Open Systems & Information Dynamics
Vol. 15, No. 4 (2008) 329–343

World Scientific
www.worldscientific.com

Entropy of a Quantum Error Correction Code

David W. Kribs

Department of Mathematics and Statistics, University of Guelph Guelph Ontario, N1G 2W1, Canada
and
Institute for Quantum Computing, University of Waterloo Waterloo, Ontario, N2L 3G1, Canada

e-mail: dkribs@uoguelph.ca

Aron Pasieka

Department of Physics, University of Guelph Guelph, Ontario, N1G 2W1, Canada

e-mail: aron@physics.uoguelph.ca

Karol Życzkowski

Instytut Fizyki im. Smoluchowskiego, Uniwersytet Jagielloński ul. Reymonta 4, 30-059 Kraków, Poland
and
Centrum Fizyki Teoretycznej, Polska Akademia Nauk Al. Lotników 32/44, 02–668 Warszawa, Poland

e-mail: karol@tatry.if.uj.edu.pl

(Received: August 7, 2008)

Abstract. We define and investigate the notion of entropy for quantum error correcting codes. The entropy of a code for a given quantum channel has a number of equivalent realisations, such as through the coefficients associated with the Knill-Laflamme conditions and the entropy exchange computed with respect to any initial state supported on the code. In general the entropy of a code can be viewed as a measure of how close it is to the minimal entropy case, which is given by unitarily correctable codes (including decoherence-free subspaces), or the maximal entropy case, which from dynamical Choi matrix considerations corresponds to non-degenerate codes. We consider several examples, including a detailed analysis of the case of binary unitary channels, and we discuss an extension of the entropy to operator quantum error correcting subsystem codes.

1. Introduction

Quantum error correcting codes are a central weapon in the battle to overcome the effects of environmental noise associated with attempts to control quantum mechanical systems as they evolve in time [1, 2]. It is thus important to develop techniques that assist in determining whether one code is

better than another one for a given noise model. In this paper we make a contribution to this study by introducing the notion of entropy for quantum error correcting codes.

No single quantity can be expected to hold all information on a code, its entropy included. Nevertheless, the entropy of a code is one way in which the amount of effort required to recover a code can be quantified. In the extremal case, a code has zero entropy if and only if it can be recovered with a single unitary operation. This is the simplest of all correction operations in that a measurement is not required as part of the correction process. These codes have been recently coined *unitarily correctable* [3, 4, 5], and include *decoherence-free subspaces* [6 – 10] in the case that recovery is the trivial identity operation. Thus, more generally, the entropy can be regarded as a measure of how close a code is to being unitarily correctable, or decoherence-free in some cases.

In the next section we introduce the entropy of a code, along with required nomenclature. We also consider an example motivated by the stabilizer formalism [11] and discuss an extension of code entropy to operator quantum error correcting subsystem codes [12 – 15]. We then consider in detail an illustrative class of quantum operations for which the code structure has recently been characterised, the class of *binary unitary channels* [16 – 22].

2. Entropy of a Quantum Error Correction Code

Let ρ denote a quantum state: a Hermitian, positive operator, satisfying the trace normalisation condition $\mathrm{Tr}\rho = 1$. A linear quantum operation (or channel) Φ, which sends the density operator ρ of size N into its image ρ' of the same size may be given in the Choi-Kraus form [23, 24]

$$\rho' \;=\; \Phi(\rho) \;=\; \sum_{i=1}^{M} E_i \rho E_i^\dagger \,. \tag{1}$$

The Kraus operators E_i can be chosen to be orthogonal $\langle E_i|E_j\rangle = \mathrm{Tr}E_i^\dagger E_j = d_i\delta_{ij}$, so that the non-negative weights d_i become eigenvalues of the dynamical (Choi) matrix, $D_\Phi = (\langle E_i|E_j\rangle)$. We refer to the rank of the Choi matrix as the *Choi rank* of Φ. Observe that the Choi rank of Φ is equal to the minimal number of Kraus operators required to describe Φ as in (1).

Hence in the canonical form the number M of non-zero Kraus operators does not exceed N^2. Due to the theorem of Choi, the map Φ is completely positive (CP) if and only if the corresponding dynamical matrix is positive if and only if Φ has a form as in (1). The map Φ is *trace preserving*, $\mathrm{Tr}\rho' = \mathrm{Tr}\rho = 1$, if and only if $\sum_{i=1}^{N^2} E_i^\dagger E_i = \mathbb{1}$ where we assume some E_i are zero if M is less than N^2. The family of operators E_i is not unique. However, if

$\{F_j\}$ is another family of operators that determine Φ as in (1), then there is a scalar unitary matrix $U = (u_{ij})$ such that $E_i = \sum_j u_{ij} F_j$ for all i. We refer to this as the *unitary invariance* of Choi-Kraus decompositions.

2.1. Entropy exchange and Lindblad theorem

To characterise the information missing in a quantum state one uses its *von Neumann* entropy,

$$S(\rho) \;=\; -\mathrm{Tr}\,\rho \log \rho\,. \tag{2}$$

We will use the convention that log refers to logarithm base two as this provides a cleaner operational qubit definition in the context of quantum information.

