Quantum Inf Process
DOI 10.1007/s11128-009-0131-z

Protected subspaces in quantum information

Krzysztof Majgier · Hans Maassen · Karol Życzkowski

Received: 27 February 2009 / Accepted: 2 September 2009
© Springer Science+Business Media, LLC 2009

Abstract In certain situations the state of a quantum system, after transmission through a quantum channel, can be perfectly restored. This can be done by "coding" the state space of the system before transmission into a "protected" part of a larger state space, and by applying a proper "decoding" map afterwards. By a version of the Heisenberg Principle, which we prove, such a protected space must be "dark" in the sense that no information leaks out during the transmission. We explain the role of the Knill–Laflamme condition in relation to protection and darkness, and we analyze several degrees of protection, whether related to error correction, or to state restauration after a measurement. Recent results on higher rank numerical ranges of operators are used to construct examples. In particular, dark spaces are constructed for any map of rank 2, for a biased permutations channel and for certain separable maps acting on multipartite systems. Furthermore, error correction subspaces are provided for a class of tri-unitary noise models.

Keywords Quantum error correction · Quantum operations · Protected spaces · Decoherence free subspaces

PACS 03.67.Pp · 03.65.Yz

K. Majgier · K. Życzkowski
Instytut Fizyki im. Smoluchowskiego, Uniwersytet Jagielloński, ul. Reymonta 4,
30-059 Kraków, Poland

H. Maassen
Department of Mathematics, University of Nijmegen, Heyendaalseweg 135,
6525 AJ Nijmegen, The Netherlands

K. Życzkowski (✉)
Centrum Fizyki Teoretycznej, Polska Akademia Nauk, Al. Lotników 32/44, 02-668 Warszawa, Poland
e-mail: karol@tatry.if.uj.edu.pl

Published online: 23 September 2009

1 Introduction

We consider a quantum channel of finite dimension through which a quantum system in some state is sent. The output consists of another quantum state, and possibly some classical information. We are interested in the question to what extent the original quantum state can be recovered from that state and that information. In particular, we investigate if there are subspaces of the Hilbert space of the original system, on which the state can be perfectly restored.

In the literature a hierarchy of such spaces, which we shall call *protected subspaces* here, has been described. The strongest protection possible is provided in the case of a "decoherence free subspace" [1–4]. In this case the channel acts on the subspace as a isometric transformation. All we have to do in order to recover the state, is to rotate it back.

The next strongest form of protection occurs when the channel acts on the subspace as a random choice between isometries, whose image spaces are mutually orthogonal. Then by measuring along a suitable partition of the output Hilbert space, it can be inferred from the output state which isometry has occurred, so that it can be rotated back. This situation is characterized by the well-known Knill–Laflamme criterion, [5,6] and the protected subspace in this case is usually called an *error correction subspace*.

The weakest form of protection is provided in yet a third situation, which was encountered in the context of quantum trajectories and the purification tendency of states along these paths [7]. In this case the deformation of the state is not caused by some given external device, but by the experimenter himself, who is performing a Kraus measurement [8]. Also in this case the "channel" acts as a random isometry, but the image spaces need not be orthogonal. It is now the *measurement outcome* (not the output state), that betrays to the experimenter which isometry has taken place. Using this information, he is able to undo the deformation of the component of the state that lies in the subspace considered.

It should be emphasized that the latter form of protection is far from a general error correction procedure. The experimenter only repairs the damage that he himself has incurred by his measurement.

Nevertheless, the above situations seem mathematically sufficiently similar to deserve study under a common title.

In all these three cases the experimenter learns nothing during the recovery operation about the component of the state inside our subspace. In this sense these subspaces can be considered "dark", and this darkness is essential for the protection of information. Our main result (Theorem 3) is concerned with the equivalence between protection and darkness, which is a consequence of Heisenberg's principle that no information on an unknown quantum state can be obtained without disturbing it (Corollary 2).

The question arises, for what channels protected subspaces are to be be found. We consider several examples in their Kraus decompositions. In each decomposition, we look for subspaces on which the channel acts as a multiple of an isometry, to be called a *homometry* here. Obviously, every (Kraus) operator A acts homometrically on a one-dimensional space $\mathbb{C}\psi$; its image $\mathbb{C}A\psi$ is another one-dimensional space, and the shrinking factor is $\sqrt{\langle A\psi, A\psi \rangle} = \|A\psi\|$. However, one-dimensional spaces

are useless as coding spaces for quantum states. What we shall need, therefore, is the recent theory of higher rank numerical ranges [9,10]. With the help of this we shall be able to construct several examples.

The paper is organized as follows. A brief review of basic concepts including channels and instruments is presented in Sect. 2. We discuss Heisenberg's principle in Sect. 3. and prove our main Theorem, Theorem 3 in Sect. 4. In subsequent sections we analyze different forms of protected subspaces and compare their properties. In Sect. 5 we review the notion of higher rank numerical range and quote some results on existence in the algebraic compression problem. Some examples of dark subspaces are presented in Sect. 6, while an exemplary problem of finding an error correction code for a specific model of tri-unitary noise acting on a $3 \times K$ system is solved in Sect. 7.

2 Channels and instruments

Let $\mathcal{H}$ be a finite-dimensional complex Hilbert space, and let $\mathcal{B}(\mathcal{H})$ denote the space of all linear operators on $\mathcal{H}$. We consider $\mathcal{H}$ as the space of pure states of some quantum system. By a *quantum operation* or *channel* on this system we mean a completely positive map $\Phi : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ mapping the identity operator $\mathbb{1} = \mathbb{1}_{\mathcal{H}}$ to itself. The map Φ describes the operation "in the Heisenberg picture", i.e. as an action on observables. Its description "in the Schrödinger picture", i.e. as an action on density matrices ρ, is described by its adjoint Φ^*. The maps Φ and Φ^* are related by

$$\forall_\rho \forall_{X \in \mathcal{B}(\mathcal{H})} : \quad \mathrm{tr}\left(\Phi^*(\rho)X\right) = \mathrm{tr}\left(\rho\Phi(X)\right).$$

We note that the property $\Phi(\mathbb{1}) = \mathbb{1}$, which we require for Φ, is equivalent to trace preservation by Φ^*:

$$\mathrm{tr}\left(\Phi^*(\rho)\right) = \mathrm{tr}\left(\Phi^*(\rho) \cdot \mathbb{1}\right) = \mathrm{tr}\left(\rho \cdot \Phi(\mathbb{1})\right) = \mathrm{tr}(\rho \cdot \mathbb{1}) = \mathrm{tr}(\rho).$$

By Stinespring's theorem, every channel $\Phi : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ can be written as

$$\Phi(X) = V^\dagger (X \otimes \mathbb{1}_{\mathcal{M}}) V, \tag{2.1}$$

where V is an isometry $\mathcal{H} \to \mathcal{H} \otimes \mathcal{M}$ for some auxiliary Hilbert space $\mathcal{M}$. The minimal dimension r of $\mathcal{M}$ admitting such a representation is called the *Choi rank* [11,12] of Φ.

Any Stinespring representation of Φ naturally leads to a wider quantum operation

$$\Psi : \mathcal{B}(\mathcal{H}) \otimes \mathcal{B}(\mathcal{M}) \to \mathcal{B}(\mathcal{H}) : X \otimes Y \mapsto V^\dagger (X \otimes Y) V, \tag{2.2}$$

which can be interpreted (in the Heisenberg picture) as the result of coupling the system to some *ancilla* having Hilbert space $\mathcal{M}$.

Thus Stinespring's representation (2.1) can be symbolically rendered as in Fig. 1. In this picture, the cross stands for the substitution of $\mathbb{1}_{\mathcal{M}}$ (in the Heisenberg picture, reading from right to left), or the partial trace (in the Schrödinger picture, reading from

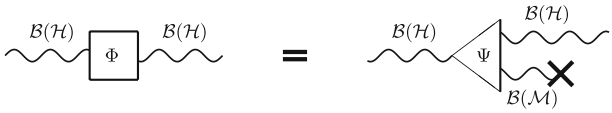

Fig. 1 Stinespring's dilation of Φ seen as coupling to an ancilla $\mathcal{M}$

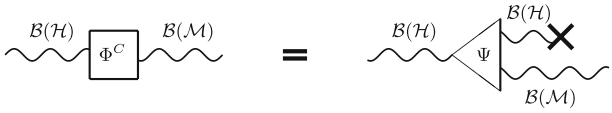

Fig. 2 The conjugate channel Φ^C

left to right). Physically, it corresponds to throwing away, or just ignoring, the ancilla after the interaction. In the picture, the fact that Ψ is a *compression*, i.e. $\Psi = V^\dagger \cdot V$ for some isometry V, is symbolized by the triangular form of its box.

Now, by blocking the other exit in Fig. 1, we obtain the conjugate channel [13], Φ^C:

$$\Phi^C : \mathcal{B}(\mathcal{M}) \to \mathcal{B}(\mathcal{H}) : \quad Y \mapsto \Psi(\mathbb{1}_{\mathcal{H}} \otimes Y) = V^\dagger(\mathbb{1}_{\mathcal{H}} \otimes Y)V.$$

See also Fig. 2.

The main message of this paper is the following. The conjugate channel can be viewed as the flow of information into the environment. By Heisenberg's Principle, to be explained below, such a flow prohibits the faithful transmission of information through the original channel Φ. In particular, if the information encoded in some subspace of $\mathcal{H}$ is to be transmitted faithfully, nothing of it is visible from the outside: protection implies darkness. The degree of protection (decoherence free, strong or weak) is related to the degree of darkness, for which we shall define some terminology.

