Quantum Zero-Error Secrecy Capacity

Elloá B. Guedes and Francisco M. de Assis

***Abstract*—Aiming at transmitting secret classical messages through noisy quantum channels, the present work proposes quantum codes in which no decoding erros occur nor information leakage out to a wiretapper. These codes are based on error-free codes and on decoherence-free subspaces and subsystems. A consequence of such proposition is the rise of the *quantum zero-error secrecy capacity* (ZESC), the maximum rate in which information can be transmitted through a noisy quantum channel using such codes with unconditional security. We also propose a graph-theoretic approach to obtain ZESC, and show that, in certain situations, this capacity is single-letter characterized.**

***Index Terms*—Decoherence-Free Subspaces and Subsystems; Quantum Secrecy Capacity; Quantum Zero-Error Capacity.**

I. Introduction

QUANTUM *information theory* deals with problems related to information treatment and transmission through quantum channels. Its research areas include the study of quantum error-correction codes, quantum entanglement, and quantum channel capacity [1]. The *capacity* is defined as the transmission rate optimized over all possible quantum codes such that decoding errors vanish in the limit of asymptotically many uses of the channel.

In the case of noisy channels, the interaction with the environment and the subsequent *decoherence* is a source of errors and information leakage out to a wiretapper. Then, the *secrecy capacity* of a noisy quantum channel is the transmission rate optimized over all possible *wiretap codes* such that decoding errors between legitimate parts and information leakage to a wiretapper vanish in the limit of asymptotically many uses of the channel [2] [3].

For overcoming decoherence, some good methods have been proposed such as quantum error-correcting codes, dynamical decoupling, decoherence-free subspaces and subsystems (DFS), and so on [4]. Regarding DFS, in particular, if the error operators that affect the qubits have some symmetries, then the qubits will suffer from the same noise in the quantum channel and that will compensate the resulting effects, keeping the invariability of these states, what means that no decoherence takes place in such subspaces and subsystems [5].

Taking advantage of DFS to prevent information leakage out, Guedes and de Assis [6], [7] showed that quantum codes built with states from a DFS are instances of wiretap codes with the particularity that no information is gathered by the wiretapper. They also showed that the rate of these codes can reach the maximum rate of the channel to send ordinary classical information, i.e., the Holevo-Schumacher-Westmoreland (HSW) capacity [8], [9].

Medeiros et al. [10] proposed a method to find DFS in error-free quantum codes, based on a technique for obtaining DFS created by Choi and Kribs [11]. Based on such ideas, the present paper characterizes a strategy to obtain (when possible) wiretap codes from error-free quantum codes, with the particularity that no decoding erros occur nor information leakage. It results in a new concept: the *quantum zero-error secrecy capacity* (ZESC), defined as the maximum rate that information can be conveyed through a noisy quantum channel using such codes and with unconditional security.

We show a graph-theoretic approach to ZESC, taking advantage of a similar procedure to the quantum zero-error capacity [12]. We also show that ZESC, in certain situations, has a single-letter characterization. It contrasts with the secrecy capacity of quantum channels which, so far, has been considered as not having a computable version [2].

The rest of this paper is structured as follows. Section II introduces the concepts regarding decoherence-free subspaces and subsystems as well as a method for obtaining them; Section III recalls the results of Guedes and de Assis [6], [7] on the use of DFS to build wiretap codes; Section IV introduces the theory of quantum zero-error capacity, including its graph theoretical approach, and the relation between error-free codes and DFS. Our main results are presented in Section V in which ZESC is formalized, its relation with Graph Theory is established, and detailed examples are presented. Relations of such propositions with already existing works in the literature are discussed in Section VI. Lastly, final remarks are presented in Section VII.

A. Notation and Conventions

Here we introduce some notation and conventions that will be used throughout the paper. Logarithms are taken on base 2. Let $\mathcal{B}(\mathcal{H})$ denote the set of operators in a d-dimensional Hilbert space $\mathcal{H}$. The quantum information theory measure S denotes the von Neumann entropy; and χ denotes the Holevo quantity. Tr denotes the partial trace over a quantum state. Moreover, we use the Dirac notation to denote quantum states and operations.

II. Decoherence-Free Subspaces and Subsystems

Due to decoherence, a quantum system may begin to lose energy into the environment and decay to a ground state, its relative phase may be erased and, thus, the information

Elloá B. Guedes and Francisco M. de Assis. IQuanta – Institute for Studies in Quantum Computation and Information, Federal University of Campina Grande, Av. Aprígio Veloso, 882 – 58429-140, Campina Grande – Paraíba – Brazil. E-mails: {elloaguedes,fmarassis}@gmail.com. This work was supported by the Brazilian funding agencies CAPES and CNPq.

it carries may be lost [13]. In this section, we will show how to avoid these undesired effects despite the existence of decoherence.

Let a closed quantum system be composed by the *system of interest* S defined on a Hilbert space $\mathcal{H}$ and by the *environment* E. The Hamiltonian that describes this system is defined as follows

$$\mathbb{H} = \mathbb{H}_S \otimes \mathbb{1}_E + \mathbb{1}_S \otimes \mathbb{H}_E + \mathbb{H}_{SE} \tag{1}$$

where $\mathbb{1}$ is the identity operator; and $\mathbb{H}_S$, $\mathbb{H}_E$ and $\mathbb{H}_{SE}$ denote the Hamiltonians of system, environment and system-environment interaction, respectively.

In order to prevent errors, it would be ideal that $\mathbb{H}_{SE}$ were equal to zero, indicating that system and environment are decoupled and evolve independently and unitarily under their respective Hamiltonians $\mathbb{H}_S$ and $\mathbb{H}_E$ [5]. However, in practical scenarios, such an ideal situation is not possible since no system is noiseless. So, after isolating a system to the best of our ability, we should aim for the realistic goals of the identification and correction of errors when they occur and/or avoiding noises when possible and/or suppressing noise in the system [4].

If some symmetries exist in the interaction between the system and the environment, it is possible to find a "quiet corner" in the system Hilbert space not experiencing decoherence. Let $\{A_i(t)\}$ be a set of operators in the *operator-sum representation* (OSR) corresponding to the evolution of the system. We say that a system density matrix ρ_S is *invariant* under the OSR operators $\{A_i(t)\}$ if $\sum_i A_i(t)\rho_S A_i^\dagger(t) = \rho_S$. We are now able to define the decoherence-free subspaces whose states are invariant despite a non-trivial coupling between the system and the environment.

Definition 1. *A subspace $\tilde{\mathcal{H}}$ of a Hilbert space $\mathcal{H}$ is called decoherence-free with respect to a system-environment coupling if every pure state from this subspace is invariant under the corresponding OSR evolution for any possible environment initial condition:*

$$\sum_i A_i(t)|\tilde{k}\rangle\langle\tilde{k}|A_i^\dagger(t) = |\tilde{k}\rangle\langle\tilde{k}|, \forall|\tilde{k}\rangle\langle\tilde{k}| \in \tilde{\mathcal{H}}, \forall\rho_E(0) \tag{2}$$

Let the Hamiltonian of the system-environment interaction be $\mathbb{H}_{SE} = \sum_j \mathbf{S}_j \otimes \mathbf{E}_j$, where $\mathbf{S}_j$ and $\mathbf{E}_j$ are the system and environment operators, respectively. We consider that the environment operators $\mathbf{E}_j$ are linearly independent. The symmetries required to define a decoherence-free subspace are described in the theorem below. For a detailed proof or different formulations see [5, Sec. 5].

