OPERATOR ALGEBRAIC FORMULATION OF THE STABILIZER FORMALISM FOR QUANTUM ERROR CORRECTION

NATHANIEL JOHNSTON[1], DAVID W. KRIBS[1,2], AND CHING-WEI TENG[1]

Abstract. We give an operator algebraic formulation of the stabilizer formalism for error correction in quantum computing. The approach relies on an analysis of commutant structures, and gives a natural extension of the classic stabilizer formalism to the general case of arbitrary (not necessarily abelian) Pauli subgroups and subsystem codes. We show how to identify the largest stabilizer subsystem for every Pauli subgroup and discuss examples.

1. Introduction

The classic stabilizer formalism of Gottesman [**1, 2**] provides the simplest technique to generate codes for the standard model of error correction (QEC) in quantum computing [**3, 4, 5, 6**]. Recently the formalism was extended by Poulin [**7**] to the case of subsystem codes in "operator quantum error correction" (OQEC) [**8, 9**]. An important subsystem refinement of Shor's 9-qubit stabilizer code [**3**] was recently discovered by Bacon [**10**], and also elucidated by Poulin [**7**]. The so-called "Bacon-Shor code" has now been used by Aliferis-Cross [**11**] to improve the crucial threshold theorem for fault-tolerant quantum computation.

The mathematical starting point for the classic stabilizer formalism is an abelian subgroup of the n-qubit Pauli group. There are a number of naïve and natural questions that can be asked, such as: Does there exist an extension of the stabilizer formalism that begins with an arbitrary (not necessarily abelian) subgroup of the Pauli group? If so, how does it relate to Poulin's extension? Moreover, is there an operator algebraic formulation of the stabilizer formalism? In this paper we present a natural subsystem extension of the stabilizer formalism that starts with an arbitrary Pauli subgroup. The operator algebraic approach we take may be viewed as complementary to Poulin's, in that

Draft, April 17 2007.

the same subsystem codes are obtained from a different perspective. In particular, we argue that this affirms the subsystem generalization of [**7**] is indeed the "right" generalization of the stabilizer formalism to arbitrary Pauli subgroups. Intuitively, the approach allows the "gauge freedom" of stabilizer subsystem codes to be injected at an earlier stage in the process. Formally, stabilizer subsystems are obtained via the operator commutant structure of Pauli subgroups.

The operator algebra approach has the advantage that it yields a simple way to generate stabilizer subsystem codes. However, it has the drawback that more complicated Pauli groups must be considered throughout the analysis in contrast to the original formulation. Nevertheless, we derive a conceptual technique to identify the largest stabilizer subsystem of a Pauli subgroup in terms of the structure of its largest abelian subgroup. We also discuss examples.

Our goals in presenting this article are two-fold: We feel that the quantum computing community will benefit from having this complementary perspective on the stabilizer formalism. Moreover, we believe the perspective is an inviting one for mathematicians, and in particular for those in operator algebras and representation theory. For these reasons the article has been written with an introductory flavour.

2. Error Correction and Operator Algebras

Noise in the context of quantum computing is modelled by completely positive trace-preserving maps (i.e., quantum operations), and in QEC error-correcting codes take the form of subspaces [**12**]. Quantum codes form linearly closed sets since, in contrast to classical computing, linear combinations of code words are physically viable (corresponding to superpositions of classical states). For experimental reasons we primarily focus on finite-dimensional Hilbert space $\mathcal{H} = \mathcal{H}^V$, representing a quantum system V with finitely many degrees of freedom. Thus a noise model $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ is determined by a set of *error operators* $\{E_a\}$ on $\mathcal{H}$ such that $\mathcal{E}(\sigma) = \sum_a E_a \sigma E_a^\dagger$ for all $\sigma \in \mathcal{B}(\mathcal{H})$. As a convenience we write $\mathcal{E} = \{E_a\}$.

More generally, quantum information can be encoded into subsystems of $\mathcal{H}$. A quantum system B represented on a Hilbert space $\mathcal{H}^B$ is a *subsystem* of $\mathcal{H}$ if there is another quantum system A such that $\mathcal{H} = (\mathcal{H}^A \otimes \mathcal{H}^B) \oplus (\mathcal{H}^A \otimes \mathcal{H}^B)^\perp$. We shall regard $\mathcal{H}^B$ as containing the encoded states for transmission, and $\mathcal{H}^A$ as the associated ancilla.

Thus, B is called a "subsystem code". Observe that the case of subspace codes is captured when $\dim A = 1$. We are of course only interested in cases for which $\dim B \geq 2$, as $\mathcal{H}^B$ encodes $\log(\dim B)$ logical qubits in general.

