators, we will compute the 2-disjointness. Here we allow each qubit to be part of the support of two members in our family of Pauli operators. We construct a family of logical X operators by choosing a plane in the A and B lattice. These planes are perpendicular to each other and to the base. In the base the two planes form an "L" shape. The corner of the "L" intersects the front edge of the base. In the C lattice we choose a surface that ends on the "L" in the base. There are $L + 1$ operators in this family.

Y **Operators:** We construct a family of 2-disjoint Y operators starting from our family of X operators. For each X operator, we multiply by a Z logical operator that intersects the base at the corner of the "L" shaped X operator. This Z operator is a member of the family of Z operators we constructed above. This gives $L + 1$ 2-disjoint Y operators.

To use the disjointness bound, we need the maximum and minimum code distance for different types of logical Pauli operators. For this code, the minimum distance is $L + 1$ for Z logical operators and the maximum distance is $L^2 + 2L$ for X logical operators. The disjointness is a maximum over all families of logical operators of the quantity

$$\Delta_c = \frac{\max\{|A| : \text{ at most } c \text{ elements } a \in A \text{ have support on any one qubit }\}}{c}. \tag{4.16}$$

We found

$$\begin{aligned}\Delta_1(Z) &= \frac{1}{2}(L^2 + L)\\ \Delta_2(X) &= \frac{1}{2}(L + 1)\\ \Delta_2(Y) &= \frac{1}{2}(L + 1).\end{aligned} \tag{4.17}$$

This allows us conclude that

$$\Delta \geq L/2. \tag{4.18}$$

Then the disjointness gives a bound on the maximum level of the Clifford Hierarchy attainable in a given code via constant depth circuits. We have the following inequality:

$$d_{max} < d_{min}(\Delta)^{M-1} \implies L^2 + 2L < (L + 1)(L/2)^{M-1}. \tag{4.19}$$

If this holds for an integer M, then all transversal logical gates are in the Mth level of the Clifford hierarchy. For us this gives $M = 3$, so the fault-tolerant T gate we find in our 3D toric code scheme represents the highest level of the Clifford hierarchy attainable. □

4.3 Higher dimensional stabilizer code

We can extend our construction to higher than three-dimensional toric codes. In d dimensions, the base will be a $d - 1$-dimensional color code. We will have d copies of toric code in the bulk. The simplest higher dimensional extension is for the lowest distance ($d = 2$) version of the code. In 3D this code has a seven qubit base and three qubits above the base, one each for the A, B, and C codes. In higher dimensions, we continue to have a single qubit in each copy of toric code. The base will be a $d - 1$-dimensional color code. We can construct the code by starting with a $d - 1$-dimensional color code and add one extra qubit to each $d - 1$-dimensional cell. The X stabilizer for each cell is the product of X on each qubit in the cell and X on the one bulk qubit in the cell. The Z stabilizers consist of Z on $d - 2$-dimensional faces in the base times Z on the bulk qubit in an adjacent d-dimensional cell. This gives a family of d-dimensional error detecting codes.

This family of error-detecting codes will exhibit a fault-tolerant $R(\pi/d)$ gate for $d > 2$, where $R(\theta)$ is defined in equation (4.4). The form of the gate is directly analogous to the fault-tolerant T gate in the 3D example. It consists of $R(\pi/d)$ acting on the qubits of the base and $C^{d-1}Z$ acting on the d qubits of the bulk.

4.4 Subsystem 3D toric code

We can define a subsystem version of our 3D stabilizer toric code. We will introduce gauge generators that recover the larger stabilizer generators for the A and B codes. For the C code, the gauge generators will be the same as the stabilizer generators. This will allow us to perform a fault tolerant Hadamard gate. We can then use a standard gauge-fixing procedure to map back to the stabilizer version, where we have a fault-tolerant T gate. This gives a scheme for universal fault tolerant quantum computation in 3D.

We need a modification to the stabilizer generators to achieve a fault tolerant Hadamard gate. We must change some of the operators in the base to be Y instead of X and Z. The resulting code will no longer be CSS. (A CSS code is one where there exists a generating set of stabilizer operators such that every operator is either X on each qubit in its support or Z.) The gauge group for the code contains every Z stabilizer operator from the original stabilizer code with the following modification: each operator acts as Y on the qubits in the intersection of its support and the base. Then at the base we have many triangles with a Z operator in the A or B lattice and two Y operators in the base. In the stabilizer version, the C lattice stabilizers included six-body Z operators at the base, which will become gauge generators with two Y operators in the base and four Z operators above. In addition, we take the Z-type gauge operators from the A lattice and replace Z by X to get a set of gauge generators in the B code. We do the same with the Z-type generators of the B lattice to get X-type gauge generators in the A lattice. These gauge generators break up the large X volumes in the original stabilizer code into three-body operators, so that X and Z gauge operators have the same form in the bulk. Next we add the X stabilizers of the C code to the gauge group without modification. This is not quite enough yet. We also add X and Z along the base on faces of the A and B volumes.

The stabilizer generators of this code will include all of the gauge generators in the C lattice and 12-body X and Z volume operators in the A and B lattices. Y operators on every face of the base are also stabilizers. In addition, around the base there are stabilizer generators that consist of fused volumes, where we have the product of two adjacent volumes in the A and B lattices, respectively, times X or Z on the base face.

Fault-tolerant Hadamard

In the 3D subsystem toric code version, a logical Hadamard gate consists of H applied transversally to all qubits in the A and B lattice including the base but excluding the qubits in the C lattice. Then we swap the A and B codes. We constructed the subsystem toric code in the A and B lattices such that the X gauge generators in one lattice are the Z gauge generators in the other. The C lattice does not have any additional gauge generators. That code is still a stabilizer code and has no symmetry between X and Z generators. The modification we made at the base, when we changed the operators at the base to be Y operators for many of the gauge generators, is essential for our Hadamard gate. This is what allows us to act only on the qubits in the A and B lattices and remain in the code space.

Proposition 3. *The gate*

$$\tilde{\mathrm{H}} = \mathrm{SWAP}_{A,B}\, \mathrm{H}_{A\cup B} \tag{4.20}$$

is a logical Hadamard gate in the 3D subsystem toric code built out of three code copies A, B, and C joined at the base of the tetrahedron. $A \cup B$ denotes the union of *the qubits in the A and B codes.*

Proof. We will prove that this gate is a logical Hadamard by arguing first that our map preserves the gauge group under conjugation and second that our map takes a representative of logical X to logical Z under conjugation. Our subsystem 3D toric code is constructed such that the A and B codes are dual to each other in the sense that the X gauge generators of the A code are the same as the Z gauge generators of the B code. When we apply Hadamard on each qubit in the A and B lattices, we exchange X and Z gauge generators. Then the swap gates applied between the A and B lattices exchange the A and B codes. Overall the X gauge generators of the A code are mapped to Z generators of the B code, and similarly for the Z generators. In the C code, only the generators intersecting the base are affected. The Z generators along the base are unchanged because these generators act on the base qubits with Y operators. The X generators along the base are mapped to X above the base in the C code and Z in the base. However, Y operators acting on the qubits of each face in the base are stabilizer generators. If we take the C code X generators in the base, act with Hadamard in the base, and multiply by Y operators in the base face, we recover the original C code X generator. We conclude that the logical Hadamard gate preserves the gauge group.

Now we must show that our proposed logical Hadamard gate maps a representative of logical X to a logical Z operator and vice versa. We will choose the logical X and Z operators supported entirely on the base. X applied to every qubit in the base is a logical X operator, and Z on every qubit in the base is logical Z:

$$\mathrm{Swap}_{A,B}\mathrm{H}_{A\cup B}X_{A\cap B}\mathrm{H}_{A\cup B}\mathrm{Swap}_{A,B} = Z_{A\cap B}. \tag{4.21}$$

The label $A \cup B$ refers to the union of the qubits in the A and B codes, and $A \cap B$ refers to the intersection, i.e. the base of the tetrahedron. We conclude that the gate $\mathrm{Swap}_{A,B}\mathrm{H}_{A\cup B}$ is a logical Hadamard on our 3D subsystem toric code. The gate is fault-tolerant because it is implemented by a constant-depth circuit. The depth is two. □

Gauge-Fixing

The gauge-fixing implementation of the T gate in our subsystem code has the following steps:

1. Measure Z-type gauge generators.

2. Compute corrected gauge syndrome.

3. Apply gauge-fixing operator (an X-type gauge operator).

4. Apply $\mathrm{H}_{Y,Z}^{\dagger}\,\mathrm{T}\,\mathrm{H}_{Y,Z}$ and $\mathrm{H}_{Y,Z}^{\dagger}\,\mathrm{T}^{\dagger}\,\mathrm{H}_{Y,Z}$ in alternating fashion to the base and $\mathrm{CCZ}_{A,B,C}$ to the qubits above the base.

5. Measure X-type stabilizer generators.

Here the gate $\mathrm{H}_{Y,Z}$ is given by

$$\mathrm{H}_{Y,Z} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ -i & -1 \end{pmatrix}. \tag{4.22}$$

This rotates Z to Y and vice versa. First, we will consider the noiseless case to show that our protocol is correct. Then we will move on to the noisy case and analyze each step individually, with a focus on how the noise is transformed. We will prove that this protocol is fault-tolerant by considering initial qubit noise and noisy measurement outcomes and calculating the output noise distribution.

Noiseless Case

When we measure all of the Z-type gauge generators, we recover the stabilizer code previously discussed (albeit with Y- and Z-type operators on the base instead of X and Z). In our subsystem construction, every Z-type gauge generator matched exactly the Z-type stabilizers of the stabilizer code. In addition, we recover the X-type stabilizers of the stabilizer code. In the bulk, none of the three-body X-type gauge generators commute with the nearby Z-type gauge generators. However, the product of four X-type generators in the A and B codes forms an X-type volume, that matches the stabilizer generators in the original stabilizer version of the code. These volumes commute with all Z gauge generators. Around the non-base facets of the code, the X-type gauge generators that commute with the Z-gauge generators are exactly the X-type boundary terms in our stabilizer code. At the base, we recover Y acting on all the base faces from the Z-type gauge generators (remember these were modified to have Y operators in the base). Also, the fused volume type stabilizer generators along the base in the subsystem code are broken up by the Z gauge generators into single volumes in the A or B lattice adjacent to the base. In this way we recover the original stabilizer code, albeit with some Y operators in the base.

The outcome of the Z-type gauge generator measurements will be random. The arrangement of gauge generators in the lattice gives constraints on the observable gauge syndromes. The first is that the Z gauge generators around an octahedron multiply to identity. This means the product of the measurement outcomes must be +1 for a valid gauge syndrome. This further means that if one of the Z gauge generators is violated, then at least one other generator around the octahedron must also be violated. This implies that the gauge-fixing operator will consist of closed loops. The smooth boundaries of each code allow X gauge-flux loops to condense, the same way that an X-type logical operator can terminate there. For this reason, the smooth boundaries of the code are valid endpoints for loops of gauge-flux. Second, we observe that the Z-type stabilizer generators in the gauge code, which are weight-12 volumes, can be recovered from two disjoint sets of gauge generators. The stabilizer measurement must yield +1 in the ideal case, so the product of the gauge measurement outcomes in each of the two disjoint sets must give +1. It follows that we can bipartition the Z-type gauge generators, and within each subset, the gauge syndrome must form closed loops. We choose the following bipartition: two-color the octahedral volumes in the lattice—call them white and black. Then the two sets of Z-gauge generators are those that lie at the faces of white octahedra and those in black octahedra. Valid gauge syndromes will consist of closed loops connecting only black octahedra and only white octahedra. The gauge-fixing operator will form a membrane with a boundary fixed by the loop of violated Z-type gauge generators. Gauge-fixing does not require us to apply any corrections to the C lattice. The C code is unchanged from the previous stabilizer version of our code. All the gauge generators are stabilizer generators, so that part of the code is automatically in the correct gauge. The gauge fluxes will be in the A and B code only.

The gauge flux can be represented on the gauge flux graph. This graph is dual to the original code lattice and is constructed by placing vertices at the center of each cell and edges intersecting each face. Each violated Z-type gauge generator appears as a highlighted edge in the flux graph. The highlighted edges must form cycles. We can define two subgraphs. Recall that we two-colored the octahedra in a checkerboard fashion. One subgraph is formed by removing all the vertices corresponding to black octahedra and the edges touching those vertices. The other is formed by removing all the vertices corresponding to white octahedra. The error syndrome is generated by the points where the gauge flux loops pass from one subgraph to the other. The trivial error syndrome corresponds to the case where each gauge flux is contained in one of the two subgraphs.

In order to reach the code state of the stabilizer code, we must apply a gauge-fixing operator that enforces the condition that every Z-type gauge measurement gives $+1$. This gauge-fixing operator will be a product of X-type gauge generators. Once the gauge-fixing operator is applied, the Z gauge generators have been upgraded to stabilizer generators. These stabilizers match the stabilizer code we described previously except that we now have some Y operators acting on qubits in the base. We perform a rotation on the base qubits given by equation 4.22, which maps Y to Z, Z to Y, and X to $-X$. This rotation modifies the stabilizer generators in the base, such that we recover exactly the stabilizer version of our code. Then we can apply the T gate from Section 4.2. After the gate, we rotate the qubits in the base back to return to the gauge code. In total we have applied a logical T gate to the subsystem code.

Noisy Case

The question remains whether this process can be done fault-tolerantly in the presence of qubit errors and measurement errors. These faults will mean that the gauge-fixing operator we apply will differ from the ideal one, and as a result the code will not be in exactly the correct gauge as we apply the T gate. First, we will analyze how physical qubit and measurement errors appear in our gauge syndrome. Second, we will describe how to correct the measured gauge syndrome. Next we will calculate how errors in the gauge-fixing propagate under our T gate operation. Finally, we will prove that local noise on qubits and measurements will give rise to local noise with a slightly higher error rate after we perform our fault-tolerant T gate.

We will suppose that the code is subject to local Pauli noise and local measurement noise. This means that in each time step the code block undergoes a Pauli error $P \in \mathcal{P}$ with probability $\mathrm{prob}(P) \leq p^{|P|}$, where $|P|$ denotes the weight of the Pauli operator P and p is a parameter called the local noise strength. Also when measurements are performed, a set of measurements A has a probability of being wrong that satisfies $\mathrm{prob}(A) \leq p_m^{|A|}$, where $|A|$ denotes the cardinality of the set A and p_m is a parameter called the local measurement noise strength.

Theorem 8. *Suppose that the gauge-fixing protocol defined at the start of Section 4.4 is used on the subsystem code defined above subject to local Pauli noise on the* *code qubits and local noise on the gauge generator measurement outcomes. Then the residual noise after the gauge-fixing procedure is local.*

Proof. X errors acting on the code qubits will cause the surrounding Z-type gauge generators to give the opposite measurement outcome. A single, isolated X error will appear as a loop that joins a white and a black vertex on the gauge syndrome graph. Valid gauge syndromes consist of closed loops within the black or white subgraphs. Therefore, in the case of X errors on code qubits, we will correct the gauge syndrome by forming independent closed loops in the two subgraphs. Qubit errors lead to broken loops when the subgraphs are viewed separately. Measurement errors change the parity of the octahedron to which they belong. In other words, the flux conservation of gauge syndrome loops is violated. The closed loops in the gauge syndrome are broken at the positions where measurement errors occur. To recover a valid gauge syndrome, we must correct the faulty syndrome by closing all loops within the white and black subgraphs. We do this with a minimal-weight matching procedure. We flip the minimum number of Z-type gauge measurement outcomes to produce a valid gauge syndrome. For a single, isolated X error, the lowest-weight gauge correction will lead to no gauge flux in both subgraphs. For more complicated configurations of X errors, a non-trivial gauge flux may result. Similarly, a single, isolated measurement fault will be corrected, but a configuration of many faults will in general lead to an erroneous gauge flux.

Using minimal-weight matching for our gauge syndrome correction implies a bound on the weight of the erroneous gauge flux in terms of the weight of the measurement faults and code qubit errors. The weight of the corrected gauge flux will differ from the true gauge flux by no more than double the number of measurement errors. The gauge syndrome correction always has a trivial error syndrome, i.e. the flux loops are closed within the black or white subgraphs. Therefore, qubit X errors are equivalent to four measurement errors, two in each subgraph. In order for qubit X errors to lead to an erroneous gauge flux, the errors must fill most of an X gauge operator with gauge flux equal to the erroneous gauge flux. The number of qubit errors required will be much larger than the number of measurement faults required to produce the same erroneous gauge flux.

This is all directly analogous to 3D gauge color codes [7]. In those codes, the gauge syndrome consists of color-flux conserving closed loops. Measurement errors lead to color-flux non-conservation, which breaks up the gauge syndrome loops. The syndrome correction closes the loops to produce a valid gauge syndrome. Finally, the error syndrome is the set of branching points where a string with one coloring turns into two differently colored strings.