Theorem 1. *(*Decoherence-Free Subspace Conditions*) A subspace $\tilde{\mathcal{H}}$ is decoherence-free iff the system operators $\mathbf{S}_j$ act proportional to the identity on the subspace:*

$$\mathbf{S}_j|\tilde{k}\rangle = c_j|\tilde{k}\rangle \quad \forall j, |\tilde{k}\rangle \in \tilde{\mathcal{H}} \tag{3}$$

The notion of a subspace which remains decoherence-free throughout the evolution of a system is not, however, the most general method for providing decoherence-free encoding of information in a quantum system [5]. Knill et al. [14] discovered a method for decoherence-free encoding into subsystems instead of into subspaces which is presented below.

Definition 2. *(Decoherence-Free Subsystem) Consider a decomposition of the whole Hilbert space $\mathcal{H} = (\mathcal{H}^A \otimes \mathcal{H}^B) \oplus \mathcal{K}$, where $\dim(\mathcal{H}) = \dim(\mathcal{H}^A) \cdot \dim(\mathcal{H}^B) + \dim(\mathcal{K})$. A subspace $\mathcal{H}^B$ of the full Hilbert space is a* decoherence-free subsystem *if*

$$\forall\rho^A, \forall\rho^B, \exists\tau^A : \mathcal{E}(\rho^A \otimes \rho^B) = \tau^A \otimes \rho^B \tag{4}$$

where $\rho^A, \tau^A \in \mathcal{B}(\mathcal{H}^A)$, and $\rho^B \in \mathcal{B}(\mathcal{H}^B)$.

In fact, B is said to encode a decoherence-free subsystem if (4) is satisfied. In particular, when $dim(\mathcal{H}^A) = 1$, B is a decoherence-free subspace.

To make explicit the difference between decoherence-free subspaces and subsystems, consider the encoding of a generic qubit $\alpha|0\rangle + \beta|1\rangle$ into $\alpha|01\rangle + \beta|10\rangle$. In this case, the information has been encoded into a *subspace* of the two qubit Hilbert space. Suppose now that the information is encoded only into the first qubit of the two qubits available, i.e., $\alpha|0\rangle + \beta|1\rangle \mapsto (\alpha|0\rangle + \beta|1\rangle) \otimes |\psi\rangle$. Since this second encoding is a one-to-many mapping from the quantum information in one qubit to a two qubit Hilbert space, then it is said that the information has been encoded into a *subsystem* [15].

A. A Method for Obtaining DFS

In practice, identifying a useful symmetry and taking advantage of it can be very difficult [4]. To overcome such problem, Choi and Kribs [11] proposed a systematic method to identify DFS when the model of errors is known.

Let $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ be a quantum operation. We shall write $\mathcal{E} \equiv \{E_a\}$ when the error model for $\mathcal{E}$ is known. The operation elements $\{E_a\}$ determine $\mathcal{E}$ through the familiar OSR, i.e., $\mathcal{E}(\sigma) = \sum_a E_a \sigma E_a^\dagger$.

The *noise commutant* $\mathcal{A}'$ for $\mathcal{E}$ is the set of all operators in $\mathcal{B}(\mathcal{H})$ that commute with the operators E_a and $E_a^\dagger$. In the unital case ($\mathcal{E}(\mathbb{1}) = \mathbb{1}$), every $\sigma \in \mathcal{A}'$ satisfies $\mathcal{E}(\sigma) = \sigma$. As a consequence, $\mathcal{A}'$ is a †-algebra generated by E_a, which is called *interaction algebra* associated with $\mathcal{E}$.

However, not all channels are unital and, because of that, it is necessary to propose a more general approach. In these more general cases, all that can be said for operators $\sigma \in \mathcal{A}'$ is that they satisfy $\mathcal{E}(\sigma) = \sigma\mathcal{E}(\mathbb{1}) = \mathcal{E}(\mathbb{1})\sigma$. Given a projection P in $\mathcal{B}(\mathcal{H})$, the goal will be the identification of a subalgebra $P\mathcal{B}(\mathcal{H})P$ with the algebra $\mathcal{B}(P\mathcal{H})$.

Theorem 2. *(Choi and Kribs [11]) Let $\mathcal{E} = \{E_a\}$ be a quantum operation on $\mathcal{B}(\mathcal{H})$. Suppose P is a projection on $\mathcal{H}$ such that*

$$\mathcal{E}(P) = P\mathcal{E}(P)P \tag{5}$$

Then $E_aP = PE_aP$, $\forall a$. Define

$$\mathcal{A}_P^{'} \equiv \left\{\sigma \in \mathcal{B}(P\mathcal{H}) : [\sigma, PE_aP] = 0 = \left[\sigma, PE_a^{\dagger}P\right]\right\} \quad (6)$$

and

$$\mathrm{Fix}_P(\mathcal{E}) \equiv \{\sigma \in \mathcal{B}(P\mathcal{H}) : \mathcal{E}(\sigma) = \sigma\mathcal{E}(P) = \mathcal{E}(P)\sigma, \quad (7)$$
$$\mathcal{E}(\sigma^{\dagger}\sigma) = \sigma^{\dagger}\mathcal{E}(P)\sigma, \mathcal{E}(\sigma, \sigma^{\dagger}) = \sigma\mathcal{E}(P)\sigma^{\dagger}\} \quad (8)$$

Then $\mathrm{Fix}_P(\mathcal{E})$ is a $\dagger$-algebra inside $\mathcal{B}(P\mathcal{H})$ that coincides with the algebra $\mathcal{A}_P^{'}$; that is

$$\mathrm{Fix}_P(\mathcal{E}) = \mathcal{A}_P^{'} \quad (9)$$

Projectors P satisfying (5) have some properties. For instance, a quantum channel $\mathcal{E} \equiv \{E_a\}$ acts in a quantum state $\sigma \in \mathcal{A}_P^{'}$ projecting it into another state σ' in the subspace P. To show this, we have

$$\begin{aligned} \sigma' &= \mathcal{E}(\sigma) && (10)\\ &= \sigma\mathcal{E}(P) && (11)\\ &= (P\sigma P)(P\mathcal{E}(P)P) && (12)\\ &= P[\sigma P\mathcal{E}(P)]P \in \mathcal{B}(P\mathcal{H}) && (13)\end{aligned}$$

In this particular case, we have $\mathcal{E}(\sigma) = \sigma$ only if $\mathcal{E}(P) = \mathbb{1}$.

The next step is to show how projectors with such characterization identify the DFS in a quantum operation $\mathcal{E}$.