In order to describe the action of a CP map Φ, represented in the canonical Choi-Kraus form (1), for an initial state ρ we may compare its entropy with the entropy of the image $S(\rho') = S(\Phi(\rho))$. To obtain a bound for such an entropy change, we can define an operator $\sigma = \sigma(\Phi, \rho)$ acting on an extended Hilbert space $\mathcal{H}_{N^2}$,

$$\sigma_{ij} \;=\; \mathrm{Tr}\,\rho E_i^\dagger E_j\,, \quad i,j = 1,\ldots,N^2. \tag{3}$$

If the map Φ is stochastic, the operator σ is positive definite and normalised so it represents a density operator in its own right, $\sigma \in \mathcal{M}_{N^2}$ (specifically, it is an initially pure environment evolved by the unitary dilation of Φ). Observe that for any unitary map, $\Phi_U(\rho) = U\rho U^\dagger$, the form (1) consists of a single term only. Hence in this case the operator σ reduces to a single number equal to unity and its entropy vanishes, $S(\sigma(\Phi_U, \rho)) = 0$.

The auxiliary state σ acting in an extended Hilbert space was used by Lindblad to derive bounds for the entropy of an image $\rho' = \Phi(\rho)$ of any initial state. The bounds of Lindblad [25],

$$0 \;\le\; |S(\rho') - S(\sigma)| \;\le\; S(\rho) \;\le\; S(\sigma) + S(\rho')\,, \tag{4}$$

are obtained by defining another density matrix in the composite Hilbert space $\mathcal{H}_N \otimes \mathcal{H}_M$,

$$\omega \;=\; \sum_{i=1}^{M}\sum_{j=1}^{M} E_j \rho E_i^\dagger \otimes |i\rangle\langle j|\,, \tag{5}$$

where $M = N^2$ and $|i\rangle$ forms an orthonormal basis in $\mathcal{H}_M$. Thus, ω is simply the system and an initially pure environment evolved by the unitary dilation of Φ. Computing partial traces one finds that $\mathrm{Tr}_N \omega = \sigma$ and $\mathrm{Tr}_M \omega = \rho'$. It is possible to verify that $S(\omega) = S(\rho)$, so making use of the subadditivity of entropy and the triangle inequality [26] one arrives at (4).

If the initial state is pure, that is if $S(\rho) = 0$, we find from (4) that the final state ρ' has entropy $S(\sigma)$. For this reason $S(\sigma)$ was called the *entropy*

exchange of the operation by Shumacher [27]. In that work an alternative formula for the entropy exchange was proved,

$$S(\sigma(\Phi,\rho)) \;=\; S\Big((\Phi\otimes\mathbb{1})|\psi\rangle\langle\psi|\Big)\,, \tag{6}$$

where $|\psi\rangle$ is an *arbitrary* purification of the mixed state, $\mathrm{Tr}_B|\psi\rangle\langle\psi| = \rho$. Thus, the entropy exchange is invariant under purification of the initial state and remains a function only of the initial density operator ρ and the map Φ.

2.2. Quantum error correcting codes

A quantum operation Φ allows for an error correction scheme in the standard framework for quantum error correction [11, 28, 29, 30, 31] if there exists a subspace $\mathcal{C}$ such that for some set of complex scalars $\Lambda = (\lambda_{ij})$ the corresponding projection operator $P_{\mathcal{C}}$ satisfies

$$P_{\mathcal{C}}E_i^\dagger E_j P_{\mathcal{C}} \;=\; \lambda_{ij}P_{\mathcal{C}} \quad \text{for all} \quad i,j=1,\ldots,N^2. \tag{7}$$

Specifically, this is equivalent to the existence of a quantum *recovery operation* Ψ such that

$$\Psi\circ\Phi\circ\mathcal{P}_{\mathcal{C}} \;=\; \mathcal{P}_{\mathcal{C}}\,, \tag{8}$$

where $\mathcal{P}_{\mathcal{C}}$ is the map $\mathcal{P}_{\mathcal{C}}(\rho) = P_{\mathcal{C}}\rho P_{\mathcal{C}}$. The subspace related to $P_{\mathcal{C}}$ determines a *quantum error correcting code* (QECC) for the map Φ. A special class of codes are the *unitarily correctable codes* (UCC), which are characterised by the existence of a unitary recovery operation $\Psi(\rho) = U\rho U^\dagger$. These codes include *decoherence-free subspaces* (DFS) in the case that Ψ is the identity map, $\Psi(\rho) = \rho$.

It can be shown that the matrix $\Lambda = (\lambda_{ij})$ is Hermitian and positive, and is in fact a density matrix, so it can be considered as an auxiliary state acting in an extended Hilbert space of size at most N^2. It is easy to obtain a more refined global upper bound on the rank of Λ in terms of the map Φ.

LEMMA 1 *Let Λ be the matrix determined by a code $\mathcal{C}$ for a quantum map Φ. Then the rank of Λ is bounded above by the Choi rank of Φ.*