We have described how the faulty gauge syndrome is corrected and how after correction qubit errors and measurement faults lead to a gauge syndrome that differs from the true gauge syndrome. The error after gauge syndrome correction is the product of whatever qubit errors were present before gauge-fixing and the erroneous gauge flux. These errors are transformed by our fault-tolerant T gate. Recall that our T gate protocol involves applying T and T† gates in an alternating pattern on the qubits in the base of the tetrahedron. Above the base, we apply CCZ gates on corresponding qubits in the A, B, and C codes. The T gates map X errors to S errors under conjugation. The CCZ gates map X errors in one code to CZ errors on the corresponding qubits in the other two codes. The final step of the gauge-fixing protocol is to measure X-type stabilizers. This measurement will transform the non-Pauli errors introduced by our T gate implementation into random Pauli errors.

Suppose that we have an erroneous X gauge flux in the A code after the first three steps of our gauge-fixing T gate protocol. In step four this erroneous gauge flux will be transformed into a non-Pauli error that spans all three codes. The final step is to measure X-type stabilizer generators. Consider two types of X stabilizers: one stabilizer intersects the interior of the erroneous gauge flux (the membrane-like X operator) and the other intersects the gauge flux loop (the boundary of the membrane). We will show that the first stabilizer is never violated, but the second stabilizer has a 1/2 chance of being violated.

In the first case, consider the intersection of the bulk of the X gauge flux surface, G_A^X in the A code and an X stabilizer operator in the B code. Call this stabilizer operator S_B^X. If the intersection is non-empty, then the intersection will match the support of a Z-type stabilizer operator in the C code. Call this operator S_C^Z. We will calculate the expectation value of the stabilizer S_B^X in the state produced from the maximally mixed code state with an erroneous X gauge flux acted on by the logical T gate. This gives

$$\langle S_1^X \rangle_{id} = \mathrm{Tr}\left(S_B^X \, \mathrm{CCZ}_{A,B,C} \, G_A^X \, P \, G_A^X \, \mathrm{CCZ}_{A,B,C} \right), \tag{4.23}$$

where CCZ is a CCZ gate between each set of corresponding qubits in the A, B, and C codes and P is the projector onto the code space, which includes a projector onto the +1 eigenspace of both S_B^X and S_C^Z. The CCZ gates transform the erroneous X gauge flux in the A code into CZ gates between the B and C codes with support on the qubits in G_A^X:

$$\mathrm{CCZ}_{A,B,C}\, G_A^X = G_A^X\, \mathrm{CZ}_{B,C}, \tag{4.24}$$

where $\mathrm{CZ}_{B,C}$ acts on the support of G_A^X. Then the code space projector is transformed to

$$\mathrm{CZ}_{B,C}\, P\, \mathrm{CZ}_{B,C} = \mathrm{CZ}_{B,C}\,(1 + S_B^X)(1 + S_C^Z)\ldots \mathrm{CZ}_{B,C} = (1 + S_B^X S_C^Z)(1 + S_C^Z)\ldots. \tag{4.25}$$

Finally, we are left with

$$\begin{aligned} \langle S_1^X \rangle_{id} &= \mathrm{Tr}\left(S_B^X G_A^X \left((1 + S_B^X S_C^Z)(1 + S_C^Z)\ldots \right) G_A^X \right) \\ &= \mathrm{Tr}\left(\left((S_B^X + S_B^X S_C^Z + S_C^Z + 1)\ldots \right) \right) \\ &= 1. \end{aligned} \tag{4.26}$$

The outcome of measuring the stabilizer generator S_B^X is +1 with certainty.

Now, consider a stabilizer generator in the B code that borders the edge of the erroneous gauge flux operator. Denote this operator S_B^X. The difference between this case and the previous one is that here the intersection of the geometric supports of G_A^X and S_B^X does not match a stabilizer operator in the C code. Let $Z_C^{G\cap S}$ denote Z operators acting in the C code on each element of the intersection of the geometric supports of G_A^X and S_B^X. In this case equation 4.26 reads

$$\begin{aligned} E_{id}(S_1^X) &= \mathrm{Tr}\left(S_B^X G_A^X \left((1 + S_B^X Z_C^{G\cap S})\ldots \right) G_A^X \right) \\ &= \mathrm{Tr}\left(\left((S_B^X + Z_C^{G\cap S})\ldots \right) \right) \\ &= 0. \end{aligned} \tag{4.27}$$

The outcome of measuring the stabilizer generator S_B^X in this case is ±1 with probability $1/2$. The many X-type stabilizer generators in the B code that lie in the region around the boundary of the X gauge flux in the A code are subject to a constraint. The intersections of all X-type stabilizers in the B code with the boundary of the gauge flux loop multiply to the identity. Therefore, the number of violated X-type stabilizers in the B code around the erroneous gauge flux loop must be even, or in other words, charge neutral. Precisely the same statements hold if we permute the A, B, and C codes in the preceding discussion.

We have shown how local noise on the qubits and the gauge measurement outcomes leads to a particular kind of residual noise after the gauge-fixing protocol. Next we will prove that this residual is local, and therefore there exists an efficient decoding scheme with a fault-tolerant threshold against this type of noise.

Consider a configuration of residual Z errors. These errors could arise from Z errors on the code qubits or from X gauge measurement errors in another code (Z errors in the B code result from gauge measurement errors in the A code). Let us bound the probability of this error configuration. Supposing that the errors arise from local Z qubit errors, the probability would be bounded by p_z^w where p_z is the local noise strength and w is the number of errors in the error configuration. If instead the error configuration arises from gauge measurement errors, the probability of the error configuration is a sum over errant gauge flux loops. Each errant flux loop can be produced in several ways from combinations of gauge measurement errors and our minimal-weight syndrome corrections. We can bound the number of loops and ultimately the number of configurations of gauge measurement errors that could lead to our given error configuration.

Fix a configuration of w errors that come entirely from measurement errors that are propagated by the gauge-fixing procedure. These errors must result from a loop length $\geq 2w$. Let the length of the loop be 2ℓ. Then the number of such loops of length 2ℓ starting at the first error, say, is $\leq \mu^{2\ell}$, where μ is the lattice connective constant. Each loop can be split into many configurations of gauge measurement errors that could be corrected by minimal-weight decoding to produce the given loop. We can bound the number by 4^ℓ, that is the total number of ways of subdividing the loop. Then there are many possible random configurations of Z errors that might result from each loop. The desired configuration is only one of many. For a fixed loop, there are $2\binom{2\ell}{w}$ possible syndromes produced by errors on the qubits in the loop. The factor of 2 comes from the fact that each error along the loop has a partner with the same syndrome produced by multiplying by a membrane-like stabilizer operator that terminates on the loop. The probability of recovering the given error configuration from a fixed loop of length 2ℓ is $\leq 2\binom{2\ell}{w}/4^\ell$.

We must sum over possible loop lengths with $\ell > w$. The number of measurement errors required is at least ℓ, so we have a factor of p_m^ℓ:

$$\sum_{\ell=w}^{\infty} 2p_m^\ell \mu^{2\ell}\binom{2\ell}{w}/4^\ell \leq \sum_{\ell=w}^{\infty} 2(\mu^2 p_m)^\ell \leq 4(\mu^2 p_m)^w, \tag{4.28}$$

assuming that $\mu^2 p_m \leq 1/2$. In total the probability for our fixed error configuration is $\leq \tilde{p}^w$ for $\tilde{p} = p_z + (2\mu^2 p_m)$. This implies that the residual noise is local. □

We can decode the residual noise after step 5 using none of the information from step 1. However, we expect that we can achieve a much larger fault-tolerant noise threshold if we make use of the measurement outcomes from step 1 and our knowledge of the gauge-fixing operator that we applied in step 3. We propose the following modified version of the cluster decoder [13, 15] that we expect to perform well against the particular noise model left over after our gauge-fixing procedure. The decoder operates by grouping errors at many different length scales. The decoder proceeds through length scales Q^i for $i = 1, \ldots, m$, where m is a fixed maximum level. At each level, the decoder constructs clusters of violated stabilizer generators. A "Q^i-connected component" is defined as a set of violated stabilizer generators such that the set cannot be divided into two sets separated by a distance that is at least Q^i. For each connected component, the decoder checks to see if a local error contained within the one-neighborhood of the connected component could produce the combination of violated stabilizer generators in that connected component of the syndrome. If such an error exists, then the error is added to the predicted correction that is the output of the decoder, and that connected component of the syndrome is removed. Then after all q^i-connected components are considered at level i, the decoder moves to level $i + 1$. In this way the measured syndrome is broken up level by level and a predicted correction operator is calculated. Our modification to this decoder is that we make use of our knowledge from the previous steps of the gauge-fixing protocol in the following way: when the neighborhood of each error is searched and Q^i connected components are computed, the sites along the correction to the gauge syndrome that we compute in step two of the gauge-fixing protocol are considered to be a distance 0 apart. This is a modification to the metric used to define the distance between violated stabilizer generators in the lattice. Whenever we correct the gauge syndrome to recover from measurement errors, we run the risk of introducing erroneous gauge flux. This decoder takes this fact into account. Because the noise is local, we know that this decoder will exhibit a threshold. To estimate how well this decoder performs will likely require extensive numerics, which we have not performed in this work.

Counting Logical Qubits

We need to prove that both our stabilizer code and our subsystem code contain one encoded qubit. We characterize the size of the code using L, the number of C volumes (octahedra) along each of its linear dimensions. Our convention here is that we count the C code generators first. Then we count the additional independent generators in the A and B codes. We will also count the number of generators that are boundary terms. This will be the maximum independent set of boundary stabilizer generators.

First, in the stabilizer code we will count X and Z for each code separately. Then we will add the base. We will count only independent stabilizer generators. In the C code each X stabilizer is an octahedron that will be truncated around the facets of the code. The number of independent C code X stabilizer generators is

$$CX = \frac{1}{6}(L^3 + 3L^3 + 2L). \tag{4.29}$$

Of these, $\frac{1}{6}L(L^2 - 1)$ lie above the base, and $\frac{1}{2}(L^2 + L)$ lie along the base. We can also count the A and B volumes. There are several types of X terms in the A and B codes. In addition to the volumes, we have a number of 2-, 3-, and 4-body boundary X stabilizer generators. In total, the number of independent A and B code X stabilizer generators is

$$AX + BX = \frac{1}{6}(L^3 + 6L^2 + 5L). \tag{4.30}$$

Of these, $L(L-1)$ are boundary terms. The non-boundary terms include $\frac{1}{2}L(L+3)$ X volumes that intersect the base.

The Z operators for the C code are the faces at the intersection of the A and B code X volumes. The number of independent ones is

$$CZ = \frac{1}{3}(L^3 + 3L^2 + 5L). \tag{4.31}$$

This includes $L(L - 1)$ boundary terms—these are all along the front facet of the tetrahedron, see figure 4.7c. Also, $L(L + 3)$ of the non-boundary Z stabilizer generators intersect the base. The set of C code Z stabilizer generators includes in their linear span the set of faces that lie in the base. When we count the independent A and B code Z stabilizer generators, we must remember that the base faces have already been counted. The A and B Z stabilizer generators are the faces of C code X volumes. We want to count only the independent generators. This means that in the bulk, each tetrahedron or C code X volume contributes 5 independent generators. There are 8 faces, but the tetrahedron and each of its adjacent volumes has the property that the product of the set of faces gives identity. This leaves 5 independent generators. In total the number of Z stabilizer generators in the A and B codes independent of the generators we already counted for the C lattices is

$$AZ + BZ = \frac{1}{6}L(5L^2 + 6L + 7). \tag{4.32}$$

This includes $\frac{1}{2}(3L^2 - 5L + 2)$ independent two-body boundary terms and $L^2 + L - 1$ independent generators intersecting the base.

All together the number of independent stabilizer generators in the code is

$$\text{Independent stabilizer generators} = \frac{1}{2}(3L^3 + 7L^2 + 8L), \tag{4.33}$$

and the number of qubits is

$$n = \frac{1}{2}(3L^3 + 7L^2 + 8L + 2). \tag{4.34}$$

The number of logical qubits is equal to the number of qubits n minus the number of independent stabilizer generators. Therefore, our stabilizer code has one encoded logical qubit.

The subsystem version includes every stabilizer generator from the C code as stabilizer (and gauge) generators. In addition, the number of gauge generators in the A and B code that are independent of each other and of the stabilizer generators we counted for the C code is

$$\text{A + B code gauge generators independent of C code} = \frac{1}{3}(5L^3 + 6L^2 + 4L + 6). \tag{4.35}$$

These gauge generators include boundary terms that match the Z boundary terms in the stabilizer code and X operators on the octagonal faces of the base. The number of independent stabilizer generators in the A and B codes not contained in the span of the C code generators is

$$\text{A + B code stabilizer generators independent of C code} = \frac{1}{3}(L^3 + 6L^2 + 2L). \tag{4.36}$$

These stabilizer generators include boundary terms that look like the X boundary terms in the stabilizer code and fused volumes at the base of the type we described in the first part of Section 4.4. The number of encoded qubits in a subsystem code is given by

$$k = n - \frac{1}{2}(\log_2 |\mathcal{G}| + \log_2 |\mathcal{S}|), \tag{4.37}$$

where $\mathcal{G}$ is the gauge group and $\mathcal{S}$ is the stabilizer group. Then the number of encoded qubits k is 1.

4.5 (2+1)-D protocol

We can follow Bombin [10] and Brown [20] and convert our 3D subsystem toric code on the tetrahedron to a (2+1)-D measurement-based protocol. Cluster states and measurement-based quantum computation are a way of implementing computations and error-correcting codes using an initial resource state and single-qubit measurements [64–66]. The idea here is to implement a measurement-based version of the 3D code by progressing through subsequent 2D layers. The key element is just-in-time decoding. In a (2+1)-D scheme, we are limited by causality. We do not have access to the full set of measurement outcomes but only to the ones in the past and present. This limitation is bound to make our decoding worse. We will introduce extra errors, but what we must show is that even with these extra errors, we still have a fault-tolerant accuracy threshold against stochastic noise. We will discuss decoding in Section 4.5.

The 3D color code can be defined on tetrahedra called colexes [7, 11]. Many colexes can be stacked in columns within a measurement-based network. This is called the "twister architecture" [10]. It allows (2+1)-D computation on any number of encoded qubits. A similar twister architecture can be built of 3D subsystem toric code tetrahedra. We have already described all the relevant logical operations. Pauli gates, S, Hadamard, and T can all be realized on each tetrahedron. CZ gates can be realized on the faces where two neighboring tetrahedra meet. This allows for universal computation on many qubits in a (2+1)-D measurement-based scheme.

The measurement-based protocol proceeds as follows: three qubits are initialized in the plus state. These are the qubits at the top of figures 4.12, 4.13, and 4.14 for the A, B, and C codes. Then the second layer of qubits is introduced. This layer contains several qubits. CZ gates are applied between the first and second layer along each of the links in the figures. Then the first layer is measured in the X basis. The third layer is introduced for each code, and the process continues until each code reaches the base. The base qubits are shared among the three codes, so the bases of the three figures are identified. After the final measurement step, the resulting state is a code state of the 2D color code on the base. Because the boundary Z stabilizers and the modified lattice at the base somewhat obscure the pattern in the bulk, we illustrate the bulk of the A, B, and C lattices in the measurement-based protocol in figures 4.11 and 4.10.

Our measurement-based protocol is flexible in that once we have translated our three code into a 3D fault-tolerant cluster state, the (2+1)-D protocol can be run any any direction to prepare a state on one of the facets of the 3D code. We will restrict ourselves to protocols that prepare a state on the base of the 3D code. The base is encoded in a 2D triangular color code.

This protocol is fault-tolerant for different reasons for X and Z errors. All single-qubit measurements are in the X basis. The value of X-type stabilizers is determined by combining the appropriate single-qubit measurement outcomes, so measurement errors directly translate to physical qubit errors. This means the protocol is fault-tolerant for errors in the X stabilizer measurements. Note, that we will always refer to stabilizers of the (3D) code rather than the stabilizers that are sometimes defined for the cluster state [64]. The fault-tolerance against X errors comes from the structure of the 3D code. The 3D toric code has the "single-shot property" for X errors [8, 23]. Single-shot error correction refers to an error-correcting code such that the code has a threshold in the presence of noisy measurements using only a single round of syndrome extraction. This resistance to measurement noise comes from redundancy in the stabilizer operators that are measured. In the 3D toric code, the A, B, and C codes all have redundancy built into the stabilizer generators we defined. The Z stabilizers surrounding the C volumes in the A and B codes and the A and B volumes in the C code multiply to the identity. This is a constraint on the valid syndrome measurement outcomes and is the source of the single-shot property.