Theorem 3. *(Choi and Kribs [11]) Let $\mathcal{E}$ be a quantum operation on $\mathcal{B}(\mathcal{H})$. Let P be a projection on $\mathcal{H}$ that satisfies (5) and let $P\mathcal{H} = \oplus_k(\mathcal{H}^{A_k} \otimes \mathcal{H}^{B_k})$ be the decomposition of $P\mathcal{H}$ induced by the $\dagger$-algebra structure of $\mathcal{A}_P^{'} = \mathrm{Fix}_P(\mathcal{E})$. Then the subsystems $\mathcal{H}^{B_k}$, with $\dim(\mathcal{H}^{B_k}) > 1$, are each decoherence-free subsystems for $\mathcal{E}$.*

It is possible to say, thus, that the essence of this method consists in the determination of all projectors P satisfying (5). From this, the structure of $\mathcal{A}_P^{'} = \mathrm{Fix}_P(\mathcal{E})$ can be used to determine the states belonging to the DFS.

An important remark about this method is its *optimality*, i.e., it is able to obtain all projectors satisfying (5) (vide [11, Theorem 3]). So far, however, there is no computational procedure already implemented to automatize the execution of this method.

III. Secrecy Capacity and Decoherence-Free Subspaces and Subsystems

In a recent work, Guedes and de Assis [6], [7] investigated the impacts of the use of DFS in Quantum Communications. They considered the case that a sender (Alice) wants to convey secret classical messages through a quantum channel to a legitimate receiver (Bob). These messages must be protected from a wiretapper (Eve) that has full access to the environment.

To exchange the messages without being deceived by Eve, Alice and Bob use a *quantum error-avoiding code* (QEAC) build from the states of a DFS according to the following definition.

Definition 3. *Let $\tilde{\mathcal{H}}$ be a DFS spanned by a set of eigenvectors $\{|\tilde{k}\rangle\}$, i.e., $\tilde{\mathcal{H}} = Span[\{|\tilde{k}\rangle\}]$. A set of codewords of length n ($n = dim(\tilde{\mathcal{H}})$) for a set $\mathcal{U}$ of classical messages is a set of input states labeled by messages in $\mathcal{U}$, $\tilde{K}(\mathcal{U}) = \{\tilde{k}(u) : u \in \mathcal{U}\} \subseteq \tilde{\mathcal{H}}$, and a decoding measurement composed of a set of positive operators $\tilde{\mathcal{D}}_u$, $u \in \mathcal{U}$ with $\sum_{u\in\mathcal{U}} \tilde{\mathcal{D}}_u \leq \mathbb{1}$. The pair $(\tilde{K}(\mathcal{U}), \{\tilde{\mathcal{D}}_u : u \in \mathcal{U}\})$ is called a QEAC of length n for the set $\mathcal{U}$ of messages. The rate of this code is $\frac{1}{n}\log|\mathcal{U}|$.*

Using the code defined, if Alice wants to send a classical message u through the quantum channel $\mathcal{E}$, now she encodes it according to the QEAC defined over $\tilde{\mathcal{H}}$, obtaining $\tilde{k}(u)$. When she sends it through the communication channel, the message interacts with the environment (which is assumed to start in a pure state $|0_E\rangle$). This scenario is depicted in Figure 1. Bob then receives $\rho_{\mathrm{Bob}}(\tilde{k}(u))$ and Eve receives $\rho_{\mathrm{Eve}}(\tilde{k}(u))$, which are given by:

$$\rho_{\mathrm{Bob}}(\tilde{k}(u)) = \mathrm{Tr}_{\mathrm{E}}\left[\mathcal{E}(\tilde{k}(u) \otimes |0_E\rangle\langle 0_E|)\right] \quad (14)$$
$$\rho_{\mathrm{Eve}}(\tilde{k}(u)) = \mathrm{Tr}_{\mathrm{B}}\left[\mathcal{E}(\tilde{k}(u) \otimes |0_E\rangle\langle 0_E|)\right] \quad (15)$$

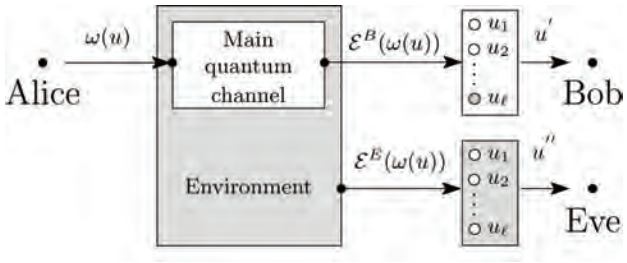


Fig. 1: General idea of the scenario described.

Since Alice used a QEAC, then the existing dynamical symmetry protected the quantum information from the interaction with the environment. It means that the joint evolution of the system and the environment occurred in a decoupled way. Hence, the state $\rho_{\mathrm{Bob}}(\tilde{k}(u))$ is given by:

$$\begin{aligned}\rho_{\mathrm{Bob}}(\tilde{k}(u)) &= \mathrm{Tr}_{\mathrm{E}}\left[\mathcal{E}(\tilde{k}(u) \otimes |0_E\rangle\langle 0_E|)\right] && (16)\\ &= \mathrm{Tr}_{\mathrm{E}}\left[\sum_i A_i\left(\tilde{k}(u) \otimes |0_E\rangle\langle 0_E|\right)A_i^{\dagger}\right] && (17)\\ &= \mathrm{Tr}_{\mathrm{E}}\left[\tilde{k}(u) \otimes \rho_E\right] && (18)\\ &= \tilde{k}(u) && (19)\end{aligned}$$

where (18) is due to the invariance of a state of the DFS under the OSR operators. The information accessible by Bob is upper bounded by the Holevo quantity which is given by

$$\chi^{\text{Bob}} = S\left(\sum_u p_u \rho_{\text{Bob}}(\tilde{k}(u))\right) - \sum_u p_u S\left(\rho_{\text{Bob}}(\tilde{k}(u))\right) \quad (20)$$

where p_u is the a priori distribution of the symbols in $\mathcal{U}$. Eve, in turn, will try to build a POVM based on the typicality of the sequences she gathers, following a strategy presented in [2, Sec. 4].

Using the theory of quantum wiretap channels [2], [3], Guedes and de Assis [6] showed that the information leaked out to the wiretapper is zero and that the secrecy capacity of such scenario is equal to the HSW capacity as showed in the theorem below.

Theorem 4. *(Guedes and de Assis [6]) The secrecy capacity of a quantum channel $\mathcal{E}$ which has a DFS $\tilde{\mathcal{H}}$ is*

$$C_{S,DFS}(\mathcal{E}) = \max_{\{P\}} \left[\chi^{Bob}\right] \quad (21)$$

where the maximum is taken over all probability distributions P over $\mathcal{U}$; and χ^{Bob} is the Holevo quantity given in (20).

This implies that the secrecy capacity when a QEAC is used can reach the maximum rate of classical information transmission through the channel.

IV. Zero-Error Capacity of Quantum Channels

The *zero-error capacity* of a discrete classical channel was first defined by Shannon [16] as the least upper bound of rates for which one transmits information with zero probability of error. Its quantum analogous, the *quantum zero-error capacity* (QZEC) generalizes this concept to include quantum channels, in a scenario where classical information is conveyed [12].

Given a quantum channel, we ask for the maximum amount of classical information that can be transmitted through it with a zero probability of error. Before defining such quantity, it is necessary to define a *quantum error-free block code* that gives a general idea of the communication protocol employed.