Proof. Without loss of generality, assume the Choi matrix D_Φ to be diagonal. We have for all i,

$$\lambda_{ii}\dim\mathcal{C} \;=\; \mathrm{Tr}(\lambda_{ii}P_{\mathcal{C}}) \;=\; \mathrm{Tr}(P_{\mathcal{C}}E_i^\dagger E_i P_{\mathcal{C}}) \;\le\; \mathrm{Tr}(E_i^\dagger E_i) = \langle E_i|E_i\rangle\,, \tag{9}$$

and the result follows from the positivity of D_Φ and Λ. □

Unitarily correctable codes are typically highly *degenerate* codes, as the map Φ collapses to a single unitary operation when restricted to the code subspace. In particular, the unitary invariance of Choi-Kraus representations implies

that the restricted operators $E_i P_{\mathcal{C}}$ are all scalar multiples of a single unitary. More generally, one can see that a code $\mathcal{C}$ is degenerate for Φ precisely when the Choi rank of Φ is strictly greater than the rank of Λ. Indeed, the Choi rank counts the minimal number of Kraus operators required to implement Φ via (2.1), and satisfaction of this strict inequality means there is redundancy in the description of $\Phi \circ \mathcal{P}_{\mathcal{C}}$ by the operators $E_i P_{\mathcal{C}}$. Thus, for these reasons we shall refer to codes as *non-degenerate* if the Choi rank of Φ coincides with the rank of Λ and if the spectrum of Λ is uniformly balanced — that is to say, that non-degenerate codes correspond to the maximally degenerate error correction matrix, Λ being proportional to the identity matrix.

2.3. Entropy of a code

Assume now that an error correcting code $\mathcal{C}$ exists and all conditions (7) are satisfied. If a quantum state ρ is supported on the code then $P_{\mathcal{C}} \rho P_{\mathcal{C}} = \rho$ and the calculation of the entropy exchange (3) simplifies,

$$\sigma_{ij} \;=\; \mathrm{Tr}\rho E_i^\dagger E_j \;=\; \mathrm{Tr}P_{\mathcal{C}}\rho P_{\mathcal{C}} E_i^\dagger E_j \;=\; \mathrm{Tr}\rho P_{\mathcal{C}} E_i^\dagger E_j P_{\mathcal{C}} \;=\; \mathrm{Tr}\rho\lambda_{ij} P_{\mathcal{C}} \;=\; \lambda_{ij}\,. \tag{10}$$

In this way, we have shown that the error correction matrix Λ is *equal* to the auxiliary matrix σ of Lindblad, provided that the initial state belongs to the code subspace.

From another direction, given an error correcting code $\mathcal{C}$ for a map Φ, in [4, 32] it was shown that there is a quantum state τ and an isometry V such that for all $\rho = P_{\mathcal{C}} \rho P_{\mathcal{C}}$,

$$\Phi(\rho) \;=\; V(\tau \otimes \rho)V^\dagger. \tag{11}$$

The result, which can be seen as a consequence of the decoupling condition of [33], gives an explicit way to "see" a code at the output stage of a quantum process for which the code is correctable. The result (and its subsystem generalization — see below) may also be viewed as a formalisation of the *subsystem principle* for preserving quantum information [7]. From the proof of this result one can see directly that the entropy of τ satisfies $S(\tau) = S(\Lambda)$. This equality follows also from the fact that τ and Λ can be interpreted as the states obtained by partial trace of an initially pure state with respect to two different subsystems.

Thus, from multiple perspectives we find motivation for the following:

DEFINITION 1 Given a quantum operation Φ with Kraus operators $\{E_i\}$ and a code $\mathcal{C}$ with matrix Λ given by (7), we call the von Neumann entropy $S(\Phi, \mathcal{C}) := S(\Lambda)$ the *entropy of $\mathcal{C}$ relative to* Φ.

The entropy of a code depends only on the map and the subspace defined by $P_{\mathcal{C}}$, not on any particular state in the code subspace. Thus, the entropy

exchange will be the same for all initial states supported on the code subspace and is therefore a property of the code itself.

In the following result we determine what possible values the code entropy can take, and we derive a characterisation of the extremal cases in terms of both the code and the map.

THEOREM 1 *Let Φ be a quantum operation and let $\mathcal{C}$ be a code with matrix Λ given by (7). Then $S(\Phi,\mathcal{C})$ belongs to the closed interval $[0,\log D]$, where D is the Choi rank of Φ. Furthermore, the extremal cases are characterised as follows:*

(i) $S(\Phi,\mathcal{C}) = 0$ *if and only if $\mathcal{C}$ is a unitarily correctable code for Φ.*

(ii) $S(\Phi,\mathcal{C}) = \log D$ *if and only if $\mathcal{C}$ is a non-degenerate code for Φ.*

Proof. By Lemma 1 and the subsequent discussion, the maximal entropy case occurs when the rank of Λ and D_Φ coincide and the spectrum of Λ is uniformly balanced; that is, the code is non-degenerate. This occurs (by a standard spectral majorization argument) precisely when the code entropy satisfies $S(\Phi,\mathcal{C}) = \log D$.

For the minimal entropy case, first suppose that $\mathcal{C}$ is a UCC for Φ. Then by (8) there is a unitary operation $\mathcal{U}(\rho) = U\rho U^\dagger$ such that $\Phi\circ\mathcal{P}_\mathcal{C} = \mathcal{U}\circ\mathcal{P}_\mathcal{C}$. Thus by the unitary invariance of Choi-Kraus decompositions, it follows that $E_iP_\mathcal{C} = \alpha_iUP_\mathcal{C}$ for some scalars α_i. Hence we have $\Lambda = (\overline{\alpha}_i\alpha_j) = |\psi\rangle\langle\psi|$, where $|\psi\rangle$ is the vector state with coordinates α_i, and so $S(\Phi,\mathcal{C}) = S(\Lambda) = 0$.

