Restrictions on Transversal Encoded Quantum Gate Sets

Bryan Eastin* and Emanuel Knill

National Institute of Standards and Technology, Boulder, Colorado 80305, USA

(Received 28 November 2008; published 18 March 2009)

Transversal gates play an important role in the theory of fault-tolerant quantum computation due to their simplicity and robustness to noise. By definition, transversal operators do not couple physical subsystems within the same code block. Consequently, such operators do not spread errors within code blocks and are, therefore, fault tolerant. Nonetheless, other methods of ensuring fault tolerance are required, as it is invariably the case that some encoded gates cannot be implemented transversally. This observation has led to a long-standing conjecture that transversal encoded gate sets cannot be universal. Here we show that the ability of a quantum code to detect an arbitrary error on any single physical subsystem is incompatible with the existence of a universal, transversal encoded gate set for the code.

DOI: 10.1103/PhysRevLett.102.110502 PACS numbers: 03.67.Lx, 03.67.Pp

Quantum computation appears to be intrinsically more powerful than its classical counterpart. Efficient quantum algorithms have been found for certain problems that, using the best known classical algorithms, require resources that scale as a superpolynomial function of the problem size [1–3]. However, implementing a computation large enough to take advantage of such scaling properties is a daunting challenge. Given the difficulty of constructing quantum hardware, it seems likely that the software for the first quantum computers will need to incorporate significant amounts of error checking.

As in the classical case, quantum errors are rendered detectable by encoding the system of interest into a subspace of a larger, typically composite, system. A quantum code simply specifies which states of a quantum system correspond to which logical (encoded) information states. Errors that move states outside of the logical subspace can be detected by measuring the projector P onto this subspace. Thus, an error E is detectable, in the sense that it can be discovered or eliminated, if and only if

$$PEP \propto P.$$

Of course, not all errors can be detected; for any nontrivial code there are operators that act in a nontrivial way within the logical subspace. Most commonly, quantum codes are designed to permit the detection of independent, local errors and, as a consequence, are incapable of detecting some errors that affect many subsystems.

For quantum computation, it is necessary not only to detect errors but also to apply operators (gates) that transform the logical state of the code. Even when error processes are local and independent, however, the operations entailed in computing can generate correlated errors from uncorrelated ones. Thus, for error detection to be effective, it is important that the logical operators employed during a quantum computation be designed to limit the spread of errors. It is particularly important that operators do not spread errors within code blocks, where a block of a quantum code is defined as a collection of subsystems for which errors on subsystems in the collection are detected independently of those on subsystems outside of it. Managing the spread of errors is the subject of the theory of fault-tolerant quantum computing [4,5]. One of the primary techniques of this theory is the use of transversal encoded gates.

We label as ''transversal'' any partition of the physical subsystems of a code such that each part contains one subsystem from each code block. Given a transversal partition of a code, an operator is called transversal if it exclusively couples subsystems within the same part. Put another way, an operator is transversal if it couples no subsystem of a code block to any but the corresponding subsystem in another code block. Transversal operators are inherently fault tolerant. They can spread errors between code blocks, thereby increasing the number of locations at which a code block's error might have originated, but, since errors on different code blocks are treated independently, the total number of errors necessary to cause a failure is unchanged. This is in contrast to nontransversal operators, where, for example, an encoded gate coupling every subsystem in a code block might convert an error on a single subsystem into an error on every subsystem of the code block.

In view of the above, it would be highly desirable to carry out quantum computations exclusively using transversal encoded gates. To allow for arbitrary computation, it is necessary that the set of gates employed be universal, that is, that it be capable of implementing any encoded operator on the logical state space to arbitrarily high accuracy. However, in spite of substantial effort, no gate set for a nontrivial quantum code has yet been found that is both universal and transversal. Consequently, a long-standing question in quantum information theory is whether there exist nontrivial quantum codes for which all logical gates can be implemented transversally. For stabilizer codes, this question has recently been answered in the negative. Zeng,

Cross, and Chuang [6] showed that transversal unitary operators are not universal for stabilizer codes on two-level subsystems (qubits); the companion result for the case of d-level subsystems (qudits) was proven by Chen *et al.* [7]. In this Letter we present a more general proof based on the structure of the Lie group of transversal unitary operators. Our result applies to all local-error-detecting quantum codes, that is, all quantum codes capable of detecting an arbitrary error on any single subsystem.