Definition 4. *((K_n, n) error-free quantum block code [17]) A (K_n, n) quantum error-free block code for a quantum channel $\mathcal{E}$ is composed of:*

1) *A set of classical messages $\{1, \ldots, K_n\}$;*
2) *An encoding function: $X^n : \{1, \ldots, K_n\} \to \mathcal{S}^{\otimes n}$ that associates a product state to each classical message;*
3) *A decoding function $g : \{1, \ldots, m\} \to \{1, \ldots, K_n\}$ which deterministically assigns a guess to each possible measurement output $y \in \{1, \ldots, m\}$ performed by a POVM $\mathcal{M} = \{M_m\}$. The decoding function has the following property*

$$\Pr[g(Y = y) \neq i | X^n(i)] = 0, \forall i \in \{1, \ldots, K_n\} \quad (22)$$

The rate of this code is $R_n = \frac{1}{n} \log K_n$ bits per channel use.

Thus, we can now define the QZEC:

Definition 5. *(Quantum zero-error capacity [17]) Let $\mathcal{E}(\cdot)$ be a positive, linear, trace-preserving quantum map representing a noisy channel. The quantum zero-error capacity of $\mathcal{E}(\cdot)$, denoted by $C^{(0)}(\mathcal{E})$, is the least upper bound of achievable rates with probability of error equal to zero, that is*

$$C^{(0)}(\mathcal{E}) = \sup_{\mathcal{S}} \sup_n \frac{1}{n} \log K_n \quad (23)$$

where K_n stands for the maximum number of classical messages that the system can transmit without error, when a (K_n, n) error-free quantum block with input alphabet $\mathcal{S}$ is used.

However, we are interested in a quantum channel where $\mathcal{E}$ has a non-vanishing zero-error capacity. To guarantee this, it is necessary that the set $\mathcal{S}$ contains at least two *non-adjacent states*, denoted by $\rho_i \perp_{\mathcal{E}} \rho_j$, where $\rho_i, \rho_j \in \mathcal{S}$. By non-adjacent states we mean states that are distinguishable at the channel's end, i.e., the Hilbert subspaces spanned by the supports of ρ_i and ρ_j are orthogonal.

In the attempt to reach the zero-error capacity, it is necessary to take into account error-free quantum codes that maximize the rate of transmission. It leads to the following definition.

Definition 6. *(Optimum $(\mathcal{S}, \mathcal{M})$ for $\mathcal{E}$ [17]) The optimum $(\mathcal{S}, \mathcal{M})$ for a quantum channel $\mathcal{E}$ is composed of a set $\mathcal{S} = \{\rho_i\}$ and a POVM $\mathcal{M} = \{M_m\}$ for which the zero-error capacity is reached.*

A. Graph-Theoretic Approach

The zero-error capacity allows an interpretation in terms of Graph Theory [17]. Given a quantum channel $\mathcal{E}$ and a set of input states $\mathcal{S} = \{\rho_1, \ldots, \rho_\ell\}$, it is possible to construct a characteristic graph $\mathcal{G} = \langle V, E \rangle$ as follows:

- $V = \{1, \ldots, \ell\}$ is the vertex set containing the index set of $\mathcal{S}$;
- $E = \{(i, j) | \rho_i \perp_{\mathcal{E}} \rho_j, \rho_i, \rho_j \in \mathcal{S}, i \neq j\}$

This notion of characteristic graph can also be extended to the n-product $\mathcal{G}^n$, where $V = V^n$ and E is composed of pairs of such indexes whose corresponding sequences are non-adjacent in $\mathcal{E}$.

From this interpretation, it is easy to see that quantum states corresponding to vertices in any complete subgraph of $\mathcal{G}$ are mutually non-adjacent. Therefore, the maximum number of messages that can be transmitted without error with a (K_n, n) error-free quantum code with input alphabet $\mathcal{S}$ is the clique number of $\mathcal{G}^n$, which is denoted by $\omega(\mathcal{G}^n)$. This way, we get an alternative and equivalent definition of the QZEC in terms of Graph Theory.

Definition 7. *(QZEC in terms of Graph Theory) The zero-error capacity of a quantum channel $\mathcal{E}$ is given by*

$$C^{(0)}(\mathcal{E}) = \sup_{\mathcal{S}} \sup_n \frac{1}{n} \log \omega(\mathcal{G}^n) \quad (24)$$

where the supremum is taken over all subsets $\mathcal{S}$ of input states, and $\omega(\mathcal{G}^n)$ is the clique number *of the n-product of the characteristic graph $\mathcal{G}$ associated with $\mathcal{S}$.*

B. Relation with Decoherence-Free Subspaces and Subsystems

Medeiros et al. [10] investigated the relation between the QZEC and DFS. Let a pair $(\mathcal{S}, \mathcal{M})$ be optimum in the sense of Definition 6. Let $\{M_1, \ldots, M_k\}$ be a subset of $\mathcal{M}$ where each M_i satisfies

$$\mathcal{E}(M_i) = M_i \mathcal{E}(M_i) M_i \quad (25)$$

$$M_i M_j = \delta_{i,j} M_i M_j \quad (26)$$

for all $i, j \leq k$.

Select one state $\rho_i = |s_i\rangle \langle s_i|$ from each subspace $P_i\mathcal{H}$ satisfying $[p_i, P_i E_a P_i] = 0$ and $\left[p_i, P_i E_a^\dagger P_i\right] = 0$. We can construct a pair $(\mathcal{S}', \mathcal{M}')$ where $\mathcal{S}' = \{\rho_i\}$, and a POVM $\mathcal{M}' = \{M_1, \ldots, M_k, M_{k+1}\}$,$M_{k+1} = \mathbb{1} - \sum_{i=1}^{k} M_i$ where $M_1, \ldots, M_k$ satisfies Eqs. (25) and (26). We have, then, the following theorem due to [10].

Theorem 5. *Let the pair $(\mathcal{S}, \mathcal{M})$ be optimum in the sense of Definition 6. Then the pair $(\mathcal{S}', \mathcal{M}')$ is also optimum.*

The results follows from Shannon's concept of adjacency-reducing mapping [16]. In the quantum-zero error scenario, this means a mapping of quantum states into letters $\rho_i \mapsto \beta(\rho_i)$, with the property that if ρ_i and ρ_j are not adjacent in the quantum channel then $\beta(\rho_i)$ and $\beta(\rho_j)$ are not adjacent. If all input states in the optimum $\mathcal{S}$ can be mapped by an adjacency-reducing map into a subset of letters no two of which are adjacent, then the zero-error capacity of the channel is equal to the logarithm of the number of letters in this subset [10].

Let $G_{(')}$ be the characteristic graph for $(\mathcal{S}', \mathcal{M}')$ then

$$C^{(')}(\mathcal{E}) = \sup_n \frac{1}{n} \log \omega(\mathcal{G}_{(')}^n) \quad (27)$$

Using results from adjacency-reducing map [16], the authors showed that $C^{(')}(\mathcal{E}) \geq C^{(0)}(\mathcal{E})$.