On the other hand, suppose $\Lambda = |\psi\rangle\langle\psi|$ is of rank one. Let V be a scalar unitary that diagonalises Λ. It follows that V induces a unitary change of representation for Φ via (7) from $\{E_i\}$ to $\{F_j\}$. But since $V\Lambda V^\dagger$ is diagonal, only one F_j, say F, is non-zero, and hence by unitary invariance we have $FP_\mathcal{C} = UP_\mathcal{C}$ for some unitary U. Thus $\Phi\circ\mathcal{P}_\mathcal{C} = \mathcal{U}\circ\mathcal{P}_\mathcal{C}$, and the result follows. □

From an operational perspective, the numerical value of the entropy of a code allows us to quantify the number of ancilla qubits needed to perform a recovery operation. Specifically, the Choi rank, D, of a map Φ gives the minimum number of Kraus operators necessary to describe the map or, by Stinespring's dilation theorem [34], the dimension of the ancilla required to implement Φ as a unitary. The rank of Λ then gives the number of Kraus operators necessary to describe the action of the map restricted to $\mathcal{C}$ and thus the number of Kraus operators, M, necessary for a recovery operation in the usual measurement cum reversal picture of recovery. Again by Stinespring's dilation theorem we need an M-dimensional ancilla to implement the recovery as a unitary, and thus this requires $\log M$ qubits.

Hence the entropy is equal to zero for a unitarily correctable code, in which the action of the noise is unitary and thus requires no ancilla to implement the recovery operation. If the code entropy is positive, then any

state of the code can potentially evolve to any one of multiple locations in the system Hilbert space under the action of the noise Φ. This fact has to be compensated by the recovery operation Ψ. The maximal entropy case for a particular Φ is characterised by evolution to each of these locations ($M = D$ by Lemma 1) with equal probability (by Theorem 1). Here the entropy and thus the number of qubits in the ancilla will be $\log D$.

2.4. Stabilizer example

As an example from the stabilizer formalism, consider a three-qubit system with the usual notation X_i, Z_i, $i = 1, 2, 3$, for Pauli operators [1]. The single-qubit stabilizer code with generators $\{Z_1Z_2, Z_2Z_3\}$, is spanned by $|0_L\rangle = |000\rangle$ and $|1_L\rangle = |111\rangle$. The set of operators $\{\mathbb{1}, X_1, X_2, X_3\}$ form a correctable set of errors for this stabilizer thus we can consider a channel, a three-qubit bit-flip channel, comprised of these operators – for example, the channel with Kraus operators

$$E_1 = \sqrt{\frac{1}{3}(3-p-q-r)}\,\mathbb{1}\,, \qquad E_2 = \sqrt{\frac{1}{3}p}\,X_1\,,$$

$$E_3 = \sqrt{\frac{1}{3}q}\,X_2\,, \qquad E_4 = \sqrt{\frac{1}{3}r}\,X_3\,.$$

Using $P_{\mathcal{C}} = |000\rangle\langle 000| + |111\rangle\langle 111|$, (7) tells us that the error correction matrix is

$$\Lambda = \begin{pmatrix} \frac{1}{3}(3-p-q-r) & 0 & 0 & 0 \\ 0 & \frac{1}{3}p & 0 & 0 \\ 0 & 0 & \frac{1}{3}q & 0 \\ 0 & 0 & 0 & \frac{1}{3}r \end{pmatrix}.$$

The entropy of this code is therefore

$$\begin{aligned} S(\Lambda) = & -\frac{1}{3}(3-p-q-r)\log\frac{1}{3}(3-p-q-r) \\ & -\frac{1}{3}p\log\frac{1}{3}p - \frac{1}{3}q\log\frac{1}{3}q - \frac{1}{3}r\log\frac{1}{3}r\,. \end{aligned}$$

As we would expect, the minimum entropy is achieved when $p = q = r = 0$.

The maximum entropy occurs when $p = q = r = 3/4$, which we might also expect since this puts the auxiliary density matrix Λ into the maximally mixed state. Here, the Choi rank of our map is 4 as is the rank of Λ, and the spectrum of Λ is uniformly balanced. So $\mathcal{C}$ is non-degenerate for Φ. Further, as we expect from Theorem 1, the entropy is $\log 4 = 2$. Since the rank of Λ is the number of Kraus operators required for a recovery operation we find that in order to dilate the recovery operation to a unitary process, we need

Qubit Code $\mathcal{C} = \{\|0_L\rangle, \|1_L\rangle\}$	Entropy $S(\Phi, \mathcal{C})$
$\{\|000\rangle, \|111\rangle\}$	$\log 3$
$\{\|000\rangle + \|100\rangle, \|011\rangle + \|111\rangle\}$	$\log 3 - \frac{2}{3}$
$\{\|000\rangle + \|100\rangle + \|010\rangle + \|110\rangle,$ $\|011\rangle + \|111\rangle + \|001\rangle + \|101\rangle\}$	0

Table 1: Codes for the noise model $\Phi = \frac{1}{\sqrt{3}}\{I, X_1, X_2\}$.

a 4-dimensional space, or equivalently a 2-qubit ancilla, which matches the value of the entropy.

We next consider a variant of this noise model, in which the third qubit undergoes no error and the first and second qubits are flipped with probability equal to that of no error. Thus the map Φ has noise operators $\{I, X_1, X_2\}$, each weighted by $1/\sqrt{3}$. The entropies for a trio of correctable codes for Φ are given in Table 2.4 (vectors are assumed to be normalised). The first code is non-degenerate, and thus yields the maximal entropy for this noise model. The second code has positive entropy less than the maximum since it is partially degenerate for Φ. Indeed, one can check that X_1 (and I) act trivially on the code, whereas X_2 maps the code to an orthogonal subspace. The final code shows zero entropy since it is fully degenerate for Φ. In fact, as can be directly verified it is a decoherence-free subspace for Φ.

