# Eastin-Knill Theorem and its Implications

A. A. Akhtar[1]

[1] *Department of Physics, University of California San Diego, La Jolla, CA 92093, USA*

(Dated: December 15, 2020)

In this paper we explore the interplay between Lie groups, symmetry and quantum error correction in the Eastin-Knill theorem [1]. The basic idea is that the generators of the group of logical, unitary product operators are the sum of local operators which can themselves be expanded in terms of the error operators in a local, quantum error correcting code and thus act trivially on the code space. This implies that the number of logical operators that can be implemented by a transversal gate set is finite, and thus cannot be universal. Furthermore, any finite code that is covariant with respect to some continuous symmetry cannot correct arbitrary single qubit errors, because logical charge information leaks into the environment [2]. Infinite codes lack these restrictions. Eastin-Knill theorem has a profound significance to fault-tolerant quantum computing and in physical systems where symmetry and quantum error correction exists.

## I. INTRODUCTION

The paradigm for storing and protecting quantum memory is a quantum error correcting code, which encodes data into highly entangled states that are robust against local measurements and noise. Quantum error correcting codes (see [6, 7] for a gentle introduction) occur across physics, such as in topological phases of matter [3], holographic quantum gravity [4], random unitary circuits with measurement [5], and they are a cornerstone of quantum computing. In addition to being able to correct quantum errors, we also must be able to limit the proliferation of quantum errors through unitary evolution. This can be achieved using transversal gates, which are inherently fault tolerant. Unfortunately, the Eastin-Knill theorem [1] precludes the possibility of such gates being universal. The primary result in the original paper [1] is that a local quantum error correcting code, i.e. a quantum code that can correct an arbitrary single-qubit error, cannot have a universal, transversal gate set.

The basic idea of error correction, both classical and quantum, is to use redundancy to protect information from erasure. The *logical* bits, which are used for computation, are encoded into a subspace, called the *code* space, of a larger many-body quantum system. The error correcting code specifies which physical states correspond to which assignment of logical bits and provides a scheme for how to correct errors like a bit flip or a measurement on a single qubit. Usually, the way this works is through a *syndrome* measurement to determine the type of error, and then a unitary to correct the error that was done.

Errors which act non-trivially in the code-space are usually called undetectable or logical errors. Errors which do nothing inside the code space are called *detectable* because they can be corrected by measuring the projector $P$ onto the code space. Thus, an error $E$ is detectable if and only if

$$PEP \propto P$$

Quantum error correcting codes (QECC) are usually designed to handle local, independent errors. However, an error can spread throughout the system through unitary evolution (i.e. computation) on the logical bits. One way to prevent the spread of errors is through *transversal* gates. Suppose that our QECC is broken up into *code blocks*, each one consisting of one or several qubits, such that independent, local errors can be corrected in each individual block. Furthermore, suppose that each code block is partitioned into subsystems, labeled $1...n$, such that the computational gates applied to our system only couple the same partition between different code blocks e.g. partition $i$ in each code block. Such operators, called transversal, are inherently fault tolerant because errors on different code blocks are treated independently and transversal gates can only spread errors between partitions of different code blocks. Practically, they don't actually increase the number of errors.

Suppose we can implement transversal gates to arbitrary accuracy. Given a local-error-correcting quantum code, can any logical operator on the code space be implemented to arbitrary accuracy using a finite composition of transversal gates? The answer turns out to be no, because of the structure of the Lie group of transversal unitary operators [1]. We will structure the paper as follows: in II, we present the argument provided in the original paper [1], which proves that the set of unitary, logical product operators can only implement a finite number of gates on a local, quantum error correcting code, corresponding to its connected components; in III, we explore some ways to circumvent the theorem and its connections to symmetry; in IV, we conclude the article.

## II. PROOF OF EASTIN-KNILL THEOREM

The proof relies on the fact that the group of logical unitary product operators, $\mathcal{G}$, only describes a finite number of inequivalent, or distinct, logical operators on the QECC, and thus cannot approximate the infinite set of logical operators.

Consider a composite quantum system, $\mathcal{Q}$, composed of $n$ physical subsystems, where the $j$th subsystem has dimension $d_j$. The dimension of the entire quantum system

is $D = \prod_{j=1}^{n} d_j$. Let $\mathcal{T}$ denote the group of all unitary product operators, i.e. operators that decompose into a tensor product of single-site unitaries.

$$\mathcal{T} = \{V \in \mathcal{U}(D) | V = \bigotimes_{j=1}^{n} V_j,\ V_j \in \mathcal{U}(d_j)\} \tag{1}$$

where $\mathcal{U}(d)$ is the unitary group on a $d$-dimensional quantum system. Since $\mathcal{U}(d)$, with $d$ finite, is a compact Lie group, so is $\mathcal{T}$, which is simply a direct product of compact Lie groups. The set of *logical* unitary operators is defined as a subset of unitary operators that preserve the code space. Therefore, if $P$ is the projector onto the code space, and $U$ is a logical unitary operator, then $(1-P)UP = 0$. It turns out that the set of logical unitary operators $\mathcal{L}_P$ is a group, and that its intersection with a unitary Lie group forms a Lie subgroup. The proof is in the appendix.