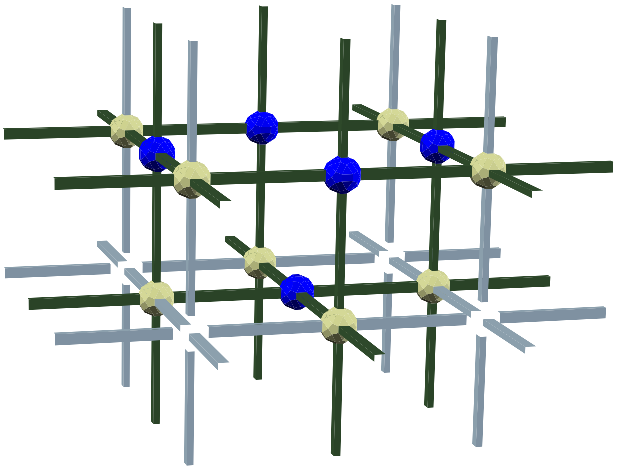


Figure 4.10: A part of the bulk of the fault-tolerant cluster state that realizes the C code in a measurement-based scheme is shown. Two times steps are shown, corresponding to the two horizontal levels. Time moves vertically. The links of the cluster state are in dark green. The edges in blue outline the primal lattice. Certain qubits are colored blue to indicate that these are ancillas in the 3D code, although in the cluster state there is no distinction between code qubits and ancillas.

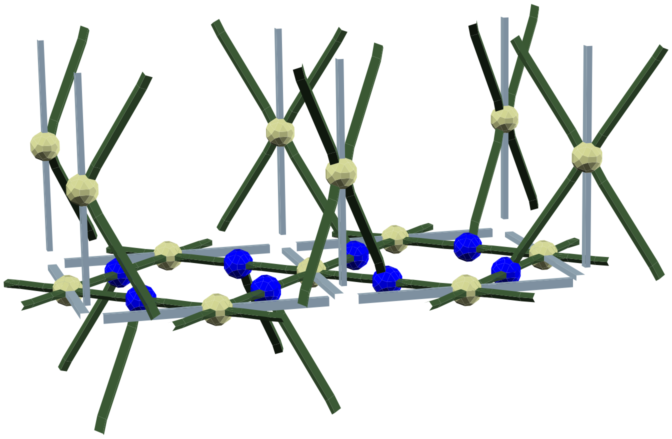


Figure 4.11: The bulk of the fault-tolerant cluster state for the A code is shown. The volume on the left is an A code X-type stabilizer. The Z stabilizers are three-body operators around the edges of the B code X-type stabilizers.

Preparation of the T magic state

Using the (2+1)-D version of our toric code on the tetrahedron, we can fault-tolerantly prepare a T magic state. Start with one qubit in the plus state for each of the three code copies. These qubits form the tip of the tetrahedron, opposite the base. Use the (2+1)-D protocol to apply the transversal T gate to the encoded plus state as we move towards the base. To prepare a T magic state, the protocol is nearly the same as the one we discussed in the previous section, except that here we additionally apply CCZ across corresponding code qubits in the three codes before measuring the qubits. Recall that the code qubits are the off-white balls in figures 4.12, 4.13, and 4.14. When the protocol reaches the base, T and T† gates are applied to each of the base qubits. The fault-tolerance of this protocol to prepare the T magic state depends on the ability to apply corrections based on the ancilla measurements at each time step. To apply a logical Pauli operator, the ancilla measurements could be saved and a correction could be applied at the end, but the logical T gate couples the codes such that errors will propagate. Therefore, it is necessary to compute corrections at every time step throughout the process. For this purpose, just-in-time decoding [10] is required.

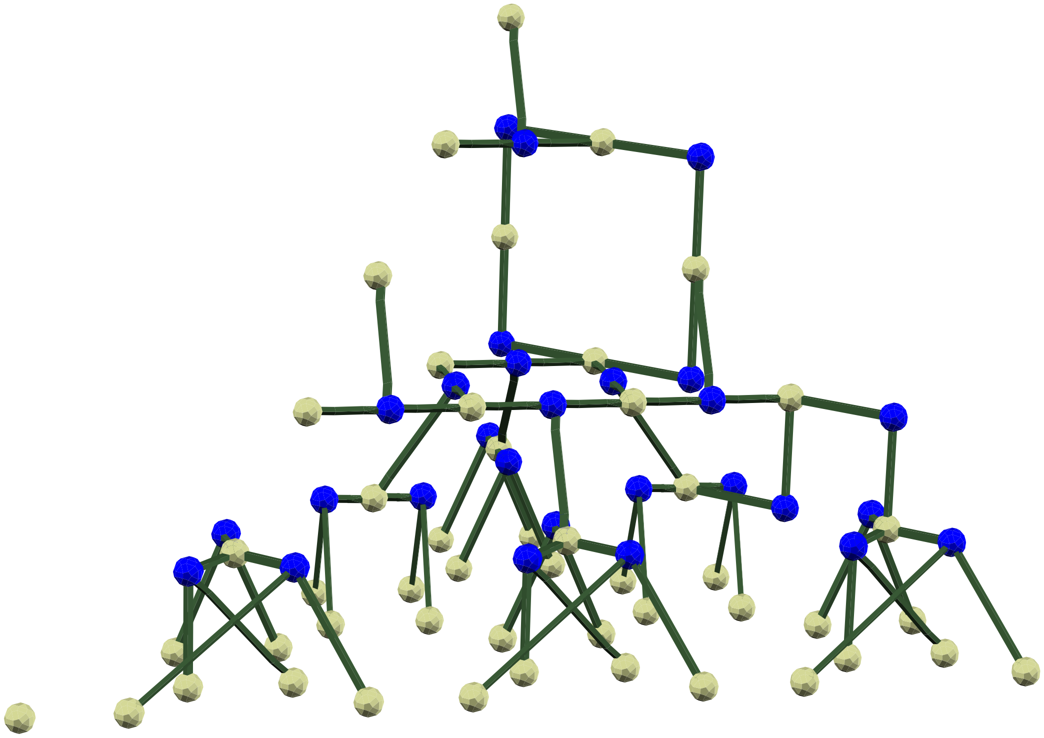


Figure 4.12: This is the fault-tolerant cluster state corresponding to the A code defined on the lattice in figure 4.6. Time moves downward, beginning with the single qubit at the top and ending with the 2D color code on the base.

Just-In-Time Decoding

The (2+1)-D protocol is equivalent to the 3D measurement-based protocol, except in (2+1)-D we are limited in that we can only apply corrections in the preset and future. This means that we are forced to decode the error that has occurred, including measurement errors, using only the partial information available from the past measurement. We do not yet have access to the future measurements. This limitation means that the just-in-time (JIT) decoding will never be as good as the 3D decoding. Nevertheless, Bombin [10] and Brown [20] were able to prove that JIT decoding will succeed if the error rate is small enough.

The JIT decoder saves a history of all measurement outcomes. At each time step, it will receive a new layer of measurement outcomes, and it will compute a correction to apply to qubits in the current layer. For our purposes JIT decoding has two steps: first, the decoder looks at the syndrome over all of the past and, armed with the new measurement outcomes in the present, it computes the most likely correction. Because of the new information, this correction might differ from the correction we applied in the past. In the present we apply a correction to correct the product of

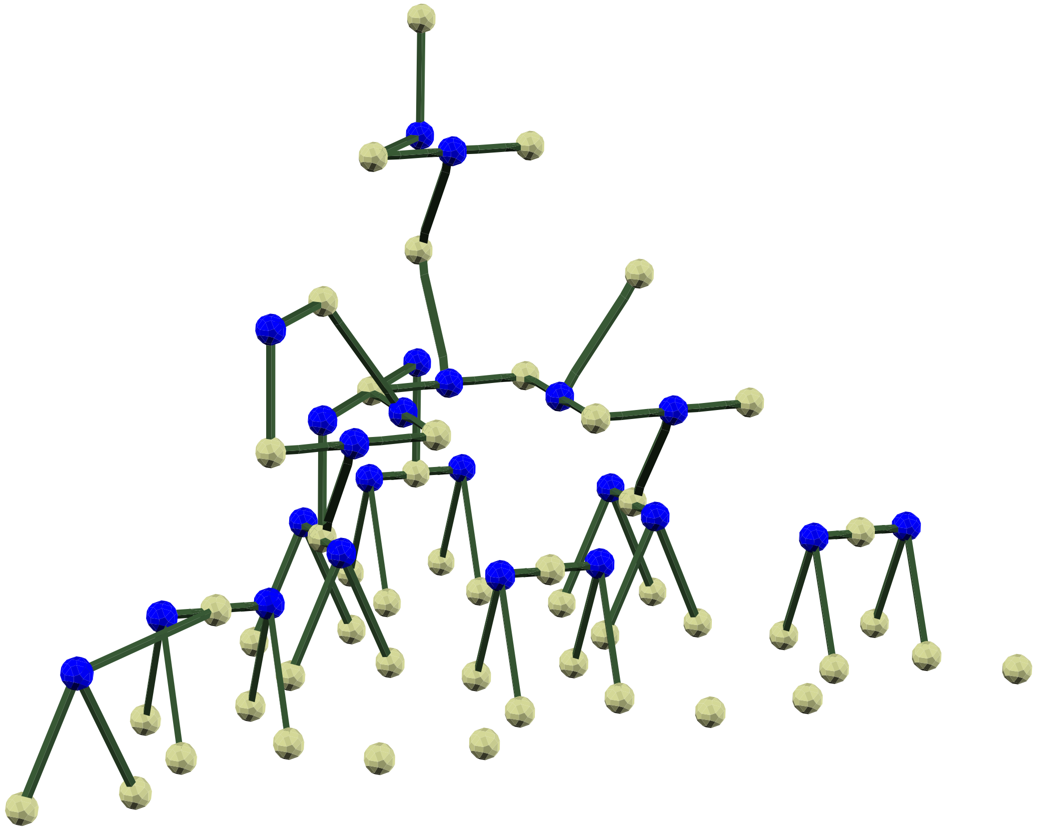


Figure 4.13: This is the fault-tolerant cluster state corresponding to the B code defined on the lattice in figure 4.6. Time moves downward, beginning with the single qubit at the top and ending with the 2D color code on the base.

the new syndrome prediction and the past corrections. The second step is to apply a correction to the syndrome defects in the present. The JIT decoder will choose to either pair the defects in the present or to propagate them into the future, whichever is lower weight.

These two rules mean that the JIT decoder will wait to pair two isolated defects distance ℓ apart until after ℓ time steps. Viewed in 3D with full knowledge of the syndrome, the most likely correction is the line connecting the two defects. JIT decoding has introduced an error supported on the surface bounded by a loop with side length ℓ.

The analysis of the errors spread by JIT decoding is carried out in [10] and [20]. Bombin proves that a just-in-time decoder based on minimal-weight decoding exhibits a fault-tolerant noise threshold for a class of topological codes and lattices that include our toric code on the 3D cubic lattice. Brown proves that a just-in-time decoder based on a renormalization group decoder similar to [15] has a fault-tolerant

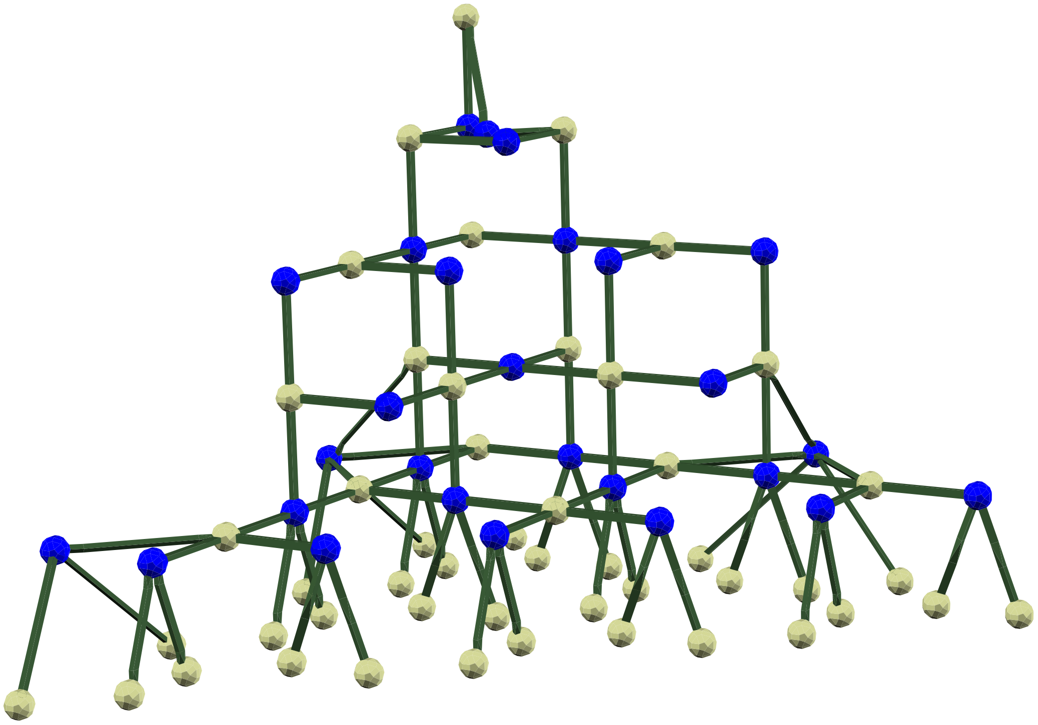


Figure 4.14: This is the fault-tolerant cluster state corresponding to the C code defined on the lattice in figure 4.6. Time moves downward, beginning with the single qubit at the top and ending with the 2D color code on the base.

noise threshold for the 3D toric code on a cubic lattice.

4.6 Conclusions

To perform universal quantum computation on a physical device will require families of error-correcting codes that support universal sets of fault-tolerant logical gates. Moreover, these codes will need to be easy to realize experimentally. They should have high fault-tolerant thresholds, low overhead, and low-weight local stabilizers. The toric codes in two or three dimensions are known to have high thresholds against local Pauli noise. The stabilizer generators are low-weight on the cubic lattice. These features, along with the simplicity of the model, make the toric code a leading candidate for fault-tolerant quantum information processing.

Past work has shown that a fault-tolerant CCZ gate can be realized in a special 3D toric code configuration [73]. It was later shown that this logical CCZ gate in the 3D code can be implemented as a protocol in time on a two dimensional lattice [20]. In this work we constructed a 3D toric code that features a fault-tolerant T gate. The T gate and CCZ gate are both in the third level of the Clifford hierarchy. The T gate

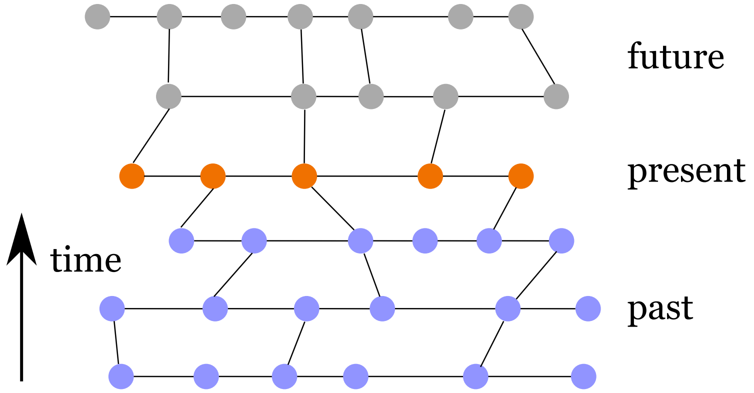


Figure 4.15: This cartoon depicts a (2+1)-D measurement-based protocol in progress. The orange layer represents the qubits that are active at the present time. The blue qubits have already been measured, and the gray qubits have not yet been initialized. The just-in-time decoding algorithm must predict the correction on the orange and blue qubits without access to any of the measurement outcomes on the gray qubits.

along with the Clifford group is perhaps the most commonly used universal gate set. We describe the 3D cubic lattice and the tetrahedral geometry that supports our code. The rectified lattice construction of [73] is used to define three different 3D toric codes. We construct the stabilizer version of our code by joining the three toric codes into one at the base of the tetrahedron and prove that the resulting code supports a fault-tolerant logical T gate (theorem 7) in addition to logical CZ gates supported on facets (Proposition 1).

We go on to define a subsystem code on the same lattice analogous to the subsystem color codes [7]. Our subsystem 3D toric code features a fault-tolerant Hadamard gate (Proposition 3). When the gauge is fixed so that the Z-type gauge generators are promoted to stabilizer generators, the original stabilizer code with fault-tolerant T gate is recovered. We proved that the gauge-fixing protocol is fault-tolerant (theorem 8), so that our 3D subsystem toric code supports a universal set of fault-tolerant logical gates. The 3D toric code-based scheme presented here offers a promising approach for universal fault tolerant quantum computation. We also described how our 3D stabilizer code with fault-tolerant T gate can be converted to a (2+1)-D protocol, in which a 2D lattice of qubits undergoes a measurement-based protocol and the time steps take the place of the third dimension of the original code. This type of protocol might be easier to realize because individually controlled 3D arrays of qubits tend to be more difficult to build and control than 2D arrays. The (2+1)-D operation of our toric code is also a promising direction for fault-tolerant quantum computation.

