QEC Book

David W. Kribs
Department of Mathematics and Statistics, University of Guelph, ON, Canada
dkribs@uoguelph.ca

David Poulin
Département de Physique, Université de Sherbrooke, QC, Canada
David.Poulin@USherbrooke.ca

Contents

1

Operator Quantum Error Correction

1.1 Introduction

In this chapter we review the basic theory of operator quantum error correction (OQEC) and present a selection of applications and examples.

OQEC began with an attempt to bring passive techniques for quantum error correction such as DFS and NS on the one hand, together with standard active quantum error correction (QEC) on the other. Broadly speaking, this meshes two distinct disciplinary approaches to quantum error correction rooted in physics (DFS/NS) and computer science (QEC). Technically the approach involves a generalization of encoding quantum information into *subsystems*; that is, a system B (or A) that arises as a tensor factor $\mathscr{C} = A \otimes B$ of a subspace inside a (potentially) larger system Hilbert space $\mathscr{H} = \mathscr{C} \oplus \mathscr{C}^{\perp}$. Hence, in one sense OQEC may be regarded as a formalization of the *subsystem principle* for encoding quantum information, first elucidated by Knill-Laflamme-Viola. In recognition of this point, often such codes B are now referred to as *subsystem codes*.

The resulting theory has led to significant advances in quantum error correction. Conceptually, the reasons for this include a simplification of recovery procedures, as subsystem codes can be more degenerate than their subspace counterpart, and a simplification of the syndrome measurement that can result. These features of subsystem codes have led to threshold improvements in fault tolerant quantum computing for instance. Additionally, OQEC gives a clean mathematical setting that more readily allows for the application of mathematical tools from operator theory and operator algebras to problems in quantum error correction.

1.1.1 Error avoidance versus error correction

As the terminology suggests, passive quantum error correction, as manifested by DFS and NS, involves finding and then encoding quantum information into sectors of the system Hilbert space that remain immune to the overall noise of a quantum map. It is easy to find simple examples of DFS and NS; in fact highly degenerate codes for Pauli channels obtained in the stabilizer formalism are often passive. An important sophisticated example of the phenomena arises in the noise model that describes photons of light travelling through an optical fibre, wherein the photon polarizations are exposed to random rotation errors. In such "collective noise" channels, there are certain sectors of the Hilbert space where symmetries in the noise exist that prevent decoherence.

Thus, NS and DFS are a form of error avoidance, in contrast to standard active error correction (QEC). OQEC formalizes the distinction between the two settings, while at the same time allowing us to see them as special cases of a general framework. Let us begin with the definition of passive codes in OQEC. Our standing assumption is that we have a subspace $\mathscr{C}$ of a larger Hilbert space $\mathscr{H}$ which has a factoring $\mathscr{C} = A \otimes B$.

Definition 1 *A subsystem code B is a* passive code *for a quantum channel $\mathscr{E}$ if there is a channel $\mathscr{F}_A$ on A such that*

$$\mathscr{E} \circ \mathscr{P}_{\mathscr{C}} = (\mathscr{F}_A \otimes \mathrm{id}_B) \circ \mathscr{P}_{\mathscr{C}}, \tag{1.1}$$

where we define the map $\mathscr{P}_{\mathscr{C}}(\sigma) = P_{\mathscr{C}} \sigma P_{\mathscr{C}}$.

The OQEC notion of NS is captured by this definition in the case that $\dim A > 1$, and DFS when $\dim A = 1$.

The first query one might make is, how often do such codes exist? While they are rather restrictive, it turns out that many noise models do have passive codes. For instance, consider the case of a *unital* channel ($\mathscr{E}(I) = I$) with Kraus operators $\{E_i\}$. Observe that any operator ρ that belongs to the *noise commutant* $\mathscr{A}'$ for $\mathscr{E}$, which is given by $\mathscr{A}' = \{\sigma : [\sigma, A_i] = 0 \, \forall i\}$, satisfies $\mathscr{E}(\sigma) = \sigma \mathscr{E}(I) = \sigma$. Thus, $\mathscr{A}'$ is an algebra contained inside the operator space given by the fixed point set $\mathrm{Fix}(\mathscr{E}) = \{\sigma : \mathscr{E}(\sigma) = \sigma\}$. In fact, a basic result for unital channels shows that the converse is true, $\mathrm{Fix}(\mathscr{E}) = \mathscr{A}'$. Therefore, as a $*$-closed algebra this set induces an orthogonal decomposition of the Hilbert space $\mathscr{H} = \oplus_k (A_k \otimes B_k) \oplus \mathscr{K}$, such that the algebra consists of all operators of the form $\oplus (I_{A_k} \otimes X_k) \oplus 0_{\mathscr{K}}$ where X_k is an arbitrary operator on B_k. It is not hard to see that each subsystem B_k (of dimension at least 2) defines a passive code for $\mathscr{E}$. In fact, it has

been shown that *all* passive codes for a unital channel $\mathscr{E}$ are encoded into the algebra $\mathscr{A}'$ in this way.

No such structure theory exists for arbitrary (not necessarily unital) channels. Nevertheless, we can establish the following testable conditions for passive codes strictly in terms of the Kraus operators for the channel. The result readily follows from the unitary freedom of operator-sum decompositions for completely positive maps.

Proposition 1 *Let $\mathscr{E}$ be a channel on $\mathscr{H}$ with Kraus operators $\{E_i\}$ and let B be a subsystem of $\mathscr{H}$. Then B is a passive code for $\mathscr{E}$ if and only if there exist operators F_i on A such that $E_i P_{\mathscr{C}} = (F_i \otimes I_B) P_{\mathscr{C}}$ for all i.*

Thus, this result provides a test for passivity when a candidate code has been identified. However, actually *finding* passive codes for a given channel (or class of channels) is a much harder problem for which considerable progress has been made. The fixed point results mentioned above show how this may be accomplished in the unital case. The arbitrary case has been addressed elsewhere.

1.1.2 OQEC: basic definition

As a straightforward generalization of the definition for passive subsystem codes above, we arrive at the definition of a general OQEC code.

Definition 2 *A subsystem code B is* correctable *for a quantum channel $\mathscr{E}$ on $\mathscr{H}$ if there are channels $\mathscr{R}$ on $\mathscr{H}$ and $\mathscr{F}_A$ on A such that*

$$\mathscr{R} \circ \mathscr{E} \circ \mathscr{P}_{\mathscr{C}} = (\mathscr{F}_A \otimes \mathrm{id}_B) \circ \mathscr{P}_{\mathscr{C}}. \tag{1.2}$$

In other words, B is correctable for $\mathscr{E}$ if there is a channel $\mathscr{R}$ such that B is a passive code for $\mathscr{R} \circ \mathscr{E}$. In terms of states, this is equivalent to the following quantification:

$$\forall \rho_A \ \forall \rho_B \ \exists \tau_A \quad : \quad (\mathscr{R} \circ \mathscr{E})(\rho_A \otimes \rho_B) = \tau_A \otimes \rho_B, \tag{1.3}$$

where we have written ρ_A for states on A, etc, and $\rho_A \otimes \rho_B$ for the operator on $\mathscr{H}$ given by $(\rho_A \otimes \rho_B) \oplus 0_{\mathscr{C}^\perp}$.

It is evident that passive DFS and NS are captured by the special case in this definition with $\mathscr{R} = \mathrm{id}$ the identity channel. Standard (subspace) QEC is obtained when one focuses on the subsystem codes that can be regarded as subspace codes; that is when the ancilla is trivial $\dim A = 1$. There are a number of other special cases and characterizations that have emerged in subsequent OQEC inspired investigations, including unitarily correctable,

unitarily noiseless, and measurement stabilized codes, as well as an extension of the stabilizer formalism for subsystem codes. Each of these special cases can be justified by operational constraints in the laboratory, or by a desire to understand the theory at a deeper level.

1.2 Equivalent conditions for OQEC

In this section we present a number of characterizations of OQEC codes, ranging from testable conditions in terms of Kraus operators for a given channel, an entirely information theoretic characterization, and a description based in operator algebra and representation theory. The conditions are all equivalent, however they come from very different perspectives. We shall sketch the proofs and point the reader to the original journal articles for full details.

1.2.1 Kraus operator testable conditions

As in QEC, the need for testable conditions in OQEC is obvious. Indeed, the condition Eq. (1.2) for a subsystem code cannot be tested explicitly as it *a priori* involves an uncountable number of conditions; $\forall \rho_A$, etc. Fortunately, also as in QEC and the theorem of Knill-Laflamme, testable conditions for subsystem codes may be derived in terms of Kraus operators.

Theorem 1 *Let $\mathscr{E}$ be a quantum channel on $\mathscr{H}$ with Kraus operators $\{E_i\}$ and let B be a subsystem of $\mathscr{H}$. Then $\mathscr{E}$ is correctable on B if and only if there exist operators F_{ij} on A such that*

$$P_{\mathscr{C}} E_i^\dagger E_j P_{\mathscr{C}} = (F_{ij} \otimes I_B) P_{\mathscr{C}} \quad \forall i, j. \tag{1.4}$$

In the QEC case ($\dim A = 1$) the operators F_{ij} are simply complex scalars that determine a density matrix Λ. One direction of the general subsystem proof is straightforward and essentially the same as QEC: If $\mathscr{R}$ is a correction operation for $\mathscr{E}$ on B with Kraus operators $\{R_k\}$, then by Proposition 1 there are operators G_{ik} on A such that $R_k E_i P_{\mathscr{C}} = (G_{ik} \otimes I_B) P_{\mathscr{C}}$, and we have

$$P_{\mathscr{C}} E_j^\dagger E_i P_{\mathscr{C}} = \sum_k P_{\mathscr{C}} E_j^\dagger R_k^\dagger R_k E_i P_{\mathscr{C}} = (\Big(\sum_k G_{jk}^\dagger G_{ik} \Big) \otimes I_B) P_{\mathscr{C}}.$$

There are multiple ways to establish the other direction, which is more delicate than the proof for QEC. One approach links both of these conditions via a technical result that we will use below, hence we state it for completeness.