Any orthonormal basis $f = (f_1, \ldots, f_m)$ in $\mathcal{M}$ corresponds to a possible von Neumann measurement Π_f^* on the ancilla, which maps a density matrix ρ on $\mathcal{M}$ to a probability distribution $(\langle f_1, \rho f_1 \rangle, \langle f_2, \rho f_2 \rangle, \ldots, \langle f_m, \rho f_m \rangle)$ on $\{1, 2, \ldots, m\}$. (Cf. Fig. 3.) In the Heisenberg picture this is the map from the algebra $\mathbb{C}^m$ with generators $e_1 = (1, 0, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, ..., $e_m = (0, 0, \ldots, 0, 1)$, to $\mathcal{B}(\mathcal{M})$, given by

$$\Pi_f : \quad e_i \mapsto |f_i\rangle\langle f_i|.$$

In Fig. 3 the abelian algebra $\mathbb{C}^m$ is indicated by a straight line since it only carries classical information. Quantum information is designated by a wavy line.

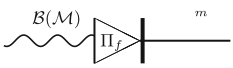

Fig. 3 Von Neumann measurement on $\mathcal{M}$

Let us now denote by I_f the "partial inner product map"

$$\mathcal{H} \otimes \mathcal{M} \to \mathcal{H} : \quad \varphi \otimes \theta \mapsto \langle f, \theta \rangle \varphi,$$

and let us write

$$A_i := I_{f_i} V \quad \in \mathcal{B}(\mathcal{H}).$$

Then since $I_{f_i}^\dagger X I_{f_j} = X \otimes |f_i\rangle\langle f_j|$, we obtain a decomposition of Φ along the basis $(f_i)_{i=1}^m$ as follows:

$$\Phi(X) = \Psi(X \otimes \mathbb{1}_{\mathcal{M}}) = \sum_{i=1}^m \Psi\left(X \otimes |f_i\rangle\langle f_i|\right) = \sum_{i=1}^m V^\dagger I_{f_i}^\dagger X I_{f_i} V = \sum_{i=1}^m A_j^\dagger X A_j. \tag{2.3}$$

This is a *Kraus decomposition* of Φ. Combining the coupling to the ancilla with a von Neumann measurement on the latter, we obtain an *instrument* in the language of Davies and Lewis [14]:

$$\Psi_f : \mathcal{B}(\mathcal{H}) \otimes \mathbb{C}^m \to \mathcal{B}(\mathcal{M}) : \quad X \otimes e_i \mapsto V^\dagger (X \otimes |f_i\rangle\langle f_i|) V = A_i^\dagger X A_i. \tag{2.4}$$

The isometric property of V is now expressed as

$$V^\dagger V = \sum_{i=1}^m A_i^\dagger A_i = \mathbb{1}. \tag{2.5}$$

3 Heisenberg's principle or observer effect

In quantum mechanics observables are represented as self-adjoint operators on a Hilbert space. When A and B are commuting operators, then they possess a common complete orthonormal set of eigenvectors. Each of these eigenvectors ψ determines a state which associates sharply determined values to both observables A and B.

But when A and B do not commute, such states may not exist. This important property of quantum mechanics was first discussed by Heisenberg [15], and is called the *Heisenberg Uncertainty Principle*. It was formulated by Robertson [16] in the form

$$\sigma_\psi(A) \cdot \sigma_\psi(B) \geq \tfrac{1}{2} |\langle \psi, (AB - BA)\psi \rangle|.$$

Here $\sigma_\psi(X)$ is the standard deviation of X in the distribution induced by ψ. Already in the very same paper, Heisenberg introduced a second and very different principle, which is sometimes designated as the "Observer Effect", and which we shall call the Heisenberg Principle here. Roughly speaking, it says that:

if A and B do not commute,
a measurement of B perturbs the probability distribution of A. (3.1)

In the first half century of quantum mechanics, physicists, including Heisenberg himself, were satisfied with this formulation, and even considered it more or less identical to the Uncertainty Principle above.

In recent years it was realized that in fact we have here two different principles. Good quantitative formulations have been given of the Heisenberg Principle (for example [17,18]). For the purpose of the present paper we are satisfied with a qualitative ('yes-or-no') version.

Let us first note that the formulation of the principle needs sharpening. As it stands, the condition is not needed: already in the trivial case that $A = B$ measurement of B changes the probability distribution of A. Indeed changing the probability distribution of an observable is the very purpose of measurement! And also, when A and B commute, but are correlated, then gaining information on B typically changes the distribution of A. A characteristic property of quantum theory only arises if we require that the outcome of the measurement of A is not used in the determination of the new probability distribution of B. Even then, some states may go through unchanged.

Corrected for these observations, the Heisenberg Principle reads:

For noncommuting A and B we cannot avoid that,
for some initial states, a measurement of B changes the distribution of A
even if we ignore the outcome of the measurement. (3.2)

The contraposition of the statement turns out to be mathematically more tractible:

If the probability distribution of A is not altered in any initial state—
by us performing some measurement and ignoring its outcome—then
the object measured must commute with A. (3.3)

In this form it is sometimes called the 'nondemolition principle'.

Now let us make this statement precise. We start with a self-adjoint operator A on $\mathcal{H}$. Its distribution in the state ρ is determined by the numbers $\mathrm{tr}(\rho g(A))$ when g runs through the functions on the spectrum of A. Then some quantum operation is performed which on $\mathcal{B}(\mathcal{H})$ is described by a completely positive unit preserving map Φ. We require that for all states ρ and all functions f

$$\mathrm{tr}\left(\Phi^*(\rho)g(A)\right) = \mathrm{tr}\left(\rho g(A)\right),$$

which is equivalent to

$$\Phi\left(g(A)\right) = g(A).$$

I.e.: all elements of the *-algebra $\mathcal{A}$ consisting of functions of A are left invariant by Φ. Let us denote the *commutant* of $\mathcal{A}$ by $\mathcal{A}'$,

$$\mathcal{A}' = \{X \in \mathcal{B}(\mathcal{H}) \,|\, \forall_{Y \in \mathcal{A}} \ : XY = YX\}. \tag{3.4}$$

Now, the quantum operation Φ is due to a measurement, so it is actually of the form

$$\Phi(X) = \Theta(X \otimes \mathbb{1}),$$

where $\Theta : \mathcal{B}(\mathcal{H}) \otimes \mathbb{C}^m \to \mathcal{B}(\mathcal{H})$ is some instrument whose outcomes, labeled $1, 2, \ldots, m$, in the state ρ have probabilities $p_1, p_2, \ldots, p_m$ to occur, where

$$p_j = \mathrm{tr}\left(\rho\Theta(\mathbb{1} \otimes e_j)\right),$$

and where $\mathrm{tr}\left(\rho\Theta(X \otimes e_j)\right)/p_j$ is the expectation of X, conditioned on the outcome j. (This situation is comparable to, but more general than, that of Ψ_f in (2.4).) Here $\mathbb{C}^m$ is the algebra of measurement outcomes. Generalizing to arbitrary $\mathcal{A}$, we may now formulate the Heisenberg Principle as follows.

Proposition 1 (Heisenberg Principle) *Let $\mathcal{H}$ be a finite dimensional Hilbert space, and $\mathcal{B}$ some finite dimensional *-algebra. Let $\mathcal{A}$ be a sub-*-algebra of $\mathcal{B}(\mathcal{H})$, and let Θ be a completely positive unit preserving map $\mathcal{B}(\mathcal{H}) \otimes \mathcal{B} \to \mathcal{B}(\mathcal{H})$. Suppose that for all $A \in \mathcal{A}$ we have*

$$\Theta(A \otimes \mathbb{1}) = A.$$

Then for all $B \in \mathcal{B}$

$$\Theta(\mathbb{1} \otimes B) \in \mathcal{A}'.$$

Proof For any density matrix ρ on $\mathcal{H}$, define the quadratic form D_ρ on $\mathcal{B}(\mathcal{H}) \otimes \mathcal{B}$ by

$$D_\rho(X, Y) := \mathrm{tr}\rho\left(\Theta(X^*Y) - \Theta(X)^*\Theta(Y)\right).$$

By the Cauchy–Schwartz inequality for the completely positive map Θ this quadratic form is positive semidefinite. By assumption we have for all $A \in \mathcal{A}$:

$$\begin{aligned} D_\rho(A \otimes \mathbb{1}, A \otimes \mathbb{1}) &= \mathrm{tr}\rho\left(\Theta(A^*A \otimes \mathbb{1}) - \Theta(A \otimes \mathbb{1})^*\Theta(A \otimes \mathbb{1})\right) \\ &= \mathrm{tr}\rho\left(A^*A \otimes \mathbb{1} - (A \otimes \mathbb{1})^*(A \otimes \mathbb{1})\right) = 0. \end{aligned}$$

It then follows from the Cauchy–Schwartz inequality for D_ρ itself that $D_\rho(A \otimes \mathbb{1}, \mathbb{1} \otimes B) = 0$ for all $B \in \mathcal{B}$. But then

$$\begin{aligned} \mathrm{tr}\rho\left(A\Theta(\mathbb{1} \otimes B)\right) &= \mathrm{tr}\rho\left(\Theta(A \otimes \mathbb{1})\Theta(\mathbb{1} \otimes B)\right) = \mathrm{tr}\rho\left(\Theta\left((A \otimes \mathbb{1})(\mathbb{1} \otimes B)\right)\right) \\ &= \mathrm{tr}\rho\left(\Theta\left((\mathbb{1} \otimes B)(A \otimes \mathbb{1})\right)\right) = \mathrm{tr}\rho\left(\Theta(\mathbb{1} \otimes B)\Theta(A \otimes \mathbb{1})\right) \\ &= \mathrm{tr}\rho\left(\Theta(\mathbb{1} \otimes B)A\right). \end{aligned}$$