An outline of the argument is as follows: The set of logical unitary product operators, $\mathcal{G}$, is a Lie subgroup of the Lie group of unitary product operators, $\mathcal{T}$. As a Lie group, $\mathcal{G}$ can be partitioned into cosets of the connected component of the identity, $\mathcal{C}$; these cosets form a discrete set, $\mathcal{Q}$. Using the fact that the Lie algebra of $\mathcal{C}$ is a subalgebra of $\mathcal{T}$, it can be shown that the connected component of the identity acts trivially for any local-error-detecting code. This implies that the number of logically distinct operators implemented by elements of $\mathcal{G}$ is limited to the cardinality of $\mathcal{Q}$. Because of the compactness of $\mathcal{T}$, this number must be finite. A finite number of operators can approximate infinitely many only up to some fixed accuracy; thus, $\mathcal{G}$, the set of logical unitary product operators, cannot be universal. Transversal operators may be viewed as product operators with respect to a transversal partitioning of the code, so the ability to detect an arbitrary error on a transversal part implies the nonexistence of a universal, transversal encoded gate set.

We begin by exploring the structure of various sets of unitary operators and subsequently move to our central theorem. The following material relies heavily on results from topology and the theory of Lie groups. An accessible introduction to these topics can be found, for example, in Refs. [8,9] and on Wikipedia [10].

Consider a quantum system of finite dimension d. The set $\mathcal{U}(d)$ of unitary operators on a d-dimensional quantum system forms a compact, connected Lie group with a Lie algebra consisting of the Hermitian operators. (Following the convention in physics, we include a factor of i in the mapping between elements of the Lie algebra and Lie group.) Thus, any unitary operator $U \in \mathcal{U}(d)$ satisfies

$$U = e^{iH}$$

for some Hermitian operator H.

Now consider a composite quantum system Q composed of n physical subsystems, where the dimension of the jth subsystem is d_j. Let $\mathcal{T}$ denote the set of all unitary product operators, that is, all operators of the form

$$\bigotimes_{j=1}^{n} U_j,$$

where $U_j \in \mathcal{U}(d_j)$. Being a direct product of a finite number of compact Lie groups, $\mathcal{T}$ is also a compact Lie group. For the same reason, $\mathcal{T}$ has a Lie algebra $\mathfrak{t}$ given by the direct sum of the Lie algebras of the component groups.

Given a quantum code C on the system Q, the set of logical unitary operators on Q is defined as the subset of unitary operators that preserve the code space. In terms of a projector P onto the code states of C, this is the statement that a unitary operator U is a logical operator if and only if

$$(I - P)UP = 0. \tag{1}$$

Note that $(I - P)UP$ is a continuous function of U.

Lemma 1.—The set of logical unitary operators forms a group.

Proof.—Let P be the projector onto the logical subspace of a quantum code. The set of logical unitary operators, $\mathcal{L}$, consists of all unitary operators U satisfying

$$PUP = UP.$$

The set $\mathcal{L}$ fulfills the four requirements of a group: The multiplication of unitary operators is associative. The identity, I, is contained in $\mathcal{L}$ as

$$PIP = P^2 = P = IP.$$

The group property of closure is satisfied since

$$PUVP = PUPVP = UPVP = UVP$$

for any U, $V \in \mathcal{L}$. The inverse $U^\dagger$ of any $U \in \mathcal{L}$ is contained in $\mathcal{L}$ since

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

which implies that $PU^\dagger P$ is the inverse of PUP on the subspace P and therefore that

$$U^\dagger(P) = U^\dagger(PUPPU^\dagger P) = U^\dagger UPPU^\dagger P = PU^\dagger P.$$

□

Lemma 2.—The logical operators contained in a Lie group of unitary operators form a Lie subgroup.

Proof.—Let $\mathcal{L}$ be the set of logical unitary operators for a given code, let $\mathcal{A}$ be a Lie group of unitary operators, and let $\mathcal{B} = \mathcal{A} \cap \mathcal{L}$. Lemma 1 shows that $\mathcal{L}$ is a group. Because the intersection of two groups is a group, $\mathcal{B}$ is a subgroup of $\mathcal{A}$. Topologically speaking, $\mathcal{L}$ is a closed set since, as seen from Eq. (1), it is a preimage of a closed set under a continuous function. Being a Lie group, $\mathcal{A}$ is also a topologically closed set, and therefore B is as well. That $\mathcal{B}$ is a Lie subgroup of $\mathcal{A}$ follows from a theorem by Cartan (see p. 3 of Ref. [11]), which states that a topologically closed subgroup of a Lie group is a Lie subgroup. □

Theorem 1.—For any nontrivial local-error-detecting quantum code, the set of logical unitary product operators is not universal.

Proof.—Let Q, as defined earlier, be a composite quantum system supporting a local-error-detecting code C. The set of unitary product operators on Q is the compact Lie group that was earlier denoted by $\mathcal{T}$.