Lemma 1 *Let $\mathscr{E}$ be a channel on $\mathscr{H}$ with Kraus operators $\{E_i\}$ and let B be a subsystem of $\mathscr{H}$. The B is correctable for $\mathscr{E}$ if and only if there are unitary operators U_i on $\mathscr{H}$ and mutually commuting positive operators D_i on A such that $\mathscr{E} \circ \mathscr{P}_{\mathscr{C}} = \mathscr{F} \circ \mathscr{P}_{\mathscr{C}}$ where $\mathscr{F}$ is the channel with Kraus operators $\{U_i(D_i \otimes I_B)\}$ and the subspaces $\mathrm{Ran}(D_i) \otimes B$ are mutually orthogonal.*

In the case of QEC, this piece of argument arises in the Knill-Laflamme proof when the code matrix Λ is diagonalized (the positive operators D_i are square roots of probabilities in that case). For general subsystems the proof can be found in [?]. To see how this technical condition implies B is correctable, for each i, let $P_{\mathscr{C}_i}$ be the projection of $\mathscr{H}$ onto the subspace $U_i(\mathrm{Ran}(D_i) \otimes B)$. Then a correction operation $\mathscr{R}$ for $\mathscr{E}$ on B is defined by using the Kraus operators $\{U_i^\dagger P_{\mathscr{C}_i}\}$.

1.2.2 Information-theoretic conditions

In this section, we will derive a set of information theoretic conditions for OQEC. The correlations in a system subject to an open evolution can be drastically affected: existing correlations between the system and an other system can be transferred to the environment, new correlations can be created with the environment, etc. The conditions we will demonstrate in this section set restrictions on these effects that are necessary and sufficient for the existence of a recovery map that will correct a subsystem of the noisy quantum system.

To state these conditions, we introduce three new systems: an environment E and reference systems R_A and R_B for the subsystem A and B respectively. The environment E will be used to purify the quantum map; i.e., the joint evolution of E and S is given by a unitary matrix U_{SE} such that

$$U_{SE}|\psi\rangle_S \otimes |e_0\rangle_E = \sum_a E_a|\psi\rangle_S \otimes |e_a\rangle \tag{1.5}$$

for all $|\psi\rangle_S$. It can be verified as a special case of the Stinespring Theorem [**?**] that such a unitary matrix always exists and that tracing out E reproduces the effect of $\mathscr{E}$ on the state $|\psi\rangle_S$. Thus, the dimension of E is equal to the number of Kraus operators (at most the square of the dimension of S), and it is assumed to be initially in the pure state $|e_0\rangle$.

The reference systems are used to model correlations that the quantum system could have with other systems. To account for all possible such correlations, we assume that A and R_A are initially in a maximally entangled state $|\Phi_A\rangle = \sqrt{\frac{1}{d_A}} \sum_i |i\rangle_A \otimes |i\rangle_{R_A}$, and similarly for B and R_B. Thus, the

dimensions of R_A and R_B are the same as the dimensions of A and B respectively.

The initial state of all these systems is $|\Psi\rangle_{ABR_AR_BE} = |\Phi_A\rangle_{AR_A} \otimes |\Phi_B\rangle_{BR_B} \otimes |e_0\rangle_E$. The purified open evolution transforms this state into

$$|\Psi\rangle'_{ABR_AR_BE} = (U_{SE} \otimes I_{R_AR_B})|\Psi\rangle_{ABR_AR_BE}.$$

We denote the corresponding density matrix $\rho_{ABR_AR_BE}$, and use the appropriate subscripts to denote its marginals obtained by partial trace; e.g. $\rho'_{R_BE} = \mathrm{Tr}_{ABR_A}\{\rho_{ABR_AR_BE}\}$. Similarly, we denote the entropy of a system before or after the application of a map using the associated unprimed or primed letter respectively; e.g. $S(R'_BE') = \mathrm{Tr}\{\rho'_{R_BE} \log \rho'_{R_BE}\}$.

With these definitions in hand, we can state a necessary and sufficient condition for OQEC:

Theorem 2 *Let $\mathscr{E}$ be a quantum channel on $\mathscr{H}$ and let B be a subsystem of $\mathscr{H}$. Then $\mathscr{E}$ is correctable on B if and only if*

$$I(R_B : S) = I(R'_B : S'). \tag{1.6}$$

The mutual information is defined $I(A : B) = S(A) + S(B) - S(AB)$. The mutual information $I(A : B)$ can only decrease under local operations on the two systems. This reflects the fact that we cannot increase the correlations between the two systems without having them interact either directly or indirectly. Thus, the above condition simply states that the system must not lose its correlations with the reference system R_B, and that provided these correlations are kept, the information content of B can be restored.

To prove the theorem, let us expand the mutual information and re-express the condition as

$$S(R_B) + S(S) - S(R_BS) = S(R'_B) + S(S') - S(R'_BS') \tag{1.7}$$
$$\Leftrightarrow \quad S(S) - S(R_BS) = S(S') - S(R'_BS') \tag{1.8}$$
$$\Leftrightarrow \quad S(R_B) = S(S') - S(R'_BS') \tag{1.9}$$
$$\Leftrightarrow \quad S(R'_B) = S(S') - S(R'_BS') \tag{1.10}$$
$$\Leftrightarrow \quad S(R'_B) = S(R'_AR'_BE') - S(R'_BS') \tag{1.11}$$
$$\Leftrightarrow \quad S(R'_B) = S(R'_AR'_BE') - S(R'_AE') \tag{1.12}$$
$$\Leftrightarrow \quad I(R'_B : R'_AE') = 0. \tag{1.13}$$

Here we have used the fact that the reference systems do not evolve, the fact that the global state is pure – which implies that the entropy of one part is equal to the entropy of its complement, and the fact that R_BR_A are initially in a maximally entangled state with S. The conclusion is that after

the evolution, the reference system R_B is not correlated with the reference system R_A and the environment, i.e.,

$$\rho'_{R_A R_B E} = \rho'_{R_B} \otimes \rho'_{R_A E} = \frac{1}{d_B} I_{R_B} \otimes \rho'_{R_A E}. \tag{1.14}$$

It is now straightforward to demonstrate that this condition is necessary and sufficient for B to be correctable. Using the fact that $(M_S \otimes I_{R_A R_B E})|\Psi\rangle_{ABR_A R_B E} = (M^T_{R_A R_B} \otimes I_{ABE})|\Psi\rangle_{ABR_A R_B E}$ for any operator M, we obtain

$$\rho'_{R_A R_B E} = \sum_{ab} (P E_a^T E_b^* P)_{R_A R_B} \otimes |a\rangle\langle b|_E. \tag{1.15}$$

Given this equality, it is easily seen that the condition formulated in Eq. (1.14) is equivalent to the condition Eq. (1.4) that was shown to be necessary and sufficient for B to be correctable in the previous section. We have thus demonstrated that in order for the system B to be correctable, the mutual information between the system and B's reference must not be affected by the quantum map.

1.2.3 Operator algebraic conditions

One reason the result of the previous section is powerful is that it characterizes the OQEC condition strictly in terms of the code and the map itself, without reference to Kraus operators. We next focus on a set of equivalent conditions for OQEC that includes conditions which have this important feature. In addition, it is shown that correction of subsystems is equivalent to the precise correction of certain operator algebras. These conditions are somewhat mathematical in nature, and perhaps because of this they have proved to be particularly useful as tools to establish further results on special classes of OQEC codes. We state the conditions as a single result, and then briefly sketch the proofs. Two notational points first. We shall use notation such as $\mathscr{F}_{A'|A}$ to denote a channel mapping from A to A'. Also, by a representation π of an algebra $\mathfrak{A}$ we mean a linear map that is multiplicative and positive (and hence automatically completely positive) on $\mathfrak{A}$.

Theorem 3 *Let $\mathscr{E}$ be a quantum channel on $\mathscr{H}$ and let B be a subsystem of $\mathscr{H}$. Then the following are equivalent:*

(i) $\mathscr{E}$ is correctable on B.
(ii) The algebra $\mathfrak{A}$ of operators of the form $I_A \otimes \rho_B$ is precisely correctable for $\mathscr{E}$; that is, there is a channel $\mathscr{R}$ such that $\mathscr{R} \circ \mathscr{E}(\sigma) = \sigma$ for all $\sigma \in \mathscr{A}$.

(iii) There is a representation π of $\mathfrak{A}$ on $\mathscr{H}$ such that

$$\mathscr{E}(\rho) = \pi(\rho)\mathscr{E}(P_{\mathscr{C}}) = \mathscr{E}(P_{\mathscr{C}})\pi(\rho) \quad \forall \rho \in \mathfrak{A}. \tag{1.16}$$

(iv) There is a subspace $\mathscr{C}' = A' \otimes B'$ of $\mathscr{H}$ with subsystems A' and $B' \cong B$, a channel $\mathscr{F}_{A'|A}$ and an a unitary channel $\mathscr{V}_{B'|B}$ such that

$$\mathscr{E} \circ \mathscr{P}_{\mathscr{C}} = (\mathscr{F}_{A'|A} \otimes \mathscr{V}_{B'|B}) \circ \mathscr{P}_{\mathscr{C}}. \tag{1.17}$$

Firstly, condition (ii) is *a priori* weaker than demanding that B be correctable. However, the linearity and positivity of the map $\mathscr{E}$ can be used to show that it is in fact sufficient. Simply put, correcting arbitrary states on B when in product with the maximally mixed state on A is equivalent to accomplishing the feat for arbitrary states on A.