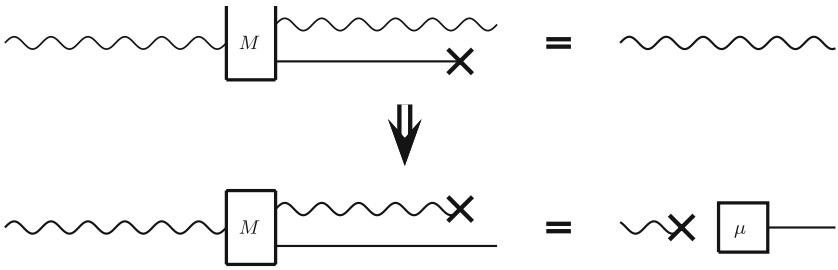

Fig. 4 Heisenberg's Principle as an implication between diagrams

Since this holds for all ρ, it follows that $\Theta(\mathbb{1} \otimes B)$ commutes with A. □

By taking $\mathcal{A}$ and $\mathcal{B}$ abelian, say $\mathcal{A}$ generated by some observable A, and $\mathcal{B} = \mathbb{C}^m$ as above, and by choosing for Θ some instrument giving information about B, we obtain a statement of the type (3.3).

But there are other possible conclusions. We may choose $\mathcal{A} = \mathcal{B}(\mathcal{H})$, so that $\mathcal{A}' = \mathbb{C} \cdot \mathbb{1}_{\mathcal{H}}$. Then the Heisenberg principle says that, if we wish to make sure that any possible state ρ on $\mathcal{H}$ be unchanged by our measurement, no information at all concerning ρ can be gained. This is expressed by the following corollary and Fig. 4.

Corollary 2 *In the situation of Proposition 1, if for all $A \in \mathcal{B}(\mathcal{H})$ we have*

$$\Theta(A \otimes \mathbb{1}) = A,$$

then there is a positive normalized linear form α on $\mathcal{B}$ such that for all $B \in \mathcal{B}$:

$$\Theta(\mathbb{1} \otimes B) = \alpha(B) \cdot \mathbb{1}_{\mathcal{H}}.$$

Indeed, the expectation of an outcome observable,

$$\mathrm{tr}(\Theta^* \rho)(\mathbb{1} \otimes B) = \mathrm{tr}(\rho \Theta(\mathbb{1} \otimes B)) = \mathrm{tr}(\rho \mathbb{1}_{\mathcal{H}}) \cdot \mathrm{tr}(\alpha B) = \mathrm{tr}(\alpha B)$$

does not depend on ρ (see Fig. 4.)

4 Protection and darkness: the Knill–Laflamme condition

Let $\mathcal{L}$ be a complex Hilbert space of dimension smaller than that of $\mathcal{H}$, and let $C : \mathcal{L} \to \mathcal{H}$ be some isometry. The range of C is a subspace of $\mathcal{H}$, isomorphic with $\mathcal{L}$. Let $\Gamma : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{L})$ denote the *compression map*

$$\Gamma(X) = C^\dagger X C.$$

Note that Γ is completely positive and identity-preserving. Compression maps are a convenient way of describing subspaces of a Hilbert space in the language of operations. Note that the operation Γ^* (in the Schödinger picture) embeds density matrices on $\mathcal{L}$ into the range of C:

$$\Gamma^*(\rho) = C\rho C^\dagger.$$

Physically, Γ is to be viewed as the "coding" operation.

Definition We say that Γ (or the subspace $C\mathcal{L}$ of $\mathcal{H}$) is *protected against* a channel $\Phi : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ if $\Gamma \circ \Phi$ is right-invertible, i.e. if there exists a "decoding" operation $\Delta : \mathcal{B}(\mathcal{L}) \to \mathcal{B}(\mathcal{H})$ such that

$$\Gamma \circ \Phi \circ \Delta = \mathrm{id}_{\mathcal{B}(\mathcal{L})}. \tag{4.1}$$

By virtue of (2.1) we may picture this state of affairs as in Fig. 5.

The subspace will be called *weakly protected against* an instrument $\Psi_f : \mathcal{B}(\mathcal{H}) \otimes \mathbb{C}^m \to \mathcal{B}(\mathcal{H})$ if $\Gamma \circ \Psi_f$ is right-invertible, i.e. if there exists a decoding operation $\Delta_f : \mathcal{B}(\mathcal{L}) \to \mathcal{B}(\mathcal{H}) \otimes \mathbb{C}^m$ such that

$$\Gamma \circ \Psi_f \circ \Delta_f = \mathrm{id}_{\mathcal{B}(\mathcal{L})}. \tag{4.2}$$

This is symbolically rendered in Fig. 6. The difference with Fig. 5 is that, in the case of weak protection, it is allowed to use the measurement outcome in the decoding. In the figure the classical information consisting of the measurement outcome, is symbolized by a straight line.

The above notions concern protection of information. Now we consider its availability to the external world.

Definition Let $\Psi_f : \mathcal{B}(\mathcal{H}) \otimes \mathbb{C}^m \to \mathcal{B}(\mathcal{H})$ denote a quantum measurement (instrument) as described in (2.4). The subspace $C\mathcal{L} \subset \mathcal{H}$ (or the compression operation $\Gamma = C^\dagger \cdot C$), will be called *dark* with respect to Ψ_f if for all $i = 1, \ldots, m$ we have

$$\Gamma \circ \Psi_f(\mathbb{1} \otimes e_i) \in \mathbb{C} \cdot \mathbb{1}_{\mathcal{L}}. \tag{4.3}$$

This condition can be written in an equivalent form,

$$C^\dagger A_i^\dagger A_i C = \lambda_i \cdot \mathbb{1}_{\mathcal{L}} \quad \text{for} \quad i = 1, \ldots, m. \tag{4.4}$$

The subspace $C\mathcal{L}$ will be called *completely dark* for a channel $\Phi : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ if it is dark for all Kraus measurements Ψ_f obtained by choosing different orthonormal bases in the ancilla space of some Stinespring dilation of Φ; i.e.

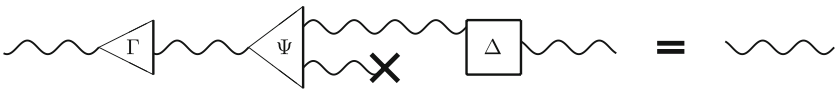

Fig. 5 Strong protection of Γ against Ψ

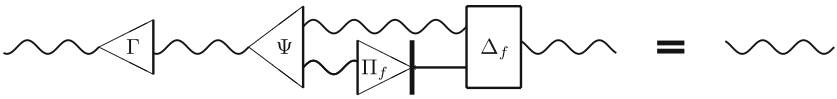

Fig. 6 Weak protection of Γ against Ψ_f

$$\forall_{Y \in \mathcal{B}(\mathcal{M})}: \quad \Gamma \circ \Psi(\mathbb{1} \otimes Y) \in \mathbb{C} \cdot \mathbb{1}_{\mathcal{L}}. \tag{4.5}$$

In terms of Kraus operators this is equivalent with the *Knill–Laflamme condition*:

$$C^{\dagger} A_i^{\dagger} A_j C = \alpha_{i,j} \cdot \mathbb{1}_{\mathcal{L}} \quad \text{for} \quad i, j = 1, \ldots, m. \tag{4.6}$$

4.1 Interpretation

From (4.3) and (4.4) we see that, if the von Neumann measurement along f is performed, the measurement outcome i has the same probability $\rho\left(\Gamma \circ \Psi_f(\mathbb{1} \otimes e_i)\right) = \rho(C^{\dagger} A_i^{\dagger} A_i C) = \lambda_i$, in all system states ρ, i.e. no information concerning the state ρ can be read off from the f-measurement on the ancilla.

Complete darkness (i.e. (4.5) or the equivalent Knill–Laflamme condition (4.6)) says that no information whatsoever concerning the input state reaches the ancilla. Mathematically, the Knill–Laflamme condition says that the range of the conjugate channel lies entirely in the center $\mathbb{C} \cdot \mathbb{1}_{\mathcal{L}}$ of $\mathcal{B}(\mathcal{L})$. Let us emphasize again that if the space C satisfies the conditions (4.6) for a map Ψ represented by a particular set of the Kraus operators $\{A_i\}_{i=1}^{m}$, then C also satisfies them for any other set of Kraus operators $\{B_i\}_{i=1}^{m'}$, used to represent the same map Ψ.

Note also that the set of conditions (4.6), which express complete darkness, naturally defines a state α, on the ancilla by a relation

$$\Gamma \circ \Psi(\mathbb{1} \otimes Y) = \mathrm{tr}(\alpha Y) \cdot \mathbb{1}_{\mathcal{L}}. \tag{4.7}$$

satisfied by any Y. This quantum state acting on an auxiliary system is called the *error correction matrix*, since the density matrix α_{ij} appears in Eq. 4.6. Observe that the density operator α depends only on the map Ψ and not on the concrete form of the Kraus operators A_i, which represent the map and determine the matrix representation α_{ij} of α. Relations between matrix elements of the same state represented in two different basis are governed by the Schrödinger lemma [12], also called GHJW lemma [19,20].

