Stabilizer Formalism for Operator Quantum Error Correction

David Poulin*

School of Physical Sciences, The University of Queensland, QLD 4072, Australia

(Received 18 September 2005; published 1 December 2005)

Operator quantum error correction is a recently developed theory that provides a generalized and unified framework for active error correction and passive error avoiding schemes. In this Letter, we describe these codes using the stabilizer formalism. This is achieved by adding a gauge group to stabilizer codes that defines an equivalence class between encoded states. Gauge transformations leave the encoded information unchanged; their effect is absorbed by virtual gauge qubits that do not carry useful information. We illustrate the construction by identifying a gauge symmetry in Shor's 9-qubit code that allows us to remove 3 of its 8 stabilizer generators, leading to a simpler decoding procedure and a wider class of logical operations without affecting its essential properties. This opens the path to possible improvements of the error threshold of fault-tolerant quantum computing.

DOI: 10.1103/PhysRevLett.95.230504 PACS numbers: 03.67.Pp, 03.67.Hk, 03.67.Lx

The theory of fault-tolerant quantum computation [1–6] demonstrates the formal possibility of efficiently storing and manipulating quantum data for arbitrarily long times even in the presence of noise, provided the noise level is below a certain threshold. Fault tolerance builds on quantum error correction (QEC) [1,2,4,7], which is a means to actively protect quantum information against noise. Encoded quantum states are restricted to a code subspace C of the system's Hilbert space $H = C \oplus C^{\perp}$. Measurements are performed to detect if the noise has taken the system out of C, and if required, a transformation is applied to restore it. A good code must protect the information against a wide range of errors, and admit simple encoding, error correction procedures, and fault-tolerant gates.

Operator quantum error correction (OQEC), recently introduced in [8,9], generalizes the standard theory of QEC and provides a unified framework for active error correction and passive error avoiding techniques such as decoherence-free subspaces [10–12] and noiseless subsystems [13–15]. In this new paradigm, information is encoded in a subsystem A of the code space $C = A \otimes B$, and errors need only to be corrected modulo a transformation on B. The standard QEC theory corresponds to the special case where B is one dimensional. While this generalization does not lead to new families of codes, it does allow for new error correction procedures, possibly enriching the fault tolerance theory. A prime example is Bacon's OQEC code [16] that appears to have self-correcting properties.

Most of the QEC codes used for fault tolerance constructions can be described with the stabilizer formalism (see Ref. [3] and references therein). In particular, the first QEC codes proposed by Shor [1] and Stean [17] are stabilizer codes. Other important examples include CSS codes [2,18], topological codes [19], and convolutional codes [20]. A stabilizer formalism has also been constructed to describe the passive error avoiding techniques of decoherence-free subspaces and noiseless subsystems [15]. Additionally, the stabilizer formalism plays a central role in other branches of quantum information science, e.g., in the so-called "one time" or "cluster state" quantum computation model [21]. Some of the advantages of the stabilizer formalism are that it provides a compact description of QEC codes, admits compact description of a restricted class of dynamical systems (the Clifford group [3]), and allows one to build on classical coding theory (particularly via the CSS construction).

In this article, we present a stabilizer formalism for OQEC. We will briefly review the basic theory of OQEC and the standard stabilizer formalism. Then, we demonstrate a general procedure based on the algebraic approach of Ref. [22] to describe the subsystem structure $A \otimes B$ using the Pauli group. We also discuss bounds that apply to these codes. Finally, we illustrate the stabilizer formalism by constructing an OQEC code based on Shor's 9-qubit code, but which contains a nontrivial B subsystem. This code has all the essential features of Shor's original code, but admits a simpler error recovery procedure and a wider class of encoded operations.