With regards to condition (iii), given the unitaries U_i and projections $P_{\mathscr{C}_i}$ from Lemma 1 when B is correctable, we can define a family of partial isometries $V_i = U_i P_{\mathscr{C}}$. It can be verified that the map $\pi(\sigma) = \sum_i V_i \sigma V_i^\dagger$ acts as a representation, and the identity Eq. (1.16) can be directly verified. A similar plan of attack can be used to prove the converse implication. Note that a subtlety imbedded in the proof is that the operator $\mathscr{E}(P_{\mathscr{C}})$ must commute with the range operators of the representation.

It is clear that if condition (iv) is satisfied, then B is correctable for $\mathscr{E}$ with any channel $\mathscr{R}$ such that $\mathscr{R} \circ \mathscr{P}_{\mathscr{C}'} = (\mathscr{G}_{A|A'} \otimes \mathscr{V}_{B'|B}^\dagger) \circ \mathscr{P}_{\mathscr{C}'}$ for some channel $\mathscr{G}_{A|A'}$ as a viable correction channel. Conversely, if B is correctable, Lemma 1 can be used to "splice" together a subsystem pair $\mathscr{C}' = A' \otimes B'$ and isometric map $\mathscr{V}_{B'|B}$ so that condition (iv) is satisfied.

Finally, we note that each of these conditions gives a characterization of correctable subsystem codes in the Schrödinger picture for quantum dynamics (evolution of states). Recent work investigates quantum error correction in the Heisenberg picture (evolution of observables) and makes use of the perspective to extend the theory to infinite-dimensional Hilbert spaces.

1.3 Stabilizer formalism for OQEC

The stabilizer formalism has proven extremely useful for the design of quantum codes. In particular, it establisher a connection between quantum and classical codes, and is particularly well suited for fault-tolerant protocols. In this section, we present a stabilizer formalism for OQEC codes, or subsystem codes.

Let us briefly review the ordinary stabilizer formalism. Although it can be done at a more abstract level, we choose to work with bases because they greatly simplify the presentation. In this language, an ordinary $[[n, k, d]]$

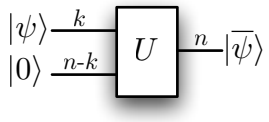

Fig. 1.1. Encoding circuit for QECC

stabilizer code is entirely specified by a canonical basis of the n-qubit Pauli group. We say that a basis of the Pauli group is canonical if its elements can be paired up in such a way that any element of the basis commutes with every other elements except with its partner with which it anti-commutes. For instance, the $2n$ single-qubit operators X_i, Z_i $i = 1, \ldots, n$ form a canonical basis. However, this is not the canonical basis we use to describe a QECC. Instead, we use the following $2n$ basis elements that fall into three categories:

(i) The $2k$ logical operator $\overline{X}_i$ and $\overline{Z}_i$ that obey canonical commutation relations: $\{\overline{X}_i, \overline{Z}_i\} = 0$ and all other pairs commute.
(ii) The $n-k$ stabilizer generators S_j that mutually commute, and commute with all logical operators.
(iii) The $n-k$ pure errors T_j that mutually commute, commute with all logical operators, and are canonically conjugated to the stabilizer generators: $\{S_j, T_j\} = 0$ and $[S_j, T_{j'}] = 0$ for $j \neq j'$.

Because they both form canonical bases, there exists a one-to-one unitary Clifford transformation U that takes the elements of one basis to the other:

$$U : \begin{cases} X_i \to \overline{X}_i & \text{for } i = 1, \ldots k \\ Z_i \to \overline{Z}_i & \text{for } i = 1, \ldots k \\ X_{i+k} \to T_i & \text{for } i = 1, \ldots n-k \\ Z_{i+k} \to S_i & \text{for } i = 1, \ldots n-k \end{cases} . \tag{1.18}$$

This transformation is the encoder for the QECC, i.e., it takes the unencoded k-qubit state $|\psi\rangle$ and additional $n-k$ qubits in the state $|0\rangle$, and produces an encoded state $|\overline{\psi}\rangle$, see Fig. 1.1. Thus, the code space is a 2^k-dimensional subspace of the n-qubit Hilbert that is the common $+1$ eigenspace of the $n-k$ stabilizer generators. Thus, the stabilizer generators act trivially on the code space. The logical operators map the code space to itself in a non-trivial way. Finally, the pure errors map the code space to an orthogonal subspace. More precisely, all $2^{n-k}-1$ distinct non-trivial combinations of the pure errors map the code space to distinct mutually orthogonal subspaces that span the entire Hilbert space.

This choice of basis is motivated by the fact that it simplifies the error

analysis. We can decompose any Pauli errors E in this basis and write $E = \mathscr{L}(E)\mathscr{S}(E)\mathscr{T}(E)$ where $\mathscr{L}(E)$ contains all the logical operators entering in the decomposition of E, similarly $\mathscr{S}(E)$ contains all the stabilizer generators, and $\mathscr{T}(E)$ contains the pure errors. The error syndrome $s(E)$ is an $n-k$-bit string that encodes the commutation relations of the errors with the stabilizer generators: $ES_j + (-1)^{s_j(E)}S_jE = 0$. Because of the canonical commutation relations, the error syndrome is in one-to-one correspondence with the pure error component: $\mathscr{T}(E) = \prod_j T_j^{s_j(E)}$. Thus, the syndrome measurement completely reveals the pure error component. On the other hand, the stabilizer component $\mathscr{S}(E)$ acts trivially on the code space. Thus, syndrome-based decoding consists in identifying the logical component $\mathscr{L}(E)$ of the error given its pure error component $\mathscr{T}(E)$. Errors that only differ in their syndrome component need not be distinguished because they have the same effect on the code space. Such errors are said to be degenerate.

1.3.1 Gauge operator

We now transpose this formalism to the case of OQEC. Similarly to an ordinary QECC, an $[[n, k, r, d]]$ subsystem code can be specified by a canonical basis of the n-qubit Pauli group. The $2n$ basis elements are now divided into four groups:

(i) The $2k$ logical operator $\overline{X}_i$ and $\overline{Z}_i$ that obey canonical commutation relations: $\{\overline{X}_i, \overline{Z}_i\} = 0$ and all other pairs commute.

(ii) The $n-k-r$ stabilizer generators S_j that mutually commute, and commute with all logical operators.

(iii) The $n-k-r$ pure errors T_j that mutually commute, commute with all logical operators, and are canonically conjugated to the stabilizer generators: $\{S_j, T_j\} = 0$ and $[S_j, T_{j'}] = 0$ for $j \neq j'$.

(iv) The $2r$ gauge operators G_j^x and G_j^z that commute with all logical operators, stabilizer generators, and pure errors, and form canonically conjugate pairs: $\{G_j^x, G_j^z\} = 0$ and all other pairs of gauge operators commute.

Once again, there exists a Clifford unitary transformation taking the elements of the canonical basis formed of single-qubit Pauli operators to this

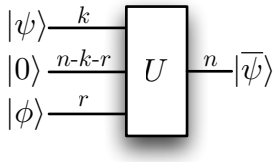

Fig. 1.2. Encoding circuit for OQECC

basis,

$$U : \begin{cases} X_i \to \overline{X}_i & \text{for } i = 1, \dots k \\ Z_i \to \overline{Z}_i & \text{for } i = 1, \dots k \\ X_{i+k} \to T_i & \text{for } i = 1, \dots n-k-r \\ Z_{i+k} \to S_i & \text{for } i = 1, \dots n-k-r \\ X_{i+k+r} \to G_i^x & \text{for } i = 1, \dots r \\ Z_{i+k+r} \to G_i^z & \text{for } i = 1, \dots r \end{cases} . \tag{1.19}$$

As before, this transformation can serve as an encoder for the OQECC where the first k qubits contain the unencoded information $|\psi\rangle$ and the $n-k-r$ stabilizer qubits are in the all-zero state. The novelty is that the following r "gauge" qubits can be in any state $|\phi\rangle$. The coding scheme does not specify the state of these qubits and they can be in any mixed or pure state.

We can decompose any Pauli error E in this basis and write

$$E = \mathscr{L}(E)\mathscr{S}(E)\mathscr{T}(E)\mathscr{G}(E)$$

with the same meaning as above: $\mathscr{L}$, $\mathscr{S}$, and $\mathscr{T}$ contain the logical, stabilizer, and pure error component of the error respectively and $\mathscr{G}$ contains the gauge component. The syndrome measurement reveals the pure error component $\mathscr{T}(E)$ and decoding consists in identifying the logical component $\mathscr{L}(E)$ given this information. Errors that only differ by their stabilizer and/or *gauge* components have the same syndrome and have the same effect on the encoded information so they are regarded as equivalent. Thus, in a sense, the gauge operators play a role analogous to the stabilizer generators: they generate equivalence classes among the errors because they act trivially on the encoded information. But contrarily to the stabilizer generators, the gauge operators are not (a priori) used to extract information about the error that has corrupted the information. In fact, since the gauge operators generate a non-abelian group, they could not possibly all be measured simultaneously without disturbing each other's outcome.