Definition 2.1. *A subsystem code B is correctable for a noise map $\mathcal{E}$ if there is a quantum operation $\mathcal{R} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ such that $\forall \sigma^A \in \mathcal{B}(\mathcal{H}^A)$, $\forall \sigma^B \in \mathcal{B}(\mathcal{H}^B)$, $\exists \tau^A \in \mathcal{B}(\mathcal{H}^A)$:*

$$\big(\mathcal{R} \circ \mathcal{E}\big)(\sigma^A \otimes \sigma^B) = \tau^A \otimes \sigma^B. \tag{1}$$

This is the definition from [**8, 9**] of an OQEC error-correcting subsystem. A correctable subspace code in QEC is captured when $\dim A = 1$. It is important to note that an operation $\mathcal{R}$ which corrects B for a noise map $\mathcal{E} = \{E_a\}$, also corrects B for all noise models whose error operators are linear combinations of the E_a.

If B is a correctable subsystem for $\mathcal{E}$, then observe that the C*-algebra $\mathcal{A}_B = I^A \otimes \mathcal{B}(\mathcal{H}^B)$ is perfectly correctable for $\mathcal{E}$. Indeed, if Eq. (1) is satisfied, then there is a τ^A (which only depends on I^A and $\mathcal{E}$) such that $(\mathcal{R}\circ\mathcal{E})(I^A\otimes\sigma^B) = \tau^A\otimes\sigma^B$ for all $\sigma^B \in \mathcal{B}(\mathcal{H}^B)$. We can define an operation $\mathcal{R}'$ that simply fixes σ^B and depolarizes the A subsystem, in particular mapping τ^A to I^A. Then we have $((\mathcal{R}'\circ\mathcal{R})\circ\mathcal{E})(\sigma) = \sigma$ for all $\sigma \in \mathcal{A}_B$. Hence, correctability of a subsystem B implies the algebra $\mathcal{A}_B$ is perfectly correctable. In fact, as proved in [**9**], the converse is true.

Proposition 2.2. *A subsystem B is correctable for $\mathcal{E}$ if and only if the algebra $\mathcal{A}_B$ is perfectly correctable for $\mathcal{E}$.*

Thus, the basic framework for quantum error correction can be formulated in operator algebraic language. The operator algebra perspective has recently been used in [**13**] as part of a generalization of the entire framework to arbitrary finite-dimensional C*-algebras and the correction of hybrid classical and quantum information.

The following result from [**8, 9, 14**] gives testable conditions for correction of a subsystem in terms of the error operators. Here we have added the operator algebraic condition (iii).

Theorem 2.3. *The following conditions are equivalent for a subsystem B and noise map $\mathcal{E} = \{E_a\}$:*

(i) *B is correctable for $\mathcal{E}$.*

(ii) *Let* $P_{AB} = I^A \otimes I^B$. *For all* a, b, *there is an operator* $F_{ab} \in \mathcal{B}(\mathcal{H}^A)$ *such that*

$$P_{AB}\, E_b^\dagger E_a\, P_{AB} = F_{ab} \otimes I^B. \tag{2}$$

(iii) *For all* a, b, *the operator* $P_{AB}E_b^\dagger E_a P_{AB}$ *belongs to the compressed commutant* $P_{AB}(I^A \otimes \mathcal{B}(\mathcal{H}^B))' P_{AB}$.

3. Stabilizer Formalism For Pauli Subgroups

We begin with a brief description of the framework for the classic (subspace) stabilizer formalism, emphasizing an operator commutant perspective, and then segue into the subsystem generalization.

Given a positive integer $n \geq 1$, consider n-qubit Hilbert space $\mathcal{H} = \mathbb{C}^{2^n} = (\mathbb{C}^2)^{\otimes n}$. A fixed basis $\{|0\rangle, |1\rangle\}$ for $\mathbb{C}^2$ yields a "computational basis" for $\mathcal{H}$ with elements $|i_1 i_2 \cdots i_n\rangle = |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle$ such that $i_j = 0$ or 1. The unitary Pauli operators on $\mathbb{C}^2$ have matrix representations in the basis $\{|0\rangle, |1\rangle\}$ given by

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3}$$

Let I_2 be the identity operator on $\mathbb{C}^2$. Any operator X on $\mathbb{C}^2$ defines operators on $\mathcal{H}$ denoted by $X_1, \ldots, X_n$, where $X_1 = X \otimes I_2 \otimes \ldots \otimes I_2$, etc. For simplicity we shall sometimes write $XI \cdots I$ for such an operator. The n-qubit Pauli group $\mathcal{P}_n$ is the subgroup of the unitary group on $\mathcal{H}$ generated by X_j, Y_j, Z_j, $j = 1, \ldots, n$, and the scalar matrix iI, and it plays a central role in quantum computing. In the context of quantum error correction operators inside $\mathcal{P}_n$ are interpreted as errors. For instance, X corresponds to the natural extension of the classical bit flip error to the quantum case. See [**17**] for a more complete discussion.