In summary, the authors show that if the optimum $\mathcal{S}$ contains DFS, then the QZEC is readily calculated by finding projectors fulfilling some properties. So, it is reasonable to believe in a close connection between these subsystems and any scheme allowing information transmission with error probability equal to zero [10].

V. Quantum Zero-Error Secrecy Capacity

We consider the same scenario described in Section III in which Alice wants to send a secret classical message to Bob through a noisy channel wiretapped by Eve who has full access to the environment. This channel, in particular, has its zero-error capacity a greater than zero.

Definition 8. *Let $\mathcal{E}$ be a trace-preserving quantum map representing a noisy channel. The error-model for $\mathcal{E}$ is known and can be represented by the operation elements $\{E_a\}$, i.e., $\mathcal{E} \equiv \{E_a\}$. We impose that $\mathcal{E}$ has a strictly positive zero-error capacity, $C^{(0)}(\mathcal{E}) > 0$, reached by a optimum pair $(\mathcal{S}, \mathcal{M})$.*

Let's suppose that a subset $\mathcal{M}' = \{M_1, \ldots, M_k\}$ of $\mathcal{M}$ satisfies the conditions of Eqs. (25) and (26) giving rise to a pair $(\mathcal{S}', \mathcal{M}')$ which is also optimum, with $\mathcal{S}' = \{\rho_i = |s_i\rangle \langle s_i|\}_{i=1}^k$, where each ρ_i belongs to the subspace $M_i\mathcal{H}$ satisfying $[\rho_i, M_i E_a M_i] = 0$ and $\left[\rho_i, M_i E_a^\dagger M_i\right] = 0$.

The optimum pair $(\mathcal{S}', \mathcal{M}')$ was obtained according to the procedures described in Section IV-B. Due to that, it defines a decoherence-free subsystem that can be used to encode information that is free from a wiretapper, as it is going to be proved by the following lemmas.

Lemma 1. *The pair $(\mathcal{S}', \mathcal{M}')$ is a quantum-error avoiding code (vide Definition 3).*

Proof: To prove this lemma we must show that it is possible to characterize the elements of a QEAC from the pair $(\mathcal{S}', \mathcal{M}')$.

Let $\mathcal{U} = \{u_1, \ldots, u_k\}$ be a set of classical messages, each uniquely associated to a state of $\mathcal{S}'$. It defines a set of codewords $\tilde{K}(\mathcal{U}) = \{\tilde{k}(u_i) = \rho_i\} \equiv \mathcal{S}'$ of length n ($n = \dim(\mathcal{H})$). The decoding measurement is composed of a set of positive operators $M_i \in \mathcal{M}'$, $i \in 1, \ldots, |\mathcal{U}|$, with $\sum_{i=1}^{k} M_i \leq \mathbb{1}$. Each M_i is uniquely associated with a message $u_i \in \mathcal{U}$. So, the pair $(\tilde{K}(\mathcal{U}), \mathcal{M}')$ is a QEAC of length n with rate $\frac{1}{n} \log |\mathcal{U}|$. ∎

Lemma 2. *The optimum pair $(\mathcal{S}', \mathcal{M}')$ is a wiretap code*[1] *with parameters $(n, |\mathcal{U}|, 0, 0)$*

Proof: In the previous lemma, it was proved that $(\mathcal{S}', \mathcal{M}')$ is a QEAC. Guedes and de Assis [6, Lemma 1] established a proof that every QEAC is a wiretap code with parameters $(n, |\mathcal{U}|, \lambda, \mu)$. The parameters n and $|\mathcal{U}|$ come from the proof of Lemma 1. We must recall that the parameter λ regards the average decoding error probability and that μ is the average accessible information by the wiretapper. In this particular case, we must prove that $\lambda = 0$ and $\mu = 0$.

Since the pair $(\mathcal{S}', \mathcal{M}')$ is optimum, then it allows the channel $\mathcal{E}$ to reach $C^{(0)}$, so the communication can be carried out without decoding errors, what implies $\lambda = 0$.

Then we proceed to analyze the second criterion. Recall from (18) that the final state of Eve is given by ρ_E which is not known. Since Alice and Bob used states from a DFS, it is possible to guarantee that the interaction Hamiltonian $\mathbb{H}_{SE}$ from (1) did not govern the joint evolution of system and environment. Instead of that, each system evolved completely unitary under its own Hamiltonian, i.e., the environment suffered only the action of $\mathbb{H}_E$. It implies that the environment ended in a pure state. Taking this fact into account, we can obtain the Holevo quantity of Eve which is an upper bound to her accessible information

[1]The formal definition of a wiretap code and its requirements can be found in [2, Sec. 3, Eqs. (9) and (10)].

$$\chi^{\text{Eve}} = S(\rho_{\text{Eve}}(\tilde{k}(u))) - \sum_u p_u S(\rho_{\text{Eve},u}\tilde{k}(u)) \quad (28)$$

$$= S(\rho_E) - \sum_u p_u S(\rho_{\text{Eve},u}\tilde{k}(u)) \quad (29)$$

$$= 0 - \sum_u p_u S(\rho_{\text{Eve},k}\tilde{k}(u)) \quad (30)$$

It is well known that the Holevo quantity $\chi^{\text{Eve}} \geq 0$. Since $S(\rho) \geq 0$ for any ρ, and that the probabilities $p_u \geq 0$ for any u, then it is the case that the remaining term is zero. Thus, $\chi^{\text{Eve}} = 0$. Since the Holevo quantity is an upper bound for the accessible information, then it is also equal to zero, what implies $\mu = 0$. This concludes the proof. ∎

Although an optimum pair $(\mathcal{S}', \mathcal{M}')$ defines a wiretap code with parameters $(n, |\mathcal{U}|, 0, 0)$, it is not always the case that is possible to extract a pair $(\mathcal{S}', \mathcal{M}')$ from an optimum pair $(\mathcal{S}, \mathcal{M})$. According to Lemma 1, we have that finding this pair is equivalent to identify a DFS $\tilde{\mathcal{H}}$. However, considering practical scenarios, a DFS may exist although with a smaller dimension than the one considered by the error-free code, i.e., $dim(\tilde{\mathcal{H}}) < n$. This consideration leads to the definition of a wiretap code $(dim(\tilde{\mathcal{H}}), |\mathcal{U}|, 0, 0)$ which still allows the communication between the parties without decoding errors and information leakage. Taking into account these considerations and also the two lemmas previously proved, it is possible to characterize a new capacity of quantum channels which definition is given as follows.

Definition 9. *(Quantum Zero-Error Secrecy Capacity) The quantum zero-error secrecy capacity of a quantum channel $\mathcal{E}$, as given in Definition 8, is the maximum real number $C_S^{(0)}$ such that for all $\epsilon > 0$ and for sufficiently large n there exists a wiretap code $(n, |\mathcal{U}|, 0, 0)$ such that*

$$C_S^{(0)} \leq \frac{1}{n} \log |\mathcal{U}| + \epsilon \quad (31)$$

Two interesting features of the ZESC is that there are no decoding errors, and the information leakage out to a wiretapper is zero. It is in contrast with the regular secrecy capacity of quantum channels in which the decoding errors between legitimate parts and information leakage to a wiretapper vanish in the limit of asymptotically many uses of the channel.