1.3.2 Bounds for subsystem codes

We next discuss work of Klappenecker and Sarvepalli that investigates quantum Hamming and Singleton bounds for subsystem codes. In the spirit of the stabilizer formalism, the results apply to generalized Pauli noise models.

We shall consider n-qudit Hilbert space $\mathscr{H} = (\mathbb{C}^q)^{\otimes n} = \mathbb{C}^{q^n}$, where q is the power of a prime number p. Let $\mathbb{F}_q$ be a finite field with q elements and characteristic p. (For instance, if $q = p$, then the integers $\{1, 2, \ldots, p\}$ with addition and multiplication modulo p forms such a field.) Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be an $\mathbb{F}_q$-linear classical code denoted by $[n, k, d]_q$, where k is the dimension of $\mathscr{C}$ over $\mathbb{F}_q$ and d is the minimum distance of $\mathscr{C}$, where $\mathrm{wt}(\mathscr{C}) = \min\{\mathrm{wt}(c) | 0 \neq c \in \mathscr{C}\} = d$ and $\mathrm{wt}(c)$ is the Hamming weight of c. If $\mathscr{C}$ is a linear subspace over $\mathbb{F}_q$, then it is called an *additive* code.

The noise models considered here are defined as follows. Let $\mathscr{B} = \{|x\rangle : x \in \mathbb{F}_q\}$ be an orthonormal basis for $\mathbb{C}^q$. Let $X(a)$ and $Z(b)$ be the unitary operators on $\mathbb{C}^q$ defined by

$$X(a)|x\rangle = |x + a\rangle \quad \text{and} \quad Z(b)|x\rangle = \omega^{(bx)_p}|x\rangle,$$

where $\omega = e^{j2\pi/p}$ is a primitive pth root of unity and $(bx)_p$ is multiplication modulo p. Let $\mathfrak{E}$ be the error group on $\mathscr{H}$, the natural generalization of the Pauli group, defined as the tensor product of n such operators;

$$\mathfrak{E} = \{\omega^c E_1 \otimes \ldots \otimes E_n \mid E_i = X(a_i)Z(b_i);\ a_i, b_i \in \mathbb{F}_q;\ c \in \mathbb{F}_p\}.$$

The *weight* $\mathrm{wt}(E)$ of an error $E \in \mathfrak{E}$ is equal to the number of E_i not equal to the identity operator.

Every non-trivial normal subgroup N of $\mathfrak{E}$ defines a subsystem code $\mathscr{C}$ as follows. Let $C_{\mathfrak{E}}(N)$ be the centralizer of N inside $\mathfrak{E}$ and $Z(N)$ the centre of N. As a subspace, the subsystem code $\mathscr{C}$ defined by N is precisely the same as the stabilizer code defined by $Z(N)$. It follows that $\mathscr{C}$ can be decomposed as $A \otimes B$ where $\dim B = |N : Z(N)|^{1/2}$ and

$$\dim A = |Z(\mathfrak{E}) : N||\mathfrak{E} : Z(\mathfrak{E})|^{1/2}|N : Z(N)|^{1/2}/|N|.$$

In this formulation, information is stored inside subsystem A. An error E in $\mathfrak{E}$ is detectable by A if and only if E is contained in the set $\mathfrak{E} - (N\, C_{\mathfrak{E}}(N) - N)$. The distance of the code is defined as

$$d = \min\{\mathrm{wt}(E) | I \neq E \in NC_{\mathfrak{E}}(N) - N\} = \mathrm{wt}(NC_{\mathfrak{E}}(N) - N).$$

If $NC_{\mathfrak{E}}(N) = N$, then the code distance is defined as $\mathrm{wt}(N)$. The group N is the *gauge group* of $\mathscr{C}$ and $Z(N)$ is its *stabilizer*. Observe the gauge group acts trivially on A. Klappenecker and Sarvepalli construct a special class of such subsystem codes, a class that includes the Bacon-Shor codes, such

that the subsystem A can detect all errors in $\mathfrak{E}$ of weight less than d, and can correct all errors in $\mathfrak{E}$ of weight at most $\lfloor (d-1)/2 \rfloor$. They called these codes *Clifford subsystem codes.*

There is a natural notion of purity for Clifford subsystem codes. Let N be the gauge group of a subsystem code $\mathscr{C}$ with distance d. Then $\mathscr{C}$ is *pure to* d' if there is no error of weight less than d' in N. The code is said to be *exactly pure to* d' if $\mathrm{wt}(N) = d'$ and it is *pure* if $d' \geq d$. The code is said to be impure if it is exactly pure to $d' < d$.

K.-S. prove the following upper bound for Clifford subsystem codes. This result generalizes the quantum Singleton bound obtained for the subspace version of the stabilizer formalism (which is captured in the case that $r = 0$).

Theorem 4 *An $\mathbb{F}_q$-linear $[n, k, r, d \geq 2]_q$ Clifford subsystem code satisfies*

$$k + r \leq n - 2d + 2. \tag{1.20}$$

Observe that one implication of this result is that the number $n - k - r$ of syndrome measurements is bounded by $2d - 2$, which indicates for a fixed distance d a tradeoff between the code dimension k and the difference $n - r$ between length and number of gauge qubits.

While there are attractive features of subsystem codes, including a potential reduction of the number of syndrome measurements, there are limitations to the benefits of Clifford subsystem codes over stabilizer codes. One such limitation can be formally proved as a consequence of the Singleton bound. An open problem suggested by Poulin's works asks whether a subsystem code can use fewer syndrome measurements than an optimal MDS stabilizer code, while encoding the same number of qubits and having the same distance. There are now several examples of subsystem codes that improve upon non-optimal stabilizer codes, so the question is made interesting by assuming the stabilizer code is optimal. As a straightforward application of Theorem 4, K.-S. show this question has a negative answer. Specifically, they show an $\mathbb{F}_q$-linear $[n, k, r, d \geq 2]_q$ Clifford subsystem code cannot use fewer syndrome measurements than an $\mathbb{F}_q$-linear $[k + 2d - 2, k, d]_q$ stabilizer code. If there were such a code, then the number of syndrome measurements would yield the inequality $k + 2d - 2 - k > n - k - r$, which is equivalent to $k + r > n - 2d + 2$, contradicting the Singleton bound.

The following quantum Hamming bound for pure Clifford subsystem codes has also been established.

Theorem 5 *A pure Clifford subsystem code $\mathscr{C} = A \otimes B$ of distance d, with*

$K = \dim A$ *and* $R = \dim B$*, satisfies*

$$\sum_{j=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{j} (q^2-1)^j \leq q^n/KR. \tag{1.21}$$

On the one hand, this result (along with its subspace version) suggests it might be unlikely that highly degenerate subsystem codes could lead to much more efficiency in terms of packing subspaces more compactly in Hilbert space. On the other hand, and quite surprisingly, there exist impure subsystem codes that do not satisfy this Hamming bound. The $[9, 1, 4, 3]_2$ Bacon-Shor code provides a nice example of this fact. Notice first that, as predicted by Theorem 4, it satisfies (in fact optimally) the Singleton bound for Clifford subsystem codes since

$$k + r = 1 + 4 = n - 2d + 2 = 9 - 6 + 2.$$

However, substituting these parameters into Eq. (1.21) yields

$$\sum_{j=0}^{1} \binom{9}{j} 3^j = 27 > 2^{9-5} = 16,$$

and hence the Bacon-Shor code beats the quantum Hamming bound for pure subsystem codes.

The reasons why impure codes can pack more efficiently than pure codes are somewhat subtle. One important reason is that impure subsystem codes can have more degeneracy. For instance, in a pure single error correcting code all single errors must take the code subspace to mutually orthogonal subspaces. In an impure code, this is not required as two or more distinct errors can take the code subspace to the same subspace. In the case of the Bacon-Shor code, a phase flip error on any of the first three qubits takes the code to the same subspace, and so the errors cannot be distinguished on the full code subspace. But this is not an issue since the A qubit subsystem can still be recovered.

1.4 Examples

1.4.1 Bacon-Shor code

An important example of a stabilizer OQECC, often referred to as the Bacon-Shor code [**?**, **?**], is obtained from a modification of Shor's original QECC [**?**]. Recall that the stabilizer generators for this 9-qubit code are given by $Z_i Z_{i+1}$ for $i = 1, 2, 4, 5, 6, 7$ and $X_i X_{i+1} X_{i+2} X_{i+3} X_{i+4} X_{i+5}$ for $i = 1, 4$. These can nicely visualized if we place the qubits on a 3×3 lattice

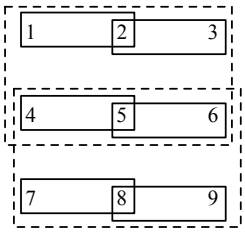

Fig. 1.3. Shor's 9-qubit QECC. The full lines represent Z stabilizer generators and the dash lines X stabilizer generators.

as shown on Fig. 1.3. There is an obvious asymmetry between the X and the Z stabilizer generators. This is because the code is constructed from the concatenation of a 3-qubit repetition code in the Z basis with a 3-qubit repetition code in the X basis. Bit flip errors are corrected independently in each row of 3 qubits and are not degenerate. Phase errors are corrected collectively and are highly degenerate: it is only necessary to identify the row in which a phase error occurred, since phase errors on distinct qubits in a given row have the same effect on the encoded information.