We are now going to prove the equivalence of protection and darkness. In the case of strong protection and complete darkness this reproduces and puts into perspective the result of Knill and Laflamme [6]. In that case, if the state α is pure, then the decoding operation Δ can be realized by a unitary evolution, Hence the purity constraint for the error correction matrix, $\alpha = \alpha^2$, is the correct condition for a decoherence free subspace [21]—see also the proof of Theorem 3. As a quantitative measure, which characterizes to what extent a given protected space is close to a decoherence free space, one can use the von Neumann entropy of this state, $S = -\mathrm{Tr}\alpha \ln \alpha$. This *code entropy* [22] is equal to zero if the protected space is decoherence free or if the information lost can be recovered by a reversible unitary operation. Observe that the code entropy S characterizes the map Ψ and the code space C, but does not depend on the particular Kraus form used to represent Ψ.

In this way we have determined a hierarchy in the set of protected spaces. Every decoherence free subspace belongs to the class of completely dark subspaces, which

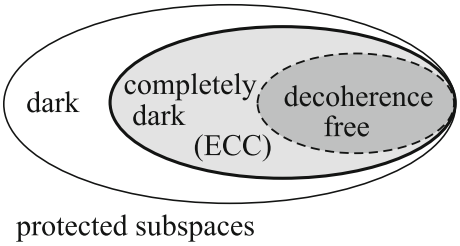

Fig. 7 Sketch of the hierarchy of protected subspaces

correspond to error correction codes. In turn the completely dark subspaces form a subset of the set of dark subspaces—see Fig. 7.

Theorem 3 (Equivalence of protection and darkness) *Let $\mathcal{H}$, $\mathcal{M}$, and $\mathcal{L}$ be finite dimensional Hilbert spaces. Let $C : \mathcal{L} \to \mathcal{H}$ and $V : \mathcal{H} \to \mathcal{H} \otimes \mathcal{M}$ be isometries, and let Φ, Ψ and Ψ_f be as defined in (2.1), (2.2) and (2.4). Then $C\mathcal{L}$ is weakly protected against the instrument Ψ_f if and only if $C\mathcal{L}$ is dark for Ψ_f. It is strongly protected against Φ if and only if it is completely dark for Φ.*

Proof First assume that $C\mathcal{L}$ is strongly protected against Φ, i.e. (4.1) holds for some decoding operation Δ. Let $\Phi(X) = \Psi(X \otimes \mathbb{1})$ for some compression Ψ. Define

$$\Theta : \mathcal{B}(\mathcal{L}) \otimes \mathcal{B}(\mathcal{M}) \to \mathcal{B}(\mathcal{L}) : X \otimes Y \mapsto \Gamma \circ \Psi(\Delta(X) \otimes Y).$$

Then $\Theta(X \otimes \mathbb{1}) = X$ for all $X \in \mathcal{B}(\mathcal{L})$, and by Corollary 2, since $\Delta(\mathbb{1}) = \mathbb{1}$,

$$\Gamma \circ \Psi(\mathbb{1} \otimes Y) = \Theta(\mathbb{1} \otimes Y) \in \mathbb{C} \cdot \mathbb{1}.$$

So (4.5) holds, and $C\mathcal{L}$ is completely dark for Φ.

Conversely, suppose that $C\mathcal{L}$ is completely dark for Ψ, and let α denote the density matrix given by (4.7) Then we may diagonalize:

$$\mathrm{tr}(\alpha Y) = \sum_{i=1}^{m} a_i \langle f_i, Y f_i \rangle$$

for some orthonormal set $(f_i)_{i=1}^{m'}$ (with $m' \leq m$) of $\mathcal{B}(\mathcal{M})$ and positive numbers $a_1, a_2, \ldots, a_{m'}$ summing up to 1. Now let $A_i := I_{f_i} V$. Then for all $\psi \in \mathcal{L}$:

$$\begin{aligned}
\left\langle A_i C\psi, A_j C\psi \right\rangle &= \left\langle I_{f_i} V C\psi, I_{f_j} V C\psi \right\rangle \\
&= \left\langle \psi, C^\dagger V^\dagger (\mathbb{1} \otimes |f_i\rangle\langle f_j|) V C\psi \right\rangle \\
&= \alpha(|f_i\rangle\langle f_j|) \cdot \|\psi\|^2 \\
&= a_i \delta_{ij} \cdot \|\psi\|^2.
\end{aligned}$$

So the ranges of $A_i C$ and $A_j C$ are orthogonal for $i \neq j$ and A_i is homometric on $C\mathcal{L}$. Now define D_i for $i = 1, 2, \ldots, m'$ on these orthogonal ranges by

$$D_i \varphi = 0 \quad \text{if} \quad \varphi \perp \text{Range}\,(A_i C), \qquad D_i A_i C \psi = \sqrt{a_i}\,\psi.$$

(D_i "rotates back" the action of $A_i C$.) Let Δ denote the operation

$$\Delta(Z) := \sum_{i=1}^{m'} D_i^\dagger Z D_i + \rho(Z) \left(\mathbb{1}_{\mathcal{H}} - \sum_{j=1}^{m'} D^\dagger D_j \right).$$

for some arbitrary state ρ on $\mathcal{B}(\mathcal{L})$. (The term with ρ is intended to ensure that $\Delta(\mathbb{1}_{\mathcal{L}}) = \mathbb{1}_{\mathcal{H}}$.) Then we have for all $Z \in \mathcal{B}(\mathcal{L})$:

$$\begin{aligned} \Gamma \circ \Phi \circ \Delta(Z) &= \sum_{j=1}^{m'} \sum_{i=1}^{m'} C^\dagger A_j^\dagger D_i^\dagger Z D_i A_j C \\ &= \sum_{j=1}^{m'} \sum_{i=1}^{m'} \frac{1}{a_i} C^\dagger A_j^\dagger A_i C Z C^\dagger A_i^\dagger A_j C = \sum_{ij=1}^{m'} \delta_{ij} a_i Z = Z. \end{aligned}$$

So $C\mathcal{L}$ is strongly protected against Φ by (4.1).

Now let us prove the equivalence between weak protection and darkness. Assume that $C\mathcal{L}$ is weakly protected against Ψ_f, i.e. (4.2) holds for some $\Delta_f : \mathcal{B}(\mathcal{L}) \to \mathcal{B}(\mathcal{H}) \otimes \mathbb{C}^m$, say $\Delta_f(X) = \sum_{j=1}^m \Delta_f^j(X) \otimes e_j$. Define $\Theta : \mathcal{B}(\mathcal{H}) \otimes \mathbb{C}^m \to \mathcal{B}(\mathcal{H})$ by

$$\Theta(X \otimes g) := \sum_{j=1}^{m} g(j) \Gamma \circ \Psi_f(\Delta^j(X) \otimes e_j).$$

Then by (4.2), $\Theta(X \otimes \mathbb{1}) = X$ for all $X \in \mathcal{B}(\mathcal{L})$. Hence by Corollary 2,

$$\Gamma \circ \Psi_f(\mathbb{1} \otimes e_i) = \Theta(\mathbb{1} \otimes e_i) \in \mathcal{B}(\mathcal{H})' = \mathbb{C} \cdot \mathbb{1}_{\mathcal{L}}.$$

So (4.3) holds, and $C\mathcal{L}$ is dark for Ψ_f.

Conversely, assuming that $C\mathcal{L}$ is dark for Ψ_f, then $A_l C$ is homometric on $\mathcal{L}$ by (4.4), and we may define $D_l : \mathcal{H} \to \mathcal{L}$ by

$$D_l A_l C \psi := \sqrt{\lambda_l}\,\psi \quad \text{if } \psi \in \mathcal{L}, \qquad D_l \varphi = 0 \quad \text{if } \varphi \perp \text{Range}\,(A_l C).$$

(Briefly: $D_l = C^\dagger A_l^\dagger / \sqrt{\lambda_l}$ if $\lambda_l \neq 0$, zero otherwise.) Define the decoding operation $\Delta_f : \mathcal{B}(\mathcal{L}) \to \mathcal{B}(\mathcal{H}) \otimes \mathbb{C}^m$ by

$$\Delta_f(Z) := \bigoplus_{l=1}^{m} \left(D_l^\dagger Z D_l + (\mathbb{1}_{\mathcal{H}} - D_l^\dagger D_l) \rho(Z) \right)$$

for some arbitrary state ρ on $\mathcal{B}(\mathcal{L})$. Then, for $Z \in \mathcal{B}(\mathcal{L})$:

$$\begin{aligned}\Gamma \circ \Psi_f \circ \Delta_f(Z) &= \Gamma \circ \Psi_f \left(\sum_{l=1}^{m} \left(D_l^\dagger Z D_l + (\mathbb{1} - D_l^\dagger D_l)\rho(Z) \right) \otimes e_l \right) \\ &= C^\dagger V^\dagger \left(\sum_{l=1}^{m} \left(D_l^\dagger Z D_l + (\mathbb{1} - D_l^\dagger D_l)\rho(Z) \right) \otimes |f_l\rangle\langle f_l| \right) VC \\ &= \sum_{l=1}^{m} C^\dagger A_l^\dagger D_l^\dagger Z D_l A_l C = \sum_{l=1}^{m} \frac{1}{\lambda_l} (C^\dagger A_l^\dagger A_l C) Z (C^\dagger A_l^\dagger A_l C) \\ &= \sum_{l=1}^{m} \lambda_l Z = Z.\end{aligned}$$

□

5 Compression problems and generalized numerical range

For a given channel $\Phi : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ we are interested in the protected subspaces of $\mathcal{H}$. These are the subspaces on which the compressions of $A_i^\dagger A_j$ act as scalars. In this section we review this compression problem.