Let S be an abelian subgroup of the Pauli group $\mathcal{P}_n$ for which there exists a common multidimensional eigenspace $\mathcal{V}_S$. Because of the symmetries involved, without loss of generality we may assume that $\mathcal{V}_S$ is an eigenvalue-1 eigenspace for elements of S; that is, $M|\psi\rangle = |\psi\rangle$ $\forall M \in S$, $\forall |\psi\rangle \in \mathcal{V}_S$. In quantum computing, such subspaces are often called "decoherence-free subspaces" [**12**]. As elements of $\mathcal{P}_n$ either commute or anti-commute, it follows that $-I \notin S$, and so as a convenience we assume S is generated by $Z_1, \ldots, Z_k$ for some $k \geq 1$. The subspace $\mathcal{V}_S$ is a quantum code that encodes $\log \mathcal{V}_S$ logical qubits. The code is correctable, in the sense of QEC, for errors belonging to either S or the complement of the centralizer of S inside $\mathcal{P}_n$ [**2, 17**].

The focus on abelian subgroups of $\mathcal{P}_n$ in the context of the QEC case is, in retrospect, no accident. Such subgroups typically do have joint eigenspaces. In fact, if S is generated by $n-k$ independent elements, say $Z_1, \ldots, Z_{n-k}$ for instance, then $\mathcal{V}_S$ is 2^k-dimensional and encodes k logical qubits. Indeed, it is spanned by the vectors $\{|0\rangle^{\otimes n-k}|i_1 \cdots i_k\rangle : i_j = 0, 1\}$. On the other hand, this is not the case for non-abelian subgroups of $\mathcal{P}_n$. In particular, any Pauli group that contains two elements which anti-commute also contains $-I$, and thus has no joint eigenvalue-1 space. In fact, a non-abelian Pauli group has no non-trivial joint eigenspaces.

An attempt to extend the stabilizer formalism to the case of arbitrary (not necessarily abelian) Pauli groups naturally leads one to subsystem codes. The first step is to recognize how the subspace case arises from a different perspective. The commutant S' of a set of operators S is defined as the set of operators that commute with each element of S. In the case of a Pauli group, this set forms a C*-algebra that induces a decomposition of $\mathcal{H}$ as $\mathcal{H} = \oplus_k (\mathcal{H}^{A_k} \otimes \mathcal{H}^{B_k})$ such that with respect to this decomposition the operators of S' take the form

$$S' = \bigoplus_k \left(I^{A_k} \otimes \mathcal{B}(\mathcal{H}^{B_k}) \right), \tag{4}$$

and hence elements of S belong to

$$S \subseteq S'' = \mathrm{Alg}\{S\} = \bigoplus_k \left(\mathcal{B}(\mathcal{H}^{A_k}) \otimes I^{B_k} \right). \tag{5}$$

We shall write $\mathcal{M}_m \otimes I_n$ for $\mathcal{B}(\mathcal{H}^A) \otimes I^B$, where $\dim A = m$ and $\dim B = n$, when an orthonormal basis for $\mathcal{H}^A \otimes \mathcal{H}^B$ has been identified that yields this matrix form. The commutant of a set of operators may be computed directly, and there is computational software available for this purpose.

Now consider an abelian subgroup S of $\mathcal{P}_n$ as above, with joint stabilizer space $\mathcal{V}_S$. As $M = M^\dagger \ \forall M \in S$, we have $M|\psi\rangle = |\psi\rangle = M^\dagger|\psi\rangle$ $\forall |\psi\rangle \in \mathcal{V}_S$. Thus,

$$M|\psi\rangle\langle\phi| = |\psi\rangle\langle\phi| = |\psi\rangle(M^\dagger|\phi\rangle)^\dagger = |\psi\rangle\langle\phi|M. \tag{6}$$

It follows that the algebra $\mathcal{B}(\mathcal{V}_S)$ is contained in S'. Hence, stabilizer subspace codes for S can be obtained through an analysis of the commutant S'. Moreover, the Spectral Theorem and its associated functional calculus can be applied jointly to the elements of S to show that the commutant structure of S' is entirely determined by such subspaces; that is, $\dim A_k = 1$ for all k in Eq. (4). In particular, there is no genuine subsystem structure induced on the system Hilbert space

$\mathcal{H}$ from this commutant, there is only a sub*space* splitting of $\mathcal{H}$. This scenario is exclusive to the case of abelian subgroups.