On the other hand, the logical operators of the code are completely symmetric, $\overline{X} = X^{\otimes 9}$ and $\overline{Z} = Z^{\otimes 9}$. This is in contrast with the stabilizer generators and the recovery procedure. The Bacon-Shor code restores this symmetry. Its stabilizer generators are shown on Fig. 1.4. This code has fewer stabilizer generators than Shor's code. As a consequence it cannot distinguish between as many errors. Contrarily to Shor's code, these stabilizers cannot identify the precise qubit on which a bit flip occurs, they can only identify the column in which it occurs. This loss is compensated by new gauge operators that make bit flip errors in a column al equivalent to one another. In more detail, the complete canonical basis associated with the Bacon-Shor code is

$$\begin{array}{ll} \overline{X} = X^{\otimes 9} & \overline{Z} = Z^{\otimes 9} \\ S_1 = Z_1 Z_2 Z_4 Z_5 Z_7 Z_8 & T_1 = X_5 X_6 \\ S_2 = Z_2 Z_3 Z_5 Z_6 Z_8 Z_9 & T_2 = X_4 X_5 \\ S_3 = X_1 X_2 X_3 X_4 X_5 X_6 & T_3 = Z_2 Z_5 \\ S_4 = X_4 X_5 X_6 X_7 X_8 X_9 & T_4 = Z_5 Z_8 \\ G_1^z = Z_1 Z_2 & G_1^x = X_1 X_4 \\ G_1^z = Z_2 Z_3 & G_1^x = X_3 X_6 \\ G_1^z = Z_7 Z_8 & G_1^x = X_4 X_7 \\ G_1^z = Z_8 Z_9 & G_1^x = X_6 X_9 \end{array} \quad . \tag{1.22}$$

By combining the generators of the gauge and the stabilizer groups, we can

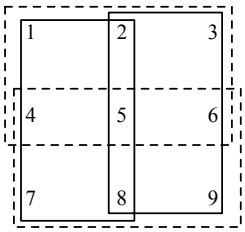

Fig. 1.4. The Bacon-Shor code. The full lines represent Z stabilizer generators and the dash lines X stabilizer generators.

obtain any pair of Z operators in the same row and any pair of X operators from the same column. Thus, all single phase errors in a given row are equivalent, and all single qubit flip errors in a given column are equivalent.

1.4.2 Generalization: Klappenecker-Sarvepalli-Bacon-Casaccino

To understand how to generalize the Bacon-Shor code, we first need to generalize the concatenation scheme that led to Shor's code. This code is obtained from the concatenation of two classical codes, one used to correct bit-flip errors and one used to correct phase errors. The bit-flip code, which we refer to as "code A", has stabilizer generators $S_1^A = ZZI$ and $S_2^A = IZZ$ and logical operators $\overline{X}^A = XXX$ and $\overline{Z}^A = ZZZ$. The second code, "code B", is also a repetition code but it is used in as a phase code. Its stabilizers are $S_1^B = XXI$ and $S_2^B = IXX$ and its logical operators are $\overline{X}^B = XXX$ and $\overline{Z}^B = ZZZ$. Shor's code, which we denote $A \triangleright B$, is obtained from the concatenation of these two codes. It is defined on a 3×3 array of qubits and has two type of stabilizer generators:

(i) The stabilizer generators of A acting independently on each row of the array, represented by the full rectangles in Fig. 1.3. There are 6 of those.
(ii) The operators $\overline{X}_i^A \triangleright S_j^B$ obtained by forming a column with the operator S_j^B, and expanding each X operator in the horizontal direction as a logical operator X_i^A of the code A. These 2 stabilizers are represented by the dotted rectangles in Fig. 1.3.

The logical operators of $A \triangleright B$ are $L_i^A \triangleright L_j^B$, obtained by forming a column with the operator L_j^B, and expanding each single qubit operator by a logical operator of the code A, i.e., $X \to \overline{X}_i^A$ and $Z \to \overline{Z}_i^A$.

This construction can be generalized using any two classical codes. Let A and B be two classical codes with parameters $[n^A, k^A, d^A]$ and $[n^B, k^B, d^B]$ respectively. Code A is used as a bit-flip code and code B as a phase code. In other words, the stabilizer generators of A are obtained from the columns of the parity-check matrix of the associated classical code by substituting each 1 by a Z. The logical operators $\overline{X}_i^A$ are obtained from the lines of the generating matrix of the associated classical code by substituting each 1 by an X. The commutation properties of these operators follow directly from the orthogonality of the parity-check matrix and generator matrix. The logical operators $\overline{Z}_i^A$ are composed uniquely of Z's and I's and can be found by Gaussian elimination as the operators that are canonically conjugated to the $\overline{X}$'s (they will hence automatically be independent from the stabilizer generators). The stabilizer generators and logical operators of code B are obtained in a similar way, but with the roles of Z and X reversed.

Given these two codes, we can follow the same steps that led to Shor's code. The code $A \triangleright B$ is defined on a $n^A \times n^B$ qubit array. It has two kind of stabilizer generators:

(i) The stabilizer generators of A acting independently on each row of the array. We denote them $S_{j,r}^A$ where j labels a stabilizer generator of A and r a row for the qubit array. There are $(n^A - k^A)n^B$ of those.

(ii) The operators $\overline{X}_i^A \triangleright S_j^B$ obtained by forming a column with the operator S_j^B, and expanding each X operator in the horizontal direction as a logical operator X_i^A of the code A. There are $k^A(n^B - k^B)$ of those.

Thus, there are a total of $n^A n^B - k^A k^B$ stabilizer generators for $A \triangleright B$. The logical operators of the concatenated code are $L_i^A \triangleright L_j^B$, of which there are $k^A k^B$.

That these stabilizers generate an abelian group can be verified straightforwardly. On each row of the array, the stabilizers generators of $A \triangleright B$ are formed by either stabilizer generators of A or logical operators $\overline{X}^A$. These operators all commute with one another, and this commutativity is inherited by the generators of $A \triangleright B$. Similarly, the canonical commutation of the logical operators of the concatenated code is inherited from the canonical commutation relations of the logical operators of the constituent codes.

The code $A \triangleright B$ has minimal distance $d^{A \triangleright B} = \min\{d_c^A, d_c^B\}$. Indeed, it is obvious that the code has a bit-flip distance equal to d_c^A since code A is independently used on each row of the qubit array. On the other hand, any phase errors on a given row decompose into S_j^A's and $\overline{Z}_i^A$'s on that row.

Since B has a phase flip distance d_c^B, it takes that many rows with phase errors to produce an undetectable phase error. Thus, this concatenation scheme can be used to produce a quantum code from any two classical codes, without any orthogonality condition. The code obtained from this scheme has parameters $[[n^A n^B, k^A k^B, \min\{d^A, d^B\}]]$.

Again we observe an asymmetry in the two codes. Another concatenated code $A \triangleleft B$ can be constructed with stabilizers formed of the stabilizers of B acting independently on each column of the qubit array, denoted $S_{j,c}^B$, and the operators $S_j^A \triangleleft \overline{Z}_i^B$ obtained by forming a row with the operator S_j^A, and expanding each of its Z operator in the vertical direction as a logical operator $\overline{Z}_i$ of the code B. The logical operators of $A \triangleleft B$ are $L_i^A \triangleleft L_j^B$, which is the same as $L_i^A \triangleright L_j^B$ used for the code $A \triangleright B$. We will use the notation $L_i^A \triangle L_j^B$ to emphasize this symmetry. Thus, the asymmetry is only in the code, not in the logical operators.

The concatenated OQECC, denoted $A \triangle B$, restores this symmetry. It has parameters $[[n^A n^B, k^B k^B, (n^A - k^A)(n^B - k^B), \geq d^A d^B]]$. Its logical operators $L_i^A \triangle L_j^B$ are the same as those obtained from the two distinct asymmetric constructions $A \triangleright B$ and $A \triangleleft B$. It also uses the second set of stabilizer generators $\overline{X}_i^A \triangleright S_j^B$ of $A \triangleright B$. However, the first set of stabilizers of $A \triangleright B$ is modifie. Instead of using the stabilizers of A independently on each row $S_{j,c}^A$, only the combinations $S_j^A \triangleleft \overline{Z}_i^B$ are used. These correspond to the first set of stabilizers of the code $A \triangleleft B$. The other combinations are recycled as gauge operators. What do these operators look like? In general, they are operators of the form $S_i^A \triangle S_j^B$ obtained by substituting each Z operators of S_j^B by S_i^A, or equivalently substituting each X operators of S_i^A by S_j^B.

The minimal distance of this code is also $\min\{d_A, d_B\}$. This can easily be seen from the fact that both $A \triangleright B$ and $A \triangleleft B$ have that minimal distance and correct bit-flip and phase errors independently, and the fact that $A \triangle B$ has the same bit-flip stabilizers as the code $A \triangleleft B$, and the same phase stabilizers as the code $A \triangleright B$.

1.5 Measuring gauge operators

The previous section presented a family of OQECC that are a modified version of generalized Shor codes. The modification consisted in removing a subset of stabilizer generators and promoting them to gauge operators. Removing some stabilizers implies that less information about the error is available to the decoder. However, this loss is compensated by an increase in the code's degeneracy and the minimal distance is unaffected. The main

advantage of this construction is that fewer stabilizer generators need to be measured to diagnose the error. The drawback however is that the weight of the stabilizer generators increases. Indeed, if w^A and w^B denote the minimal weight of the stabilizers of code A and B respectively, then the minimal weight of a stabilizers of $A \triangle B$ is $\min\{w^A d^B, w^B d^A\}$.

Having low-weight stabilizers is a serious advantage from an implementation and fault-tolerance perspective. Indeed, performing collective measurements on a very large number of qubits is a daunting experimental task, and requires the purification of complex ancillary states to be executed fault tolerantly. A code with low-weight stabilizer generators is thus highly favorable.