2.5. Entropy of a subsystem code

We next consider an extension of code entropy to the case of operator quantum error correcting subsystem codes. We shall only introduce this notion here and leave a potential further investigation for elsewhere. Subsystem codes were formally introduced under the umbrella of *operator quantum error correction* [3, 12], a framework that unifies the active and passive approaches to quantum error correction. These codes now play a central role in fault tolerant quantum computing.

Let $\mathcal{H}$ be a Hilbert space of finite dimension N. Any decomposition $\mathcal{H} = (\mathcal{A} \otimes \mathcal{B}) \oplus \mathcal{K}$ determines subsystems A and B of $\mathcal{H}$. Given a quantum operation Φ acting on $\mathcal{H}$, we say that a subsystem B of $\mathcal{H}$ is *correctable* for Φ if there exist maps Ψ on $\mathcal{H}$ and τ_A on A such that

$$\Psi \circ \Phi \circ \mathcal{P}_{\mathcal{AB}} \;=\; (\tau_{\mathcal{A}} \otimes \mathrm{id}_{\mathcal{B}}) \circ \mathcal{P}_{\mathcal{AB}}\,, \tag{12}$$

where $\mathcal{P}_{AB}(\rho) = P_{AB}\rho P_{AB}$ and P_{AB} is the projection onto the subspace $A \otimes B$.

Subsystem codes generalize standard (subspace) codes (8) in the sense that subspaces may be regarded as subsystems with trivial ancilla ($\dim A = 1$). Thus, it is natural to suggest that a notion of entropy for subsystem codes

should generalize the subspace definition. We find motivation for such a notion through the main result of [4] alluded to above. To every correctable subsystem for Φ, there are subsystems C and $B' \cong B$, a map $\tau_{C|A}$ from A to C and a unitary map $\mathcal{V}_{\mathcal{B}'|\mathcal{B}}$ from B to B' such that

$$\Phi \circ \mathcal{P}_{\mathcal{AB}} = (\tau_{\mathcal{C}|\mathcal{A}} \otimes \mathcal{V}_{\mathcal{B}'|\mathcal{B}}) \circ \mathcal{P}_{\mathcal{AB}}\,. \tag{13}$$

Recall that the *maximal output entropy* of a channel Ψ is given by $S(\Psi) := \max_\rho S(\Psi(\rho))$. This motivates the following.

DEFINITION 2 Let Φ be a quantum operation with correctable subsystem B that satisfies (12). Then we define the entropy of B relative to Φ as the maximal output entropy of the associated ancilla channel, $S(\tau_{C|A})$ from (13).

Observe that this generalizes Definition 1, since a density operator may be regarded as a channel from a one-dimensional input space. The minimal entropy case is characterised by the ancilla channel $\tau_{C|A}$ having range supported on a one-dimensional subspace. Such codes are unitarily correctable, in fact as subspaces, but the converse is not true. Instead, in the more general subsystem setting, the minimal entropy case is described by the associated ancilla subsystem A undergoing "cooling" to a fixed state. In principle, one should be able to conduct a deeper analysis of subsystem code entropy. We leave this as an open investigation for elsewhere.

3. Entropy of a Code for Binary Unitary Channels

A binary unitary channel has the form

$$\rho' \;=\; \Phi(\rho) \;=\; (1-p)W_1\rho W_1^\dagger + pW_2\rho W_2^\dagger, \tag{14}$$

where W_1 and W_2 denote two arbitrary unitary operators and the probability p belongs to $[0,1]$.

It is clear that the problem of finding an error correcting code subspace $\mathcal{C}$ for the above map is equivalent to the case

$$\rho'' \;=\; \Phi_U(\rho) \;=\; (1-p)\rho + pU\rho U^\dagger, \tag{15}$$

where $U = W_1^\dagger W_2$. The number M of Kraus operators is equal to 2, with $E_1 = \sqrt{1-p}\,\mathbb{1}$ and $E_2 = \sqrt{p}\,U$. Thus the error correction matrix Λ is of size two and reads

$$\Lambda \;=\; \begin{pmatrix} 1-p & \sqrt{p(1-p)}\lambda \\ \sqrt{p(1-p)}\lambda^* & p \end{pmatrix}, \tag{16}$$

where λ is a solution of the *compression problem* for U

$$P_{\mathcal{C}} U P_{\mathcal{C}} \;=\; \lambda P_{\mathcal{C}}\,. \tag{17}$$

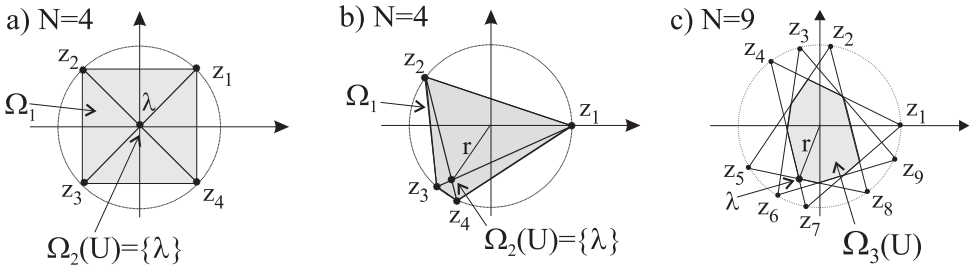

Fig. 1: Higher rank numerical range Ω_k for unitary matrices U describing a bi-unitary channel: two-qubit system, a) example 2 with $\lambda = 0$, b) case with $r = |\lambda| >> 0$ for which code entropy is smaller, c) two-qutrit case with $\lambda \in \Omega_3(U)$ chosen to maximize its modulus r and to minimize the code entropy $S(\Lambda)$.