Let T be an operator acting on a Hilbert space $\mathcal{H}$ of dimension n, say. For any $k \geq 1$, define the *rank-k numerical range* of T to be the subset of the complex plane given by

$$\Lambda_k(T) = \left\{ \lambda \in \mathbb{C} : C^\dagger T C = \lambda \mathbb{1} \quad \text{for} \quad \text{some } C : \mathbb{C}^k \to \mathcal{H} \right\}, \tag{5.1}$$

The elements of $\Lambda_k(T)$ can be called "compression-values" for T, as they are obtained through compressions of T to a k-dimensional *compression subspace*. The case $k = 1$ yields the standard numerical range for operators [23]

$$\Lambda_1(T) = \{\langle\psi|T\psi\rangle \ : \ |\psi\rangle \in \mathcal{H}, \langle\psi|\psi\rangle = 1\}. \tag{5.2}$$

It is clear that

$$\Lambda_1(T) \supseteq \Lambda_2(T) \supseteq \cdots \supseteq \Lambda_n(T). \tag{5.3}$$

The sets $\Lambda_k(T)$, $k > 1$, are called *higher-rank numerical ranges* [9,24]. For any normal operator acting on $\mathcal{H}_n$ this is a compact subset of the complex plane. For unitary operators this set is included inside every convex hull $(\mathrm{co}\,\Gamma)$, where Γ is an arbitrary $(n+1-k)$-point subset (counting multiplicities) of the spectrum of T [9]. It was recently shown that for any normal operator the sets $\Lambda_k(T)$ are convex [25,26] while further properties of higher rank numerical range were investigated in [27–29].

The higher rank numerical range is easy to find for any Hermitian operator, $T = T^\dagger$ acting on an n-dimensional Hilbert space $\mathcal{H}$. Let us quote here a useful result proved in [9].

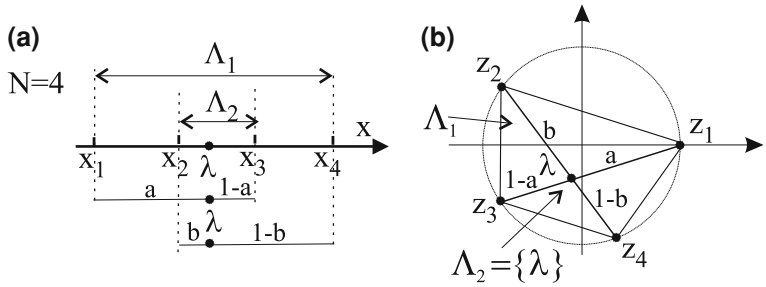

Fig. 8 Standard numerical range Λ_1 and higher rank numerical range Λ_2 for **a** Hermitian operator T of size 4 and **b** non-degenerate unitary $U \in U(4)$. Observe similarity in finding the weights a and b used to construct superposition of states forming the subspace $C\mathcal{L}$ in both problems

Lemma 4 *Let $x_1 \leq x_2 \leq \cdots \leq x_n$ denote the ordered spectrum (counting multiplicities) of a hermitian operator T. The rank-k numerical range of T is given by the interval*

$$\Lambda_k(T) = [x_k, x_{n+1-k}] \,, \tag{5.4}$$

Note that the higher rank numerical range of a hermitian T is nonempty for any $k \leq \mathrm{int}[(n+1)/2]$. Let us demonstrate an explicit construction of a compression to $\mathbb{C}^2$ which solves Eq. 5.1 for a Hermitian matrix T of size $n = 4$. The latter's eigenvalue equation reads $T|\phi_i\rangle = x_i|\phi_i\rangle$. Choose any real $\lambda \in \Lambda_2(T) = [x_2, x_3]$. It may be represented as a convex combination of two pairs of eigenvalues $\{x_1, x_3\}$ and $\{x_2, x_4\}$—see Fig. 8a. Writing

$$\lambda \;=\; (1-a)x_1 + ax_3 \;=\; (1-b)x_2 + bx_4 \tag{5.5}$$

one obtains the weights

$$a = \frac{\lambda - x_1}{x_3 - x_1} =: \sin^2\theta_1 \quad \text{and} \quad b = \frac{\lambda - x_2}{x_4 - x_2} =: \sin^2\theta_2 \tag{5.6}$$

which determine real phases θ_1 and θ_2. These phases allow us to define an isometry $C : \mathbb{C}^2 \to \mathcal{H}$ by

$$C : \begin{cases} e_1 \mapsto \cos\theta_1|\phi_1\rangle + \sin\theta_1|\phi_3\rangle \\ e_2 \mapsto \cos\theta_2|\phi_2\rangle + \sin\theta_2|\phi_4\rangle \end{cases} , \tag{5.7}$$

Observe that

$$\left\langle e_1, C^\dagger T C e_1 \right\rangle = \cos\theta_1 x_1 \langle\phi_1|\psi_1\rangle + \sin\theta_1 x_3 \langle\phi_3|\psi_1\rangle = (1-a)x_1 + ax_3 = \lambda. \tag{5.8}$$

Similarly, we have $\left\langle e_2, C^\dagger T C e_2 \right\rangle = \lambda$. Further, we also have $\left\langle e_1, C^\dagger T C e_2 \right\rangle = 0 = \left\langle e_2, C^\dagger T C e_1 \right\rangle$. It follows that $C^\dagger T C = \mathbb{1}$, and the isometry (5.7) provides a solution

of the compression problem (5.1) as claimed. Note that one can select another pairing of eigenvalues, and the choice $\{x_1, x_4\}$ and $\{x_2, x_3\}$ allows us to get in this way another subspace $C'\mathcal{L}$ spanned by vectors obtained by a superposition of states $|\phi_1\rangle$ with $|\phi_4\rangle$ and $|\phi_2\rangle$ with $|\phi_3\rangle$, respectively.

For a given operator T one may try to solve its compression equation (5.1) and look for its numerical range $\Lambda_k(T)$. Alternatively, one may be interested in the following simple *compression problem*: For a given operator T find all possible subspaces $C\mathcal{L}$ of a fixed size k which satisfy (5.1).

Furthermore, it is natural to raise a more general, *joint compression problem* of order M. For a given set of M operators $\{T_1, \ldots T_M\}$ acting on $\mathcal{H}_n$ find a subspace $C\mathcal{L}$ of dimensionality k which solves simultaneously M compression problems:

$$C^\dagger T_m C = \lambda_m \mathbb{1} \quad \text{for} \quad m = 1, \ldots, M. \tag{5.9}$$

Note that all compression constants, $\lambda_m \in \Lambda_k(T_m)$, can be different, but the isometry C needs to be the same.

6 Dark subspaces

In this section we provide several results concerning existence of darks spaces for several classes of quantum maps.

6.1 Random external fields

Consider a noisy channel Φ given by

$$\Phi_U(X) = \sum_{i=1}^{r} q_i \, U_i^\dagger X U_i, \tag{6.1}$$

where all operators U_i are unitary while positive weights q_i sum up to unity. Such maps are called *random external fields* [30] or random unitary channels. The standard Kraus form (2.3) is obtained by setting $A_i = \sqrt{q_i} U_i$.

In this Kraus decomposition the whole space, and hence every subspace, is dark. This corresponds to the fact that the choice between the unitaries, which is made with the probability distribution $(q_1, \ldots, q_r)$, gives no information on the quantum state. And indeed, knowledge of the "external field", i.e. of the outcome i, permits us to undo, by the inverse of U_i, the action of the channel.

6.2 Rank two quantum channels

Let us now analyze a rank two channel,

$$\rho' = \Phi_2(\rho) = A_1 \rho A_1^\dagger + A_2 \rho A_2^\dagger \,, \tag{6.2}$$

Lemma 5 *For any Kraus representation of any rank-two channel acting on a system of size N there exist a dark subspace of dimension $k = int[(N+1)/2]$.*

Proof We need to solve a joint compression problem (5.9) of order two, for two Hermitian operators $T_1 = A_1^\dagger A_1$ and $T_2 = A_2^\dagger A_2$. Due to Lemma 4 there exists a subspace P_k of dimension $k = \mathrm{int}[(N+1)/2]$ which solves the compression problem for the Hermitian operator T_1 of size N. It is also a solution of the compression problem for the other operator, since the trace preserving condition implies $T_2 = \mathbb{1} - T_1$. □

6.3 Biased permutation channel

Consider a quantum map acting on a system of arbitrary size n described by the Kraus form (2.3). Let us assume that all Kraus operators are given by 'biased permutations'

$$A_i = P_i \sqrt{D_i}, \quad i = 1, \ldots, r. \tag{6.3}$$

where D_i is a diagonal matrix containing non-negative entries, and P_i denotes an arbitrary permutation of the N-element set. Hence all elements of the POVM form diagonal matrices,

$$T_i = A_i^\dagger A_i = \sqrt{D_i} P_i^\dagger P_i \sqrt{D_i} = D_i \ , \tag{6.4}$$

in general not proportional to identity. Note that the Kraus operators defined in this way need not to be Hermitian. To satisfy the trace preserving condition (2.5) we need to assume that $\sum_{i=1}^r D_i = \mathbb{1}$. Let us define an auxiliary rectangular matrix of size $r \times N$, namely $S_{im} := (D_i)_{mm} \geq 0$. Then the above constraints for the matrices D_i is equivalent to the statement that S is *stochastic*, since the sum of all elements in each column is equal to 1,

$$\sum_{i=1}^r S_{im} = 1 \quad \text{for} \quad m = 1, \ldots, N. \tag{6.5}$$

A map described by Kraus operators fulfilling relations (6.3) and (6.5) will be called a *biased permutation channel*.