On the other hand, the bit-flip stabilizers $S^A_{j,r}$ of the code $A \triangleright B$ have minimum weight w^A, and its phase stabilizers $\overline{X}^A_i \triangleright S^B_j$ have minimum weight $d^A w^B$. Thus, it has some low weight and some high weight stabilizers. Similarly, the phase stabilizers $S^B_{j,c}$ of code $A \triangleleft B$ have minimum weight w^B, and its bit-flip stabilizers $S^A_j \triangleleft \overline{Z}^B_i$ have minimum weight $d^B w^A$. The code $A \triangle B$ is obtained from the phase stabilizers of the code $A \triangleright B$ and the bit-flip stabilizers of the code $A \triangleleft B$, so it keeps only the high weight stabilizers. Can't we combine instead the low-weight stabilizers of both codes?

The short answer is no. These operators do not all mutually commute, so they cannot be used to define a code. However, it is possible to use these operators in a clever way to extract the syndrome information of the code $A \triangle B$. We start by measuring the operators $S^B_{j,rc}$. These operators are not stabilizers of the code $A \triangle B$, so the measurement outcomes are random even in the absence of errors. However, the correlations between these random measurement outcomes reveal the syndrome information.

Indeed, these are products of various subsets of the commuting operators $S^A_{j,r}$, so their values can be obtained by measuring the operators $S^A_{j,r}$ directly and taking the corresponding product of the outcomes. This is because the operators $S^B_{j,c}$ mutually commute and because each stabilizer $S^A_j \triangleleft \overline{Z}^B_i$ decomposes as a product of a subset of the $S^B_{j,c}$. More precisely

$$S^A_j \triangleleft \overline{Z}^B_i = \prod_{c:(\overline{Z}^B_i)_c = Z} S^B_{j,c} \tag{1.23}$$

where $(Q)_c$ denotes the cth tensor factor of the Pauli operator Q. Because they commute, measuring each operators $S^B_{j,c}$ and taking the product of their measurement outcomes is equivalent to measuring the operator equal to their product. Thus, we can extract the syndrome associated with the high weight

stabilizers $S_j^A \triangleleft \overline{Z}_i^B$ through a measurement of the low-weight operators $S_{j,c}^B$. Similarly, the syndrome associated with the stabilizers $\overline{X}_i^A \triangleleft S_j^B$ can be extracted through the measurement of $S_{j,r}^A$.

Note that this procedure is somewhat wasteful. The low weight stabilizers $S_{j,r}^A$ and $S_{j,c}^B$ cannot be used jointly to define a code, but it is not necessary to replace both sets by high-weight operators; we can choose to replace only one of them. This restores the asymmetry in the code. Such an asymmetric code can be relevant when one type of noise dominates. It is indeed often the case that phase errors are much more prominent than bit-flip errors. Thus, we can choose the code $A \triangleleft B$. In that case, we must begin by measuring the stabilizers $S_{j,c}^B$. These directly reveal the phase error syndrome, there is no need to coarse-grain the measurement outcomes a was done in the previous scheme, so there is more information about phase errors. The measurement of the bit-flip stabilizers $S_j^A \triangleleft \overline{Z}_i^B$ proceeds indirectly as above through a measurement of the $S_{j,r}^A$. These measurements will take the state outside the code space defined by the operators $S_{j,c}^B$, but without affecting its logical content because the measurements consist of gauge operators. Thus, the state can simply be returned to the code space before the next error-correction round.

1.5.1 Sparse quantum codes?

What we have learned so far is that it is possible to construct OQECC from any two linear classical codes, and that moreover, the syndrome can be extracted by measuring operators of weight equal to the weight of the columns of the associated parity-check matrix. This is exciting because among the best classical codes are sparse (or low density parity check, LDPC) codes that, as their names suggest, have sparse parity-check matrices. Thus, they can be used to produce OQECC's with very simple syndrome extraction schemes. These classical codes are nearly capacity achieving on a variety of channels and have efficient decoding algorithms (see Chapter **??**).

Unfortunately, these nice properties do not all transpose to the quantum setting. Firstly, near-capacity achieving codes must have a minimal distance that grows proportionally to the code length n. (Atypical low-weight codewords can be tolerated.) Assume that codes A and B are good in this sense, so $d^A \sim n^A$ and $d^B \sim n^B$. The resulting OQECC has $n = n^A n^B$ and $d = \min\{d^A, d^B\} \sim \sqrt{n}$. Thus, as n grows, the failure probability on the depolarizing channel will approach unity.

The second difficulty has to do with the decoding algorithm. This algo-

rithm is used to identify the most likely error on the encoded information given the syndrome. The decoding algorithms used for sparse classical codes are described in Chapter **??**. Unfortunately, they are not suitable for the OQECC presented in the previous section. In fact, this problem is not limited to sparse codes. The decoding algorithm used for most classical coding schemes will not be suitable for the derived OQECC.

The problem steams from the fact that the error model changes under concatenation. Suppose that we use the coding scheme $A \triangleleft B$ and that the noise depolarizes each qubit independently. The phase errors can be handled by the decoding algorithm. Indeed, this consists in using the code B independently on each column of the qubit array, i.e., with stabilizers $S^B_{j,c}$. Thus, as far as decoding is concerned, this is just like decoding the corresponding classical code with a bit error rate $2p/3$ independently on each column.

For the bit-flip errors, we measure the operators S^A_j and extract from them the syndrome associated with the stabilizers $S^A_j \triangleleft \overline{Z}^B_i$. The outcome of each S^A_j individually is meaningless, they are random because they do not commute with the phase stabilizers. Thus, the decoder uses the error syndrome associated with $S^A_j \triangleleft \overline{Z}^B_i$. From this perspective, the problem is just like decoding a single copy of the code A, but with an error model given by the probability that an $\overline{X}^B_i$ operation was applied. In other words, this is the probability that the error that has affected the qubits anti-commutes with $\overline{Z}^B_i$. These logical error are highly correlated, something that decoding algorithm are usually not tailored to. Even if we ignore these correlations, we see that the logical error rate is greater than $w_i 2p/3$ where w_i is the weight of $\overline{X}^B_i$. Since $w_i \sim n^B$ for good codes, the code's error threshold is decrease by a factor proportional to $n^B \sim \sqrt{n}$.

Despite this negative analysis, the coding scheme can find useful applications. The solution is to keep the size relatively small, such that the error rate increase $w_i 2p/3$ does not become problematic. This rules out for the time being the design of capacity-achieving OQECC based on this scheme. However, as discussed in Chapter **??**, fault-tolerant protocols using this coding scheme have a significantly large error threshold than protocols based on conventional QEC because they can be realized by measuring only low-weight operators.

1.6 Unitarily correctable codes

Recall that the typical recovery operation in quantum error correction consists of a measurement followed by a unitary reversal conditioned on the result of the measurement. One situation that could realistically arise in the laboratory would be if we had a system with good unitary control but poor measurement apparatus. Moreover, a primary difficulty encountered in fault tolerant quantum computing is the size of the Hilbert space required to implement a typical recovery operation. Thus we find motivation for consideration of error correcting codes that do not require a measurement as part of the recovery process. In other words, codes that have evolved unitarily, and hence can be recovered by a unitary operation. Note that this does not mean the noise model itself is unitary, only that it acts unitarily when restricted to the code.

Thus, in OQEC we say that a subsystem B is a *unitarily correctable code* (UCC) for a channel $\mathscr{E}$ if B can be corrected with a unitary recovery operation $\mathscr{R} = \mathscr{U}$; that is, there is a channel $\mathscr{F}_A$ such that

$$\mathscr{E} \circ \mathscr{P}_C = \mathscr{U} \circ (\mathscr{F}_A \otimes \mathrm{id}_B) \circ \mathscr{P}_C. \tag{1.24}$$

Observe that DFS and NS are precisely the UCC with trivial unitary correction $U = I$. Interestingly, the analysis of UCC connects with certain aspects of the theory of completely positive maps. We shall briefly describe this connection in the case of unital channels, and show how it leads to a technique to compute UCC for arbitrary unital channels.

Notice that if $\mathscr{E}$ is both unital and trace-preserving, then so is $\mathscr{E}^\dagger$ and consequently so is $\mathscr{E}^\dagger \circ \mathscr{E}$. It is also easy to see that if B is a noiseless subsystem for $\mathscr{E}^\dagger \circ \mathscr{E}$, and hence $\mathscr{E}^\dagger \circ \mathscr{E} \circ \mathscr{P}_C = (\mathscr{G}_A \otimes \mathrm{id}_B) \circ \mathscr{P}_C$, then B is a correctable subsystem for $\mathscr{E}$ because $\mathscr{E}^\dagger$ is trace-preserving and thus constitutes a correction operation that satisfies the OQEC definition. But more than this is true, it turns out that B is a UCC for $\mathscr{E}$. Together with its converse, this fact gives us the following result.

Theorem 6 *Let $\mathscr{E}$ be a unital quantum channel. Then B is a UCC for $\mathscr{E}$ if and only if B is a NS for $\mathscr{E}^\dagger \circ \mathscr{E}$.*

The proof relies on a number of ancillary results for unital trace preserving maps, and previously stated characterizations of OQECC. We shall briefly sketch the proof here. An intuitive point that is imbedded several places in the analysis (and one that can be formulated as a result) is that unital channels can only increase the impurity or mixedness of quantum states.