The code we presented here is also interesting from the perspective of defect boundaries in topological phases. In the 2D toric code, a type of defect line called a “twist defect” is intimately related to the 2D color codes. In this work a novel kind of defect exists on the base of the tetrahedron where the three copies of 3D toric code are joined. This defect can be thought of as arising from the unfolding of a 3D color code. Constructions like ours may be a path to studying or classifying defects in 3D topological phases.

BIBLIOGRAPHY

[1] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error. *Proc. 29th Ann. ACM Symnp. on Theory of Computing*, page 176, 1998.

[2] D. Aharonov, A. Kitaev, and J. Preskill. Fault-tolerant quantum computation with long-range correlated noise. *Physical Review Letters*, 96(5):050504, 2006.

[3] P. Aliferis, D. Gottesman, and J. Preskill. Quantum accuracy threshold for concatenated distance-3 codes. *Quant. Inf. Comp.*, 6:97–165, 2006. arXiv:quant-ph/0504218.

[4] J. T. Anderson, G. Duclos-Cianci, and D. Poulin. Fault-tolerant conversion between the steane and reed-muller quantum codes. *Physical review letters*, 113(8):080501, 2014.

[5] S. J. Beale, J. J. Wallman, M. Gutiérrez, K. R. Brown, and R. Laflamme. Quantum error correction decoheres noise. *Physical review letters*, 121(19): 190501, 2018.

[6] P. Benioff. The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines. *Journal of statistical physics*, 22(5):563–591, 1980.

[7] H. Bombín. Gauge color codes: optimal transversal gates and gauge fixing in topological stabilizer codes. *New Journal of Physics*, 17(8):083002, 2015.

[8] H. Bombín. Single-shot fault-tolerant quantum error correction. *Physical Review X*, 5(3):031043, 2015.

[9] H. Bombín. Dimensional jump in quantum error correction. *New Journal of Physics*, 18(4):043038, 2016.

[10] H. Bombín. 2d quantum computation with 3d topological codes. *arXiv preprint arXiv:1810.09571*, 2018.

[11] H. Bombín and M. A. Martin-Delgado. Topological quantum distillation. *Physical review letters*, 97(18):180501, 2006.

[12] S. Bravyi and A. Cross. Doubled color codes. *arXiv preprint arXiv:1509.03239*, 2015.

[13] S. Bravyi and J. Haah. Analytic and numerical demonstration of quantum self-correction in the 3d cubic code. december 2011. *arXiv preprint arXiv:1112.3252*, 2011.

[14] S. Bravyi and J. Haah. Magic-state distillation with low overhead. *Physical Review A*, 86(5):052329, 2012.

[15] S. Bravyi and J. Haah. Quantum self-correction in the 3d cubic code model. *Physical review letters*, 111(20):200501, 2013.

[16] S. Bravyi and A. Kitaev. Universal quantum computation with ideal clifford gates and noisy ancillas. *Physical Review A*, 71(2):022316, 2005.

[17] S. Bravyi and R. König. Classification of topologically protected gates for local stabilizer codes. *Physical review letters*, 110(17):170503, 2013.

[18] S. Bravyi, M. Suchara, and A. Vargo. Efficient algorithms for maximum likelihood decoding in the surface code. *Phys. Rev. A*, 90:032326, Sep 2014. doi:10.1103/PhysRevA.90.032326.

[19] S. Bravyi, M. Englbrecht, R. Koenig, and N. Peard. Correcting coherent errors with surface codes. *arXiv preprint arXiv:1710.02270*, 2017.

[20] B. J. Brown. A fault-tolerant non-clifford gate for the surface code in two dimensions. *arXiv preprint arXiv:1903.11634*, 2019.

[21] Z. Cai, X. Xu, and S. C. Benjamin. Mitigating coherent noise using pauli conjugation. *npj Quantum Inf*, 6(17), 2020. DOI:10.1038/s41534-019-0233-0.

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

[23] E. Campbell. A theory of single-shot error correction for adversarial noise. *Quantum Science and Technology*, 2019.

[24] E. T. Campbell, B. M. Terhal, and C. Vuillot. Roads towards fault-tolerant universal quantum computation. *Nature*, 549(7671):172–179, 2017.

[25] A. Carignan-Dugas, J. J. Wallman, and J. Emerson. Efficiently characterizing the total error in quantum circuits. *arXiv preprint arXiv:1610.05296*, 2016.

[26] C. Chamberland, J. Wallman, S. Beale, and R. Laflamme. Hard decoding algorithm for optimizing thresholds under general markovian noise. *Physical Review A*, 95(4):042332, 2017.

[27] C. Chamberland, P. Iyer, and D. Poulin. Fault-tolerant quantum computing in the pauli or clifford frame with slow error diagnostics. *Quantum*, 2:43, 2018.

[28] D. M. Debroy, M. Li, M. Newman, and K. R. Brown. Stabilizer slicing: Coherent error cancellations in low-density parity-check stabilizer codes. *Physical review letters*, 121(25):250502, 2018.

[29] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill. Topological quantum memory. *Journal of Mathematical Physics*, 43(9):4452–4505, 2002.

[30] G. Duclos-Cianci and D. Poulin. Fast decoders for topological quantum codes. *Phys. Rev. Lett.*, 104:050504, 2010. DOI:10.1103/PhysRevLett.104.050504.

[31] B. Eastin and E. Knill. Restrictions on transversal encoded quantum gate sets. *Physical review letters*, 102(11):110502, 2009.

[32] J. Edmonds. Paths, trees, and flowers. *Canadian Journal of mathematics*, 17: 449–467, 1965.

[33] J. Emerson, R. Alicki, and K. Życzkowski. Scalable noise estimation with random unitary operators. *J. Opt. B: Quantum Semiclass. Opt.*, 7(10):S347–S352, 2005. doi:10.1088/1464-4266/7/10/021.

[34] J. Fern, J. Kempe, S. N. Simic, and S. Sastry. Generalized performance of concatenated quantum codes—a dynamical systems approach. *IEEE transactions on automatic control*, 51(3):448–459, 2006.

[35] R. P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6/7), 1982.

[36] D. Gottesman. Stabilizer codes and quantum error correction. *Caltech Ph.D. thesis*, 1997. arXiv:quan-ph/9705052.

[37] D. Greenbaum and Z. Dutton. Modeling coherent errors in quantum error correction. *Quantum Science and Technology*, 3(1):015007, 2017.

[38] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79:325–328, Jul 1997.

[39] M. Gutiérrez, C. Smith, L. Lulushi, S. Janardan, and K. R. Brown. Errors and pseudothresholds for incoherent and coherent noise. *Phys. Rev. A*, 94:042338, 2016.

[40] A. J. Guttmann. On two-dimensional self -avoiding random walks. *J. Phys. A*, 17:455–468, 1984. DOI: 10.1088/0305-4470/17/2/030.

[41] A. J. Guttmann and A. R. Conway. Square lattice self-avoiding walks and polygons. *Annals of Combinatorics*, 5:319–345, 2001.

[42] J. Haah, M. B. Hastings, D. Poulin, and D. Wecker. Magic state distillation with low space overhead and optimal asymptotic input count. *Quantum*, 1:31, 2017.

[43] J. M. Hammersley. The number of polygons on a lattice. *Mathematical Proceedings of the Cambridge Philosophical Society*, 57:516–523, 1960. doi:10.1017/S030500410003557X.

[44] E. Huang, A. C. Doherty, and S. Flammia. Performance of quantum error correction with coherent errors. *arXiv preprint arXiv:1805.08227*, 2018.

[45] P. S. Iyer and D. Poulin. A small quantum computer is needed to optimize fault-tolerant protocols. *Quant. Science and Tech.*, 3(3):030504, 2018. arXiv:1711.04736v1.

[46] T. Jochym-O'Connor and S. D. Bartlett. Stacked codes: universal fault-tolerant quantum computation in a two-dimensional layout. *Physical Review A*, 93(2): 022323, 2016.

[47] T. Jochym-O'Connor and R. Laflamme. Using concatenated quantum codes for universal fault-tolerant quantum gates. *Physical review letters*, 112(1): 010505, 2014.

[48] T. Jochym-O'Connor, A. Kubica, and T. J. Yoder. Disjointness of stabilizer codes and limitations on fault-tolerant logical gates. *Physical Review X*, 8(2): 021047, 2018.

[49] A. Kitaev, A. Shen, M. N. Vyalyi, and M. N. Vyalyi. *Classical and quantum computation*, volume 47. American Mathematical Soc., 2002.

[50] A. Y. Kitaev. Quantum computations: algorithms and error correction. *Russian Math. Surveys*, 52:1191–1249, 1997.

[51] E. Knill and R. Laflamme. Theory of quantum error-correcting codes. *Physical Review A*, 55(2):900, 1997.

[52] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation: error models and thresholds. *Proc. Roy. Soc. London*, Ser. A 454:365, 1998. arXiv:quan-ph/9702058.

[53] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J Wineland. Randomized benchmarking of quantum gates. *Physical Review A*, 77(1):012307, 2008. doi:10.1103/PhysRevA.77.012307.

[54] A. Kubica, B. Yoshida, and F. Pastawski. Unfolding the color code. *New Journal of Physics*, 17(8):083026, 2015.

[55] A. Kubica, M. E. Beverland, F. Brandao, J. Preskill, and K. M. Svore. Three-dimensional color code thresholds via statistical-mechanical mapping. *Physical review letters*, 120(18):180501, 2018.

[56] R. Kueng, D. M. Long, A. C. Doherty, and S. T. Flammia. Comparing experiments to the fault-tolerance threshold. *Physical review letters*, 117(17): 170502, 2016.

[57] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek. Perfect quantum error correcting code. *Physical Review Letters*, 77(1):198, 1996.

[58] Y. Manin. Computable and uncomputable. *Sovetskoye Radio, Moscow*, 128, 1980.

[59] A. M. Meier, B. Eastin, and E. Knill. Magic-state distillation with the four-qubit code. *arXiv preprint arXiv:1204.4221*, 2012.

[60] J. Napp and J. Preskill. Optimal bacon-shor codes. *Quantum Information and Computation*, 13(5&6):0490–0510, 2013.

[61] D. Poulin. Optimal and efficient decoding of concatenated quantum block codes. *Physical Review A*, 74(5):052333, 2006.

[62] J. Preskill. Sufficient condition on noise correlations for scalable quantum computing. *Quantum Information & Computation*, 13(3-4):181–194, 2013.

[63] B. Rahn, A. C. Doherty, and H. Mabuchi. Exact performance of concatenated quantum codes. *Physical Review A*, 66(3):032304, 2002.

[64] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188, 2001.

[65] R. Raussendorf, D. E. Browne, and H. J. Briegel. Measurement-based quantum computation on cluster states. *Physical review A*, 68(2):022312, 2003.

[66] R. Raussendorf, S. Bravyi, and J. Harrington. Long-range quantum entanglement in noisy cluster states. *Physical Review A*, 71(6):062313, 2005.

[67] R. Raussendorf, J. Harrington, and K. Goyal. Topological fault-tolerance in cluster state quantum computation. *New J. Phys.*, 9:199, 2007.

[68] Y. R. Sanders, J. J. Wallman, and B. C. Sanders. Bounding quantum gate error rate based on reported average fidelity. *New Journal of Physics*, 18(1):012002, 2015.

[69] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.*, 41(2):303–332, 1999.

[70] L. J. Slater. *Generalized hypergeometric functions*. Cambridge University Press, 1966.

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

[72] Y. Suzuki, K. Fujii, and M. Koashi. Efficient simulation of quantum error correction under coherent error based on non-unitary free-fermionic formalism. *Physical Review Letters*, 119(19):190503, 2017.

[73] M. Vasmer and D. E. Browne. Three-dimensional surface codes: Transversal gates and fault-tolerant architectures. *Physical Review A*, 100(1):012312, 2019.

[74] J. Wallman, C. Granade, R. Harper, and S. T. Flammia. Estimating the coherence of noise. *New Journal of Physics*, 17(11):113020, 2015.

[75] J. J. Wallman and J. Emerson. Noise tailoring for scalable quantum computation via randomized compiling. *Physical Review A*, 94(5):052325, 2016.

[76] J. J. Wallman and S. T. Flammia. Randomized benchmarking with confidence. *New Journal of Physics*, 16(10):103032, 2014.

[77] T. J. Yoder, R. Takagi, and I. L. Chuang. Universal fault-tolerant gates on concatenated stabilizer codes. *Physical Review X*, 6(3):031039, 2016.

Appendix A

CHI MATRIX AND PAULI TRANSFER MATRIX FOR QUBITS

Here we verify Lemma 1 for qubits by expressing all non-diagonal terms in N_{kl} in terms of χ_{ij} explicitly:

$$\begin{aligned}
I \mapsto\ & (\chi_{XI}+\chi_{IX})\,X+(\chi_{YI}+\chi_{IY})\,Y+(\chi_{ZI}+\chi_{IZ})\,Z\\
&+(\chi_{XY}-\chi_{YX})\,(iZ)+(\chi_{ZX}-\chi_{XZ})\,(iY)+(\chi_{YZ}-\chi_{ZY})\,(iX),\\[2ex]
X \mapsto\ & (\chi_{XY}+\chi_{YX})\,Y+(\chi_{XZ}+\chi_{ZX})\,Z+(\chi_{IX}+\chi_{XI})\,I\\
&+(\chi_{ZY}-\chi_{YZ})\,(iI)+(\chi_{IY}-\chi_{YI})\,(iZ)+(\chi_{ZI}-\chi_{IZ})\,(iY),\\[2ex]
Y \mapsto\ & (\chi_{XY}+\chi_{YX})\,X+(\chi_{ZY}+\chi_{YZ})\,Z+(\chi_{IY}+\chi_{YI})\,I\\
&+(\chi_{ZX}-\chi_{XY})\,(iI)+(\chi_{IZ}-\chi_{ZI})\,(iX)+(\chi_{XI}-\chi_{IX})\,(iZ),\\[2ex]
Z \mapsto\ & (\chi_{ZY}+\chi_{YZ})\,Y+(\chi_{XZ}+\chi_{ZX})\,X+(\chi_{IZ}+\chi_{ZI})\,I\\
&+(\chi_{YX}-\chi_{XY})\,(iI)+(\chi_{IX}-\chi_{XI})\,(iY)+(\chi_{YI}-\chi_{IY})\,(iX).
\end{aligned} \tag{A.1}$$

When we collect all the terms in $\sum_{a\neq b} N_{ab}^2$ which are quadratic in $\{\chi_{XY},\chi_{YX}\}$, we obtain

$$2\,(\chi_{XY}+\chi_{YX})^2-2\,(\chi_{XY}-\chi_{YX})^2=8|\chi_{XY}|^2=4\left(|\chi_{XY}|^2+|\chi_{YX}|^2\right), \tag{A.2}$$

using $\chi_{ij}=\chi_{ji}^*$, as required by complete positivity. The same applies to the terms involving $\chi_{IX},\chi_{IY},\chi_{IZ},\chi_{ZX},\chi_{YZ}$, and their complex conjugates.

To prove the claim we must verify that the linear terms cancel. This can be shown using the general argument in Lemma 1, but in the qubit case it may be easier to verify the cancellation explicitly. For example, the contributions to N_{ab} involving

$\chi_{IX}, \chi_{XI}, \chi_{YZ}, \chi_{ZY}$ are

$$\begin{aligned} N_{IX} &= (\chi_{XI} + \chi_{IX}) + i\,(\chi_{YZ} - \chi_{ZY}) + \cdots\,, \\ N_{XI} &= (\chi_{XI} + \chi_{IX}) - i\,(\chi_{YZ} - \chi_{ZY}) + \cdots\,, \\ N_{YZ} &= (\chi_{ZY} + \chi_{YZ}) + i\,(\chi_{XI} - \chi_{IX}) + \cdots\,, \\ N_{ZY} &= (\chi_{ZY} + \chi_{YZ}) - i\,(\chi_{XI} - \chi_{IX}) + \cdots\,, \end{aligned} \tag{A.3}$$

and we therefore see that the cross terms cancel in $N_{IX}^2 + N_{XI}^2$ and in $N_{YZ}^2 + N_{ZY}^2$. Similar cancellations occur for all other cross terms.