We are going to construct a dark space for a wide class of such channels. For simplicity assume that the size of the system is even, $N = 2k$. Let us additionally assume that all elements in each row of B are ordered (increasingly or decreasingly) and that the matrix S enjoys a symmetry relation,

$$S_{i,m} + S_{i,n-m+1} = \text{const} =: \kappa_i \quad \text{for} \quad i = 1, \ldots, r; \quad m = 1, \ldots, k = n/2. \tag{6.6}$$

Then the numbers κ_i depend on the sum of all entries in each row, $\kappa_i = \frac{2}{N} \sum_{m=1}^N S_{im}$.

Lemma 6 *Assume that a biased permutation channel acting on a system of size $N = 2k$ possesses the symmetry relation (6.6). Then it has a dark space of dimension $k = n/2$.*

Proof We need to find a joint compression subspace for the set of r elements of POVM given by diagonal matrices D_i, with $i = 1, \ldots, r$. Since these matrices commute, they have the same set of eigenvectors, denoted by $|v_m\rangle$, $m = 1, \ldots, N$. Due to symmetry relation (6.6) we know that the barycenter of each spectrum, $\lambda_i = \kappa_{i/2}$ belongs to the higher rank numerical range, $\Lambda_k(D_i)$. Furthermore, this relation shows that (for any i) the number λ_i can be represented as a sum of two eigenvalues of D_i with the same weights, $\lambda_i = \frac{1}{2}(D_i)_{mm} + \frac{1}{2}(D_i)_{m'm'}$ with $m' = n + 1 - m$. By construction this property holds for all operators D_i, $i = 1, \ldots r$. Hence the general construction of the higher order numerical range for Hermitian operators [10] implies that the subspace

$$C_k := \sum_{i=1}^{k} |\psi_i\rangle\langle\psi_i| \quad \text{where} \quad |\psi_i\rangle := \frac{1}{\sqrt{2}}\left(|v_i\rangle + |v_{1-i+N}\rangle\right) \tag{6.7}$$

fulfills the joint compression problem for all operators $T_i = D_i$, $i = 1, \ldots r$. Hence this subspace is dark as advertised. □

To watch the above construction in action consider a three biased permutation channel acting on a two qubit system. Hence we set $r = 3$ and $N = 4$, and assume that five real weights satisfy $0 < a < b < x/2 < 1/2$ and $0 < c < d < x/2$. They can be used to define the channel by a stochastic matrix S

$$S = \begin{pmatrix} a & b & x-b & x-a \\ c & d & x-d & x-c \\ a' & b' & b'' & a'' \end{pmatrix}, \tag{6.8}$$

where $a' = 1 - a - c$, $b' = 1 - b - d$, $a'' = 1 - 2x + a + c$ and $b'' = 1 - 2x + b + d$. Note that this matrix satisfies the symmetry condition (6.6), the elements in each row are ordered, while mean weights in each row read $\lambda_1 = \lambda_2 = x/2$ and $\lambda_3 = 2(1 - x)$.

To complete the definition of the channel we need to specify three permutation matrice of size four. For instance let us choose $P_1 = P_{(1,2,3,4)}$, $P_2 = P_{(1,2),(3,4)}$ and $P_3 = P_{(1,4,3,2)}$, where according to the standard notion, the subscripts contain the permutation cycles. Then the biased permutation channel is defined by the three Kraus operators

$$A_1 = \begin{pmatrix} 0 & \sqrt{b} & 0 & 0 \\ 0 & 0 & \sqrt{x-b} & 0 \\ 0 & 0 & 0 & \sqrt{x-a} \\ \sqrt{a} & 0 & 0 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & \sqrt{d} & 0 & 0 \\ \sqrt{c} & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{x-c} \\ 0 & 0 & \sqrt{x-d} & 0 \end{pmatrix},$$

$$A_3 = \begin{pmatrix} 0 & 0 & 0 & \sqrt{a''} \\ \sqrt{a'} & 0 & 0 & 0 \\ 0 & \sqrt{b'} & 0 & 0 \\ 0 & 0 & \sqrt{b''} & 0 \end{pmatrix} \tag{6.9}$$

which satisfy the trace preserving condition (2.5).

Since the barycenter λ_i of the spectrum of the POVM element $T_i = D_i$ (given by a row of matrix (6.8)), is placed symmetrically, in all three cases it can be represented by a convex combination of pairs of eigenvalues with weights equal to $1/2$. Thus we define two pure states

$$|\psi_1\rangle := \frac{1}{\sqrt{2}}(|v_1\rangle + |v_4\rangle)\,, \quad |\psi_2\rangle := \frac{1}{\sqrt{2}}(|v_2\rangle + |v_3\rangle)\,, \tag{6.10}$$

and the two dimensional subspace spanned by them, $C = |\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2|$. It is easy to verify that the subspace C satisfies $C^\dagger T_1 C = \lambda_1 \mathbb{1} = C^\dagger T_2 C$ while $C^\dagger T_3 C = \lambda_3 \mathbb{1}$ so this space is dark. Note that the subspace $C\mathcal{L}$ cannot be used to design an error correcting code since $C^\dagger A_1^\dagger A_2 C \notin \mathbb{C} \cdot \mathbb{1}$.

6.4 Composed systems and separable channels

Consider a bipartite system of size $n = n_A \times n_B$. A quantum operation Φ acting on this bipartite system is called *local*, if it has a tensor product structure, $\Phi = \Phi_A \otimes \Phi_B$, where both maps Φ_A and Φ_B are completely positive and preserve the identity. If for both individual operations, Φ_A and Φ_B, there exist protected subspaces C_k and Q_l, respectively, then the product subspace $C_k \otimes Q_l$ of size kl is also a protected subspace for the composite map $\Phi_A \otimes \Phi_B$.

Similar protected subspaces of the product form can be constructed for a wider class of *separable maps* (see e.g. [12]),

$$\rho' = \Phi^*(\rho) = \sum_{i=1}^{r} (A_i \otimes B_i)\rho(A_i \otimes B_i)^\dagger. \tag{6.11}$$

Assume that a subspace $C_k \in \mathcal{H}_{N_A}$ is a solution of the joint compression problem for the set of r operators $A_i^\dagger A_i$, while a subspace $Q_l \in \mathcal{H}_{N_B}$ does the job for the set of r operators $B_i^\dagger B_i$. It is then easy to see that the product subspace $C_k \otimes Q_l$ of dimension kl is a dark subspace for the separable map (6.11).

It is straightforward to extend lemmas 3 and 4 for separable maps acting on composite systems and apply them to construct protected subspaces with a product structure.

On the other hand, if for certain problems such product code subspace do not exist, one may still find a code subspace spanned by entangled states. Such a problem for the tri-unitary model is solved in following section.

7 Unitary noise and error correction codes

In this section we are going to study multiunitary noise (6.1), also called random external fields, and look for existence of error correction codes, i.e. completely protected subspaces. In general the number r of unitary operators defining the channel can be arbitrary but we will restrict our attention to the cases in which this number is small.

7.1 Bi-unitary noise model

The case in which $r = 2$, referred to as *bi-unitary noise* was recently analyzed in [10,24]. Let us rewrite the dynamics in the form

$$\rho' = \Phi^*(\rho) = q V_1^\rho V_1^\dagger + (1-q) V_2 \rho V_2^\dagger. \tag{7.1}$$

and assume that we deal with the system of two qubits. Then both unitary matrices V_1 and V_2 belong to $U(4)$ while probability p belongs to [0, 1]. The problem of finding the compression C for the above map is shown to be equivalent to the case

$$\rho'' = \Phi^*(\rho) = q\rho + (1-q) U \rho U^\dagger \tag{7.2}$$

where $U = V_1^\dagger V_2$.

Thus the error correction matrix α of size two defined by eq. 4.7 reads

$$\alpha = \begin{pmatrix} q & \sqrt{q(1-q)}\lambda \\ \sqrt{q(1-q)}\lambda^* & 1-q \end{pmatrix} \tag{7.3}$$

where λ is solution of the compression problem for U

$$C^\dagger U C = \lambda \cdot \mathbb{1}. \tag{7.4}$$

Thus to find the error correction space for the bi-unitary model it is sufficient to solve the compression equation for a single operator U. A solution exists for any unitary U [10], but for simplicity we will consider here the generic case if the spectrum of U is not degenerated. Assume that the phases these unimodular numbers $z_1, \ldots, z_4$ are ordered and that $|\psi_i\rangle$ denote the corresponding eigenvectors.