The set of solutions to this problem can be phrased in terms of the *higher-rank numerical range* of the matrix U. The rank-k numerical range of U is defined as

$$\Omega_k(U) \;=\; \{\lambda \in \mathbb{C} \,:\, PUP = \lambda P \text{ for some rank-}k \text{ projection } P\}\,. \qquad (18)$$

Given the dimension k that defines the size of the desired correctable code, each λ in $\Omega_k(U)$ corresponds to a particular correctable code defined by the associated projection P that solves (17). The following is a straightforward application of (7).

PROPOSITION 1 *Given a binary unitary channel Φ, there exists a rank-k correctable code for Φ if and only if the rank-k numerical range of U is non-empty.*

Thus, the problem of finding the correctable codes for a given binary unitary channel can be reduced to the problem of finding the higher-rank numerical range of U. This problem has recently been solved in its entirety [16 – 22]. Most succinctly, in terms of the eigenvalues $\sigma(U)$ of U, the kth numerical range of U is the convex subset of the unit disk given by

$$\Omega_k(U) \;=\; \bigcap_{\Gamma \subseteq \sigma(U);\; |\Gamma| = N-k+1} \mathrm{conv}\,(\Gamma)\,, \qquad (19)$$

where $\mathrm{conv}\,\{\lambda_1, \ldots, \lambda_m\}$ is the set of linear combinations $\lambda = t_1\lambda_1 + \ldots + t_m\lambda_m$ such that $\sum_{j=1}^{m} t_j = 1$ and $t_j \geq 0$. Figures 1.a and 1.b depict the case of a generic two-qubit unitary ($N = 4$) with $k = 2$, while Fig. 1.c shows the case of a generic two-qutrit unitary noise ($N = 3 \times 3 = 9$) with $k = 3$.

With a particular λ in-hand, straightforward algebra provides us with the spectrum of the matrix (16),

$$\Lambda_{\pm} \;=\; \frac{1}{2}\left(1 \pm \sqrt{1-4p(1-p)(1-|\lambda|^2)}\right), \tag{20}$$

which allows us to calculate the entropy of the code,

$$S(\Phi,\mathcal{C}) \;=\; S(\Lambda) \;=\; -\Lambda_+ \log \Lambda_+ - \Lambda_- \log \Lambda_- \,. \tag{21}$$

We are then led to the following:

THEOREM 2 *The minimum entropy rank-k code for a binary unitary channel* $\Phi(\rho) = (1-p)\rho + pU\rho U^\dagger$ *corresponds to any code for which the magnitude* $|\lambda|$ *of the compression values* $\lambda \in \Omega_k(U)$ *is closest to unity, while the maximum entropy corresponds to* $|\lambda|$ *closest to zero. Moreover, the code with minimal entropy can be constructively obtained.*

Proof. The first statement follows directly from an application of first and second derivative tests on (21), constrained to the unit disk. A minimal entropy code can be explicitly constructed based on the analysis of higher-rank numerical ranges [16 – 22]. □

EXAMPLE 1 As an illustration of the code construction in the simplest possible case ($N = 4, k = 2$), let U be unitary with spectrum depicted in Figure 1.a, $\sigma(U) = \{z_k = \exp(k\pi/4) : k = 1,3,5,7\}$. Let $|\psi_k\rangle$ be the associated eigenstates, $U|\psi_k\rangle = z_k|\psi_k\rangle$. In this case we have $\Omega_2(U) = \{0\}$, so $\lambda = 0$, and one can check directly that a single qubit correctable code for Φ is given by $\mathcal{C} = \text{span}\,\{|\phi_1\rangle, |\phi_2\rangle\}$, where

$$\begin{cases} |\phi_1\rangle &=& \frac{1}{\sqrt{2}}(|\psi_1\rangle + |\psi_3\rangle) \\ |\phi_2\rangle &=& \frac{1}{\sqrt{2}}(|\psi_2\rangle + |\psi_4\rangle)\,. \end{cases}$$

For a concrete example, in the case that $p = 0.01$, (21) yields a code entropy of $S(\Phi,\mathcal{C}) = 0.081$.

The general case requires a more delicate construction, nevertheless it can be done. The "eigenstate grouping" procedure used above can be applied whenever k divides N. For instance, in the generic $N = 9$ and $k = 3$ case depicted in Figure 1.c, a single qutrit code can be constructed for all λ in the region $\Omega_3(U)$. The states $|\phi_i\rangle$, $i = 1,2,3$, can be constructed in an analogous manner by grouping the nine eigenstates for U into three groups of three, and writing λ in three different ways as a linear combination of the associated unimodular eigenvalues z_j, $j = 1,\ldots,9$.