The following theorem aims at quantifying ZESC.

Theorem 6. *The zero-error secrecy capacity of a quantum channel $\mathcal{E}$ as in Definition 8 is*

$$C_S^{(0)} \equiv \min\left\{C^{(0)}(\mathcal{E}), C_S(\mathcal{E})\right\} \quad (32)$$

$$\equiv \min\left\{\sup_{\tilde{\mathcal{H}}} \sup_n \frac{1}{n} \log \left|\dim \tilde{\mathcal{H}}\right|^n, \max_{\{P\}} \chi^{Bob}\right\} \quad (33)$$

where n is the code length; the maximum is taken over all probability distributions P over $\mathcal{U}$; and χ^{Bob} denotes the Holevo quantity of Bob as given in (20).

Proof: This proof takes into account some facts about quantum capacities of the channel $\mathcal{E}$. Let $C(\mathcal{E})$ denote the ordinary classical capacity of $\mathcal{E}$ defined by the HSW theorem [8], [9]; $C_S(\mathcal{E})$ be the secrecy capacity of $\mathcal{E}$ [2], [3]; and $C^{(0)}$ be the zero-error capacity of $\mathcal{E}$ [12]. We have that $C_S(\mathcal{E}) \leq C_(\mathcal{E})$ as well as $C^{(0)}(\mathcal{E}) \leq C_(\mathcal{E})$.

Considering $n = \dim(\tilde{\mathcal{H}})$, a code with parameters $(n, |\mathcal{U}|, 0, 0)$ is simultaneously error-free and also wiretap. By definition, it is known that the zero-error capacity is related to the maximum quantity of messages that are distinguishable at the channel's end. Since every word of the alphabet $\mathcal{U}$ was associated to a state of a DFS, according to Lemma 1, we have that

$$C^{(0)}(\mathcal{E}) = \sup_{\tilde{\mathcal{H}}} \sup_n \frac{1}{n} \log \left|\dim \tilde{\mathcal{H}}\right|^n \quad (34)$$

where n is the code length.

Regarding the wiretap part, we have that $C_S(\mathcal{E}) = \chi^{\text{Bob}} - \chi^{\text{Eva}}$. As a consequence of Lemma 2 we have

$$C_S^{(0)}(\mathcal{E}) \geq \max_{\{P\}} \left[\chi^{\text{Bob}} - \chi^{\text{Eva}}\right] \quad (35)$$

$$\geq \max_{\{P\}} \left[\chi^{\text{Bob}} - 0\right] \quad (36)$$

$$= \max_{\{P\}} \chi^{\text{Bob}} \quad (37)$$

where the maximum is taken over all probability distributions P over $\mathcal{U}$ in Bob's Holevo quantity. The equality comes from the HSW theorem.

There are, however, two situations to consider:

1) There is an optimum pair $(\mathcal{S}', \mathcal{M}')$ derived from $(\mathcal{S}, \mathcal{M})$ according to Eqs. (25) and (26). Thus, $n = |\mathcal{S}'|$ and $C_S^{(0)}(\mathcal{E}) = C_S(\mathcal{E}) = C^{(0)}(\mathcal{E})$;
2) There is a DFS $\tilde{\mathcal{H}}$ in the channel which is not directly obtained from the error-free code. In this situation, $C_S(\mathcal{E}) < C^{(0)}(\mathcal{E})$, i.e., there is error and leakage free communication only if $C_S^{(0)}(\mathcal{E}) = \min\left\{C^{(0)}, C_S(\mathcal{E})\right\}$.

This way, the final expression for the quantum zero-error secrecy capacity of a quantum channel $\mathcal{E}$ can be written by means of its zero-error and secrecy capacities, i.e.

$$C_S^{(0)}(\mathcal{E}) = \min\left\{C^{(0)}(\mathcal{E}), C_S(\mathcal{E})\right\} \quad (38)$$

where $C^{(0)}(\mathcal{E})$ and $C_S(\mathcal{E})$ are the zero-error and secrecy capacities, respectively. It concludes the proof. ∎

When $C_S^{(0)} = \sup_{\tilde{\mathcal{H}}} \sup_n \frac{1}{n} \log \left|\dim \tilde{\mathcal{H}}\right|^n$, the QZESC has single-letter characterization what is in sharp contrast with the ordinary quantum secrecy capacity which has not [2], [3]. Besides, according to a result provided by Medeiros et al. [18], the zero-error capacity can be reached when pure states are used in the input. It is also true for the definition made in this work regarding $\mathcal{S}'$, what implies that the QZESC can also be reached using pure states in certain situations.

Regarding the security, the results shown in this section are in accordance with Schumacher and Westmoreland [19].

According to them, the ability of a quantum channel to send private information is at least as great as its ability to send coherent information. In our case, since the information sent can be retrieved completely free of errors, then the ability to send private information is maximized.

A. Relation with Graph Theory

Let $\tilde{\mathcal{H}}$ be a DFS existing in the channel $\mathcal{E}$ obtained as described in the previous section. The graph $\mathcal{G}_{(')} = \langle V, E \rangle$ for $\mathcal{E}$ is characterized as follows:

- The set of vertices V is composed by the elements in $\tilde{\mathcal{H}}$ which will be referred by their corresponding index , i.e., $V = \{1, 2, \ldots, k\}$;
- The set of edges E connects two vertices if they are distinguishable at the channel's end. Since the elements of a DFS characterize an error-free code, the states in $\tilde{\mathcal{H}}$ taken pairwise are distinguishable (from the proof of the Theorem 6). This way, the resulting graph is *complete*.

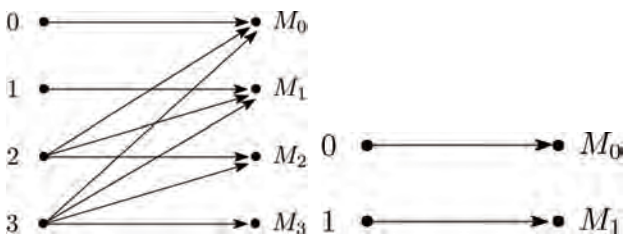
The n-product of $\mathcal{G}_{(')}$, denoted by $\mathcal{G}^n_{(')}$, has $V = V^n$ and the set of edges E is composed of pairs of such indexes whose corresponding sequences are non-adjacent in $\mathcal{E}$. The maximum number of messages that can be transmitted without error with $\mathcal{G}^n_{(')}$ is the clique number of $\mathcal{G}^n$, which is denoted by $\omega(\mathcal{G}^n)$

$$C_S^{(0)} = \sup_{\tilde{\mathcal{H}}} \sup_n \frac{1}{n} \log \omega(\mathcal{G}^n) \tag{39}$$

Given an integer and a graph, finding a clique of the size of the given integer is a $\mathcal{NP}$-Complete problem. However, some characteristics of the zero-error and of the DFS can be taken into account in the determination of $C_S^{(0)}$. Since the graphs produced from $\tilde{\mathcal{H}}$ are complete, the clique number of $\mathcal{G}^n_{(')}$ turns out to be equal to $\left|\dim(\tilde{\mathcal{H}})\right|^n$. Such relation between the clique number and the cardinality of the vertices set in the corresponding graph is not observed in ordinary error-free codes. This is a particularity due to the use of DFS.