Let λ denote the intersection point between two chords of the unit circle, $z_1 z_3$ and $z_2 z_4$; compare Fig. 8b. This point can be represented as a convex combination of each pair of complex eigenvalues,

$$\lambda = (1-a) z_1 + a z_3 = (1-b) z_2 + b z_4, \tag{7.5}$$

where the non-negative weights read

$$a = \frac{\lambda - z_1}{z_3 - z_1} =: \sin^2\theta_1 \quad \text{and} \quad b = \frac{\lambda - z_2}{z_4 - z_2} =: \sin^2\theta_2 \tag{7.6}$$

and determine real phases θ_1 and θ_2. Note similarity with respect to the construction used in the Hermitian case, in which (5.5) represents a convex combination of points on the real axis. In an analogy with the reasoning performed for a hermitian T we define according to (5.7) an orthonormal pair of vectors $|\psi_1\rangle$ and $|\psi_2\rangle$ and define the associated isometry $C : e_j \mapsto \psi_j$. Since $\langle U\psi_1|\psi_1\rangle = \lambda = \langle U\psi_2|\psi_2\rangle$ and $\langle U\psi_1|\psi_2\rangle = 0 = \langle U\psi_2|\psi_1\rangle$ then $CUC = \lambda\mathbb{1}$. Therefore λ belongs to $\Lambda_2(U)$ as claimed and the range of C provides the error correction code for the bi-unitray noise (7.2) acting on a two-qubit system.

In the case of doubly degenerated spectrum of U the complex number λ is equal to the degenerated eigenvalue, so its radius, $|\lambda|$, is equal to unity. In this case the matrix α given in (4.6) represents a pure state, $\alpha = \alpha^2$, so the two-dimensional subspace spanned by both eigenvectors corresponding to the degenerated eigenvalues is *decoherence free*.

Bi-unitary noise model for higher dimensional systems was analyzed in [24]. It was shown in this work that for a generic U of size N there exists a code subspace of dimensionality $k = \text{int}[(N+2)/3]$. This result implies that for a system of m qubits and a generic U of size $N = 2^m$ there exists an error correction code supported on $m-2$ qubits. Furthermore, if $N = d^m$ and $d \geq 3$, there exists a code supported on $m-1$ quantum systems of size d.

7.2 Tri-unitary noise model

Consider now a model of noise described by three unitary operations acting on a bipartite, $N = 2 \times N_B$ system,

$$\rho' = \Phi^*(\rho) = q_1 V_1 \rho V_1^\dagger + q_2 V_2 \rho W_2^\dagger + (1 - q_1 - q_2) V_3 \rho V_3^\dagger. \tag{7.7}$$

Performing a unitary rotation in analogy to (7.2) we obtain an equivalent form

$$\rho'' = \Phi^*(\rho) = q_1 \rho + q_2 U_1 \rho U_1^\dagger + (1 - q_1 - q_2) U_2 \rho U_2^\dagger. \tag{7.8}$$

The model is thus characterized by two unitary matrices of size N, namely $U_1 = V_1^\dagger V_2$ and $U_2 = V_1^\dagger V_3$. and two weights q_1 and q_2, which we assume to be positive with their sum smaller than unity.

To find a simplest error correction code for this model one needs to find a two-dimensional subspace, which forms a joint solution of three compression problems

$$\begin{cases} C^\dagger U_1 C = \lambda_{U_1}\mathbb{1} \\ C^\dagger U_2 C = \lambda_{U_2}\mathbb{1} \\ C^\dagger W C = \lambda_W \mathbb{1} \end{cases}, \tag{7.9}$$

where $W = U_1^\dagger U_2$. Each of the above three problems may be solved using the notion of the higher rank numerical range of a unitary matrix. However, for generic unitary matrices U_1 and U_2 of size 4 the corresponding compression subspaces do differ. Thus for a typical choice of the unitary matrices the tri-unitary noise model will not have an error correction code, for which it is required that the subspace C solves all three problems simultaneously.

There exist several examples of two commuting matrices U_1 and U_2 of size $N = 4$, such that they possess the same solution C of the compression problem. However, to assure that it coincides with the solution of the same problem for $W = U_1^\dagger U_2$, we will analyze an exemplary system of size $n = 2 \times 3$. Consider two unitary matrices of a tensor product form,

$$\begin{cases} U_1 = U_A^\dagger \otimes U_B \\ U_2 = U_A \otimes U_B \end{cases} \tag{7.10}$$

where

$$U_A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{-i\alpha} & 0 \\ 0 & 0 & e^{i\alpha} \end{pmatrix} \quad \text{and} \quad U_B = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\xi} \end{pmatrix}. \tag{7.11}$$

Observe that U_1 and U_2 do commute, so they share the same set of eigenvectors. Assume that the phases satisfy $\alpha \in (\pi/2, \pi)$ and $\xi \in (0, \min\{\alpha, 2(\pi - \alpha)\})$. Then the ordered spectra of both matrices read

$$\begin{aligned} U_1 &= \operatorname{diag}\left\{1, e^{i\xi}, e^{i\alpha}, e^{i(\alpha+\xi)}, e^{-i\alpha}, e^{i(\xi-\alpha)}\right\}, \\ U_2 &= \operatorname{diag}\left\{1, e^{i\xi}, e^{-i\alpha}, e^{i(\xi-\alpha)}, e^{i\alpha}, e^{i(\alpha+\xi)}\right\}, \end{aligned} \tag{7.12}$$

and differ only by the order of the eigenvalues. Both unitary matrices are represented in Fig. 9 in which z_i, $i = 1, \ldots, 6$ denote the ordered eigenvalues of U_1 while $|\varphi_i\rangle$, $i = 1, \ldots, 6$ are eigenvectors of this matrix. The same states form also the set of eigenvectors of U_2, but they correspond to other eigenvalues. Let z_i' denote the ordered eigenvalues of U_2. Then $|\varphi_3\rangle$ corresponds to $z_3' = z_5$ while $|\varphi_5\rangle$ corresponds to $z_5' = z_3$.

The third of the unitaries also has also a tensor product form,

$$W = U_1^\dagger U_2 = (U_A^\dagger \otimes U_B)^\dagger (U_A \otimes U_B) = U_A^2 \otimes \mathbb{1}_2. \tag{7.13}$$

Hence the spectrum of W, denoted by z_i'', consists of three pairs of doubly degenerated eigenvalues, $W = \operatorname{diag}\left\{1, 1, e^{-2i\alpha}, e^{-2i\alpha}, e^{2i\alpha}, e^{2i\alpha}\right\}$, see Fig. 10.

Numerical range of rank two for matrices U_1, U_2 and W is shown in the pictured as a gray region. Each point $\lambda \in \Lambda_2(U_1)$ offers a subspace C_2 which forms a solution of the first of three equations (7.9). However, the other two equations restrict further constraints for λ.

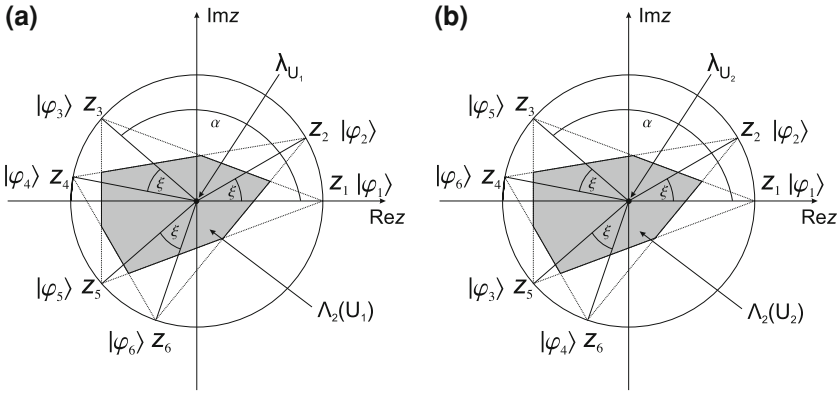

Fig. 9 Numerical range (*gray space*): **a** $\Lambda_2(U_1)$; **b** $\Lambda_2(U_2)$

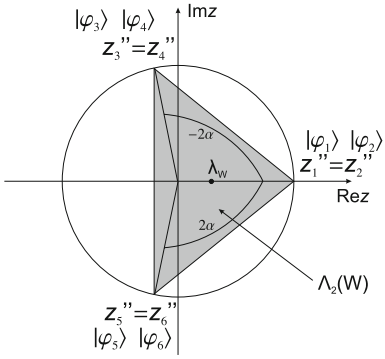

Fig. 10 Numerical range $\Lambda_2(W)$ is represented by a *dark triangle*

To construct an error correction code for the tri-unitary noise model we are going to follow the strategy used above for solving the compression problem: we split the Hilbert space into a direct sum of two subspaces of size three, and try to construct a single state in each subspace. More formally we define the subspace

$$C_2 = \sum_{i=1}^{2} |\psi_i\rangle\langle\psi_i| \tag{7.14}$$

where each state is obtained by a coherent superposition of three eigenstates of U_1,

$$\begin{cases} |\psi_1\rangle = \sqrt{a_1}|\varphi_1\rangle + \sqrt{a_3}|\varphi_3\rangle + \sqrt{a_5}|\varphi_5\rangle \\ |\psi_2\rangle = \sqrt{a_2}|\varphi_2\rangle + \sqrt{a_4}|\varphi_4\rangle + \sqrt{a_6}|\varphi_6\rangle \end{cases} . \tag{7.15}$$

Since the unitary operators U_i can be expressed as tensor product of diagonal matrices (e.g. $U_2 = U_A \otimes U_B$), their joint set of eigenvectors consits of product pure states only. On the other hand, the states $|\psi_1\rangle$ and $|\psi_2\rangle$ are by construction entangled.