First consider the case that B is a UCC for $\mathscr{E}$. Given that B is a cor-

rectable subsystem, it follows from the testable conditions of Theorem 1 or condition (iv) of Theorem 3 that $\mathscr{P}_{\mathscr{C}} \circ \mathscr{E}^\dagger \circ \mathscr{E} \circ \mathscr{P}_{\mathscr{C}} = (\mathscr{G}_A \otimes \mathrm{id}_B) \circ \mathscr{P}_{\mathscr{C}}$ for some channel $\mathscr{G}_A$. Now, it is clear that if not for the leading $\mathscr{P}_{\mathscr{C}}$ in this expression, B would satisfy the definition of a NS for $\mathscr{E}^\dagger \circ \mathscr{E}$. The rest of the proof for this direction of the theorem is focused on establishing that the leading $\mathscr{P}_{\mathscr{C}}$ can be dropped from this expression in the case of UCC and unital channels. A surprising amount of technical effort is required to do so, we point the reader to [?] for details.

For the other direction, note that if B is a passive code for $\mathscr{E}^\dagger \circ \mathscr{E}$, then B is correctable for $\mathscr{E}$ since the dual map $\mathscr{E}^\dagger$ is a valid correction operation. Thus by condition (iv) of Theorem 3, there exists subsystems $\mathscr{C}' = A' \otimes B'$, a channel $\mathscr{F}_{A'|A}$, and a unitary channel $\mathscr{V}_{B'|B}$ such that $\mathscr{E} \circ \mathscr{P}_{\mathscr{C}} = (\mathscr{F}_{A'|A} \otimes \mathscr{V}_{B'|B}) \circ \mathscr{P}_{\mathscr{C}}$. The technical component in this direction of the proof again uses properties of unital channels to show that $\mathrm{rank}(\mathscr{F}_{A'|A}(I_A)) = \mathrm{rank}(I_A)$. This implies the existence of a unitary $\mathscr{U}$ such that $\mathscr{U} \circ \mathscr{E} \circ \mathscr{P}_{\mathscr{C}} = \mathscr{U} \circ (\mathscr{F}_{A'|A} \otimes \mathscr{V}_{B'|B}) \circ \mathscr{P}_{\mathscr{C}} = (\mathscr{F}_A \otimes \mathrm{id}_B) \circ \mathscr{P}_{\mathscr{C}}$ for some channel $\mathscr{F}_A$ on A, and hence B is a UCC for $\mathscr{E}$.

It has recently been discovered that there is an important object from the theory of completely positive maps that connects with the UCC theory for channels. The *multiplicative domain* of a completely positive map $\mathscr{E}$ was first considered in operator theory over thirty years ago, and is defined as $MD(\mathscr{E}) := \{\sigma : \mathscr{E}(\sigma\gamma) = \mathscr{E}(\sigma)\mathscr{E}(\gamma)$ and $\mathscr{E}(\gamma\sigma) = \mathscr{E}(\gamma)\mathscr{E}(\sigma)\ \forall\gamma\}$. It is evident that this set forms a $*$-closed algebra, and in the case that $\mathscr{E}$ is a unital completely positive map, Choi proved that it is defined through its internal structure as follows:

$$MD(\mathscr{E}) := \{\sigma : \mathscr{E}(\sigma\sigma^\dagger) = \mathscr{E}(\sigma)\mathscr{E}(\sigma)^\dagger,\ \ \mathscr{E}(\sigma^\dagger\sigma) = \mathscr{E}(\sigma)^\dagger\mathscr{E}(\sigma)\}.$$

Interestingly, it has been shown that subsystem codes defined via the algebra structure of $MD(\mathscr{E})$ are *precisely* the UCC for $\mathscr{E}$. In the arbitrary (not necessarily unital) case, one can still consider the multiplicative domain, though Choi's characterization no longer holds. In that case, the algebra $MD(\mathscr{E})$ encodes a proper subclass of UCC that can be computed from properties of the map.

By combining Theorem 6 with the fixed point theorem for unital channels, we obtain a method for finding the UCC for *any* unital channel $\mathscr{E}$. Specifically, the DFS and NS of $\mathscr{E}^\dagger \circ \mathscr{E}$ are obtained from the fixed point set $\mathrm{Fix}\,(\mathscr{E}^\dagger \circ \mathscr{E})$ via its algebra structure, as discussed above in the case of passive codes for unital channels.

Of course, for an arbitrary unital quantum map $\mathscr{E}$, not every correctable subsystem is a UCC, and consequently the passive codes of $\mathscr{E}^\dagger \circ \mathscr{E}$ do not in

general capture all OQEC codes for a typical unital channel $\mathscr{E}$. There are many unital maps, however, for which the composition of this map with its dual does have passive codes.

Example 1 *First as a simple example, consider the swap operation* $|\psi\rangle \otimes |\phi\rangle \mapsto |\phi\rangle \otimes |\psi\rangle$ *on a composite quantum system* $\mathscr{H} = \mathscr{A} \otimes \mathscr{R}_A$ *made up of a subsystem* $\mathscr{A}$ *and a replication* $\mathscr{R}_A = \mathscr{A}$*. It is clear that both the subsystem* $\mathscr{A}$ *and its copy can be returned to their initial locations by simply applying the swap operation again (which is equal to its dual). Now, one could note that the swap operation itself has a NS of the same size; namely the symmetric space* $|\psi\rangle \otimes |\psi\rangle$*. But it is easy to find examples of channels with no passive codes, for which the composition map has a non-trivial passive code. To this end, consider a two-qubit system exposed to decoupled phase flips. The associated error model satisfies* $\mathscr{E}(\rho) = pZ_1\rho Z_1 + (1-p)Z_2\rho Z_2$ *for some fixed probability* $0 < p < 1$ *and* $Z_1 = Z \otimes I_2$*,* $Z_2 = I_2 \otimes Z$*. In this case* $\mathscr{E}$ *has no passive codes. This follows from the fact that the noise commutant* $\{Z_1, Z_2\}'$ *is isomorphic to the algebra* $\mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$*. Thus, only classical information can be safely sent through the channel. However, the operators supported on the subspace spanned by* $|0_L\rangle = |00\rangle$ *and* $|1_L\rangle = |11\rangle$ *form a DFS for* $\mathscr{E}^\dagger \circ \mathscr{E}$*. Indeed, the set of operators* $\sigma = a|00\rangle\langle 00| + b|00\rangle\langle 11| + c|11\rangle\langle 00| + d|11\rangle\langle 11|$ *form a subalgebra of the commutant* $\mathrm{Fix}\,(\mathscr{E}^\dagger \circ \mathscr{E}) = \{Z_1^\dagger Z_2, Z_1^\dagger Z_1, Z_2^\dagger Z_1 Z_2^\dagger Z_2\}' = \{Z_1 Z_2\}'$*. A unitary correction operation guaranteed by Theorem 6 in this case happens to be the controlled phase flip operation* $U = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11|$.

1.7 Connection with quantum cryptography

Lastly, we outline a connection between basic notions in quantum cryptography and error correction. The following discussion is motivated by the presentation of [**?**], and includes introductory details on some mathematical tools that are used more broadly in quantum information.

As we have seen, in OQEC a correctable subsystem is one that, among other things, merely suffers a unitary change of representation and therefore does not decohere. In quantum cryptography a *private subsystem* is the extreme opposite: it is one that completely decoheres under the action of the noise in the sense that no information about the state of the subsystem remains at the output of the map [**?**]. One important application arises in the context of private quantum communication schemes. If Alice encodes quantum information using a secret key that she shares with Bob, then Eve's ignorance of this key can be modelled as a quantum channel. For instance,

suppose Alice and Bob share a secret classical key in the form of a random variable X with distribution p which they use to select a unitary from a set $\{U_x\}$ to implement on a system prior to transmitting it. Then Eve's description of the system is $\mathscr{E}(\rho) = \sum_x p(x) U_x \rho U_x^\dagger$. The private subsystems of this channel are precisely the subsystems about which Eve obtains no information [**?**, **?**, **?**].

Finding the private subsystems for an arbitrary channel is thus a problem of significant import in quantum cryptography. As it turns out, it is the counterpart of a central problem in quantum error correction, that of finding correctable codes for arbitrary channels. This is a basic problem that has been discussed in detail elsewhere in this book, including the special cases of this chapter. On the other hand, relatively little work has been done on the corresponding problem for private codes. In this section we shall show how these two problems are in fact dual to each other, and that there is a straightforward algebraic technique to move between the two perspectives. This duality between private and correctable in the case of subspaces was used implicitly in work such as [**?**, **?**], and recent work [**?**] has formalized the idea for both subspaces and subsystems. Specifically, the private subsystems for a map are simply the correctable subsystems for a complementary map, where the notion of complementarity of maps is the one introduced in [**?**]. The complements of a channel may be readily obtained, and hence it follows that all the techniques and progress on finding correctable subsystems can be immediately appropriated for the problem of finding private subsystems. The implication also holds in the opposite direction: the correctable subsystems for a map are the private subsystems for a complementary map. Consequently, results from the field of cryptography may also provide novel insights for error correction.