On the other hand, consider a non-abelian subgroup S of $\mathcal{P}_n$. In this case the commutant S' still has the general form given in Eq. (4), but now there will be k such that $\dim A_k > 1$, and thus we have bona fide subsystems. The discussion below motivates the following definition.

Definition 3.1. *Given a Pauli subgroup S, we say the subsystems B_k in Eq. (4) are* stabilizer subsystems *for S.*

Let g be an element of S. Then Eq. (5) gives us operators $g^{A_k} \in \mathcal{B}(\mathcal{H}^{A_k})$ such that $g = \oplus_k g^{A_k} \otimes I^{B_k}$. For the moment fix k and put $A_k = A$, $B_k = B$. If we take an arbitrary σ^A and σ^B, then

$$g(\sigma^A \otimes \sigma^B) = g^A \sigma^A \otimes \sigma^B \quad \text{and} \quad (\sigma^A \otimes \sigma^B)g = \sigma^A g^A \otimes \sigma^B. \tag{7}$$

In this sense, the subsystem B is stabilized by the action of G. From another perspective, such subsystems are called "noiseless subsystems" [**12**] for the elements of G.

In fact, if g_a, g_b belong to S (and recalling that $P_{AB} = I^A \otimes I^B$) we see that

$$P_{AB} g_a^\dagger g_b P_{AB} = (g_a^A)^\dagger (g_b) \otimes I^B. \tag{8}$$

Thus the following result is an immediate consequence of Theorem 2.3.

Proposition 3.2. *Let B be a stabilizer subsystem for a Pauli group S. Let $\mathcal{E} = \{E_a\}$ be a quantum operation such that each E_a is a linear combination of elements from S. Then B is a correctable subsystem for $\mathcal{E}$.*

Remark 3.3. There is an important aspect of stabilizer subsystems that does not arise for stabilizer subspaces. In general, if B is a correctable subsystem for $\mathcal{E}$, then it is easy to see that for all states $|\alpha\rangle \in A$, the subspace code $|\alpha\rangle \otimes B$ is also correctable for $\mathcal{E}$. However, if S is non-abelian and B is a subsystem (but not subspace) stabilizer code for S, then *no* subspace of the form $|\alpha\rangle \otimes B$ can be a stabilizer subspace for S (even though each such subspace is still correctable for error models from S). Indeed, as noted above non-abelian S do not have stabilizer subspaces. From another perspective in quantum error correction, this is a consequence of the fact that if B is a noiseless subsystem for an error model $\mathcal{E}$, then any subspace of the form $|\alpha\rangle \otimes B$ will be correctable for $\mathcal{E}$, but typically it will not be a decoherence-free subspace (and hence requires a non-trivial correction operation). It should be noted, however, that there are many cases in which the existence of

a subsystem code implies the existence of a classic stabilizer code with comparable features [**16**].

We conclude this section with an illustrative two-qubit example.

Example 3.4. If $S =< ZI >= \{ZI, II\}$, then $S' = \mathcal{M}_2 \oplus \mathcal{M}_2$ and the associated decomposition of two-qubit space is $\mathbb{C}^4 = B_1 \oplus B_2$ where $B_1 = \text{span}\{|00\rangle, |01\rangle\}$ and $B_2 = \text{span}\{|10\rangle, |11\rangle\}$. The subspace B_1 (and its symmetric counterpart B_2) is the simplest example of a stabilizer subspace code.

Consider now the non-abelian Pauli subgroup

$$S =< ZI, XX >= \{\pm ZI, \pm XX, \pm I, \pm iYX\}.$$

One can check by direct calculation that with respect to the standard ordered basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, we have

$$S' = \left\{ \begin{pmatrix} \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} & 0 \\ 0 & \begin{smallmatrix} d & c \\ b & a \end{smallmatrix} \end{pmatrix} : a, b, c, d \in \mathbb{C}^2 \right\} \cong I_2 \otimes \mathcal{M}_2. \tag{9}$$

The controlled-NOT operator $U = I_2 \oplus X$ is a unitary that induces the unitary equivalence $S' \cong I_2 \otimes \mathcal{M}_2$. Thus a single-qubit stabilizer subsystem for S is identified with the second sector of the new tensor structure $\mathbb{C}^4 = A \otimes B = \text{span}\{|i'_1 i'_2\rangle\}$ given by $|0'0'\rangle \equiv |00\rangle$, $|0'1'\rangle \equiv |01\rangle$, $|1'0'\rangle \equiv |11\rangle$, $|1'1'\rangle \equiv |10\rangle$.