Appendix B

APPROXIMATING SUMS

We wish to evaluate the sum in equation (2.86):

$$P_n(p) = \sum_{w=0}^{(n-1)/2} \binom{n}{w} p^{n-w}\,(1-p)^w = \sum_{w=(n+1)/2}^{n} \binom{n}{w} p^w (1-p)^{n-w}, \tag{B.1}$$

where $p = s^2 = \sin^2\theta/2$, and $(1-p) = c^2 = \cos^2\theta/2$. Note that $P_n(p)$ is the probability of a decoding error for the n-bit repetition code subject to independent noise with bit-flip probability p. It is convenient to redefine the summation index obtaining

$$P_n(p) = p^{(n+1)/2}(1-p)^{(n-1)/2} \sum_{r=0}^{(n-1)/2} \binom{n}{\frac{n+1}{2}+r} \left(\frac{p}{1-p}\right)^r. \tag{B.2}$$

From the Stirling approximation, we have

$$\binom{n}{\frac{n+1}{2}+r} \approx \left(\sqrt{\frac{2}{\pi n}}\right) 2^n \exp\left(-\frac{2}{n}\left(r+\frac{1}{2}\right)^2\right), \tag{B.3}$$

neglecting a multiplicative $(1+O(1/n))$ correction. Making another $(1+O(1/n))$ multiplicative error, we may replace the exponential inside the sum over r by 1, obtaining

$$P_n(x) \approx p^{(n+1)/2}(1-p)^{(n-1)/2} \left(\sqrt{\frac{2}{\pi n}}\right) 2^n \sum_{r=0}^{(n-1)/2} \left(\frac{p}{1-p}\right)^r, \tag{B.4}$$

and we also make a negligible error (assuming $p < \frac{1}{2}$) by extending the upper limit on the sum to infinity, finding

$$\sum_{r=0}^{\infty} \left(\frac{p}{1-p}\right)^r = \frac{1-p}{1-2p}. \tag{B.5}$$

We conclude that

$$P_n(x) = \left(\sqrt{\frac{2}{\pi n}}\right) \left(\frac{\sqrt{p(1-p)}}{1-2p}\right) [4p(1-p)]^{n/2} \left(1 + O\left(\frac{1}{n}\right)\right), \tag{B.6}$$

assuming $p < \frac{1}{2}$. Using

$$4p(1-p) = (2sc)^2 = \sin^2\theta, \quad 1-2p = c^2 - s^2 = \cos\theta, \tag{B.7}$$

we find

$$P_n(x) = \frac{1}{\sqrt{2\pi n}} \left(\frac{\sin^{n+1}\theta}{\cos\theta} \right) \left(1 + O\left(\frac{1}{n} \right) \right), \quad \text{for} \quad \sin^2\theta/2 < 1/2. \tag{B.8}$$

Appendix C

CORRELATED NOISE: LEADING BEHAVIOR FOR LARGE n

Here we'll describe an alternative way of understanding equation (2.164), where the coefficient of h_2^q in the logical channel is $O(m^{3q/2})$. This leading behavior results from cancellations of higher order terms in m that occur when we perform the sum over k_R in equation (2.161). What is the explanation for these cancellations?

In Section 2.5 we calculated the coherent and incoherent logical components for the bit-flip code of size n subject to correlated unitary rotations given by a Hamiltonian of the form:

$$H = \sum_i h_1 X_i + \sum_{j,k|j\neq k} h_2 X_j X_k. \tag{C.1}$$

We expressed the logical coherent component $\tilde{\chi}_{XI}$ and the logical incoherent component $\tilde{\chi}_{XX}$ in terms of functions Ω and Δ such that

$$\begin{aligned}\tilde{\chi}_{XI}(q) &= \sum_{k_R=0}^{q} \Omega(q-k_R, k_R) h_2^q h_1^{n-2q},\\ \tilde{\chi}_{XX}(q) &= \sum_{k_R=0}^{q} \Delta(q-k_R, k_R) h_2^q h_1^{n+1-2q} + O(h_2^q h_1^{n+3-2q}),\end{aligned} \tag{C.2}$$

where

$$\tilde{\chi}_{XI} = \sum_{q=0}^{(n-1)/2} \tilde{\chi}_{XI}(q), \quad \tilde{\chi}_{XX} = \sum_{q=0}^{(n+1)/2} \tilde{\chi}_{XX}(q), \tag{C.3}$$

and only even values of q contribute. Here k_R is the number of times the Hamiltonian term ih_2XX acts on the density operator from the right, and $k_L = q - k_R$ is the number of times $-ih_2XX$ acts from the left.

We were able to compute Ω and Δ by counting the ways of decomposing each physical noise term into combinations of one- and two-body Hamiltonian terms. Repeating equations (2.149) and (2.152), we found

$$\begin{aligned}\Omega(q-k_R, k_R) = &\frac{(i)^{n-q}(-1)^m(m+1)}{(n-2q)2^q}\binom{n}{m}\\ &\times(-1)^{k_R}\frac{(m!)^2}{k_R!(q-k_R)!(m-2k_R)!(m-2q+2k_R)!},\end{aligned} \tag{C.4}$$

and

$$\Delta(q-k_R,k_R) = \frac{(i)^q}{2^q}\binom{n}{m} \\ \times(-1)^{k_R}\frac{((m+1)!)^2}{(m+1-2q+2k_R)!(m+1-2k_R)!k_R!(q-k_R)!}. \tag{C.5}$$

Let's evaluate the sum over k_R to leading order in $1/m$ in both equation (C.4) and (C.5). We focus on the second factor in each equation, which contains all of the k_R dependence. In equation (C.4) this factor is

$$(-1)^{k_R}\frac{(m)(m-1)\dots(m-2k_R+1)\times(m)(m-1)\dots(m-2q+2k_R+1)}{(k_R)!(q-k_R)!}. \tag{C.6}$$

The dominant term for m large is given by

$$(-1)^{k_R}\frac{(m)^{2q}}{(k_R)!(q-k_R)!} = (-1)^{k_R}\frac{(m)^{2q}}{q!}\times\binom{q}{k_R}. \tag{C.7}$$

Then when we sum over k_R, we have

$$\frac{(m)^{2q}}{q!}\sum_{k_R=0}^{q}(-1)^{k_R}\binom{q}{k_R} = 0, \tag{C.8}$$

where we have made use of the identity

$$\sum_{b=0}^{a}P_c(b)(-1)^b\binom{a}{b} = 0 \quad \forall c < a. \tag{C.9}$$

Here $P_c(b)$ denotes any polynomial in b of degree $c < a$. The situation for Δ is the same except that m is replaced by $m+1$. Therefore, the leading term for m large in equations (C.4) and (C.5) vanishes.

Similar cancellations occur for higher-order corrections which are suppressed by powers in $1/m$. These corrections are computed by expanding the numerator, equation (C.6), as a $2q$th order polynomial in m. For example, the coefficient of m^{2q-1} is

$$(-1)^{k_R}(-1)\frac{2q^2-4qk_R+q+4k_R^2}{q!}\binom{q}{k_R}, \tag{C.10}$$

in which the prefactor multiplying $\binom{q}{k_R}$ is a second-degree polynomial in k_R, so that equation (C.9) implies that the sum over k_R vanishes if $q > 2$. Likewise, the coefficient of m^{2q-r} is a polynomial in k_R of degree of $2r$, and the sum over

k_R vanishes if $2r < q$. Recalling that only even q contribute, we see that the leading term that survives the summation over k_R has $r = q/2$ and is therefore order $m^{2q-r} = m^{3q/2}$. We have now seen why terms higher order in m cancel. The term of order $m^{3q/2}$ can be evaluated using the identity

$$\sum_{b=0}^{a} (-1)^b b^a \binom{a}{b} = (-1)^a a!. \tag{C.11}$$

The identities in equations (C.9) and (C.11) can be derived by performing the binomial expansion of $(1 + x)^a$, differentiating repeatedly, and then setting $x = -1$.

Appendix D

THE SHAPE OF THE LOGICAL STRING

In this appendix, we prove that among short logical strings nearly all have typical shape as in Definition 6.

Lemma 9. *In a size L toric code, all but order $1/L$ of the logical strings running left to right across the code with length $\leq L+2\zeta$ consist of single steps up and down, so that no vertical segment is longer than one qubit.*

Proof. If the size of the code is L and we consider all length $L+2\zeta$ logical strings for fixed ζ, we will count the number of strings that satisfy the condition that each step up or down is only length one. First, we start with a horizontal logical string of length L and then pick ζ sites along it. We have ζ upward steps and ζ downward steps, and we need to fix an ordering. Alternatively, we could think of choosing ζ sites for the upward steps and another ζ sites for the downward steps. In total the number of strings of this type is

$$\text{number of strings with steps of one} = \binom{L}{2\zeta}\binom{2\zeta}{\zeta} = \binom{L}{\zeta}\binom{L-\zeta}{\zeta}. \tag{D.1}$$

The L dependence in equation (D.1) is

$$\frac{L!}{(L-2\zeta)!}. \tag{D.2}$$

Next we will count the total number of strings that consist of no backwards steps, that is starting from the left of the code block the strings move only right, up, and down. These strings potentially contain upward and downward steps of more than one. In general, such a string involves q_1 distinct steps up with ζ total length and q_2 steps down also totaling ζ in length. The number of ways of writing ζ as a sum of q_1 terms, not ignoring order, is given by the number of compositions of the integer ζ into q_1 terms, which is $\binom{\zeta-1}{q_1-1}$. Each of the q_1 steps up and q_2 steps down can be placed independently. This gives us $\binom{L}{q_1}\binom{L-q_1}{q2}$ combinations of possible configurations. In total we have

$$\binom{\zeta-1}{q_1-1}\binom{L}{q_1}\binom{\zeta-1}{q_2-1}\binom{L-q_1}{q_2} \tag{D.3}$$

such strings. When $q_1 = q_2 = \zeta$, we recover the case where each step up or down is by one lattice site. Then we can isolate the L dependence in equation (D.3):

$$\frac{L!}{(L - q_1 - q_2)!}. \tag{D.4}$$

We can compare this to equation (D.2), and we see that there are fewer paths with steps larger than one. The ratio is proportional to

$$\frac{\text{number with } q_1 \text{ steps up and } q_2 \text{ steps down}}{\text{number with } \zeta \text{ single steps up and down}} = O(L^{q_1+q_2-2\zeta}). \tag{D.5}$$

Then if we count the paths with a single step of two and the other steps are all one, there are order $1/L$ of these relative to the number of paths with single steps up and down.

We must also count the number of logical strings where the string backtracks on itself. There are even fewer of these than the strings with jumps up or down by two. Each string with backtracking can be produced from a string with a jump up or down of at least two lattice spacings. We add some additional cap onto the vertical segment of at least length 2. The number of strings with one instance of backtracking like figure D.1 will be proportional to the number of strings of length two shorter that also have at least one step up or down of more than one. For this reason, strings like the one in figure D.1 are an exponentially smaller minority than the strings with steps up and down of more than one. Then we conclude that nearly all short logical strings spanning the code left to right consist of steps up and down by only one qubit.

□

Lemma 10. *For the class of length $L + 2\zeta$ strings described in Lemma 9 (those with exactly ζ steps up and ζ steps down as they span the code block from left to right), for large L nearly all will have spacings between the steps growing proportional to $\sqrt{L}$. We choose a small constant γ and define typical strings as those for which all vertical steps are separated by at least $\gamma\sqrt{L}$. If we fix the length of logical strings and combine this lemma with Lemma 9, we can make the following statement about the fraction of strings of that length that have atypical shape:*

$$\frac{\textit{Number of strings with atypical shape}}{\textit{Total number of strings}} = \frac{8\gamma\zeta^2}{\sqrt{L}} + O\left(\frac{1}{L}\right). \tag{D.6}$$

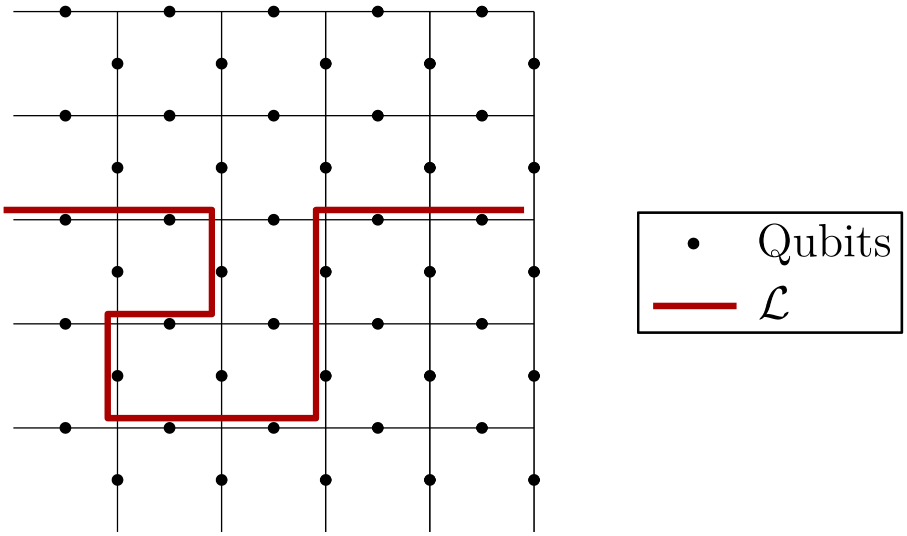


Figure D.1: The logical string $\mathcal{L}$ has backtracking. Among short logical strings, those with backtracking are unlikely relative to strings without.

Proof. The total number of strings of the type in Lemma 9 is $\binom{L}{2\zeta}\binom{2\zeta}{\zeta}$. Now let us compute the number of strings such that each step up or down is separated from others by $\gamma\sqrt{L}$ for some constant γ. We can lower bound the number by starting with a length L string running left to right across the code and placing our steps up and down. We suppose that each step we place prohibits placing another step on a further $2\gamma\sqrt{L}$ of the sites. This is a lower bound because in the true answer these intervals will sometimes overlap. The lower bound is

$$\frac{L\left(L-(2\gamma\sqrt{L}+1)\right)\left(L-2(2\gamma\sqrt{L}+1)\right)\cdots\left(L-(2\zeta-1)(2\gamma\sqrt{L}+1)\right)}{(2\zeta)!}\binom{2\zeta}{\zeta}. \tag{D.7}$$

Compared to the total, $n-i$ has been replaced by $n-i(2\gamma+1)$ for each i, so that when $\gamma=0$, we recover the total number of strings. In general, the ratio of this limited set to the total for fixed ζ and γ is given by

$$\frac{\text{number of length } L+2\zeta \text{ strings with widely separated steps}}{\text{number of length } L+2\zeta \text{ strings}} \approx \prod_{i=1}^{2\zeta-1}\left(1-\frac{2i\gamma}{\sqrt{L}}\right). \tag{D.8}$$

We can lower bound this by

$$>\left(1-\frac{4\zeta\gamma}{\sqrt{L}}\right)^{2\zeta} = 1-\frac{8\gamma\zeta^2}{\sqrt{L}}+O\left(\frac{1}{L}\right). \tag{D.9}$$

This approaches 1 as L increases, and we see that with high probability a short logical string will have the property that the steps up and down are separated by more than $\gamma\sqrt{L}$, as L becomes large.

□

Appendix E

DISCONNECTED ERRORS

Fix a coherent logical noise component and consider the sum in equation (3.7). In Section 3.6 we argued that the disconnected term is 1 for disconnected errors that do not change how a given connected term is decoded. This allows us to write the sum as

$$\tilde{\chi}_{Z_1,I} = \left(\sum_{\mathcal{L}} \sum_{p \in \mathcal{P}(s)} \text{Connected part} \right) + \text{Error}. \tag{E.1}$$

The sum over $\mathcal{L}$ includes all typical short connected logical strings. $\mathcal{P}(\mathcal{L})$ is the set of likely partitions of connected logical string $\mathcal{L}$. This excludes the partitions we called "exceptional terms" in Definition 7 and Lemma 4. "Error" contains all the terms we have neglected. This includes the contribution of long logical strings, short logical strings with atypical shape, and exceptional terms. It also includes the terms with disconnected pieces that we did not consider in Section 3.6. These are all of the terms where the disconnected errors flip the way the partition is decoded, where we start with a partition and after adding disconnected errors to each side, the error that was originally uncorrectable becomes correctable and vice versa. These terms will not follow the analysis we did in Section 3.6. We will describe these terms now and show that they are negligible in the following lemma.

Lemma 11. *In equation (E.1) the error from the neglected terms $\mathcal{E}$ can be expressed*

$$\mathit{Error} = \mathcal{E}_1 + \mathcal{E}_2, \tag{E.2}$$

where $\mathcal{E}_1$ contains the contributions that we have already proven are negligible—long connected logical strings, logical strings with an atypical shape, and exceptional partitions. $\mathcal{E}_2$ contains the contributions from terms where the disconnected errors have flipped the way the partition is decoded. These are the terms we neglected in Section 3.6. The following is true:

$$|\mathcal{E}_2| \leq |\mathcal{E}_1|. \tag{E.3}$$

Proof. We start with a typical short connected logical string and take a partition into a correctable operator and an uncorrectable operator, denoted $(O_U \rho\, O_C)$. Now we add disconnected errors, D_L and D_R to the left and right side of the partition. In some cases the uncorrectable error may become correctable and vice versa. That is, $O_U D_L$ will be correctable, while $O_C D_R$ is uncorrectable. For example, the term that contributes to the $\tilde{\chi}_{Z_1 I}$ component of the logical noise might be $(O_C D_R \rho \, O_U D_L)$. Our treatment of the disconnected part in Section 3.6 assumed that the added errors did not flip the correctable and uncorrectable sides of the original partition. Now we will justify this assumption by proving that such terms are negligible.