In real-world applications, demanding perfect recovery or complete decoherence of quantum information is often too restrictive. Fortunately an approximate version of the correctable-private complementarity has also been proved, and we shall discuss it briefly here. The norm distance $||\cdot||_\diamond$ that we use to quantify the approximate version is the *diamond norm* for superoperators, originally introduced in the context of quantum computing and error correction [**?**, **?**]. It is defined by $\|\mathscr{E} - \mathscr{F}\|_\diamond := \sup_{k\geq 1} \|\mathrm{id}_k \otimes (\mathscr{E} - \mathscr{F})\|_1$ where id_k denotes the identity operation on the complex-valued $(k \times k)$ matrices, and $\|\cdot\|_1$ denotes the superoperator 1-norm $\|\mathscr{E}\|_1 := \sup_{\|\sigma\|_1 \leq 1} \|\mathscr{E}(\sigma)\|_1$ where $\|\sigma\|_1 = \mathrm{Tr}|\sigma|$. The diamond norm stabilizes in the sense that this supremum is attained for k equal to the dimension of the output Hilbert space for the superoperator. (In fact, it is the dual of the *completely bounded*

norm, $\|\mathscr{E}\|_\diamond = \left\|\mathscr{E}^\dagger\right\|_{cb}$ [**?**].) Channels $\mathscr{E}$ and $\mathscr{F}$ are said to be ϵ-*close* if $\|\mathscr{E} - \mathscr{F}\|_\diamond \leq \epsilon$. If two channels are ϵ-close, then the maximum probability of distinguishing the output states of the channels, in an optimization over all input states entangled with an ancilla of arbitrary dimension, is $1/2+\epsilon/4$. This follows from the fact that $\frac{1}{2}+\frac{1}{4}\left\|\rho_{\mathscr{E}} - \rho_{\mathscr{F}}\right\|_1$ is the maximum probability of discriminating $\rho_{\mathscr{E}} = \mathrm{id}_k \otimes \mathscr{E}(\sigma)$ and $\rho_{\mathscr{F}} = \mathrm{id}_k \otimes \mathscr{F}(\sigma)$, and that the supremum over σ in $\|\mathscr{E} - \mathscr{F}\|_\diamond = \sup_{k\geq 1} \sup_{\|\sigma\|_1 \leq 1} \left\|\mathrm{id}_k \otimes \mathscr{E}(\sigma) - \mathrm{id}_k \otimes \mathscr{F}(\sigma)\right\|_1$ captures the optimization.

Definition 3 *Let $\epsilon \geq 0$. Then B is an* ϵ-private subsystem *for $\mathscr{E}_{S'|S}$ if there is a channel $\mathscr{F}_{S'|A}$ such that*

$$\left\|\mathscr{E}_{S'|S} \circ \mathscr{P}_{\mathscr{C}} - \mathscr{F}_{S'|A} \otimes \mathrm{Tr}_B\right\|_\diamond \leq \epsilon\,. \tag{1.25}$$

If Eq. (1.25) holds with $\epsilon = 0$, then B a private subsystem.

Definition 4 *Let $\epsilon \geq 0$. Then B is an* ϵ-correctable subsystem *for $\mathscr{E}_{S'|S}$ if there is a channel $\mathscr{R}_{S|S'}$ and a channel $\mathscr{F}_A$ such that*

$$\left\|\mathscr{R}_{S|S'} \circ \mathscr{E}_{S'|S} \circ \mathscr{P}_{\mathscr{C}} - \mathscr{N}_A \otimes \mathrm{id}_B\right\|_\diamond \leq \epsilon. \tag{1.26}$$

If Eq. (1.26) holds with $\epsilon = 0$, then B is a correctable subsystem.

The notion of complementarity for channels we use first arose in the analysis of channel capacity problems [**?**, **?**, **?**].

Definition 5 *Let $\mathscr{E}_{S'|S}$ and $\mathscr{E}^\sharp_{S''|S}$ be channels on a system S with output spaces S' and S'' respectively. Then $\mathscr{E}$, $\mathscr{E}^\sharp$ form a* complementary pair *if there is an isometric channel $\mathscr{V}_{S'S''|S}$ such that*

$$\mathscr{E}_{S'|S} = \mathrm{Tr}_{S''} \circ \mathscr{V}_{S'S''|S}\,, \quad \mathscr{E}^\sharp_{S''|S} = \mathrm{Tr}_{S'} \circ \mathscr{V}_{S'S''|S}. \tag{1.27}$$

The Hilbert space S'' (respectively S') is a *dilation space* for $\mathscr{E}$ (respectively $\mathscr{E}^\sharp$), and $\mathscr{V}_{S'S''|S}$ is an *isometric dilation* of both. As a consequence of the Stinespring Dilation Theorem [**?**], every channel can be seen to be part of a complementary pair. This follows from the fact that every channel may be seen to arise from an environment Hilbert space E (of dimension at most the product of the input and output Hilbert space dimensions if the dilation is minimal), a pure state $|\psi\rangle$ on the environment, and a unitary operator U on the composite SE in the following sense: $\mathscr{E}(\sigma) = \mathrm{Tr}_E\big(\mathscr{U}(\sigma \otimes |\psi\rangle\langle\psi|)\big)$. Tracing out the system instead yields a complementary channel: $\mathscr{E}^\sharp(\sigma) = \mathrm{Tr}_S\big(\mathscr{U}(\sigma \otimes |\psi\rangle\langle\psi|)\big)$. The corresponding isometric form is $\mathscr{E}^\sharp(\sigma) = \mathrm{Tr}_S\big(\mathscr{V}(\sigma)\big)$, where $\mathscr{V}$ is implemented by the isometry

$V|\phi\rangle = U|\phi\rangle\,|\psi\rangle$. As a simple example of the concept, it is easy to verify that the identity channel and the trace channel form a complementary pair.

[Possibly include a figure here illustrating complementarity]

The main result from [**?**] is stated as follows.

Theorem 7 *Let $\mathscr{E}$ and $\mathscr{E}^\sharp$ be complementary channels. If a subsystem B is ϵ-correctable (respectively ϵ-private) for $\mathscr{E}$, then it is $2\sqrt{\epsilon}$-private (respectively $2\sqrt{\epsilon}$-correctable) for $\mathscr{E}^\sharp$. The ideal result, obtained by setting $\epsilon = 0$ implies that B is a correctable subsystem for $\mathscr{E}$ if and only if B is a private subsystem for $\mathscr{E}^\sharp$.*

The key technical ingredient in the proof is the following theorem from [**?**], which can be regarded as a fundamental result in quantum information. Roughly speaking, the result says that two channels are close in diamond norm precisely when they have two isometric dilations that are close in operator norm.

Theorem 8 *Let $\mathscr{E}$, $\mathscr{E}'$ be arbitrary quantum channels both from Hilbert space $\mathscr{X}$ to $\mathscr{Y}$, and let V and V' be two corresponding isometric dilations with a common dilation space $\mathscr{Z}$. Then*

$$\left\|\mathscr{E} - \mathscr{E}'\right\|_\diamond \leq 2 \min_{\mathrm{U}} \left\|(I_{\mathscr{Y}} \otimes U)V - V'\right\|_\infty , \tag{1.28}$$

where the minimum is taken over all unitary U on $\mathscr{Z}$. Moreover, if $\dim \mathscr{Z} \geq 2 \dim \mathscr{X} \dim \mathscr{Y}$ we also have

$$\min_{\mathrm{U}} \left\|(I_{\mathscr{Y}} \otimes U)V - V'\right\|_\infty^2 \leq \left\|\mathscr{E} - \mathscr{E}'\right\|_\diamond . \tag{1.29}$$

One simple application of Theorem 7 is in the standard paradigm of quantum communication, where it is presumed that any dilation space for the channel $\mathscr{E}$ linking Alice to Bob ends up in the hands of an adversary. The theorem then implies that any subsystem that is ϵ-correctable for Bob is $2\sqrt{\epsilon}$-private for the adversary. This result is akin to Theorem II of Ref. [**?**], which establishes the sufficiency of decoupling from the environment for the preservation of entanglement by a channel.

Example 2 *As a simple example of complementarity for the ideal case, consider a two-qubit noise model that induces a phase flip Z_1 on the first qubit with probability one half. The associated channel on $\mathbb{C}^2 \otimes \mathbb{C}^2$ is $\mathscr{E}(\sigma) = \frac{1}{2}(\sigma + Z_1 \sigma Z_1)$. The code subspace $\mathscr{C}$ with basis $\{|00\rangle, |01\rangle\}$ is a DFS for $\mathscr{E}$,*

since $\mathscr{E}(\sigma) = \sigma$ *for all* σ *supported on the code* $\mathscr{C}$*. The map* $\mathscr{E}$ *can be obtained by tracing out a single qubit environment* E *as* $\mathscr{E}(\sigma) = \mathrm{Tr}_E(\, U(\sigma \otimes |0\rangle\langle 0|)U^\dagger\,)$*, where* U *is the unitary* $U \propto I_2 \otimes |0\rangle\langle 0| + Z_1 \otimes |0\rangle\langle 1| + I_2 \otimes |1\rangle\langle 0| - Z_1 \otimes |1\rangle\langle 1|$*. Direct computation reveals the complementary channel* $\mathscr{E}^\sharp(\sigma) = \mathrm{Tr}_S(\, U(\sigma \otimes |0\rangle\langle 0|)U^\dagger\,)$*, satisfies* $\mathscr{E}^\sharp(\sigma) = \mathrm{Tr}(\sigma)\rho_1 + \mathrm{Tr}(\sigma Z_1)\rho_2$*, where* $\rho_1 \propto |0\rangle\langle 0| + |1\rangle\langle 1|$ *and* $\rho_2 \propto |0\rangle\langle 1| + |1\rangle\langle 0|$*. Theorem 7 predicts the messenger space* $\mathscr{C}$ *is a private subspace for* $\mathscr{E}^\sharp$*. Indeed, one can easily verify that for all* σ *supported on the code* $\mathscr{C}$ *we have* $\mathscr{E}^\sharp(\sigma) = \mathrm{Tr}(\sigma)\, P$*, with the projector* $P = \rho_1 + \rho_2$*.*