With these lemmas, we are ready to move on to the main result, which states that logical unitary product operators are not universal for any non-trivial, local QECC. By the previous result, we know that $\mathcal{G}$, the set of logical unitary product operators, is a Lie subgroup of $\mathcal{T}$, since

$$\mathcal{G} = \mathcal{T} \cap \mathcal{L}_P \tag{2}$$

It turns out that for non-trivial, local QECCs, $\mathcal{G}$ can only do so much on the logical state because the generators of the connected component of the identity can be expanded in terms of local, detectable errors that leave the code space invariant. Let $\mathcal{C}$ be the connected component containing the identity in $\mathcal{G}$. $\mathcal{C}$ is a connected Lie group and a general element $C \in \mathcal{C}$ can be written using the exponential map on an element $\mathsf{c}$ of the Lie algebra. Furthermore, since $C$ is a logical operator,

$$0 = (1 - P)e^{i\epsilon \mathsf{c}}P$$

Since this holds for all $\epsilon$, we know that $\mathsf{c}$ is also a logical operator.

$$0 = \lim_{\epsilon \to 0}(1 - P)\frac{e^{i\epsilon \mathsf{c}} - I}{i\epsilon}P = (1 - P)\mathsf{c}P$$

Since $\mathcal{C}$ is a Lie subgroup of $\mathcal{T}$, its Lie algebra is a subalgebra of the algebra for $\mathcal{T}$. Since $\mathcal{T}$ is the Lie group of unitary product operators, its Lie algebra consists of local hermitian operators, and so $\mathsf{c}$ can be expanded in a sum of local hermitian operators. But, by assumption, our system is a local QECC. Therefore, there is a complete set of error operators that spans any local hermitian operator, and so

$$P\mathsf{c}P \propto P$$

Combining this with the fact that $\mathsf{c}$ is a logical operator, we get that $\mathsf{c}$ keeps the code space invariant.

$$\mathsf{c}P = P\mathsf{c}P \propto P$$

Since $\mathsf{c}$ is unitary on $P$ and hermitian, the constant of proportionality must be one or minus one. Thus any element $\mathsf{c}$ of the Lie algebra of $\mathcal{C}$ acts trivially on $P$. Hence, thinking about the connected components of the logical, unitary product operators $\mathcal{Q} = \mathcal{G}/\mathcal{C}$, there are only as many distinct operators as the cardinality $|\mathcal{Q}|$. Since $\mathcal{G}$ is a compact Lie group, it can only have a finite number of connected components so $|\mathcal{Q}| < \infty$. Hence, logical unitary product operators can only implement a finite number of distinct computational gates in this QECC, and therefore cannot be universal. Furthermore, since transversal gates only act on the specific subsystems across code blocks, they are unitary, logical product operators on the transversal components. Hence no non-trivial, local QECC can have a universal, transversal gate set.

## III. CIRCUMVENTIONS AND EXTENSIONS

There are different directions that one may try to circumvent the theorem, for example, by relaxing unitarity, transversality, or universality. Another loophole could be to make our Hilbert space infinite-dimensional. We can either increase the on-site degree of freedom $d$ or the number of qudits $N$. This leads to an approximate Eastin-Knill theorem [2], which says how many physical qubits are needed per logical qubit to correct arbitrary error to some fixed accuracy. Thus, we can implement a universal, transversal gate set in a local, quantum error correcting code if we encode each logical bit in an exponentially diverging number of physical bits as the accuracy approaches one.

The Eastin-Knill theorem may be viewed as a restriction on codes covariant with respect to some continuous symmetry group $G$ that acts as a product of local symmetries. Covariant means performing the symmetry on the physical bits is the same as performing it on the logical bits. Using a similar argument to the one presented in II, it can be shown that no perfect, covariant, finite-dimensional, local QECC exists [8]. Essentially, the code must encode an eigenstate of the logical charge operator. Thus, by measuring the physical charge, the environment can learn about the charge information of the code state. Since logical charge information is leaking into the environment, the code cannot be perfect. Crucially, we can construct perfect, covariant local QECC if we allow infinite dimensions–this loophole is indeed exploited by holographic theories of quantum gravity [2]. A symmetric code's accuracy relies on small charge fluctuations in the (encoded) logical space, large charge fluctuations on the individual physical subsystems, and a large number of physical qubits [2].