OQEC theory.—Let us first summarize the OQEC theory. A fixed partition of the system's Hilbert space $H = A \otimes B \oplus C^{\perp}$ is assumed. Information is encoded on the A subsystem, i.e., the logical quantum state $\rho^A \in \mathcal{B}(A)$ is encoded as $\rho^A \otimes \rho^B \oplus 0^{C^{\perp}}$ with an arbitrary ρ^B. We say that the physical map $\mathcal{E}$: $\mathcal{B}(H) \to \mathcal{B}(H)$ is *correctable* on subsystem A when there exists a physical map $\mathcal{R}$: $\mathcal{B}(H) \to \mathcal{B}(H)$ that reverses its action, up to a transformation on the B subsystem, i.e., for all ρ^A and ρ^B, $\mathcal{R} \circ \mathcal{E}(\rho^A \otimes \rho^B) = \rho^A \otimes \rho'^B$ for some arbitrary ρ'^B. In terms of the operator-sum representation $\mathcal{E}(\rho) = \sum_a E_a \rho E_a^{\dagger}$, the existence of a recovery map $\mathcal{R}$ requires the following condition to hold (see [8,9])

$$P E_a^{\dagger} E_b P = \mathbb{1}^A \otimes g_{ab}^B \, \forall \, a, b, \tag{1}$$

where P is the projector onto the code space—i.e.,

$PH = C = A \otimes B$—and g^B_{ab} is an arbitrary operator in $\mathcal{B}(B)$. That this condition is also sufficient for $\mathcal{E}$ to be correctable was proven in [23], along with alternative information-theoretic necessary and sufficient conditions. As expected, when the B subsystem is one dimensional, Eq. (1) reduces to the familiar error correction condition [4,7].

Stabilizer formalism.—Let us now focus on the case where the system is composed of n qubits, so $H = \mathbb{C}^{2^n}$. The Pauli matrices are defined as

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We denote X_j the matrix X acting on the jth qubit, and similarly for Y_j and Z_j. The Pauli group on n qubits $\mathcal{P}_n$ is generated under multiplication by the Pauli matrices acting on each qubit, together with the imaginary number i. In terms of independent generators, we have $\mathcal{P}_n = \langle i, X_1, Z_1, \ldots, X_n, Z_n \rangle$.

The first step in constructing a stabilizer code is to choose a set of $2n$ operators $\{X'_j, Z'_j\}_{j=1,\ldots n}$ from $\mathcal{P}_n$ that is Clifford isomorphic to the set of single-qubit Pauli operators $\{X_j, Z_j\}_{j=1,\ldots n}$ in the sense that the primed and unprimed operators obey the same commutation relations among themselves. The operators $\{X'_1, Z'_j\}_{j=1,\ldots n}$ generate $\mathcal{P}_n$ and behave as single-qubit Pauli operators—we can think of them as acting on n virtual qubits. However, these virtual qubits have no relation whatsoever with the original "bare" qubits (those related to the *unprimed* Pauli operators): the operators X'_j and Z'_j can act nontrivially on several bare qubits, i.e., they are collective degrees of freedom. It is crucial to note that there are several ways of choosing these operators, and that these various choices will lead to different codes. It should therefore be kept in mind that besides the imposed commutation relations, the X'_j and Z'_j are arbitrary.

The stabilizer group $S = \langle S_1, \ldots S_s \rangle$ with $s \leq n$ is an Abelian subgroup of $\mathcal{P}_n$ that does not contain -1. Without loss of generality, we can choose $S_j = Z'_j$ for $j = 1, \ldots, s$. These generators are independent commuting elements of $\mathcal{P}_n$, so they can be simultaneously diagonalized. The code space C is the span of the vectors fixed by S, i.e., $S_j|\psi\rangle = |\psi\rangle$ for all $j = 1, \ldots s$, and it has dimension 2^{n-s}. The projector onto the code space is denoted P and obviously satisfies $S_j P = P$ for all j.

The normalizer of S, denoted $N(S)$, is the subgroup of $\mathcal{P}_n$ that commutes with every element of S. (This simple definition of the normalizer follows from the fact that every pair of elements of $\mathcal{P}_n$ either commutes or anticommutes.) Clearly then, elements of $N(S)$ map the code subspace to itself. Given the above construction, we see that $N(S) = \langle i, Z'_1, \ldots Z'_n, X'_{s+1}, \ldots X'_n \rangle$.