However, without going into the details of this construction we can still analyze the corresponding code entropies. For simplicity assume the nine

eigenvalues are distributed evenly around the unit circle with $z_1 = 0$. By Theorem 2, we know that the entropy will be minimized for any λ that gives the minimum distance from $\Omega_3(U)$ to the unit circle. An elementary calculation shows that one such λ, given by the intersection of the lines through the first and seventh, and sixth and ninth eigenvalues (counting counterclockwise) is approximately $\lambda_0 = 0.092 - 0.524\,i$. With the probability $p = 0.01$, the corresponding error correction matrix Λ has spectrum $\{0.007, 0.993\}$. Thus, (20) and (21) yield the minimal qutrit code entropy for this channel as

$$\min_{\dim \mathcal{C}=3} S(\Phi, \mathcal{C}) \;=\; \min_{\lambda \in \Omega_3(U)} S(\Lambda) \;=\; S(\Lambda_{\lambda=\lambda_0}) \;=\; 0.060\,.$$

On the other hand, as $\lambda = 0$ belongs to $\Omega_3(U)$, by Theorem 2 and (16) we also see the maximal entropy for $p = 0.01$ occurs for any code with $\lambda = 0$. In such cases we have Λ spectrum $\{0.01, 0.99\}$, and hence the maximal entropy is $S(\Lambda_{\lambda=0}) = 0.081$.

Changing focus briefly, if we fix an arbitrary unitary U, then we could consider the family of channels determined by varying the probability p. It follows from (21) that the channel with the correctable codes of maximal entropy corresponds to the $p = \frac{1}{2}$ channel, and the channels whose correctable codes possess minimal entropy correspond to $p = 0$ and $p = 1$. Indeed, the value of λ depends on U but not p, thus a given λ will solve (17) for any p and so λ can be chosen independently using the above theorem. The result once again follows from an application of first and second derivative tests with p between 0 and 1.

The following results show that the entropy of a code for a binary unitary channel can be regarded as a measure of how close the code is to a decoherence-free subspace.

LEMMA 2 *If Φ is a binary unitary channel, then the sets of unitarily correctable subspaces and decoherence-free subspaces coincide.*

Proof. As proved in [4], for any bistochastic (unital) map Φ, a condition which is satisfied by every binary unitary channel tells that the unitarily correctable codes (respectively the decoherence-free subspaces) for Φ are imbedded in the fixed point algebra for the map $\Phi^\dagger \circ \Phi$ (respectively Φ), where $\Phi^\dagger$ is the Hilbert-Schmidt dual map of Φ. In particular, it follows from this fact that the former set is given by the set of operators that commute with U and $U^\dagger$, whereas the latter is the set of operators that commute with U. By the Spectral Theorem these two sets coincide. □

THEOREM 3 *Let Φ be a binary unitary channel. Then there is a rank-k code $\mathcal{C}$ of zero entropy, $S(\Phi, \mathcal{C}) = 0$, for Φ if and only if there is a k-dimensional decoherence-free subspace for Φ if and only if there exists $\lambda \in \Omega_k(U) \cap \sigma(U)$.*

Proof. A k-dimensional decoherence-free subspace for Φ corresponds to an eigenvalue λ of U with multiplicity at least k (see [4] and the references therein); that is, $\lambda \in \Omega_k(U) \cap \sigma(U)$. The rest follows from the lemma and previous theorem. □

In order to further illustrate these results, consider again the case of an arbitrary two-qubit system ($N = 4$). The correctable codes with largest entropy are those with $p = \frac{1}{2}$ and so the spectrum of Λ reads

$$\Lambda_{\pm} \;=\; \frac{1}{2}(1 \pm |\lambda|)\,. \tag{22}$$

In the two-qubit case, the complex number λ is given by the point inside the unit circle at which two diagonals of the quadrangle formed by the spectrum of U cross (see Figs. 1.a and 1.b). Consider the special case of the problem where U has a doubly degenerated eigenvalue, so that $|\lambda| = 1$. For example, U could be any (non-identity) element of the two-qubit Pauli group. Then the spectrum of Λ consists of $\{1, 0\}$ which implies $S(\Lambda) = 0$ (despite p having been chosen for the largest entropy correctable codes). Hence Λ is pure and there exists a decoherence free subspace — the one spanned by the degenerated eigenvalues of U.

In general, for binary unitary channels one may use the entropy (21) as a measure quantifying to what extend a given error correction code is close to a decoherence-free subspace. For instance, any channel (15) acting on a two-qubit system and described by unitary matrix $U = W_1^{\dagger} W_2$ of size 4 may be characterised by the radius $r = |\lambda|$ of the point in which two diagonals of the quadrangle of the spectrum cross. The larger r, the smaller entropy $S(\Phi, \mathcal{C})$, and the closer the error correction code is to a decoherence-free space.

The code entropy can also be used to classify codes designed for a binary unitary channel acting on larger systems. For instance in the case of two qutrits, $N = 3 \times 3 = 9$, one can find a subspace supported on $k = 3$ dimensional subspace. The solution is by far nonunique and can be parametrized by complex numbers λ belonging to an intersection of 3 triangles, which forms a convex set of a positive measure. From this set one can thus select a concrete solution providing a code $\mathcal{C}$, such that $r = |\lambda|$ is the largest, which implies that the code entropy, $S(\Phi, \mathcal{C})$, is the smallest — see Fig. 1.c. Such an error correction code is distinguished by being as close to the decoherence-free subspace as possible.

4. Conclusions

We have investigated the notion of entropy for quantum error correcting codes and quantum operations. Such entropy has multiple natural realisations through fundamental results in the theory of quantum error correction.