First, we must understand the conditions when an added error will turn the uncorrectable side of a partition into a correctable error. O_U is the uncorrectable side of the partition, so the minimal-weight correction to O_U is equal to O_C up to stabilizers. For $O_U D_L$ to be correctable, the minimal-weight correction must equal $O_U D_L$ up to stabilizers and not equal $O_C D_L$ up to stabilizers. Note that we write D_L and not D_R because D_L and D_R have the same syndrome, so as far as the decoder is concerned, they are equivalent. This implies

$$\min_{G_x \in \mathcal{S}} |G_x O_U D_L| < \min_{G_x \in \mathcal{S}} |G_x O_C D_L|, \tag{E.4}$$

where G_x is an element of $\mathcal{S}$, which denotes the stabilizer group, and $|\cdot|$ denotes the weight of a Pauli operator. The weight of the minimal-weight operator equivalent up to stabilizers to $O_C D_L$ is no greater than the sum of the weights of the minimal-weight operators equivalent up to stabilizers to O_C and D_L individually. We can continue:

$$\begin{aligned} \min_{G_x \in \mathcal{S}} |G_x O_U D_L| < \min_{G_x \in \mathcal{S}} |G_x O_C D_L| &\leq \min_{G_x \in \mathcal{S}} |G_x O_C| + \min_{G_y \in \mathcal{S}} |G_y D_L| \\ &< \min_{G_x \in \mathcal{S}} |G_x O_U| + \min_{G_y \in \mathcal{S}} |G_y D_L|. \end{aligned} \tag{E.5}$$

We conclude that the added error must be such that the minimal-weight correction of $O_U D_L$ is less than the minimal-weight correction of O_U plus the minimal-weight correction of D_L. This happens when the disconnected error D_L lies near O_U such that the minimal-weight decoder will tend to form a loop out of parts of D_L and O_U. This is possible only in cases like the one in figure E.1.

The condition in equation (E.5) requires a special combination of disconnected error and original partition. This is possible for both coherent- and incoherent-type disconnected errors as defined in Section 3.6. Let us consider incoherent-type disconnected errors first. This is what is illustrated in figure E.1. The disconnected error causes the uncorrectable side of the partition to become correctable when D_L

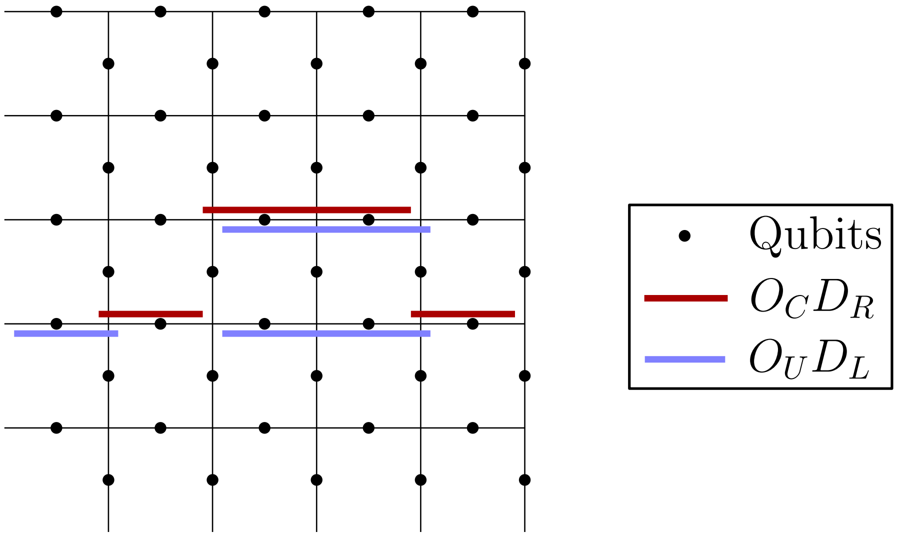


Figure E.1: This figure shows a partition of a connected logical string together with a disconnected error. The disconnected error is incoherent-type, so $D_L = D_R$. The uncorrectable error $O_C D_R$ is in red, while the correctable error $O_U D_L$ is in blue. The two form a length-5 connected logical string that runs left to right across the code. Without the disconnected errors, O_C would be correctable and O_U, uncorrectable. Therefore, the added disconnected errors have flipped the original partition.

contains at least two errors in a row adjacent to O_U. Based on our condition, we observe that the number of added errors that flip the partition is greatest for the lowest-weight partitions. These terms require the fewest added errors to flip. We also see that the number of these added errors increases with the length of the logical string. A longer string has more adjacent qubits. This implies that the value of the disconnected part is decreasing with string length. This fact was used in Lemma 3.

We seek to prove that terms like the one in figure E.1 are negligible in the coherent logical noise components. We will do this by mapping each combination of a partition of a connected logical string and a set of disconnected errors such that uncorrectable and correctable errors in the partition are flipped to a partition of a longer connected logical string. There exists a unique stabilizer operator that will multiply the starting partition plus disconnected errors and produce a partition of a longer logical string. This is illustrated in figure E.2. Our condition in equation (E.5) says that the minimum stabilizer-equivalent operator to O_U is lower weight than O_U. The stabilizer operator we need to map figure E.1 to figure E.2 is the product of $O_U D_L$ and its minimal-weight correction. The resulting connected logical string is longer than the original connected logical string, but the total weight of the noise term (connected and disconnected) is smaller. This must be true because we have

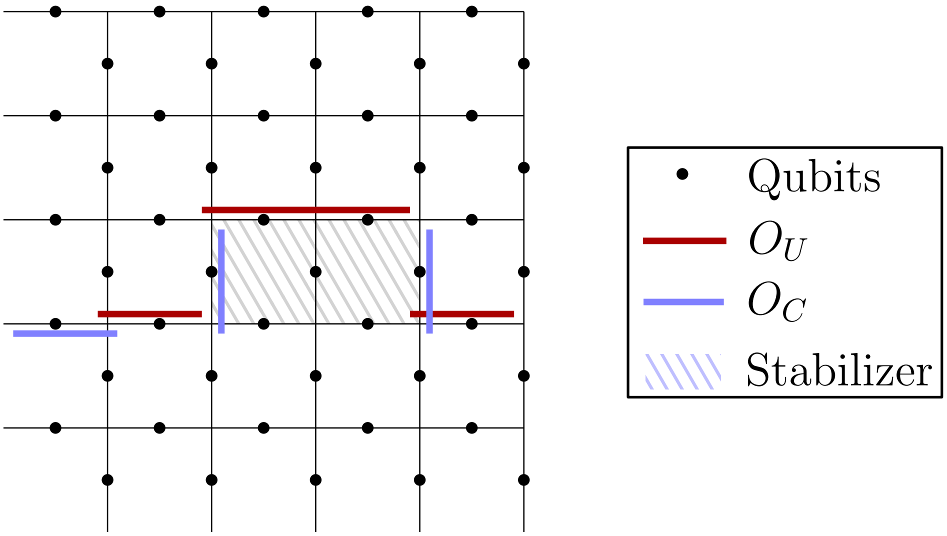


Figure E.2: Here is the partition of a connected logical string corresponding to figure E.1, with the new uncorrectable error O_U in red and the new correctable error O_C in blue. This term shares the same syndrome as the one in figure E.1. We can always multiply right or left hand sides by a stabilizer to produce different coherent terms. This term is produced from figure E.1 by multiplying the correctable side in blue by the stabilizer operator in gray crosshatching. Notice that the connected logical string is longer, but the total weight of the term is smaller.

lowered the weight of the errors in blue ($O_U D_L$), and we have not changed the weight of the errors in red ($O_C D_R$).

In our previous analysis of the connected part of the coherent logical noise, we neglected logical strings with length $> L + 2\zeta$ for a cut-off constant ζ. Then we neglected short logical strings with atypical shape. Finally, we neglected the unlikely partitions of each string, which we called exceptional terms. In this proof we began with a likely partition of a short, typical connected logical string. We added disconnected errors, and in cases like the one in figure E.1 where the added errors flipped the partition, we mapped these terms to partitions of a different connected logical string like in figure E.2. The final part of our proof is to argue that we can neglect this class of terms, where disconnected errors changed how the connected partition is decoded.

First, we observed above that the weight of the new connected term produced by our mapping is less than the weight of the original term with disconnected errors. This means that the term in figure E.1 is suppressed in powers of $\sin\theta/2$ relative to the term in figure E.2. Second, we will argue that the new connected term is one we have already neglected. Recall how we constructed new connected terms like the one in figure E.2. We took a likely partition of a typical, short, connected logical string and added disconnected errors to it in such a way that we flipped how the partition was decoded. The original uncorrectable side became correctable and vice versa. Then we multiplied the correctable error $O_U D_L$ by a particular stabilizer operator to produce a new term that is a partition of a new connected logical string. We make the following observation. One of two things must be true. One is that the new logical string has an atypical shape, specifically if the logical string runs left to right across the code, the steps up and down in the lattice are separated by less than γL. γ was our chosen constant from Lemma 10 that lower bounded the separation between the vertical steps in the logical string. The alternative is that the new connected logical string has a typical shape, but the partition we produce is unlikely. If the stabilizer we multiply by in figure E.2 has a width of at least γL, the shape of the new connected logical string may be typical. However, in that case the partition we get for the longer connected logical string has a row of γL qubits all belonging to the blue error. We proved in Lemma 4 that partitions with this feature are an exponentially small (in $\sqrt{L}$) fraction of the total partitions. We neglected these partitions in our earlier sum over connected terms. We find that the terms with disconnected errors that flip how the partition is decoded are in one-to-one correspondence with terms we have already neglected and moreover, the magnitudes of the terms with disconnected errors are smaller by a number of powers of $\sin\theta/2$. We conclude that such terms contribute less to the logical noise than the terms we have already neglected.

So far in this proof, we dealt with incoherent-type added errors. This was for simplicity, so that we had only one picture in mind. The argument for coherent-type added errors is the same. Coherent-type disconnected errors can also flip the correctable and uncorrectable sides of a partition of a connected logical string. We have already stated the condition when this occurs. The disconnected terms on the uncorrectable side D_L must contain a contiguous set of errors near a contiguous set of errors in the uncorrectable part of the partition O_U.

We bound the contribution of the disconnected coherent-type errors that flip the correctable and uncorrectable sides of the partition in the same way as we did the incoherent-type. We will use a mapping that takes such a term and produces a partition of a longer connected logical string. The mapping multiplies by a suitable stabilizer operator as depicted in figure E.4. In this case the new connected term is negligible for the same reasons as in the incoherent-type added error case.

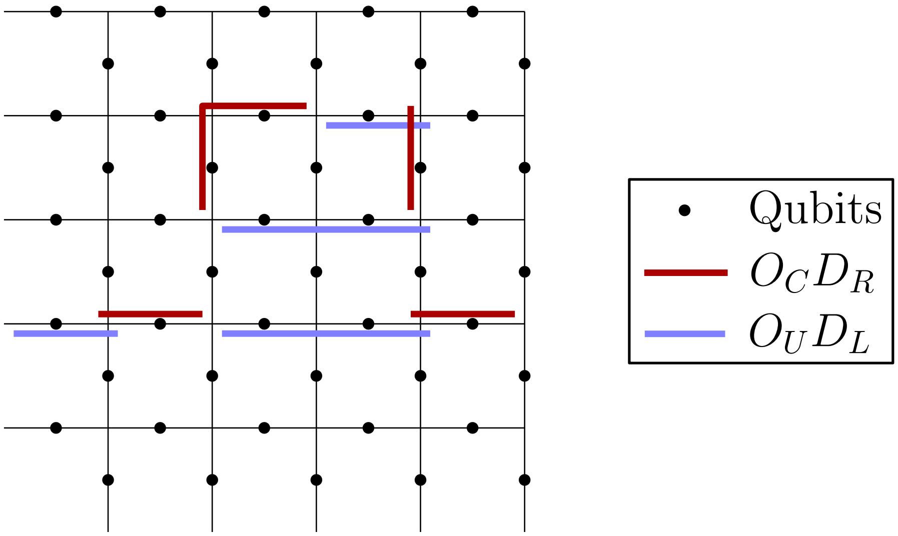


Figure E.3: Here we have a partition of a connected logical string together with a disconnected error. The partition is the same as the one in figures E.1 and E.2. The disconnected error is now a coherent-type error. The uncorrectable error $O_C D_R$ is in red, while the correctable error $O_U D_L$ is in blue. Without the disconnected errors, O_C would be correctable and O_U, uncorrectable. The added loop of disconnected errors has flipped the original partition.

The connected logical string produced from the original partition plus the disconnected coherent-type errors either has an atypical shape or the original partition was exponentially unlikely (in $\sqrt{L}$). We conclude that the contribution of terms with disconnected errors that flip the partition is negligible in the logical noise.

□

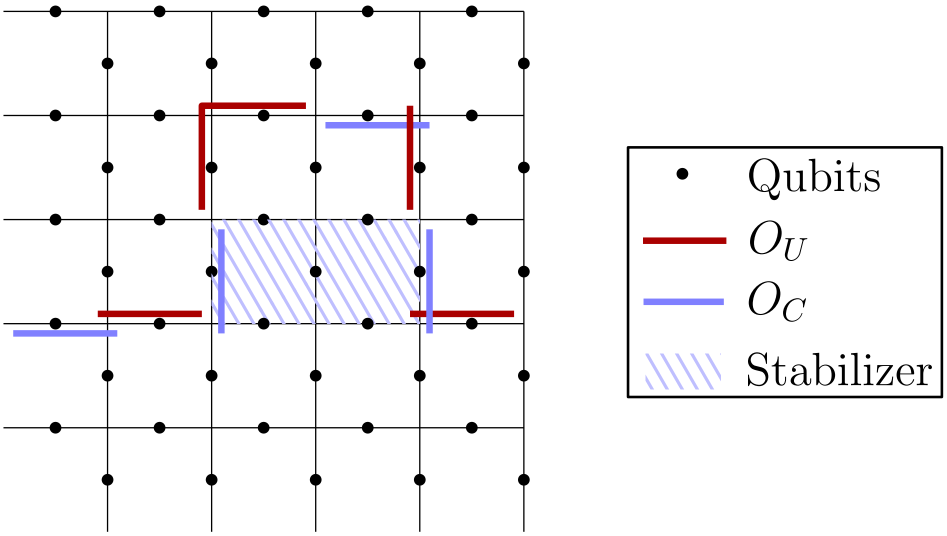


Figure E.4: This is the connected string and partition that corresponds to figure E.3, with the new uncorrectable error O_U in red and the new correctable error O_C in blue. We can always multiply right or left hand sides by a stabilizer to produce different coherent terms. This term is produced from figure E.3 by multiplying the correctable side in blue by the stabilizer operator in gray crosshatching. The connected logical string is longer than the one in figure E.3, but the total weight of the term is less.

Appendix F

THE DISCONNECTED PART OF THE INCOHERENT LOGICAL NOISE

In Appendix E we proved that for the dominant noise terms in the coherent logical noise components, the disconnected part was equal to 1 up to small corrections. We will now prove the same statement for the dominant noise terms in the incoherent logical noise components.

Lemma 12. *In equation (3.41), we wrote an incoherent logical noise component as a sum over the contributions from individual logical strings. This included a disconnected factor. Here we prove that we can set the disconnected factor equal to* 1 *and make only a small error. In other words suppose we write*

$$\tilde{\chi}_{Z_1 Z_1} \geq \sum_{\mathcal{L}} \sum_{O_U \subset \mathcal{L}} \frac{1}{|\{O'_C\}|} \sum_{O'_U} (O_U \rho\, O'_U)(1 + \mathcal{E}_1 + \mathcal{E}_2), \tag{F.1}$$

where the sum over $\mathcal{L}$ includes all short typical logical strings, O_U, $|\{O'_C\}|$, and O'_U are all as described in Section 3.8, and $\mathcal{E}_1$ is the error we make by neglecting various connected terms, including high-weight terms and terms with mismatched weight. In Lemma 5 we proved that

$$|\mathcal{E}_1| < O\left((\sin\theta)^{2\zeta}\right). \tag{F.2}$$

$\mathcal{E}_2$ represents the error we make when we set the disconnected factor equal to 1*. Then*

$$|\mathcal{E}_2| < \frac{8\gamma\zeta^2}{\sqrt{L}} + O\left(\frac{1}{L}\right). \tag{F.3}$$

Proof. We can follow the argument from Section 3.6 and Appendix E. The connected noise terms we considered in those sections had the form $(O_U \rho\, O_C)$. Here we will consider noise terms with the form $(O_U \rho\, O'_U)$. We will imagine arriving at these noise terms in the manner of Section 3.8. Namely, we begin with a short logical string with a typical shape. We partition the logical string into O_U and O_C. Then we choose an operator O'_U with the same syndrome as O_U. We denoted the set of possible O'_U by $\{O'_U\}$.

