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 actively protect quantum information against noise.

QEC and provides a unified framework for active 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 Steane [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” and “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, 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 \( H = A \otimes B \otimes C \) is assumed. Information is encoded on the \( A \) subsystem, i.e., the logical quantum state \( \rho^A \in \mathcal{B}(A) \) is encoded as \( \rho^A \otimes \rho^B \otimes \rho^C \) with an arbitrary \( \rho^B \). 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 \( \rho^A \) and \( \rho^B \), \( \mathcal{R} \circ \mathcal{E}(\rho^A \otimes \rho^B) = \rho^A \otimes \rho^B \) for some arbitrary \( \rho^B \). In terms of the operator-sum representation \( \mathcal{E}(\rho) = \sum_{a} E_{a} \rho E_{a} \), the existence of a recovery map \( \mathcal{R} \) requires the following condition to hold (see [8,9])

\[
PE_{a}^A E_{b}\rho P = 1^A \otimes g_{ab}^B \forall a, b,
\]

where \( P \) is the projector onto the code space—i.e.,
We denote similarly for definition of the normalizer follows from the fact that every specifies the code subspace information-theoretic necessary and sufficient conditions.

The projector onto the code space is denoted \( P \). Without loss of generality, we can choose \( \rho \) will lead to different codes. It should therefore be kept in freedom. It is crucial to note that there are several ways virtual qubits have no relation whatsoever with the original among themselves. The operators \( X_j;Z_j \) and behave as single-qubit Pauli operators—we can define through the group that defines an equivalence relation \( \rho \sim \rho' \Leftrightarrow \exists g \in G : \rho = g\rho'g^\dagger \). For \( \sim \) to define an equivalence relation, \( G \) must have a group structure. Clearly, \( s \) and \( i \) should be in \( G \) as they leave states of \( C \) invariant under conjugation. For \( \sim \) to keep states in the code subspace, \( G \) must be a subgroup of \( N(S) \). Given these properties, \( G \) is a normal subgroup of \( N(S) \), so \( L = N(S)/G \) also has a group structure (the quotient group).

The gauge group \( G \supseteq \{ S, (i) \} \) 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., \( G = \left\{ i, s_1, \ldots, s_{n-r-k}, x_{i_1}, \ldots, x_{i_s}, z_{j_1}, \ldots, z_{j_k} \right\} \) where \( \{ i \} \) and \( \{ j \} \) are subsets of \( \{ s+1, \ldots, n \} \). However, for the two groups \( G \) and \( L \) to induce a subsystem structure on \( C \), we must have \( [G, L] = 0 \) (see [22]). As a consequence, the \( X_{i_1} \) and \( Z_{j_1} \) generators of \( G \) must always appear in pairs, so without loss of generality, we must have \( G = \left\{ i, s_1, \ldots, s_r, x_{i_1}, \ldots, x_{i_s}, z_{j_1}, \ldots, z_{j_r} \right\} \) with \( s + r \leq n \). Clearly then, \( L \supseteq \left\{ X_{s+1}, z_{s+1}, \ldots, X_n, z_n \right\} \). With a slight abuse of notation, we will henceforth use \( L \) to denote the quotient group \( N(S)/G \) and its representation on \( H \) given above. Since \( [G, L] = 0 \) and \( G \times L = N(S) \), 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 \( L \in L \) and \( g \in G \) restricted to the code subspace is given by

\[
gP = \mathbb{1}_2^A \otimes g^B, \quad \text{for some } g^B \in \mathcal{B}(B). \tag{2}
\]

\[
LP = L^A \otimes \mathbb{1}_2^B, \quad \text{for some } L^A \in \mathcal{B}(A), \tag{3}
\]