The weights a_1 are defined as a weights obtained by representing point λ by a convex combination of the triples of eigenvalues. Since we wish to get a space C being a

joint solution of all three equations (7.9), we are going to require that the same weights a_i can be used to form the compression value λ as a combination of both triples of eigenvalues for each spectrum,

$$\begin{cases} \lambda_{U_1} = a_1 z_1 + a_3 z_3 + a_5 z_5 = a_2 z_2 + a_4 z_4 + a_6 z_6 \\ \lambda_{U_2} = a_1 z_1' + a_3 z_3' + a_5 z_5' = a_2 z_2' + a_4 z_4' + a_6 z_6' \\ \lambda_W = a_1 z_1'' + a_3 z_3'' + a_5 z_5'' = a_2 z_2'' + a_4 z_4'' + a_6 z_6'' \end{cases} \tag{7.16}$$

where z_i, z_i' and z_i'' denote ordered spectra of U_1, U_2 and W, respectively. It is now clear that for a generic choice of U_1 and U_2 (which implies $W = U_1^\dagger U_2$), such a system has no solutions. However, if both diagonal matrices are of the special form (7.12), there exists a solution of the problem. The weights a_i satisfy

$$\begin{cases} a_1 = a_2 = 1 + \dfrac{1}{-1 + \cos\alpha} \\ a_3 = a_4 = \dfrac{1}{2 - 2\cos\alpha} \\ a_5 = a_6 = \dfrac{1}{2 - 2\cos\alpha} \end{cases} \tag{7.17}$$

and imply the following compression values

$$\begin{cases} \lambda_{U_1} = 0 \\ \lambda_{U_2} = 0 \\ \lambda_W = -1 - 2\cos\alpha \end{cases} . \tag{7.18}$$

Due to the symmetry of the problem the latter number λ_W is real.

Substituting the weights (7.17) into (7.15) we get an explicit form (7.14) of the subspace C. It is now easy to check that this subspace satisfies simultaneously all three equations (7.9) with compression values given by (7.18), hence it provides a two dimensional error correction code for this noise model. This solution is correct for any unitaries U_1 and U_2 having any set of eigenvectors $|\varphi_i\rangle$, $i = 1, \ldots, 6$ and spectra given by (7.12) and parameterized by phases α and ξ.

The above construction can be generalized for a tri-unitary noise model acting on larger system of size $N = 3 \times K$ [31]. An error correction code of size K exists in this case, if matrices U_1 and U_2 have the tensor product form (7.10), where $U_A = \mathrm{diag}\{1, e^{i\alpha}, e^{-i\alpha}\}$ as before and $U_B = \mathrm{diag}\{1, e^{i\xi_2}, e^{i\xi_3}, \ldots, e^{i\xi_K}\}$. The code subspace $C = \sum_{i=1}^{K} |\psi_i\rangle\langle\psi_i|$ is then obtained in an analogous way, by representing the Hilbert space as a direct product of K subspaces of dimension three each and constructing each state $|\psi_i\rangle$ as a coherent superposition of three eigenstates of U_1 corresponding to a triple of eigenvalues z_l, z_{l+K} and z_{l+2K} for $l = 1, \ldots, K$. Note that the code space constructed here for the bipartite system does not have the tensor product structure, since it is spanned by entangled states (7.15).

8 Conclusions

This paper concerns finite dimensional instruments or Kraus measurements, acting on a quantum system with Hilbert space $\mathcal{H}$. We have proved a version of Heisenberg's Principle, which connects 'darkness' to 'protection' of a subspace $\mathcal{L}$ of $\mathcal{H}$. 'Darkness' expresses the lack of visibility of the information contained in $\mathcal{L}$ from the measurement outcome, and 'protection' the degree to which this information remains present in the quantum system. Complete darkness corresponds to complete recoverability of information as in error correction codes.

We have presented examples of darkness and protection: instruments arising from random external fields, arbitrary rank 2 channels, and biased permutation channels. Bi-unitary noise models were analyzed recently in regard to their error correction properties in [10,24]. Here we have also considered tri-unitary noise. For a a certain class of tri-unitary noise models acting on a $3 \times K$ quantum system, we have explicitly constructed an error correction code of size K. Although this particular noise model might be considered as not very realistic, we tend to believe that the technique proposed can be applied to a broader class of quantum systems.

Acknowledgments We enjoyed fruitful discussions with J. A. Holbrook, P. Horodecki and D. Kribs. We acknowledge financial support by the Polish Research Network LFPPI and by the European Research Project SCALA.

References

1. Duan, L.-M., Guo, G.-C.: Preserving coherence in quantum computation by pairing quantum bits. Phys. Rev. Lett. **79**, 1953 (1997)
2. Zanardi, P., Rasetti, M.: Noiseless quantum codes. Phys. Rev. Lett. **79**, 3306 (1997)
3. Lidar, D.A., Chuang, I.L., Whaley, K.B.: Decoherence-free subspaces for quantum computation. Phys. Rev. Lett. **81**, 2594 (1998)
4. Shabani, A., Lidar, D.A.: Theory of initialization-free decoherence-free subspaces and subsystems. Phys. Rev. A **72**, 042303 (2005)
5. Bennett, C.H., DiVincenzo, D.P., Smolin, J.A., Wootters, W.K.: Mixed-state entanglement and quantum error correction. Phys. Rev. A **54**, 3824 (1996)
6. Knill, E., Laflamme, R.: Theory of quantum error-correcting codes. Phys. Rev. A. **55**, 900 (1997)
7. Maassen, H., Kümmerer, B.: Purification of quantum trajectories. In: Denteneer, D., den Hollander, F., Verbitsky, E. (eds.) Institute of Mathematical Statistics, Lecture Notes—Monograph Series, vol. 48 , pp. 252–261 (2006) and also quant-ph/0505084
8. Kraus, K.: General state changes in quantum theory. Ann. Phys. **64**, 311 (1971)
9. Choi, M.-D., Kribs, D.W., Życzkowski, K.: Higher-rank numerical ranges and compression problems. Linear Algebra Appl. **418**, 828–839 (2006)
10. Choi, M.D., Kribs, D.W., Życzkowski, K.: Quantum error correcting codes from the compression formalism. Rep. Math. Phys. **58**, 77 (2006)
11. Choi, M.-D.: Completely positive linear maps on complex matrices. Linear Algebra Appl. **10**, 285 (1975)
12. Bengtsson, I., Życzkowski, K.: Geometry of Quantum States: An Introduction to Quantum Entanglement. Cambridge University Press, Cambridge (2006)
13. King, C., Matsumoto, K., Nathanson, M., Ruskai, M.B.: Properties of conjugate channels with applications to additivity and multiplicativity. Markov Process Relat. Fields **13**, 391–423 (2007)
14. Davies, E.B., Lewis, J.T.: An Operational Approach to Quantum Probability. Commun. Math. Phys. **17**, 239–260 (1970)
15. Heisenberg, W.: Über den anschaulichen Inhalt der Quantentheoretischen Kinematik und Mechanik. Z. Phys. **43**, 172–198 (1927)

16. Robertson, H.: The uncertainty principle. Phys. Rev. **34**, 163–164 (1929)
17. Werner, R.F.: The uncertainty relation for joint measurement of position and momentum. Quant. Inf. Comp. **4**, 546–562 (2004)
18. Janssens, B.: Unifying decoherence and the Heisenberg principle. www.arxiv.org/quant-ph/0606093
19. Gisin, N.: Stochastic quantum dynamics and relativity. Helv. Phys. Acta. **62**, 363 (1989)
20. Hughston, L.P., Jozsa, R., Wootters, W.K.: A complete classification of quantum ensembles having a given density matrix. Phys. Lett. A **183**, 14 (1993)
21. Lidar, D.A., Bacon, D., Whaley, K.B.: Concatenating decoherence-free subspaces with quantum error correcting codes. Phys. Rev. Lett. **82**, 4556 (1999)
22. Kribs, D.W., Pasieka, A., Życzkowski, K.: Entropy of a quantum error correction code. Open Syst. Inf. Dyn. **15**, 329–343 (2008)
23. Bhatia, R.: Matrix Analysis. Springer, New York (1997)
24. Choi, M.D., Holbrook, J.A., Kribs, D.W., Życzkowski, K.: Higher-rank numerical ranges of unitary and normal matrices. Oper. Matrices **1**, 409 (2007)
25. Li, C.-K., Sze, N.-S.: Canonical forms, higher rank numerical ranges, totally isotropic subspaces, and matrix equations. Proc. Am. Math. Soc. **136**, 3013–3023 (2008)
26. Woerdeman, H.: The higher rank numerical range is convex. Linear Multilinear Algebra **56**, 65–67 (2008)
27. Choi, M.-D., Giesinger, M., Holbrook, J.A., Kribs, D.W.: Geometry of higher-rank numerical ranges. Linear Multilinear Algebra **56**, 53–64 (2008)
28. Li, C.-K., Poon, Y.-T., Sze, N.-S.: Condition for the higher rank numerical range to be non-empty. Linear Multilinear Algebra. **57**, 365–368 (2009)
29. Li, C.-K., Poon, Y.-T., Sze, N.-S.: Higher rank numerical ranges and low rank perturbations of quantum channels. J. Math. Anal. Appl. **348**, 843–855 (2008)
30. Alicki, R., Lendi, K.: Quantum Dynamical Semigroups and Their Applications, LNP 286. Springer, Berlin (1987)
31. Majgier, K.: Quantum error correction codes for unitary models of noise (*in Polish*), Master thesis, Jagiellonian University, Cracow, June 2007. See http://chaos.if.uj.edu.pl/~karol/prace/Majgier07.pdf