B. Examples

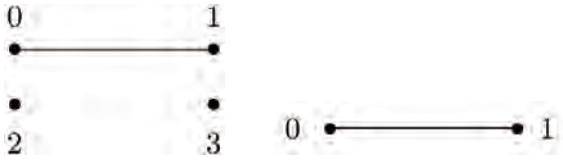
This section presents some detailed examples regarding the concepts of the ZESC. Initially let's suppose that a quantum channel $\mathcal{E}_1$ has the positive zero-error capacity achieved by an optimum pair $(\mathcal{S}_1, \mathcal{M}_1)$ as shown in Figure 2a. By following the procedures described in Section IV-B, a pair $(\mathcal{S}_1^{'}, \mathcal{M}_1^{'})$ can be derived which is shown in Figure 2b.



(a) $(\mathcal{S}_1, \mathcal{M}_1)$ (b) $(\mathcal{S}_1^{'}, \mathcal{M}_1^{'})$

Fig. 2: Representation of the channel $\mathcal{E}_1$ transitions to the input states of the optimum pairs $(\mathcal{S}_1, \mathcal{M}_1)$ and $(\mathcal{S}_1^{'}, \mathcal{M}_1^{'})$.

The characteristic graphs of $(\mathcal{S}_1, \mathcal{M}_1)$ and $(\mathcal{S}_1^{'}, \mathcal{M}_1^{'})$ are illustrated in Figures 3a and 3b, respectively.



(a) $(\mathcal{S}_1, \mathcal{M}_1)$ (b) $(\mathcal{S}_1^{'}, \mathcal{M}_1^{'})$

Fig. 3: Characteristic graphs for $(\mathcal{S}_1, \mathcal{M}_1)$ and $(\mathcal{S}_1^{'}, \mathcal{M}_1^{'})$.

According to these characteristic graphs, the maximum clique number is 2, in both cases obtained by the pairs $(0, 1)$. It leads to a zero-error secrecy capacity equal to (for $n = 1$ because the states are pure):

$$\begin{aligned} C_S^{(0)}(\mathcal{E}_1) &= \sup_{\mathcal{S}'} \sup_n \frac{1}{n} \log \left|\mathcal{S}_1^{'}\right|^n && (40) \\ &= \frac{1}{1} \log 2 && (41) \\ &= 1 \text{ bits per channel use.} && (42) \end{aligned}$$

To verify this result according to the expression of secrecy capacity, we used Mathematica® in the attempt to obtain the maximum of χ^{Bob} in Eqs. (43)-(44).

$$\begin{aligned} C_S^{(0)}(\mathcal{E}_1) &= \chi^{\text{Bob}} && (43) \\ &= \max_{\{P\}} S\left(p_0 \cdot \rho_0 + p_1 \cdot \rho_1\right) && (44) \end{aligned}$$

We simulated 30000 pairs of (p_0, p_1) taking into account the restriction that $p_0 + p_1 = 1$. As a result, we obtained the graphic of Figure 4. As it can be seen, the maximum value of Bob's Holevo quantity is also equal to 1. It means that for the channel $\mathcal{E}_1$, we have that $C_S^{(0)}(\mathcal{E}_1) = 1$ bit per channel use.

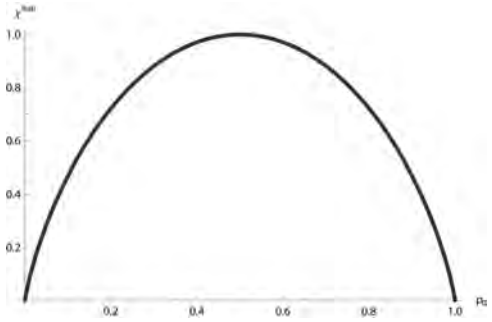
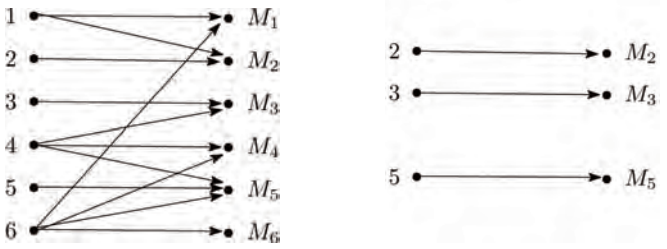


Fig. 4: Simulation performed in the attempt to maximize the value of χ^{Bob} in Eqs. (43)-(44) over the pairs (p_0, p_1).

In this second example, let's suppose that a quantum channel $\mathcal{E}_2$ has positive zero-error capacity achieved by an optimum pair $(\mathcal{S}_2, \mathcal{M}_2)$ where $\mathcal{S}_2 = \{\rho_1, \ldots, \rho_6\}$ and $\mathcal{M}_2 = \{M_i = |\rho_i\rangle \langle\rho_i|\}_{i=1}^6$. The model of errors of the channel for the input set is illustrated in Figure 5a. Since we are interested in adjacency relations, we omitted the transition probabilities.

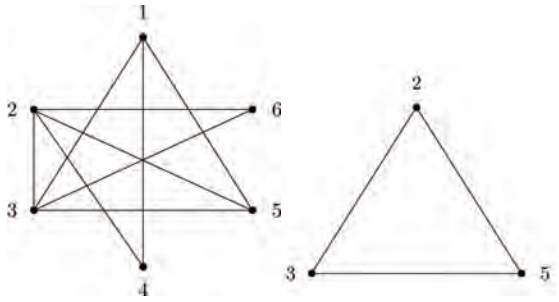
From the pair $(\mathcal{S}_2, \mathcal{M}_2)$ by following the procedures described in Section IV-B, it is possible to derive an optimum pair $(\mathcal{S}_2^{'}, \mathcal{M}_2^{'})$ where $\mathcal{S}_2^{'} = \{\rho_2, \rho_3, \rho_5\}$ and $\mathcal{M}_2^{'} = \{M_2, M_3, M_5\}$. The relation between the input states in $\mathcal{S}_2^{'}$ and the output at the channel $\mathcal{E}_2$ is illustrated in Figure 5b.



(a) $(\mathcal{S}_2, \mathcal{M}_2)$ (b) $(\mathcal{S}_2^{'}, \mathcal{M}_2^{'})$

Fig. 5: Representation of the channel $\mathcal{E}_2$ transitions to the input states of the optimum pairs $(\mathcal{S}_2, \mathcal{M}_2)$ and $(\mathcal{S}_2^{'}, \mathcal{M}_2^{'})$.

The characteristic graphs of $(\mathcal{S}_2, \mathcal{M}_2)$ and $(\mathcal{S}_2^{'}, \mathcal{M}_2^{'})$ are illustrated in Figures 6a and 6b, respectively. Notice that the clique number $\omega(\mathcal{G})$ of $(\mathcal{S}_2, \mathcal{M}_2)$ is equal to 3 and can be obtained through the vertices $(2, 3, 5)$, $(1, 3, 5)$, or also $(2, 3, 6)$. In other hand, the clique number of $\omega(\mathcal{G}_{(')})$ of $(\mathcal{S}_2^{'}, \mathcal{M}_2^{'})$ is also equal to 3, but can be easily obtained from the vertices $(2, 3, 5)$.