Lemma 2 shows that $\mathcal{G}$, the subset of unitary product operators that are also logical operators, forms a Lie subgroup of $\mathcal{T}$.

As a Lie group, $\mathcal{G}$ can be partitioned into cosets of the connected component of the identity, $\mathcal{C}$, where $\mathcal{C}$ is a Lie subgroup of $\mathcal{G}$. This set of cosets is the quotient group $\mathcal{Q} = \mathcal{G}/\mathcal{C}$ and constitutes a topologically discrete group.

Because $\mathcal{C}$ is a connected Lie group, any element $C \in \mathcal{C}$ can be written as

$$C = \prod_k e^{iD_k},$$

where D_k is in $\mathfrak{c}$, the Lie algebra of $\mathcal{C}$. For any $D \in \mathfrak{c}$ and $\epsilon \in \Re$, the operator $e^{i\epsilon D}$ is also in $\mathcal{C}$ and is, consequently, a logical gate satisfying

$$0 = (I - P)e^{i\epsilon D}P.$$

Since $(I - P)IP = 0$, we also have

$$0 = \lim_{\epsilon \to 0}(I - P)\left[\frac{e^{i\epsilon D} - I}{i\epsilon}\right]P = (I - P)DP$$

for all $D \in \mathfrak{c}$.

As $\mathcal{C}$ is a Lie subgroup of the Lie group $\mathcal{T}$, its Lie algebra $\mathfrak{c}$ must be a subalgebra of $\mathfrak{t}$, the Lie algebra of $\mathcal{T}$. Consequently, every element $D \in \mathfrak{c}$ can be written in the form

$$D = \sum_{j=1}^{n} \alpha_j H_j,$$

where $\alpha_j \in \Re$ and H_j is a Hermitian operator applied to the jth subsystem. Any local Hermitian operator can be written as a sum over local error operators, so

$$PH_jP \propto P,$$

where P is the projector onto the code space of C.

Combining the preceding three equations yields

$$DP = PDP = P\sum_{j=1}^{n} \alpha_j H_j P = \sum_{j=1}^{n} \alpha_j PH_jP \propto P$$

for all $D \in \mathfrak{c}$, which shows that

$$CP = \prod_k e^{iD_k}P \propto P.$$

Since C is a unitary operator, the constant of proportionality must be one. Thus, whether it is trivial or not, all operators contained in $\mathcal{C}$ act as the identity on the code space.

Let $\mathcal{F}$ be a set consisting of one representative from each coset of $\mathcal{C}$ in $\mathcal{G}$. The preceding paragraph shows that every operator in the group $\mathcal{G}$ acts on the code space as an operator from $\mathcal{F}$. In other words, for every $G \in \mathcal{G}$,

$$GP = FCP = FP$$

for some $F \in \mathcal{F}$ and $C \in \mathcal{C}$.

The operators induced by $\mathcal{G}$ on the logical quantum system are closed under composition and limited in number to the cardinality of $\mathcal{F}$. The set $\mathcal{F}$ is discrete since its elements are representatives taken from each of the cosets comprising the discrete group $\mathcal{Q} = \mathcal{G}/\mathcal{C}$. It follows that $\mathcal{F}$ is also finite, being a discrete subset of a compact group, namely $\mathcal{T}$. However, for a nontrivial encoded quantum system, the number of logically distinct operators is uncountably infinite. As the set of all unitary operators is a metric space, a finite number of unitary operators cannot approximate infinitely many to arbitrary precision. (By contrast, the Solovay-Kitaev theorem [12,13] states that a universal, and infinite, set of operators can be generated by composition from certain finite sets of operators. In our case, composition yields nothing new.) Thus, $\mathcal{G}$, the set of logical product operators, is not universal. □

Theorem 1 considers only product gates, but the same basic approach can be applied to the case of transversal gates.

Corollary 1.—For any nontrivial local-error-detecting quantum code, the set of transversal, logical unitary operators is not universal.

Proof.—This result follows directly from an application of Theorem 1 in which the physical subsystems are replaced by transversal parts. Each part contains a set of physical subsystems that can be coupled by transversal operators. Transversal operators may therefore be regarded as product operators on the transversal parts. Theorem 1 thus proves that the set of transversal, logical unitary operators is not universal for any nontrivial quantum code capable of detecting an arbitrary error on a single transversal part. For a local-error-detecting code, the condition that any error on a single transversal part be detectable is satisfied since this corresponds to a single-subsystem error on each of the code blocks. □

As with any impossibility proof, perhaps the most interesting aspect of Corollary 1 is how it can be circumvented. The most obvious circumvention, and an avenue that has been thoroughly explored, is to employ nonunitary operators [14–16]. The standard method of achieving universal fault-tolerant quantum computation takes this approach, making extensive use of measurements and classical feed-forward during the preparation, testing, and coupling of ancillary states. Alternatively, one might retain unitarity and instead loosen the requirements of transversality or universality or even error detection, options that we discuss in turn.