Stabilizer formalism for OQEC.—The stabilizer S specifies the code subspace C, and we must now define a partition of C into subsystems $A \otimes B$. For this, we follow the procedure of Ref. [22] and identify subsystems via the algebra of operators acting on them. (While we mostly focus on group structures here, an equivalent algebraic description can straightforwardly be obtained by considering the associated group algebras.) Central to the OQEC theory is a notion of equivalence between states: the two states $\rho^A \otimes \rho^B$ and $\rho^A \otimes \rho'^B$ are considered to carry the same information even if ρ^B and ρ'^B differ. To capture this notion, we quotient the code state space $\mathcal{B}(C)$ by a set of "gauge" transformation $\mathcal{G}$ that defines an equivalence relation $\rho \sim \rho' \Leftrightarrow \exists\, g \in \mathcal{G}$: $\rho = g\rho' g^\dagger$. For $\sim$ to define an equivalence relation, $\mathcal{G}$ must have a group structure. Clearly, S and i should be in $\mathcal{G}$ as they leave states of C invariant under conjugation. For $\sim$ to keep states in the code subspace, $\mathcal{G}$ must be a subgroup of $N(S)$. Given these properties, $\mathcal{G}$ is a normal subgroup of $N(S)$, so $\mathcal{L} = N(S)/\mathcal{G}$ also has a group structure (the quotient group).

The gauge group $\mathcal{G} \supseteq \{S, \langle i \rangle\}$ can thus be generated by the stabilizer generators, the complex number i, and an arbitrary subset of the X'_j and Z'_j with $j > s$, i.e., $\mathcal{G} = \langle i, S_1, \ldots, S_{n-r-k}, X'_{i_1}, \ldots, X'_{i_a}, Z'_{j_1}, \ldots, Z'_{j_b} \rangle$ where $\{i_k\}$ and $\{j_k\}$ are subsets of $\{s+1, \ldots n\}$. However, for the two groups $\mathcal{G}$ and $\mathcal{L}$ to induce a subsystem structure on C, we must have $[\mathcal{G}, \mathcal{L}] = 0$ (see [22]). As a consequence, the X'_i and Z'_j generators of $\mathcal{G}$ must always appear in pairs, so without lost of generality, we must have $\mathcal{G} = \langle i, S_1, \ldots S_s, X'_{s+1}, Z'_{s+1}, \ldots, X'_{s+r}, Z'_{s+r} \rangle$ with $s + r \leq n$. Clearly then, $\mathcal{L} \simeq \langle X'_{s+r+1}, Z'_{s+r+1}, \ldots, X'_n, Z'_n \rangle$. With a slight abuse of notation, we will henceforth use $\mathcal{L}$ to denote the quotient group $N(S)/\mathcal{G}$ and its representation on H given above. Since $[\mathcal{G}, \mathcal{L}] = 0$ and $\mathcal{G} \times \mathcal{L} \simeq N(S)$, it follows from Ref. [22] that these groups induce a subsystem structure on the code subspace $C = A \otimes B$, such that the action of any $L \in \mathcal{L}$ and $g \in \mathcal{G}$ restricted to the code subspace C is given by

$$gP = \mathbb{1}^A_{2^k} \otimes g^B, \quad \text{for some } g^B \in \mathcal{B}(B), \tag{2}$$

$$LP = L^A \otimes \mathbb{1}^B_{2^{r-k}}, \quad \text{for some } L^A \in \mathcal{B}(A), \tag{3}$$

with $A \simeq (\mathbb{C}^2)^{\otimes k}$ and $B \simeq (\mathbb{C}^2)^{\otimes r}$ as desired.