Remark 3.5. The stabilizer formalism for OQEC as introduced by Poulin in [**7**] is arrived at from a perspective different from that presented here. In particular, abelian Pauli groups associated with known stabilizer codes are considered first, then subsystem structure is discerned within the code. Nevertheless, the stabilizer subsystem codes that can be found through the above approach coincide with the codes discovered through the approach of [**7**]. This is one consequence of Theorem 4.1 below; namely, stabilizer subsystems for arbitrary Pauli groups still depend in an explicit way on the structure of maximal abelian subgroups.

4. Largest Stabilizer Subsystem for a Pauli Subgroup

The discussion of the previous section shows that the problem of identifying stabilizer subsystems for Pauli groups is equivalent to explicitly computing commutant structures for such groups. There is of course computer software that can be used for this purpose. However, a conceptual technique for determining this structure in terms of the group's properties, and in particular the largest subsystem available

for encoding, is highly desirable. In this section we derive such a result. Some thought reveals Theorem 4.1 to be quite intuitive, though explicitly proving it is somewhat delicate.

A key result in the classic case is that the commutant of an abelian Pauli group, with k elements in a minimal generating set, includes a maximal stabilizer subspace of dimension 2^k. The following may be regarded as a generalization of this result to the case of arbitrary Pauli groups. Note that every non-abelian group G contains the elements $\pm I$ (in fact this property determines non-abelianality for Pauli groups). As the phase factors $\mathcal{I} = \{\pm I, \pm iI\}$ do not effect commutant structure, to streamline the presentation we shall assume G contains $\mathcal{I}$.

Theorem 4.1. *Let $G = G \cup \mathcal{I}$ be a subgroup of $\mathcal{P}_n$. Let $S_0 = \mathcal{I} \cup \{g_1, \ldots, g_m\}$ be a minimal generating set for a maximal abelian subgroup S of G. Then the commutant G' contains a subalgebra isomorphic to $\mathcal{M}_r$, where $r = 2^{n-m}$, and this is the largest matrix algebra that can be imbedded into G'. In other words, there is a stabilizer subsystem for G that encodes $n - m$ logical qubits, and this is optimal.*

To prove the theorem we shall derive a number of ancillary results on Pauli subgroups. As noted above, the abelian special case of this result is a central starting point for the classic stabilizer formalism. Here we state it in operator algebraic language.

Lemma 4.2. *Let S be generated by $\{Z_1, \ldots, Z_m\}$ for some $1 \leq m \leq n$. Then the commutant S' is unitarily equivalent to the algebra direct sum $S' \cong \mathcal{M}_r^{(2^m)}$, where $r = 2^{n-m}$.*

Proof. The operators $\frac{I \pm Z_j}{2}$ project onto the ± 1 eigenspaces for Z_j. It follows that the projections $P_x = \prod_{j=1}^m \frac{I + (-1)^{x_j} Z_j}{2}$, for $x = (x_1, \ldots, x_m) \in \mathbb{Z}_2^m$, are mutually orthogonal, sum to the identity, and are the same rank (which is necessarily 2^{n-m}). They also span the algebra $\mathrm{Alg}(S)$ generated by S. Hence the stated form for S' is evident. ∎

The next result quantifies the size of minimal generating sets for Pauli groups. It relies on a straightforward combinatorial argument based on properties of the Pauli group.

Lemma 4.3. *Let G be a subgroup of $\mathcal{P}_n$. Then $|G| = 2^{k+2}$ if and only if G is minimally generated by a set $G_0 \supseteq \mathcal{I}$ such that $|G_0 \setminus \mathcal{I}| = k$.*

Proof. Sufficiency follows readily from the fact that the $4 \cdot 2^k$ elements obtained from products of elements from G_0 are distinct. To see necessity, one can proceed inductively by first letting G_1 be a subgroup of $\mathcal{P}_n$

with $|G_1| = 2^{r+2}$, such that G_1 is minimally generated by r non-phase factor elements of $\mathcal{P}_n$. Then let G_2 be a subgroup of $\mathcal{P}_n$ that contains G_1 such that $|G_2| = 2^{r+3}$. Clearly there must be at least $r+1$ generators for G_2, but simply by choosing an element belonging to $G_2 \setminus G_1$, one can check that a generating set for G_2 is obtained consisting of this element and the generators for G_1. ■

Given a group G and an element $g \in G$, we denote the centralizer of g inside G by $C(g) = \{h \in G : [h, g] = 0\}$. Of course, the centralizer of any element inside an abelian group is equal to the entire group, whereas the same is not true inside non-abelian groups.