Among the alternatives listed, nontransversal operators provide the most promising approach to circumventing Theorem 1. References [6,7] discuss the possibility of achieving universality through the addition of coordinate permutations, which, taken in isolation, are fault tolerant. Zeng, Cross, and Chuang note that the encoded Hadamard gate for the Bacon-Shor codes [17] involves a coordinate permutation and therefore is not transversal. In fact, for these codes, some sequences of encoded Hadamard and controlled-NOT gates are not fault tolerant; a single physical gate failure is capable of producing two errors on a

single code block. Strict fault tolerance is achieved by checking for errors prior to coupling code blocks using a new transversal partition. Such codes demonstrate that it is sufficient for individual logical gates to avoid directly coupling subsystems of a code block. A quantum code for which there existed a universal set of encoded gates each transversal in isolation would be extremely useful.

Along a different line, we might imagine demanding less than full universality. Finite groups of operators are already an important component of schemes for fault-tolerant quantum computing. These schemes typically take advantage of the existence of codes for which the Clifford gates, a finite subgroup of all gates, are both sufficient for error detection and transversally implementable. The Clifford gates are not the only set that can be implemented transversally, however. It would be interesting to quantify the maximum size of finite group that is achievable transversally and to investigate the computational power of the non-Clifford finite gate groups.

Given a local error model, it seems unprofitable to abandon local error detection entirely. In order to violate the assumptions of our proof, however, it is sufficient that detection not be deterministic. It might be possible to find a family of codes satisfying both the universality and transversality conditions for which the probability of failing to detect an error on a single subsystem can be made arbitrarily small. The usefulness of such a family of codes would depend on the scaling of the failure probability with the size of the code.

In conclusion, we have presented a proof that the ability of a quantum code to detect arbitrary errors on component subsystems is incompatible with the existence of a universal, transversal, and unitary encoded gate set. Our proof makes no assumptions about the dimensions of the quantum subsystems beyond requiring that they be finite. The quantum system encoded is assumed to be nontrivial, that is, to have dimension greater than one. The precise structure of the quantum code and its initialization state are unspecified. Our result rules out the use of transversal unitary operators with local error detection as an exclusive means to obtain universality, but it also suggests some interesting new avenues of investigation.

We thank Adam Meier, Scott Glancy, and Yanbao Zhang for their questions and comments during the development of this proof. Special thanks go to Sergio Boixo for the discussion that spawned the idea that local error detection and infinitesimal transversal gates were incompatible. Preliminary investigations on this topic were funded by National Science Foundation Grant No. PHY-0653596. This paper is a contribution by the National Institute of Standards and Technology and, as such, is not subject to U.S. copyright.

*beastin@nist.gov

[1] P. W. Shor, in *Foundations of Computer Science, 1994 Proceedings, 35th Annual Symposium on* (1994), p. 124.
[2] D. Aharonov, V. Jones, and Z. Landau, in *Proceedings of the Thirty-eighth Annual ACM Symposium on Theory of Computing* (ACM, New York, 2006), p. 427.
[3] M. Mosca, *Quantum Algorithms*, Springer Encyclopedia of Complexity and Systems Science (Springer, New York, 2009).
[4] P. Shor, in *Foundations of Computer Science, 1996 Proceedings, 37th Annual Symposium on* (1996), p. 56.
[5] J. Preskill, in *Introduction to Quantum Computation* (World Scientific, Singapore, 1998).
[6] B. Zeng, A. Cross, and I. L. Chuang, arXiv:0706.1382.
[7] X. Chen, H. Chung, A. W. Cross, B. Zeng, and I. L. Chuang, Phys. Rev. A **78**, 012353 (2008).
[8] J. R. Munkres, *Topology* (Prentice-Hall, Englewood Cliffs, NJ, 2000), 2nd ed..
[9] B. C. Hall, *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction* (Springer, New York, 2004).
[10] http://www.wikipedia.org/.
[11] M. R. Sepanski, *Compact Lie Groups* (Springer, New York, 2007).
[12] A. Y. Kitaev, Russ. Math. Surv. **52**, 1191 (1997).
[13] C. M. Dawson and M. A. Nielsen, Quantum Inf. Comput. **6**, 81 (2006).
[14] E. Knill, arXiv:quant-ph/0402171.
[15] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).
[16] X. Zhou, D. W. Leung, and I. L. Chuang, Phys. Rev. A **62**, 052316 (2000).
[17] D. Bacon, Phys. Rev. A **73**, 012340 (2006).