To sum up, we have partitioned the n virtual qubits defined through the X'_j and Z'_j into 3 sets: s *stabilizer* qubits, r *gauge* qubits, and k *logical* qubits, with $s + r + k = n$. The Z'_j operators from the first set are denoted S_j with $j = 1, \ldots, s$, respectively. They are stabilizer generators and fix the 2^{r+k}-dimensional code space C. The Z'_{s+j} and X'_{s+j} operators from the second set are denoted g^z_j and g^x_j with $j = 1, \ldots, r$. They generate the group $\mathcal{L}_B$ of Pauli operations acting on the r virtual qubits of the B subsystem. These qubits do not encode useful information: their sole purpose is to absorb transformations from $\mathcal{G}$, and as such, they are referred to as gauge qubits. Together with the stabilizer and the complex number i, this set generates

the gauge group that leaves the encoded information invariant under conjugation, $\mathcal{G} = \mathcal{L}_B \times S \times \langle i \rangle$. From this definition, it is clear that an Abelian gauge group corresponds to the standard stabilizer formalism, while non-Abelian $\mathcal{G}$ yield OQEC codes. Finally the Z'_{s+r+j} and X'_{s+r+j} operators from the third set are denoted $\bar{Z}_j$ and $\bar{X}_j$ with $j = 1, \ldots, k$, respectively. They generate the logical operations $\mathcal{L}$, and act only on the k virtual qubits of the A subsystem.

Although we have given an explicit set of generators for $\mathcal{L}$, we stress that only the coset structure of $\mathcal{L}$ really matters. Operations related by a gauge transformation have the same effect on the encoded qubits, e.g., any $\bar{Z}'_j = g\bar{Z}_j$ with $g \in \mathcal{G}$ can serve as the logical Z Pauli operator acting on the jth encoded qubit. This defines an equivalence relation $Z \sim Z' \Leftrightarrow ZZ' \in \mathcal{G}$ between quantum operations. As mentioned above, the definitions of the gauge group $\mathcal{G}$ and logical operations $\mathcal{L}$ can be extended by considering the associated group algebras: any linear combination of elements of $\mathcal{G}$ ($\mathcal{L}$) is an operator acting solely on the gauge system B (encoded qubits A). This extends the notion of equivalence relations between states and operations in an obvious way.

Error correction.—We now study the effect of a set of errors $\{E_a\} \subset \mathcal{P}_n$. Although this may appear restrictive, we note that a recovery procedure $\mathcal{R}$ that corrects $\{E_a\}$ will also correct any set of errors obtained from linear combination of elements of $\{E_a\}$. Error detection is made by measuring the stabilizer generators $S_1, \ldots, S_s$. These give a set of outcomes $(m_1, \ldots, m_s)$ taking values ± 1, called the error syndrome. The all-ones syndrome indicates that the state is in the code subspace C, while any other syndrome indicate that an error has taken the state out of C. Thus, *detectable* errors are those that anticommute with at least one of the stabilizer generators, i.e., $\mathcal{P}_n - N(S)$ is the set of detectable errors.

To be *correctable*, the set of errors must satisfy Eq. (1). [Note that the conjugation (†) is irrelevant here, so we will omit it.] For any pair a, b, the operator $E_a E_b$ is an element of either $\mathcal{P}_n - N(S)$, or $N(S) - \mathcal{G}$, or $\mathcal{G}$. In the first case, there exists an $S \in S$ for which $\{E_a E_b, S\} = 0$. Inserting in to Eq. (1), we get $PE_a E_b P = PE_a E_b SP = -PSE_a E_b P = -PE_a E_b P = 0$, so the operator error correction condition is fulfilled. In the second case, observe that $N(S) - \mathcal{G} \simeq \{\mathcal{L} - \mathbb{1}\} \times \mathcal{G}$, so Eqs. (3) and (2) show that $PE_a E_b P = L^A_{ab} \otimes g^B_{ab}$ for some $L^A_{ab} \neq \mathbb{1}^A$, so these errors cannot be corrected. For the third case, Eq. (2) shows that $PE_a E_b P = \mathbb{1}^A \otimes g^B_{ab}$, so the condition is satisfied. Therefore, $\{E_a\}$ is a correctable set of errors if and only if $E_a E_b \notin N(S) - \mathcal{G}$ for all pairs a, b.