Lemma 4.4. *Let G be a non-abelian subgroup of $\mathcal{P}_n$ such that $|G| = 2^{k+2}$. Let g be an element of G that anti-commutes with some element of G. Then $|C(g)| = 2^{k+1}$.*

Proof. First assume that $|C(g)| < 2^{k+1}$. Then there exist $2^{k+1} + 1$ elements $g_i \in G$ that anti-commute with g. In particular, observe that g commutes with all products $g_i g_j$. For a fixed i the elements $g_i g_j$ are distinct, and hence there are at least $2^{k+1} + 1$ distinct elements $g_i g_j$. Thus, g commutes with at least $2^{k+1} + 1$ elements of G, which yields a contradiction since $|G| = 2^{k+2}$ by hypothesis. It follows that $|C(g)| \geq 2^{k+1}$.

Since $C(g)$ is a subgroup of G and $|G| = 2^{k+2}$, if $|C(g)| > 2^{k+1}$, then necessarily we would have $C(g) = G$. But this would be a contradiction as g anti-commutes with at least one element of G by hypothesis. The result follows. ■

The following result gives information on the size of abelian subgroups of Pauli groups.

Lemma 4.5. *Let G be a subgroup of $\mathcal{P}_n$ such that $|G| = 2^{k+2}$. Then there exists an abelian subgroup S of G such that $|S| \geq 2^{(k/2)+2}$.*

Proof. The result is immediate if G is abelian, so assume this is not the case.

We may construct the group S inductively as follows. Set $r = 1$ and $G_r = G$. Let g be an element of G_r that does not commute with all of G_r. Then $|C(g)| = 2^{k-r+2}$ by Lemma 4.4. If $C(g)$ is abelian, set $S = C(g)$ and stop. If $C(g)$ is not abelian, set $r = r + 1$ and set $G_r = C(g)$. Repeat this process until $C(g)$ is abelian. As G is a finite group the process will eventually terminate.

It remains to show that the above procedure terminates with $r \leq k/2$. (Note that if $k = 1$, the group G was abelian to begin with, so we make the convention in such a situation that $r = 0$.) To see why this is the case, we consider the above procedure in terms of the generators of G_r. Let $S_r = \mathcal{I} \cup \{g_1, \ldots, g_{k-r}\}$ be a minimal set of generators for G_r, given by Lemma 4.3. When Lemma 4.4 is applied to G_r, we see that G_{r+1} is a subgroup of G_r such that $|G_{r+1}| = \frac{1}{2}|G_r|$. Hence G_{r+1} has a minimal generating set with exactly one less generator than G_r by Lemma 4.3. But note that the element used in this application of Lemma 4.4 for G_r could be a generator of G_{r+1}, as can any generator g_j of G_r that commuted with all of G_r. Thus, G_{r+1} has one less generator than G_r, but one more generator that commutes with the whole group.

Therefore, the generating set of G_r will be abelian after no more than $k/2$ iterations of this process, since each iteration results in a group that is generated by a set with two fewer elements that anti-commute with some element of the group. (If k is odd, we make use of the fact that any group generated by a single element will be abelian.) Thus, following the above process we can construct an abelian subgroup S of G with the desired property. ■

Finally, we shall make use of the following structural result on the size of intersected Pauli groups.

Lemma 4.6. *Let G and H be subgroups of $\mathcal{P}_n$ such that $|G| = 2^a$ and $|H| = 2^b$. Then $|G \cap H| \geq 2^{a+b-2n-2}$.*

Proof. We shall proceed by fixing G and inducting downwards on b. The base case $b = 2n + 2$ trivially follows since H is equal to $\mathcal{P}_n$.

Now assume the result holds for $b = r$. As in Lemma 4.3, we can add elements to a generating set of $G \cap H$ to obtain a generating set of either G or H. Suppose $|G \cap H| = 2^p$, so Lemma 4.3 implies that a minimal generating set F_0 for $G \cap H$ has at least $p - 2$ elements in addition to $\mathcal{I}$. By Lemma 4.3, G and H have minimal generating sets of $a - 2$ and $r - 2$ elements respectively, again excluding $\mathcal{I}$. Thus, we can find elements g_i and h_j such that the sets $G_0 = F_0 \cup \{g_1, \ldots, g_{a-p}\}$ and $H_0 = F_0 \cup \{h_1, \ldots, h_{r-p}\}$ generate G and H.