## IV. CONCLUSION

Though the Eastin-Knill theorem appears as a technical statement about a certain class of quantum gates, it has profound importance for quantum computer scientists and physicists alike. It rules out transversal gates as a universal gate set for fault-tolerant quantum computing, because it is incompatible with error correction. It also highlights how two attractive aspects of nature, symmetry and quantum error correction, are at odds with each other. Indeed, the Eastin-Knill theorem explains why it should be no surprise that one, namely symmetry, seems more ubiquitous than the other, quantum error correction, which seems only to occur naturally in rather extreme regimes. Like all no-go theorems, it begs the question: in what ways can we utilize, generalize, and circumvent it?

## ACKNOWLEDGMENTS

We acknowledge McGreevy and Physics 220 for explaining Lie groups and symmetry to us.

[1] B. Eastin and E. Knill, Physical Review Letters **102** (2009), 10.1103/physrevlett.102.110502.
[2] P. Faist, S. Nezami, V. V. Albert, G. Salton, F. Pastawski, P. Hayden, and J. Preskill, Physical Review X **10** (2020), 10.1103/physrevx.10.041018.
[3] B. Zeng, X. Chen, D.-L. Zhou, and X.-G. Wen, "Quantum information meets quantum matter – from quantum entanglement to topological phase in many-body systems," (2018), arXiv:1508.02595 [cond-mat.str-el].
[4] F. Pastawski, B. Yoshida, D. Harlow, and J. Preskill, Journal of High Energy Physics **2015** (2015), 10.1007/jhep06(2015)149.
[5] R. Fan, S. Vijay, A. Vishwanath, and Y.-Z. You, "Self-organized error correction in random unitary circuits with measurement," (2020), arXiv:2002.12385 [cond-mat.stat-mech].
[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. (Cambridge University Press, USA, 2011).
[7] S. J. Devitt, W. J. Munro, and K. Nemoto, Reports on Progress in Physics **76**, 076001 (2013).
[8] P. Hayden, S. Nezami, S. Popescu, and G. Salton, "Error correction of quantum reference frame information," (2017), arXiv:1709.04471 [quant-ph].

### Appendix A: Properties of logical unitary operators

**Lemma.** The set of logical unitary operators $\mathcal{L}_P$ form a group under multiplication. Furthermore, the logical operators contained in a Lie group of unitary operators form a Lie subgroup.

*Proof.* First we prove that $\mathcal{L}_P$ is a group. We may define this set in terms of the projector onto the code-space $P$.

$$\mathcal{L}_P := \{U \in \mathcal{U}(D) | (1-P)UP = 0\} \subset \mathcal{U}(D) \qquad \text{(A1)}$$

From this definition, it is clear that $I \in \mathcal{L}_P$. Let $U, V \in \mathcal{L}_P$, then $(1-P)UVP = (1-P)UPVP = 0$, where in the second step we used that any logical operator satisfies $PVP = VP$ and in the final step we used the defining property of logical operators in equation A1. Therefore, $UV \in \mathcal{L}_P$, and so the set is closed under multiplication. Lastly we need to show that $\mathcal{L}_P$ is closed under inverse. To show this, first observe that $PU^\dagger P$ is the inverse of $PUP$ in $P$, so that

$$(PU^\dagger P)(PUP) = (PU^\dagger)(UP) = P$$

Using this identity, we are able to show that $U \in \mathcal{L}_P$ implies $U^\dagger \in \mathcal{L}_P$.

$$\begin{aligned} U^\dagger P &= U^\dagger(PUPPU^\dagger P) = U^\dagger(PUP)PU^\dagger P \\ &= U^\dagger UPU^\dagger P = PU^\dagger P \end{aligned}$$

Now, consider any Lie group of unitary operators $\mathcal{A}$, and its intersection with $\mathcal{L}_P$, $\mathcal{B} = \mathcal{A} \cap \mathcal{L}_P$. Since $\mathcal{B}$ is the intersection of two groups it is also a group. Furthermore, $\mathcal{B}$ is a closed set. To see this, note that $\mathcal{L}_P$ is the pre-image of a closed set, $\{0\}$, of a continuous function,

$$f : \mathcal{U}(D) \to \mathbb{C}^{D^2}, f(U) = (1-P)UP$$

and therefore it must be closed. Since $\mathcal{B}$ is the intersection of two closed sets ($\mathcal{A}$ is closed since it is a Lie group) it is also closed. The closed-subgroup theorem due to Cartan states that closed subgroups of Lie groups are also Lie groups, hence the logical operators on the code space form a Lie subgroup.

□