To construct the recovery procedure, observe that equivalent errors $E_a \sim E_b$ have by definition and Eq. (2) $PE_a E_b P = \mathbb{1}^A \otimes g^B_{ab}$, and yield the same error syndrome: for all $S \in S$ and $g \in \mathcal{G}$, $[gE_a, S] = 0$ if and only if $[E_a, S] = 0$. Thus, syndrome measurement can identify the coset of $\{E_a\}/\mathcal{G}$ to which the error that occurred belongs. To recover the information encoded in A, we can apply any element of that coset to the state. The overall effect of this procedure will be a gauge transformation since equivalent errors have $E_a E_b P = \mathbb{1}^A \otimes g^B_{ab}$ by virtue of Eq. (2), leaving the logical qubits A unaffected.

Bounds.—The distance d of a code is given by the minimal weight of operators in $N(S) - \mathcal{G}$. (The weight of an element of $\mathcal{P}_n$ is the number of qubits on which it acts nontrivially.) A code of distance d can correct errors on up to $(d-1)/2$ qubits. A stabilizer OQEC code therefore has 4 parameters, $[[n, k, r, d]]$ representing, respectively, the number of physical qubits, the number of encoded logical qubits, the number of gauge qubits, and the distance of the code. The Knill-Laflamme or quantum Singleton bound $n \geq 2(d-1) + k$ restricts the possible values of these parameters [4]. As any bound relating n, k, and d derived in the context of stabilizer QEC, this bound also applies to OQEC. This follows straightforwardly from Theorem 3 of Ref. [8]. Indeed, a $[[n, k, r, d]]$ OQEC code can be transformed into a $[[n, k, 0, d]]$ QEC code by turning the gauge Z operators g^z_j into extra stabilizer generators, i.e., by fixing the gauge.

The theory of OQEC opens the possibility of simplifying existing codes—turning a $[[n, k, 0, d]]$ code into a $[[n, k, r, d]]$ code with $r > 0$—by identifying "gauge symmetries" in their stabilizer. This would lead to more efficient error correction procedures with less error syndromes to measure and wider classes of encoded operations to choose from. A specific example is presented in the next section. The key task is thus to find the largest value of r achievable given values of n, k, and d. We have not yet derived a general bound for the number of gauge qubits besides the trivial observation that at least one stabilizer must be measured when $d > 0$. By exhaustive search however, we have ruled out the existence of a "better than perfect" quantum code—a 5-qubit code protecting one logical qubit against any single-qubit error [7,24], but which requires less than 4 stabilizer generators, i.e., that admits one gauge qubit.

Example.—Let us illustrate the idea of reducing the number of stabilizer generators by identifying gauge symmetries using Shor's $[[9, 1, 0, 3]]$ code [1]. The stabilizer

TABLE I. Stabilizer generators and encoded Pauli's for Shor's $[[9, 1, 0, 3]]$ code.

$S_1 =$	X_1	X_2	X_3	X_4	X_5	X_6	$\mathbb{1}_7$	$\mathbb{1}_8$	$\mathbb{1}_9$
$S_2 =$	X_1	X_2	X_3	$\mathbb{1}_4$	$\mathbb{1}_5$	$\mathbb{1}_6$	X_7	X_8	X_9
$S_3 =$	Z_1	Z_2	$\mathbb{1}_3$	$\mathbb{1}_4$	$\mathbb{1}_5$	$\mathbb{1}_6$	$\mathbb{1}_7$	$\mathbb{1}_8$	$\mathbb{1}_9$
$S_4 =$	$\mathbb{1}_1$	Z_2	Z_3	$\mathbb{1}_4$	$\mathbb{1}_5$	$\mathbb{1}_6$	$\mathbb{1}_7$	$\mathbb{1}_8$	$\mathbb{1}_9$
$S_5 =$	$\mathbb{1}_1$	$\mathbb{1}_2$	$\mathbb{1}_3$	Z_4	Z_5	$\mathbb{1}_6$	$\mathbb{1}_7$	$\mathbb{1}_8$	$\mathbb{1}_9$
$S_6 =$	$\mathbb{1}_1$	$\mathbb{1}_2$	$\mathbb{1}_3$	$\mathbb{1}_4$	Z_5	Z_6	$\mathbb{1}_7$	$\mathbb{1}_8$	$\mathbb{1}_9$
$S_7 =$	$\mathbb{1}_1$	$\mathbb{1}_2$	$\mathbb{1}_3$	$\mathbb{1}_4$	$\mathbb{1}_5$	$\mathbb{1}_6$	Z_7	Z_8	$\mathbb{1}_9$
$S_8 =$	$\mathbb{1}_1$	$\mathbb{1}_2$	$\mathbb{1}_3$	$\mathbb{1}_4$	$\mathbb{1}_5$	$\mathbb{1}_6$	$\mathbb{1}_7$	Z_8	Z_9
$\bar{Z} =$	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_7	Z_8	Z_9
$\bar{X} =$	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9