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

To sum up, we have partitioned the 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 \( X_{s+j} \) and \( X_{s+j} \) operators from the second set are denoted \( g_j \) and \( g_j^s \) with \( j = 1, \ldots, r \). They generate the group \( L_B \) 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 \( G \), 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, \( \mathcal{G} = L_B \times S \times (i) \). 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 \( Z_j \) and \( X_j \) 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 \( Z_j' = gZ_j \) with \( g \in \mathcal{G} \) can serve as the logical \( Z \) Pauli operator acting on the \( j \)th encoded qubit. This defines an equivalence relation \( Z \sim Z' \Leftrightarrow ZZ' \in \mathcal{G} \) between quantum operations. As mentioned above, the definition 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 \( S_1, \ldots, S_r \). These give a set of outcomes \( (m_1, \ldots, m_r) \) taking values \( \pm 1 \), called the error syndrome. The all-ones syndrome indicates that the state is in the code subspace \( C \), while any other syndrome indicates 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 \( S \in \mathcal{S} \) for which \( \{E_a E_b S\} = 0 \). Inserting into Eq. (1), we get \( P(E_a E_b P = PE_a E_b S P = -P S E_a E_b P = -P E_a E_b P = 0 \), so the operator error correction condition is fulfilled. In the second case, observe that \( N(S) - G = (\mathcal{L} - I) \times \mathcal{G} \), so Eqs. (3) and (2) show that \( P E_a E_b P = L_{ab}^A \otimes g_{ab}^B \), so some \( L_{ab}^A \neq I_A \), so these errors cannot be corrected. For the third case, Eq. (2) shows that \( P E_a E_b P = I_A \otimes g_{ab}^B \), so the condition is satisfied. Therefore, \( \{E_a\} \) is a correctable set of errors if and only if \( E_a E_b \not\in N(S) - \mathcal{G} \) 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) \( P E_a E_b P = I_A \otimes g_{ab}^B \) and yield the same error syndrome: for all \( S \in \mathcal{S} \) and \( g \in \mathcal{G} \), \( [g E_a, S] = 0 \) 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 \( E_a E_b P = I_A \otimes g_{ab}^B \), 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 \( n \geq 2(d - 1) + 1 \) 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 \( g_j^Z \) 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>
<thead>
<tr>
<th>TABLE I.</th>
<th>Stabilizer generators and encoded Pauli’s for Shor’s ([[[9, 1, 0, 3]]]) code.</th>
</tr>
</thead>
<tbody>
<tr>
<td>5_1 = X_1</td>
<td>X_2</td>
</tr>
<tr>
<td>5_2 = X_1</td>
<td>X_1</td>
</tr>
<tr>
<td>5_3 = Z_1</td>
<td>Z_2</td>
</tr>
<tr>
<td>5_4 = I_1</td>
<td>I_2</td>
</tr>
<tr>
<td>5_5 = Z_1</td>
<td>Z_2</td>
</tr>
<tr>
<td>5_6 = I_1</td>
<td>I_2</td>
</tr>
<tr>
<td>5_7 = Z_1</td>
<td>Z_2</td>
</tr>
<tr>
<td>5_8 = I_1</td>
<td>I_2</td>
</tr>
<tr>
<td>Z = Z_1</td>
<td>Z_2</td>
</tr>
<tr>
<td>X = X_1</td>
<td>X_2</td>
</tr>
</tbody>
</table>
of quantum information science: it is our hope the general-
description of such codes. Stabilizer codes have been
methods. In this Letter, we have developed a stabilizer
provides a generalized and unified framework for active
error, and it has all the features of a CSS code (e.g., fault-
tions are the same as those of the original code. By ex-
haustive 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 general-
ization 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 QOEC 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 re-
 mains 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.

---

**TABLE II.** Stabilizer generators, encoded Pauli’s, and gen-

<p>| | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_1$</td>
<td>$X_1$</td>
<td>$X_2$</td>
<td>$X_3$</td>
<td>$X_4$</td>
<td>$X_5$</td>
<td>$X_6$</td>
<td>$I_7$</td>
<td>$I_8$</td>
</tr>
<tr>
<td>$S_2$</td>
<td>$X_1$</td>
<td>$X_2$</td>
<td>$X_3$</td>
<td>$I_4$</td>
<td>$I_5$</td>
<td>$I_6$</td>
<td>$X_7$</td>
<td>$X_8$</td>
</tr>
<tr>
<td>$S_3$</td>
<td>$Z_1$</td>
<td>$Z_2$</td>
<td>$Z_3$</td>
<td>$Z_4$</td>
<td>$Z_5$</td>
<td>$Z_6$</td>
<td>$I_7$</td>
<td>$I_8$</td>
</tr>
<tr>
<td>$S_4$</td>
<td>$I_1$</td>
<td>$I_2$</td>
<td>$I_3$</td>
<td>$Z_4$</td>
<td>$Z_5$</td>
<td>$Z_6$</td>
<td>$I_7$</td>
<td>$Z_8$</td>
</tr>
<tr>
<td>$S_5$</td>
<td>$I_1$</td>
<td>$Z_2$</td>
<td>$Z_3$</td>
<td>$I_4$</td>
<td>$I_5$</td>
<td>$I_6$</td>
<td>$Z_7$</td>
<td>$Z_8$</td>
</tr>
<tr>
<td>$Z$</td>
<td>$Z_1$</td>
<td>$Z_2$</td>
<td>$Z_3$</td>
<td>$Z_4$</td>
<td>$Z_5$</td>
<td>$Z_6$</td>
<td>$Z_7$</td>
<td>$Z_8$</td>
</tr>
<tr>
<td>$X$</td>
<td>$X_1$</td>
<td>$X_2$</td>
<td>$X_3$</td>
<td>$X_4$</td>
<td>$X_5$</td>
<td>$X_6$</td>
<td>$X_7$</td>
<td>$X_8$</td>
</tr>
</tbody>
</table>

---

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$^5$ 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 con-
catenation. Note also that there is much more freedom
in choosing the encoded operation, e.g., the operator
$1 \times I_X \times I_X \times I_X \times I_X \times I_X \times I_X \times I_X = g_2 g_4 g_6 \bar{X}$ is a valid logical $X$
operation. One can easily verify that the generators $g_8$ of
the gauge group generate $P_3$, 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 op-
erations are the same as those of the original code. By ex-
haustive search, we have established that Shor’s code does
admite more that 3 gauge qubits, while the 5-qubit code
and Stean’s 7-qubit code have no gauge symmetry at all.

---

edited by T. P. S. H. K. Lo and S. Popescu (World Scientific,
Singapore, 1999), p. 213.
(1997).
(1997).
81, 2594 (1998).
84, 2525 (2000).
1098 (1996).
(2003).
5188 (2001).
92, 060402 (2004).

---

*Electronic address: dpoulin@iqc.ca*