If we remove one generator of H and call the new group generated H_1, there are two cases to consider. If we were to remove one of the h_j, the size of H would be reduced by a factor of 2 by Lemma 4.3. Note, however, that the size of $G \cap H$ would be unaffected. If instead we were to remove one of the non-$\mathcal{I}$ elements of F_0, again by Lemma 4.3 the size of both H and $G \cap H$ would be reduced by a factor of 2. Either

way, since $p \geq a + r - 2n - 2$ from the induction hypothesis, it follows that $|G \cap H_1| \geq 2^{a+r-2n-3}$. This completes the proof since $|H_1| = 2^{r-1}$. ■

Proof of Theorem 4.1. By Lemma 4.5 we have $|S| \geq 2^{(k/2)+2}$, which by Lemma 4.3 implies that $m \geq k - m$. As in Lemma 4.3, there exists $P_1, \ldots, P_{k-m} \in \mathcal{P}_n$ such that $G_0 = S_0 \cup \{P_1, \ldots, P_{k-m}\}$ is a minimal generating set for G. We may now find a unitary U in the "Clifford group" (which is the normalizer group of $\mathcal{P}_n$ inside the group of all unitaries on n qubits) such that each $Ug_jU^\dagger = Z_j$ and each $UP_iU^\dagger$ belongs to $\mathcal{P}_n$. Hence, without loss of generality we shall assume each $g_j = Z_j$. Thus, it follows that the commutant G' is given by

$$G' = \{Z_1, \ldots, Z_m\}' \bigcap \cap_{j=1}^{k-m} \mathrm{Alg}(C(P_j)), \tag{10}$$

where $C(P_j)$ is the centralizer of P_j inside $\mathcal{P}_n$.

By Lemma 4.2, the algebra G' is a subalgebra of $\mathcal{M}_r^{(2^m)}$, where $r = 2^{n-m}$. Hence the largest full matrix algebra that can possibly be imbedded inside G' is $\mathcal{M}_r$. We complete the proof by showing that there is indeed such an imbedding.

The case of an abelian group G is covered by Lemma 4.2, so assume G is non-abelian, and in particular that $k > m$. By Lemma 4.4 we have $|C(P_j)| = 2^{2n+1}$ for each j. Let $H_0 = \mathcal{I} \cup \{Z_1, \ldots, Z_n, X_{m+1}, \ldots, X_n\}$ and let H be the group generated by H_0. Then

$$\mathrm{Alg}(H_0) = \{Z_1, \ldots, Z_m\}' \cong \mathcal{M}_r^{(2^m)}. \tag{11}$$

Thus, we have

$$\begin{aligned} G' &= \mathrm{Alg}(H_0) \bigcap \cap_{j=1}^{k-m} \mathrm{Alg}(C(P_j)) \\ &= \mathrm{Alg}\left(W \bigcap \cap_{j=1}^{k-m} C(P_j)\right) \end{aligned}$$

But Lemma 4.6 shows that the intersection $H \cap C(P_j)$ is a subgroup of $\mathcal{P}_n$ of size at least $2^{(2n-m+2)+(2n+1)-2n-2} = 2^{2n-m+1}$. Similarly, by repeatedly applying the lemma we see that $H \cap C(P_1) \cap \ldots \cap C(P_{k-m})$ is a subgroup of $\mathcal{P}_n$ of size at least 2^{2n-k+2}. By Lemma 4.4 and Lemma 4.3, for each i there is exactly one Z_j, $1 \leq j \leq m$, such that Z_j does not belong to $C(P_i)$. Thus, at each stage of intersecting H with subsequent $C(P_i)$ we can choose to remove a Z_j, $1 \leq j \leq m$, from H_0 (if a generator needs to be removed to preserve a minimal set) and leave the rest of the generating set the same. This, combined with the fact that $k - m \leq m$,

shows that

$$G' \supseteq \text{Alg}\{Z_{m+1}, \ldots, Z_n, X_{m+1}, \ldots, X_n\}. \tag{12}$$

This subalgebra is easily seen to be unitarily equivalent to the algebra $I_s \otimes \mathcal{M}_r$, where $r = 2^{n-m}$ and $s = 2^m$, and the result follows. ■

Example 4.7. The non-abelian Pauli group $G = < ZI, XX >$ of Example 3.4 provides the simplest example of a bona fide stabilizer subsystem. A maximal abelian subgroup of G is given by $S = < ZI >$, and here we have $m = 1$, $n = 2$. Thus we are told by Theorem 4.1 that G has a single qubit stabilizer subsystem and that this is optimal, or, equivalently, the algebra $\mathcal{M}_2$ is the largest full matrix algebra that can be imbedded into the commutant G'. Indeed, this is the case, as the earlier calculation showed that $G' \cong I_2 \otimes \mathcal{M}_2$.

Example 4.8. We conclude by showing how Bacon's important subsystem refinement [**10**] of Shor's 9-qubit code [**3**] can be seen from the commutant perspective. We adopt Poulin's characterization of the code from [**7**].