TABLE II. Stabilizer generators, encoded Pauli's, and generators of $\mathcal{L}_B$ for a [[9, 1, 3, 3]] version of Shor's code.

$S_1 =$	X_1	X_2	X_3	X_4	X_5	X_6	$\mathbb{1}_7$	$\mathbb{1}_8$	$\mathbb{1}_9$
$S_2 =$	X_1	X_2	X_3	$\mathbb{1}_4$	$\mathbb{1}_5$	$\mathbb{1}_6$	X_7	X_8	X_9
$S_3' =$	Z_1	Z_2	$\mathbb{1}_3$	$\mathbb{1}_4$	Z_5	Z_6	$\mathbb{1}_7$	$\mathbb{1}_8$	$\mathbb{1}_9$
$S_4' =$	$\mathbb{1}_1$	$\mathbb{1}_2$	$\mathbb{1}_3$	Z_4	Z_5	$\mathbb{1}_6$	$\mathbb{1}_7$	Z_8	Z_9
$S_5' =$	$\mathbb{1}_1$	Z_2	Z_3	$\mathbb{1}_4$	$\mathbb{1}_5$	$\mathbb{1}_6$	Z_7	Z_8	$\mathbb{1}_9$
$\bar{Z} =$	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_7	Z_8	Z_9
$\bar{X} =$	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9
$g_1^z =$	$\mathbb{1}_1$	Z_2	Z_3	$\mathbb{1}_4$	$\mathbb{1}_5$	$\mathbb{1}_6$	$\mathbb{1}_7$	$\mathbb{1}_8$	$\mathbb{1}_9$
$g_1^x =$	$\mathbb{1}_1$	$\mathbb{1}_2$	X_3	$\mathbb{1}_4$	$\mathbb{1}_5$	$\mathbb{1}_6$	X_7	$\mathbb{1}_8$	$\mathbb{1}_9$
$g_2^z =$	$\mathbb{1}_1$	$\mathbb{1}_2$	$\mathbb{1}_3$	$\mathbb{1}_4$	Z_5	Z_6	$\mathbb{1}_7$	$\mathbb{1}_8$	$\mathbb{1}_9$
$g_2^x =$	X_1	$\mathbb{1}_2$	$\mathbb{1}_3$	$\mathbb{1}_4$	$\mathbb{1}_5$	X_6	$\mathbb{1}_7$	$\mathbb{1}_8$	$\mathbb{1}_9$
$g_3^z =$	$\mathbb{1}_1$	$\mathbb{1}_2$	$\mathbb{1}_3$	$\mathbb{1}_4$	$\mathbb{1}_5$	$\mathbb{1}_6$	$\mathbb{1}_7$	Z_8	Z_9
$g_3^x =$	$\mathbb{1}_1$	$\mathbb{1}_2$	$\mathbb{1}_3$	X_4	$\mathbb{1}_5$	$\mathbb{1}_6$	$\mathbb{1}_7$	$\mathbb{1}_8$	X_9

generators and encoded Pauli operators for this code are given in Table I.