Now that we have a connected noise term $(O_U \rho\, O'_U)$, we can think of dressing it with disconnected errors in exactly the same way as we did in the coherent case.

In Section 3.6 we observed that the added errors that make up the disconnected part can be divided into coherent- and incoherent-type. The coherent-type added errors are when we add different errors to O_U and O'_U. In this case the errors we add to O_U and O'_U form a loop (with nonzero area). We saw that as long as the loop was positioned such that the added errors did not change how the connected noise term was decoded, the sum over the possible ways of dividing the errors in the loop between O_U and O'_U gave zero. We considered incoherent-type added errors where we added the same error to O_U and O'_U. In this case the contribution was nonzero. As long as the added error did not change how the connected noise term was decoded, the incoherent-type added errors contributed a $\sin^2\theta/2$ term on each qubit. Together with the $\cos^2\theta/2$ term corresponding to no error on each qubit, this gives 1 for the disconnected part. This applies to the added errors that do not change how the connected part was decoded. Therefore, our approach is to write the disconnected part as 1 plus a correction that comes from the configurations of added errors that change how the connected part is decoded.

In Lemma 11 we considered added errors that change how O_U is decoded in the coherent logical noise components. For connected noise terms that enter into the incoherent logical noise, the correction to the disconnected part comes from the same source, certain added errors that change how the connected term is decoded. In that case the added errors flipped the correctable and uncorrectable sides of the partition, which gives a phase of -1. In the incoherent case, if O_U is made correctable by the added errors, then so is O'_U, and the resulting term contributes to the identity part of the logical noise. In effect, there are disallowed added errors, which reduce the value of the disconnected part. The counting of such terms is identical to what we did in Lemma 11. Recall that these added error terms were related to connected terms that either had an atypical shape or an unlikely partition. The contribution to $\mathcal{E}_2$ from these terms is proportional to the fraction of atypical logical strings from Lemma 10. The contribution from the unlikely partitions is exponentially small in $\sqrt{L}$ as before.

There is another class of added errors that contribute to the correction to the disconnected part. Some errors are near the correction E_s so that once the errors have been added, they become part of a new connected term. An example is shown in figure F.1. This class of terms contains only incoherent-type added errors. Coherent-type added error placed here will still give 0 after we sum over the ways of splitting the errors into the left and right disconnected errors. This is the same as for coherent-

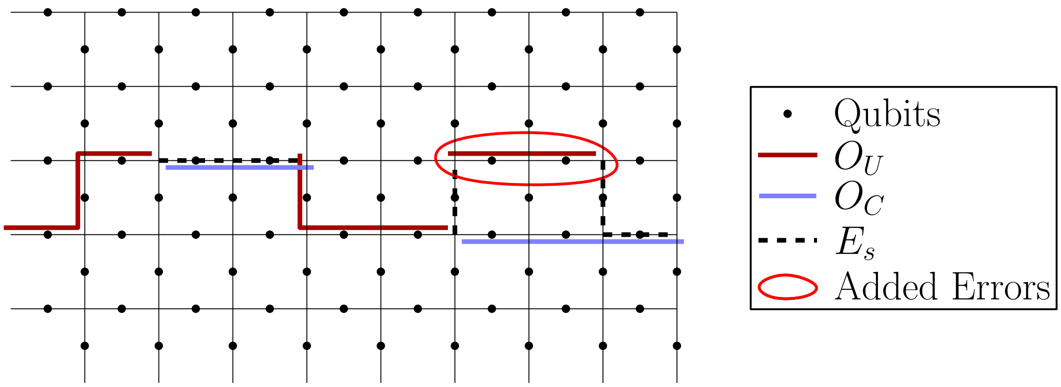


Figure F.1: This figure illustrates a certain type of added error term. We start with a short, typical logical string and partition it into operators O_U and O_C. Then we would choose some operator O'_U (not pictured) with the same weight and syndrome as O_U to produce an incoherent term. The errors in the red circle are added to both O_U and O'_U. The minimal-weight correction is shown as a black dashed line. The added errors are not disconnected but form a new connected term.

type added errors far from the connected logical string. For a likely partition of a short logical string with typical shape, E_s will have the same weight as O_C. The incoherent-type added errors that join the connected part may either lie near to E_s or they may be contained in E_s. We will first study the case where the added errors are not contained in E_s. These terms are closely related to the situation we just analyzed where the added errors sit next to O_U. The condition on the added error is analogous to equation (E.5). Let D denote the added incoherent-type error and $\mathcal{S}$ denote the stabilizer group. Then

$$\min_{G_x \in \mathcal{S}} |G_x O_C D| < \min_{G_y \in \mathcal{S}} |G_y O_c| + \min_{G_z \in \mathcal{S}} |G_z D|. \tag{F.4}$$

If this condition is satisfied, then the added error becomes part of a new connected term $(O_U D \rho\, O'_U D)$. Together with the new lowest-weight correction $O_U D$ forms a new connected logical string. This logical string is similar to the old logical string, but it contains a detour where it veers off to include the error D. This logical string either has an unlikely shape because it includes two closely spaced vertical steps, or the error D has width $> \gamma L$. In the latter case we also require that the original correction E_s contains $> \gamma L$ consecutive qubits. This is exponentially unlikely according to the counting we did in Lemma 4 and the bound we wrote in equation (3.26). We conclude that the contribution to the error term ϵ_2 from the noise terms we arrive at by adding errors proximate to O_C is small.

This leaves the added errors that lie within E_s or one of the operators with the same syndrome and weight. In this case the new connected logical string that results from adding the errors is the same as the old logical string. We will compare the set of terms we arrive at by adding errors in this manner to the set of terms with the same O_U but a higher-weight O'_U. We will argue that there are more of the terms with higher-weight O'_U. We have already neglected such noise terms in Lemma 7, so we conclude that the correction to the disconnected part is small.

We start with a connected noise term $(O_U \rho \, O'_U)$, where $|O_U| = |O'_U| = w$. We form a higher-weight noise term by adding an incoherent-type error D within one of the operators O'_C to produce a new connected noise term $(O_U D \rho \, O'_U D)$. This adds a total of two to the weight of the term. We can place the added error anywhere within one of the operators O'_C. The number of possibilities is $O(w)$. Now consider the possible connected noise terms with the same O_U, but instead of choosing O'_U with weight w, we set $|O'_U| = w + 2$. Suppose we start with an operator O'_U with weight w. We can construct one with $w + 2$ by adding an extra "cap" consisting of three qubits around a single plaquette or star. This is illustrated in figure F.2, where three possible choices of O'_U are drawn with the red dashed line. The number of possible choices is at least $O(w)$, because we can place a cap at each location along O_U. The full set of possibilities will generally be larger. If we consider a pair of added errors lying within O'_C, then we compare to the connected noise terms with $|O'_U| = |O_U| + 4$. The noise terms where O_U and O'_U have different weights were discussed in Section 3.9. We proved in Lemma 7 that the contribution of these terms is negligible. Finally we conclude, just as in Lemma 11, that each of the disconnected errors that contribute to the error $\mathcal{E}_2$ can be matched with a connected noise term that we have already neglected. In other words, the error $\mathcal{E}_2$ is less than $\mathcal{E}_1$. Therefore, we can say that the disconnected part = 1 and make only a small error for low-weight connected terms.

□

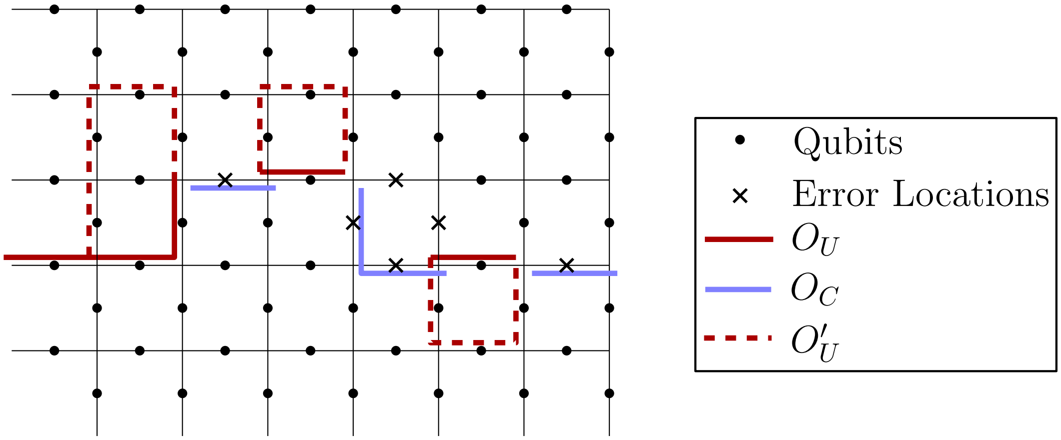


Figure F.2: This figure illustrates the idea of the proof that a certain type of added error term contributes only a small error. Consider a connected logical string that we partition into O_U and O_C, the solid red and blue lines. The class of added errors we consider are those where the added error lies along O_C or one of the operators O'_C with the same weight and syndrome. The possible locations for such an added error are marked by the × symbols. We prove that such terms are negligible by comparing to the noise terms where the operator O'_U is chosen with weight 2 greater than O_U. Three of the possible choices for O'_U are drawn with the dashed red lines. In this example there are 12 possible O'_U operators and six possible added error terms.

Appendix G

PHYSICAL Y ERRORS

In Lemma 8 we considered rotations in the $X-Z$ plane where the single-qubit rotation angles were allowed to differ. Here we prove that allowing for rotations partly around the Y axis on the physical qubits will decrease the coherence of the logical noise channel.

Lemma 13. *Consider an $L \times L$ toric code and a noise channel that consists of single-qubit rotations by an angle θ about an arbitrary axis. Suppose that $|\sin\theta| < 1/L$ as in Lemmas 3 and 5. Then the connected contribution to the logical noise from low-weight terms is most coherent when the single-qubit rotations are about an axis in the $X-Z$ plane. We proved elsewhere that the low-weight connected contribution dominates the logical noise components.*

Proof. Let θ_X, θ_Y, θ_Z denote the rotation angles about the X, Y, and Z-axis, respectively, so that $\theta_X^2 + \theta_Y^2 + \theta_Z^2 = \theta^2$. Of the coherent logical noise components, according to Lemmas 14 and 15, the dominant components are the ones $(\tilde{L}_a\tilde{\rho})$, where $\tilde{L}_a$ is a logical X or Z operator on one of the encoded qubits. We apply several of our lemmas to restrict the noise terms we consider, just as in Theorem 6. Among the noise terms that contribute to the coherent logical noise, we keep the terms with short, typical logical strings and non-exceptional partitions. Among the noise terms that contribute to the incoherent logical noise, we keep the terms where the logical string $\mathcal{L}$ is short and typical, $|O_U| = (|\mathcal{L}|+1)/2$, $|O_C| = |E_s|$, and $|O'_U| = |O_U|$.

First suppose that $\theta_Z = 0$. Then the logical $(X_1\tilde{\rho})$ noise component is generated from noise terms $(O_U\rho\, O_C)$ where O_U and O_C together contain X acting on every qubit along an X_1 logical string. Meanwhile, the incoherent logical $(X_1\tilde{\rho}X_1)$ noise component is also generated by X_1 logical strings. In Theorem 6 we state a bound on the relative magnitude of these logical noise components. Here θ_X plays the role of θ in equation (3.69). Under our θ_X and θ_Y rotation noise model, we also have a non-zero logical $(Z_1\tilde{\rho})$ noise component. This is generated by connected noise terms, $(O_U\rho\, O_C)$, where O_U and O_C together contain both X and Y acting on every qubit along a Z_1 logical string. The number of Z_1 logical strings with length ℓ is the same as the number of X_1 logical strings with length ℓ. However, the weight of the noise terms that contribute to $(Z_1\tilde{\rho})$ is ℓ^2. The contribution of each noise term is $(\sin\theta_X/2)^\ell(\sin\theta_Y/2)^\ell$. In contrast, the noise terms that contribute to $(X_1\tilde{\rho})$ are all proportional to $(\sin\theta_X/2)^\ell$. Therefore, $(Z_1\tilde{\rho})$ is exponentially smaller in L relative to $(X_1\tilde{\rho})$ for any choice of rotation axis in the $X{-}Y$ plane. The $(Z_1\tilde{\rho})$ noise component has a negligible effect on the relative magnitudes of the coherent and incoherent logical noise components. We also have an incoherent $(Z_1\tilde{\rho}\,Z_1)$ noise component. This is generated by noise terms, $(O_U\rho\,O'_U)$, where O_U and O'_U contains Y errors along an uncorrectable subset of a Z_1 logical string. These noise terms have magnitude $(\sin\theta_Y/2)^{\ell+1}$, which is exponentially large relative to the noise terms that contributed to $(Z_1\tilde{\rho})$. It follows that the logical coherence is maximized when $\theta_Y = 0$ and $\theta_X = \theta$. We began by supposing $\theta_Z = 0$. Next we will consider the case where θ_X, θ_Y, and θ_Z are all nonzero.

Suppose $|\theta_Z| \geq |\theta_X|$. If not, switch the role of X and Z in what follows. Fix a Z_1 logical string $\mathcal{L}$. The contribution of the logical string $\mathcal{L}$ to $\tilde{\chi}_{Z_1I}$ is a sum over the partitions of $\mathcal{L}$. For each partition $(O_U\rho\,O_C)$, we can replace a Z error in O_U with a Y error if we add an X error on the same qubit to O_C. Similarly we can replace a Z error in O_C by a Y error if we add an X error on the same qubit to O_U. The Z syndrome is unchanged, but now we also have a non-trivial X syndrome corresponding to the X error on the chosen site. This does not change how any partitions are decoded, but it does change the weight. The contribution of each partition to $\tilde{\chi}_{Z_1I}$ is a sum over all combinations of either a Z error or a Y and an X error on every qubit in $\mathcal{L}$. The terms with Y errors have higher weight. This means they contain extra factors of $\sin\theta_Y/2$, which is small since $|\sin\theta| < 1/L$. At the same time, the logical string $\mathcal{L}$ contributes to the $\tilde{\chi}_{Z_1Z_1}$ logical noise component. These noise terms include some that feature only Z errors and others with some number of Z errors replaced by Y errors. Unlike the contributions to $\tilde{\chi}_{Z_1I}$, these terms with Y errors are not higher-weight. There are no extra factors of $\sin\theta_Y/2$, and we conclude that the incoherent logical noise components are made larger relative to the coherent logical noise components. Therefore, the logical coherence is maximized when $\theta_Y = 0$.

□

Appendix H

OTHER LOGICAL MAPS

In Section 3.4 we restricted our attention to logical coherent terms of the form $(\widetilde{L_a}\tilde{\rho})$, where L_a is an X or Z operator on one of the encoded qubits. Now we would like to consider the case where L_a acts nontrivially on both encoded qubits or as Y on one or both of the encoded qubits.

Lemma 14. *Consider the toric code with minimal-weight decoding and a noise model that consists of uniform single-qubit unitary rotations about a fixed axis. Then the coherent logical noise components, $(\widetilde{L_a}\tilde{\rho})$, where $\tilde{L}_a$ is a Y-type logical operator or $\tilde{L}_a$ is a non-trivial logical operator on both encoded qubits, are negligible relative to the components where $\tilde{L}_a$ is an X- or Z-type logical operator on one encoded qubit.*

Proof. Suppose we have $\tilde{L}_a = X_1Z_2$. Logical strings of this type are the product of two operators of the type we have already considered. Each connected noise term that contributes to the logical noise component, $(X_1Z_2\tilde{\rho})$, is a product of a connected noise term that contributes to $(X_1\tilde{\rho})$ and a connected noise term that contributes to $(\tilde{\rho}Z_2)$. It follows that up to corrections that come from the disconnected part, $(X_1Z_2\tilde{\rho}) \approx (X_1\tilde{\rho})(Z_2\tilde{\rho})$. The logical components, $(X_1\tilde{\rho})$ and $(Z_2\tilde{\rho})$, are both small if error correction is working, so the logical $(X_1Z_2\tilde{\rho})$ component will be negligible. If $\tilde{L}_a$ is Y-type operator on the first encoded qubit, the argument is the same, since Y-type logical strings are products of X- and Z-type logical strings, $Y_1 = X_1Z_1$.