We showed how the extremal cases are characterised by unitarily correctable codes and decoherence-free subspaces on the one hand, and the nondegenerate case determined by the Choi matrix of the map on the other. We considered examples from the stabilizer formalism, and conducted a detailed analysis in the illustrative case of binary unitary channels. Recently developed techniques on higher-rank numerical ranges have been used to give a complete geometrical description of code entropies for binary unitary channels; in particular, the structure of these subsets of the complex plane can be used to visually determine how close a code is to the decoherence-free subspace. We also introduced an extension of code entropy to subsystem codes, and left a deeper investigation of this notion for elsewhere. It could be interesting to explore further applications of the code entropy in quantum error correction. For instance, although quantum error correction codes were originally designed for models of discrete time evolution in the form of a quantum operation, generalizations to the case of continuous evolution in time [35, 36, 37] have been investigated. Further, we have investigated perfect correction codes only, for which the error recovery operation brings the quantum state corrupted by the noise back to the initial state with fidelity equal one. Such perfect correction codes may be treated as a special case of more general approximate error correction codes [33, 38, 39]. Another recent investigation [40] includes analysis that suggests the measurement component of recovery may prove to be problematic in quantum error correction, and hence may motivate further investigation of unitarily correctable codes.

Acknowledgements

We thank the referee for helpful comments. D.W.K. was partially supported by NSERC grant 400160, by NSERC Discovery Accelerator Supplement 400233, and by Ontario Early Researcher Award 48142. A.P. was partially supported by an Ontario Graduate Scholarship. K.Ż. acknowledges support of an European research project SCALA and the special grant number DFG-SFB/38/2007 of Polish Ministry of Science.

Bibliography

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge, New York, 2000.

[2] D. Gottesman, in: *Encyclopedia of Mathematical Physics*, vol. 4, J.-P. Francoise, G. L. Naber, and S. T. Tsou, eds., Oxford, Elsevier, 2006, p. 196.

[3] D. W. Kribs, R. Laflamme, D. Poulin, and M. Lesosky, Quantum Inf. Comput. **6**, 382 (2006).

[4] D. W. Kribs and R. W. Spekkens, Phys. Rev. A **74**, 042329 (2006).

[5] R. Blume-Kohout, H. K. Ng, D. Poulin, and L. Viola, Phys. Rev. Lett. **100**, 030501 (2008).

[6] L.-M. Duan and G.-C. Guo, Phys. Rev. Lett. **79**, 1953 (1997).

[7] E. Knill, R. Laflamme, and L. Viola, Phys. Rev. Lett. **84**, 2525 (2000).

[8] D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).

[9] P. Zanardi, Phys. Rev. A **63**, 12301 (2001).

[10] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).

[11] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).

[12] D. Kribs, R. Laflamme, and D. Poulin, Phys. Rev. Lett. **94**, 180501 (2005).

[13] D. Poulin, Phys. Rev. Lett. **95**, 230504 (2005).

[14] D. Bacon, Phys. Rev. A **73**, 012340 (2006).

[15] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, prepint arXiv:quant-ph/0610153, 2006.

[16] M.-D. Choi, D. W. Kribs, and K. Życzkowski, Linear Algebra Appl. **418**, 828 (2006).

[17] M.-D. Choi, D. W. Kribs, and K. Życzkowski, Rep. Math. Phys. **58**, 77 (2006).

[18] M.-D. Choi, J. A. Holbrook, D. W. Kribs, and K. Życzkowski, Oper. Matrices **1**, 409 (2007).

[19] H. Woerdeman, Linear Multilinear Algebra **56**, 65 (2008).

[20] C.-K. Li and N.-S. Sze, Proc. Amer. Math. Soc. **136**, 3013 (2008).

[21] M.-D. Choi, M. Giesinger, J. A. Holbrook, and D. W. Kribs, Linear Multilinear Algebra **56**, 53 (2008).

[22] A. Y. Kazakov, J. Phys. A **41**, 255306 (2008).

[23] M.-D. Choi, Linear Algebra Appl. **10**, 285 (1975).

[24] K. Kraus, Ann. Phys. **64**, 311 (1971).

[25] G. Lindblad, in: Lecture Notes in Physics **378**, C. Bendjaballah, et al., ed., Springer-Verlag, Berlin, 1991, p. 36.

[26] H. Araki and E. Lieb, Comm. Math. Phys. **18**, 160 (1970).

[27] B. Schumacher, Phys. Rev. A **54**, 2614 (1996).

[28] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).

[29] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).

[30] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[31] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).

[32] A. Nayak and P. Sen, Quantum Inf. Comput. **7**, 103 (2007).

[33] B. Schumacher and M. D. Westmoreland, Quantum Inf. Process. **1**, 5 (2002).

[34] W. F. Stinespring, Proc. Amer. Math. Soc. **6** 211 (1955).

[35] S. L. Braunstein, Phys. Rev. Lett. **80**, 4084 (1998).

[36] S. Lloyd and J.-J. E. Slotine, Phys. Rev. Lett. **80**, 4088 (1998).

[37] O. Oreshkov, D. A. Lidar, and T. A. Brun, preprint arXiv:0806.3145, 2008.

[38] C. Crepeau, D. Gottesman, and A. Smith, preprint arXiv:quant-ph/0503139, 2005.

[39] R. Klesse, Phys. Rev. A **75**, 062315 (2007).

[40] R. Alicki, preprint arXiv:0807.2609, 2008.