By inspection, we see that it is possible to pair up the last 6 stabilizers of this code, thus eliminating 3 of them. The remaining 5 stabilizers hence define a 2^4 dimensional code space, i.e., C contains 4 virtual qubits. However, these 4 qubits are not protected against all single-qubit errors; only one logical qubit is immune to noise, while the other 3 extra qubits in C are gauge qubits. Indeed, the code defined by Table II is a [[9, 1, 3, 3]] code. This new code has all the essential features of the original code. In particular, it protects one qubit of information against any single-qubit error, and it has all the features of a CSS code (e.g., fault-tolerant transversal c-not). It has, however, lost its ability to protect the logical qubit against some 2-qubit errors, but this is not essential to achieve fault tolerance by concatenation. Note also that there is much more freedom in choosing the encoded operation, e.g., the operator $\mathbb{1}_1 X_2 \mathbb{1}_3 \mathbb{1}_4 X_5 \mathbb{1}_6 \mathbb{1}_7 X_8 \mathbb{1}_9 = g_2 g_4 g_6 \bar{X}$ is a valid logical X operation. One can easily verify that the generators g_k of the gauge group generate $\mathcal{P}_3$, so this code has 3 gauge qubits as claimed.

We stress that this code is not the 5-qubit code [7,24] or Stean's 7-qubit code [17] disguised in a 9-qubit code. Indeed, the stabilizer of this new code is a subgroup of the stabilizer of the original code, and the encoded operations are the same as those of the original code. By exhaustive search, we have established that Shor's code does not admit more that 3 gauge qubits, while the 5-qubit code and Stean's 7-qubit code have no gauge symmetry at all.

Conclusion.—Operator quantum error correction theory provides a generalized and unified framework for active error correction techniques and passive error avoiding methods. In this Letter, we have developed a stabilizer description of such codes. Stabilizer codes have been central to fault-tolerant constructions, as well as other areas of quantum information science: it is our hope the generalization presented here will enrich these subjects. We have demonstrated that bounds which restrict the families of achievable codes derived in the setting of standard stabilizer QEC theory apply straightforwardly to OQEC codes via gauge fixing. Finally, we have illustrated our formalism by identifying gauge symmetries in Shor's code that lead to substantial simplifications. An important issue which remains open is to bound the number of gauge qubits that can be identified given the other parameters of the code.

We thank Michael Nielsen for stimulating discussions on the present topic, and Andreas Klappenecker for pointing out an error in a previous version of this Letter.

*Electronic address: dpoulin@iqc.ca

[1] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[2] A. M. Steane, Phys. Rev. A **54**, 4741 (1996).
[3] D. Gottesman, Ph.D. thesis, California Institute of Technology, Pasadena, CA, 1997.
[4] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[5] E. Knill, R. Laflamme, and W. H. Zurek, Science **279**, 342 (1998).
[6] J. Preskill, in *Introduction to Quantum Computation*, edited by T. P. S. H. K. Lo and S. Popescu (World Scientific, Singapore, 1999), p. 213.
[7] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[8] D. Kribs, R. Laflamme, and D. Poulin, Phys. Rev. Lett. **94**, 180501 (2005).
[9] D. W. Kribs, R. Laflamme, D. Poulin, and M. Lesosky, quant-ph/0504189.
[10] L.-M. Duan and G.-C. Guo, Phys. Rev. Lett. **79**, 1953 (1997).
[11] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).
[12] D. Lidar, I. Chuang, and K. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).
[13] E. Knill, R. Laflamme, and L. Viola, Phys. Rev. Lett. **84**, 2525 (2000).
[14] P. Zanardi, Phys. Rev. A **63**, 012301 (2001).
[15] J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley, Phys. Rev. A **63**, 042307 (2001).
[16] D. Bacon, quant-ph/0506023.
[17] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[18] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[19] A. Y. Kitaev, Ann. Phys. (N.Y.) **303**, 2 (2003).
[20] H. Ollivier and J.-P. Tillich, Phys. Rev. Lett. **91**, 177902 (2003).
[21] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[22] P. Zanardi, D. A. Lidar, and S. Lloyd, Phys. Rev. Lett. **92**, 060402 (2004).
[23] M. A. Nielsen and D. Poulin, quant-ph/0506069.
[24] R. Laflamme, C. Miquel, J.-P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).