If we have $\tilde{L}_a = Z_1Z_2$, the logical component $(Z_1Z_2\tilde{\rho})$ is no longer a product of $(Z_1\tilde{\rho})$ and $(\widetilde{Z_2\rho})$. This is because Z_1 and Z_2-type logical strings can overlap, and this changes the counting of logical strings of a fixed weight. Figure H.1 shows two examples of this kind of logical string. At length $2L$, where L is the code distance, there are many connected logical strings because we can have a single connected string that wraps the torus along both directions. If we count the shortest paths between two points in the square lattice separated by distance l_1 in the horizontal and l_2 in the vertical, we get

$$\text{number of shortest paths travelling } l_1 \text{ horizontal and } l_2 \text{ vertical spaces} = \binom{l_1 + l_2}{l_1}. \tag{H.1}$$

We can use this to bound the number of weight-$2L$ logical Z_1Z_2 strings. Fix two sites in the code, qubit i along the vertical edge of the code and qubit j along the horizontal edge. Now count the number of shortest paths that connect these points. We have

$$\binom{i+j}{i}\binom{2L-2-i-j}{L-1-i}+\binom{L-1-i+j}{j}\binom{i+L-1-j}{i} \tag{H.2}$$

for the two ways of linking the edge points. We simply apply the result from equation (H.1). In the end we find that

$$\text{number of weight-}2L\ Z_1Z_2 \text{ logical strings} \approx \frac{4^L}{\sqrt{\pi L}}. \tag{H.3}$$

In Section 3.4 we counted logical strings that act as X or Z on one of the encoded qubits starting from length L, and we found exponentially many logical strings at higher weights. If we consider weight-$2L$ logical strings, we find order μ^{2L} logical strings, where $\mu \approx 2.64$ for the 2D square lattice. This is more than 4^L, so we have more of the high-weight logical strings that act on only one encoded qubit. Further, in our path counting in Lemma 3, we neglected all logical strings of length $> L + 2\zeta$ for a constant ζ. The strings of length $\geq 2L$ contribute negligibly for large L. Then we conclude that the logical noise components, $(\tilde{L}_a\tilde{\rho})$, where L_a is a Y-type logical operator or acts on both encoded qubits, are negligible relative to the noise components where L_a acts as X or Z on one of the encoded qubits.

□

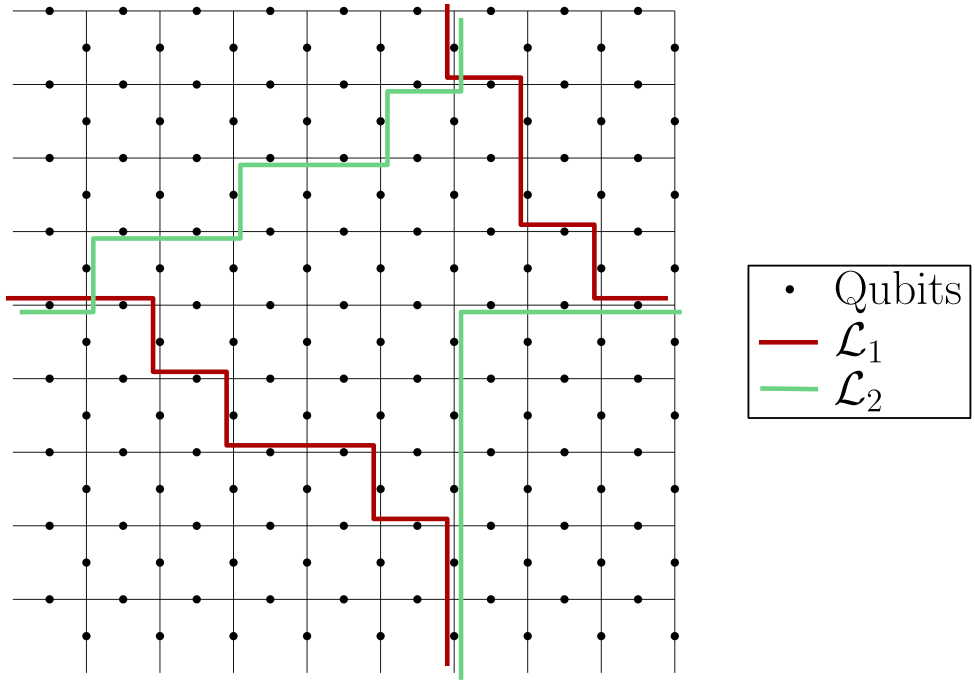


Figure H.1: Here are two examples of lowest-weight Z_1Z_2 logical strings, $\mathcal{L}_1$ and $\mathcal{L}_2$, that act as Z on both encoded qubits. Notice that red and green connect the edge points in different (but topologically equivalent) ways.

Appendix I

MORE GENERAL COHERENT TERMS

We have considered coherent logical noise components $(\tilde{L}_a\tilde{\rho})$, where $\tilde{L}_a$ is a logical operator that acts as X or Z on exactly one of the encoded qubits. We must also consider logical noise components $(\tilde{L}_a\tilde{\rho}\tilde{L}_b)$, where $\tilde{L}_a$ and $\tilde{L}_b$ are different nontrivial operators on the encoded qubits.

Lemma 15. *Consider the $L \times L$ toric code with noise that consists of single-qubit unitary rotations about a fixed axis by angle θ on every qubit, where $|\sin\theta|$ is $< 1/L$ as in Lemma 3. Each coherent logical noise component of the form $(\tilde{L}_a\tilde{\rho}\tilde{L}_b)$, where $\tilde{L}_a$ and $\tilde{L}_b$ are different nontrivial logical operators, is negligible relative to the coherent logical noise components with $\tilde{L}_b = \tilde{id}$. Each of the more general coherent terms is given by*

$$(\tilde{L}_a\tilde{\rho}\tilde{L}_b) \approx (\tilde{L}_a\tilde{\rho})(\tilde{\rho}\tilde{L}_b). \tag{I.1}$$

$(\tilde{L}_a\tilde{\rho})$ and $(\tilde{\rho}\tilde{L}_b)$ are both small (because we are interested in the regime where error correction succeeds with high probability.) Therefore, we may safely neglect all logical noise components $(\tilde{L}_a\tilde{\rho}\tilde{L}_b)$, where $\tilde{L}_a$ and $\tilde{L}_b$ are different nontrivial logical operators.

Proof. Our approach here is to bound the coherent logical noise components $(\tilde{L}_a\tilde{\rho}\tilde{L}_b)$, where $\tilde{L}_a$ and $\tilde{L}_b$ are different nontrivial logical operators, by the coherent logical noise components we have already considered. This follows because the short connected logical strings with different logical action do not overlap much. Overlap here means that the strings contain the same error acting on the same qubits. One possible overlap is between Z_1 and Z_2 logical strings. Pick a Z_1 logical string, $\mathcal{L}_1$, and a Z_2 logical string, $\mathcal{L}_2$. One string runs left to right, and the other runs top to bottom. If the horizontal string is longer than L, the code distance, then it has vertical steps along it, and these steps may overlap with the vertical logical string. An example is given in figure I.1. We assume $\mathcal{L}_1$ and $\mathcal{L}_2$ both have length $\leq L + 2\zeta$ because of Lemma 3. Then we use Lemma 9 to restrict to the case where all the steps are one lattice spacing at a time. Any possible overlap is on at most two sites as shown in figure I.1. Further, if we consider all possible pairs of a Z_1 logical string and a Z_2 logical string, only order $1/L$ strings have any overlap at all, so we can neglect possible overlap.

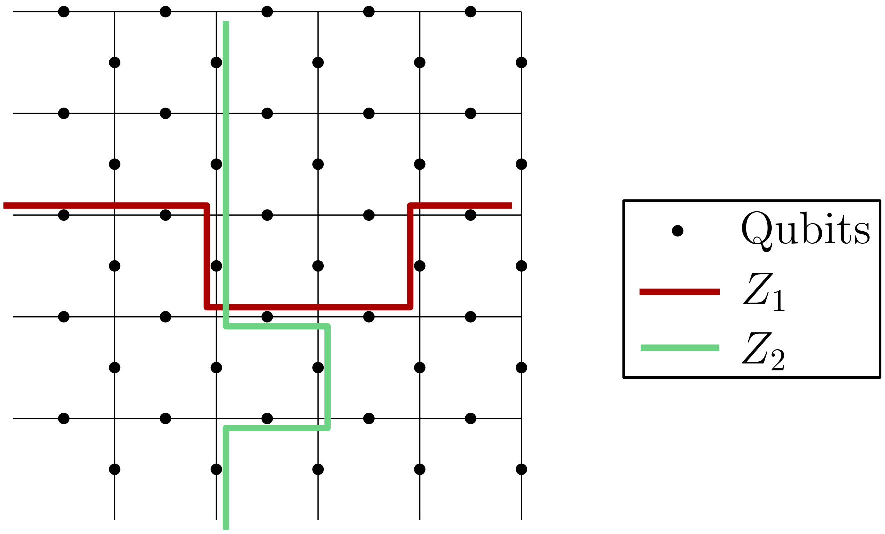


Figure I.1: Here we have a Z_1 and a Z_2 logical string. They have an overlap of two qubits, but if we fix one string and consider all possible paths for the other string, we see that only order $1/L$ have any overlap.

Because the two logical strings $\mathcal{L}_1$ and $\mathcal{L}_2$ are approximately disjoint, when we sum over partitions, each partition approximately factors into a partition of $\mathcal{L}_1$ times a partition of $\mathcal{L}_2$. That is, each connected noise term in the sum for the logical $\tilde{\chi}_{Z_1 Z_2}$ is a partition $(O_U^{(1)} O_C^{(2)} \rho\, O_C^{(1)} O_U^{(2)})$ which is approximately equal to $(O_U^{(1)} \rho\, O_C^{(1)})(O_C^{(2)} \rho\, O_U^{(2)})$ where $O_U^{(1)} O_C^{(1)} = \mathcal{L}_1$ and $O_U^{(2)} O_C^{(2)} = \mathcal{L}_2$. Therefore, $\tilde{\chi}_{Z_1 Z_2} \approx \tilde{\chi}_{Z_1 I} \tilde{\chi}_{I Z_2}$ up to small corrections from the overlap between $\mathcal{L}_1$ and $\mathcal{L}_2$ and from the disconnected part. Each of the terms $\tilde{\chi}_{Z_1 I}$ and $\tilde{\chi}_{I Z_1}$ will be $\ll 1$ if we are in a regime where error correction succeeds. Therefore, the $\tilde{\chi}_{Z_1 Z_2}$ logical noise component will be negligible relative to the $\tilde{\chi}_{Z_1 I}$ logical noise component. The same holds for the other logical noise components with a nontrivial logical operator on each side of $\tilde{\rho}$. Then we may safely neglect the more general coherent terms and consider only the $(\tilde{L}_a \tilde{\rho})$ components.

□

Appendix J

GROWTH OF INFIDELITY

The expression for the average infidelity after m applications of the noise channel from [25] is an upper bound.

$$r_m \leq rm + \frac{(d-1)\Theta^2}{2d} m(m-1), \tag{J.1}$$

where r_m is the average infidelity after m applications of a fixed noise channel, r is the average infidelity after one application of the channel, d is the dimension of the Hilbert space on which the channel acts, and Θ is the coherence angle. For anything save unitary or completely coherent channels, the upper bound has a linear component. We expect that this linear part is not only an upper bound, but that the average infidelity will grow linearly to lowest order.

Working in the Pauli transfer matrix representation, a unital noise channel is written as

$$\begin{pmatrix} 1 & 0 & 0 & \dots \\ 0 & 1-\lambda_2 & \beta_{2,3} & \dots \\ 0 & \beta_{3,2} & 1-\lambda_3 & \\ \vdots & \vdots & & \ddots \end{pmatrix}. \tag{J.2}$$

When channels are composed, we multiply the Pauli transfer matrices. After applying the same noise channel twice, we have diagonal entries

$$(1-\lambda_j)^2 + \sum_{l|l\neq j} \beta_{j,l}\beta_{l,j}. \tag{J.3}$$

After m applications of the noise channel, the diagonal entries are

$$(1-\lambda_j)^m + \binom{m}{1}(1-\lambda_j)^{m-1} \sum_{l|l\neq j} \beta_{j,l}\beta_{l,j} + \cdots . \tag{J.4}$$

Then the infidelity after composing the channel m times is proportional to

$$\begin{aligned} &\sum_{j=1}^{d} 1 - (1-\lambda_j)^m - \binom{m}{1}(1-\lambda_j)^{m-1} \sum_{i|i\neq j} \beta_{j,i}\beta_{i,j} - \cdots \\ &= \sum_{j=1}^{d} m\lambda_j - \lambda_j^2 \frac{m(m-1)}{2} + \cdots - m \sum_{l|l\neq j} \beta_{j,l}\beta_{l,j} \cdots . \end{aligned} \tag{J.5}$$

To lowest order the infidelity grows proportional to r, the first term in the upper bound in equation (J.1).

Appendix K

DIAMOND DISTANCE BOUND

The diamond distance from identity can be bounded in terms of the average infidelity, r, and the sum of squares of the off-diagonal (coherent) components of the chi matrix.

Lemma 16. *In equation (2.47), we upper bounded the diamond distance from identity for a channel by a function f based on [56]. This function depended on the components of the Pauli transfer matrix for the channel. With a little algebra, we can show*

$$f^2 \leq c_1 \left(\sum_{i,j|i\neq j} \chi_{i,j}^2 \right) + c_2 r^2. \tag{K.1}$$

where the constants are given by $c_1 = d_L^2$ and $c_2 = 2(d_L + 1)^2$ and d_L is the dimension of the logical space.

Proof. We start with equation (2.47), and rewrite the Pauli transfer matrix in terms of chi matrix. We expand $(1 - N_{i,i})^2$ and compare to r^2. Equation (2.49) reads

$$f^2 = \frac{1}{d_L^2 - 1} \left(\sum_{i,j|i\neq j} N_{i,j}^2 + \sum_l (1 - N_{l,l})^2 \right), \tag{K.2}$$

where N is the Pauli transfer matrix representation of the noise channel. The diamond distance from identity is bounded by a constant times f. We can expand f in terms of the chi matrix elements. Recall that we already have Lemma 1 concerning the off-diagonal elements. Also, the infidelity r is related to the trace of the Pauli transfer matrix or the (0,0) element of the chi matrix.

We can write the diagonal components of Pauli transfer matrix in terms of the diagonal components of the chi matrix in the following way:

$$N_{i,i} = \sum_{j\in C_i} \chi_{j,j} - \sum_{l\in A_i} \chi_{l,l}, \tag{K.3}$$

where the set C_i includes all the Pauli operators σ^j that commute with σ^i and the set A_i is all Pauli operators σ^l that anticommute with σ^i. For example, in the case of a single-qubit channel

$$N_{1,1} = \chi_{0,0} + \chi_{1,1} - \chi_{2,2} - \chi_{3,3}. \tag{K.4}$$

Then we can sum over all the diagonal components of N using the fact that the identity operator commutes with every operator:

$$\sum_{i=0}^{d_L^2} N_{i,i} = d_L^2 \chi_{0,0}, \tag{K.5}$$

where d_L is the dimension of the logical space. Next we can expand the diagonal term from equation (K.2):

$$\begin{aligned}\sum_{i=0}^{d_L^2}(1 - N_{i,i})^2 &= \sum_{i=0}^{d_L^2}\left(1 - 2N_{i,i} + N_{i,i}^2\right) \\ &= d_L^2 - 2d_L^2\chi_{0,0} + d_L^2\sum_j \chi_{j,j}^2 \\ &= d_L^2\left(1 - \chi_{0,0}\right)^2 + d_L^2 \sum_{j|j\neq 0}\chi_{j,j}^2 \\ &= d_L^2\left(\sum_{l|l\neq 0}\chi_{l,l}\right)^2 + d_L^2\sum_{j|j\neq 0}\chi_{j,j}^2,\end{aligned} \tag{K.6}$$

where we have used the trace preservation condition $\sum_i \chi_{i,i} = 1$. Because the noise channel is unitary, the diagonal components of the chi matrix are real and greater than 0. Then we can bound

$$\sum_{i=0}^{d_L^2}(1 - N_{i,i})^2 \leq 2d_L^2\left(\sum_{l|l\neq 0}\chi_{l,l}\right)^2. \tag{K.7}$$

When we substitute into equation (K.2) and use Lemma 1 for the off-diagonal terms, we have the following bound on the diamond norm distance from identity:

$$D_\diamondsuit(N)^2 \leq \frac{d_L^2}{4}\left(\sum_{i,j|i\neq j}\chi_{i,j}^2\right) + \frac{d_L^2}{2}\left(\sum_{l\neq 0}\chi_{l,l}\right)^2. \tag{K.8}$$

Finally, the average infidelity r is given by

$$r = \frac{d_L}{d_L + 1}(1 - \chi_{0,0}) = \frac{d_L}{d_L + 1}\sum_{l\neq 0}\chi_{l,l} \tag{K.9}$$

in the chi matrix representation. Equation (K.1) follows. □