The Bacon-Shor code defines a single qubit subsystem of 9-qubit Hilbert space with a 4-qubit ancilla. In our earlier notation, B is 2-dimensional, A is 2^4-dimensional, and together $A \otimes B$ defines a 2^5-dimensional subspace of 2^9-dimensional Hilbert space. The algebra $I^A \otimes \mathcal{B}(\mathcal{H}^B) \cong I_{2^4} \otimes \mathcal{M}_2$ corresponds to a simple subalgebra of the commutant G' of the Pauli group with the twelve generators given in the following table:

g_1	X	X	X	X	X	X	I	I	I
g_2	X	X	X	I	I	I	X	X	X
g_3	Z	Z	I	Z	Z	I	Z	Z	I
g_4	I	Z	Z	I	Z	Z	I	Z	Z
g_5	I	Z	Z	I	I	I	I	I	I
g_6	I	I	I	I	Z	Z	I	I	I
g_7	Z	Z	I	I	I	I	I	I	I
g_8	I	I	I	Z	Z	I	I	I	I
g_9	I	I	X	I	I	I	I	I	X
g_{10}	I	I	I	I	I	X	I	I	X
g_{11}	X	I	I	I	I	I	X	I	I
g_{12}	I	I	I	X	I	I	X	I	I

We can easily see from Theorem 4.1 that the commutant G' encodes a qubit stabilizer subsystem. Indeed, by inspection we observe that the

elements $\{g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8\}$ generate a maximal abelian subgroup of G. Thus, here we have $n = 9$ and $m = 8$, and Theorem 4.1 shows that $\mathcal{M}_2$ can be imbedded into G'.

See **[10, 7, 11]** for details on the remarkable error-correcting properties of this code. Also see **[15, 16]** for a detailed analysis of subsystem codes from a coding theory perspective.

Acknowledgements. We thank Monica Cojocaru, Daniel Gottesman, Andreas Klappenecker, and David Poulin for helpful discussions. N.J. was supported by an NSERC undergraduate research award and C.-W.T. was supported by a UofG graduate research award. D.W.K. was partially supported by ERA, NSERC, CFI and OIT, and is grateful for kind hospitality of the Banff International Research Station, workshops 06w5027 and 07w5119.

References

[1] D. Gottesman, *Class of quantum error correcting codes saturating the quantum Hamming bound*, Phys. Rev. A **54** 1862 (1996).
[2] D. Gottesman, *Stabilizer codes and quantum error correction*, Ph.D. thesis, California Institute of Technology, Pasadena, CA (1997).
[3] P. W. Shor, *Scheme for reducing decoherence in quantum computer memory*, Phys. Rev. A **52**, R2493 (1995).
[4] A. M. Steane, *Error correcting codes in quantum theory*, Phys. Rev. Lett. **77**, 793 (1996).
[5] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Mixed state entanglement and quantum error correction*, Phys. Rev. A **54**, 3824 (1996).
[6] E. Knill and R. Laflamme, *A theory of quantum error-correcting codes*, Phys. Rev. A **55**, 900 (1997).
[7] D. Poulin, *Stabilizer formalism for operator quantum error correction*, Phys. Rev. Lett.,**95**, 230504 (2005).
[8] D. Kribs, R. Laflamme and D. Poulin, *Unified and generalized approach to quantum error correction*, Phys. Rev. Lett.,**94**, 180501 (2005).
[9] D. W. Kribs, R. Laflamme, D. Poulin and M. Lesosky, *Operator quantum error correction*, Quantum Inf. & Comp.,**6** (2006), 382-399.
[10] D. Bacon, *Operator quantum error correcting subsystems for self-correcting quantum memories*, Phys. Rev. A,**73**, 012340 (2006).
[11] P. Aliferis and A. W. Cross, *Subsystem fault tolerance with the Bacon-Shor code*, quant-ph/0610063.
[12] D. W. Kribs, *A quantum computing primer for operator theorists*, Lin. Alg. Appl.,**400** (2005), 147-167.
[13] C. Beny, A. Kempf and D. W. Kribs, *Generalization of quantum error correction via the Heisenberg picture*, Phys. Rev. Lett.,**98**, 100502 (2007).
[14] M. A. Nielsen and D. Poulin, *Algebraic and information-theoretic conditions for operator quantum error-correction*, e-print quant-ph/0506069.

[15] A. Klappenecker and P. K. Sarvepalli, *Clifford code constructions of operator quantum error correcting codes*, quant-ph/0604161.
[16] S. A. Aly, A. Klappenecker and P. K. Sarvepalli, *Subsystem codes*, quant-ph/0610153.
[17] M. A. Nielsen and I. L. Chuang, *Quantum Computation & Quantum Information*, Cambridge University Press, (2000).

[1]Department of Mathematics and Statistics, University of Guelph, Guelph, Ontario, Canada N1G 2W1

[2]Institute for Quantum Computing, University of Waterloo, Waterloo, ON, CANADA N2L 3G1