(a) $(\mathcal{S}_2, \mathcal{M}_2)$ (b) $(\mathcal{S}_2^{'}, \mathcal{M}_2^{'})$

Fig. 6: Characteristic graphs for $(\mathcal{S}_2, \mathcal{M}_2)$ and $(\mathcal{S}_2^{'}, \mathcal{M}_2^{'})$.

Regarding the zero-error secrecy capacity of the optimum pair $(\mathcal{S}_2^{'}, \mathcal{M}_2^{'})$ for $n = 1$, according to (32), it is equal to

$$C_S^{(0)}(\mathcal{E}_2) = \sup_{\mathcal{S}'} \sup_n \frac{1}{n} \log \left|\mathcal{S}_2^{'}\right|^n \quad (45)$$

$$= \frac{1}{1} \log 3 \quad (46)$$

$$\approx 1.58496 \text{ bits per channel use} \quad (47)$$

To show the equivalence between this expression of ZESC in terms of graphs and the secrecy capacity form, we set up a simulation to obtain the Holevo quantity of Bob. In this particular example, we know that the states ρ_2, ρ_3, and ρ_5 are pure, what will leave us with the following expression to the Holevo quantity of Bob.

$$\chi^{\text{Bob}} = \max_{\{P\}} S\left(p_1 \cdot \rho_2 + p_2 \cdot \rho_3 + p_3 \cdot \rho_5\right) \quad (48)$$

since $S(\rho_2) = S(\rho_3) = S(\rho_5) = 0$ because they are pure states. The constrain that $p_1 + p_2 + p_3 = 1$ must also be taken into account. A simulation was carried out using Mathematica® trying to maximize the value of (48) among $20,000$ valid triples of (p_1, p_2, p_3). The results obtained are plotted in the graphic of Figure 7 in which two different perspectives are shown. According to the results observed, the highest value of χ^{Bob} obtained was 1.58491 bits per channel use, what can be considered a coincidence with the theoretical results using the graph-theoretical approach shown in (47).

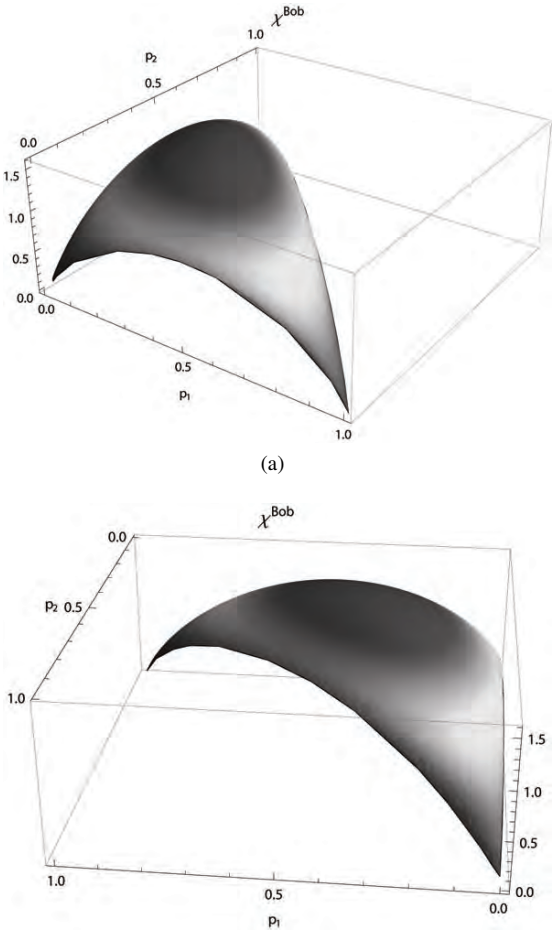
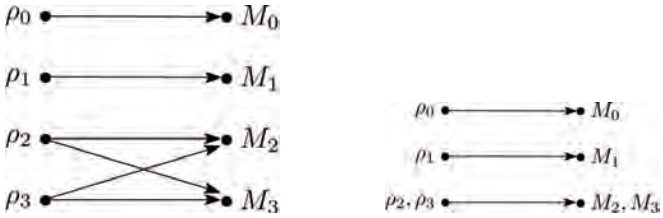


Fig. 7: Two different perspectives from the graphic obtained from the simulation of triples (p_1, p_2, p_3) in the attempt maximize (48)

A third-example is simple yet non-trivial. In this case, we have $\mathcal{S}_3 = \{\rho_i = |i\rangle\langle i|, i = 0, \ldots, 3\}$. The model of errors is known, composed by the four following operator elements: $E_0 = |0\rangle\langle 0|$, $E_1 = |1\rangle\langle 1|$, $E_2 = \frac{1}{2}|2\rangle\langle 2| + \frac{1}{2}|3\rangle\langle 2|$, and $E_3 = \frac{1}{2}|3\rangle\langle 3| + \frac{1}{2}|2\rangle\langle 3|$. The channel $\mathcal{E}_3 \equiv \{E_i\}_{i=0}^{3}$ is illustrated in Figure 8a.



(a) $(\mathcal{S}_3, \mathcal{M}_3)$ (b) $(\mathcal{S}_3^{'}, \mathcal{M}_3^{'})$

Fig. 8: Representation of the channel $\mathcal{E}_3$ transitions to the input states of the optimum pairs $(\mathcal{S}_3, \mathcal{M}_3)$ and $(\mathcal{S}_3^{'}, \mathcal{M}_3^{'})$.

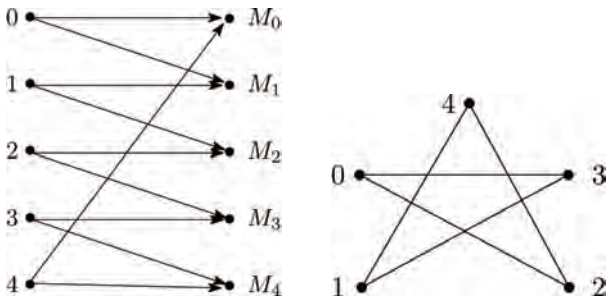
When considering this channel, one might think that there are only 2 states belonging to a DFS (ρ_0 and ρ_1). However, this is not the case. One might apply the procedures presented in Section IV-B and find out three projectors $P_0 = |0\rangle\langle 0|$, $P_1 = |1\rangle\langle 1|$, and $P_{2,3} = |2\rangle\langle 2| + |3\rangle\langle 3|$ satisfying (25) and (26) in such a way that the subsystems $P_0\mathcal{H}$, $P_1\mathcal{H}$ and $P_{2,3}\mathcal{H}$ are a DFS. The channel resulting is illustrated in Figure 8b.

The characteristics graphs related to $(\mathcal{S}_3, \mathcal{M}_3)$ and to $(\mathcal{S}_3^{'}, \mathcal{M}_3^{'})$ are illustrated in Figure 9. It is possible to see that the zero-error secrecy capacity of $(\mathcal{S}_3^{'}, \mathcal{M}_3^{'})$ is equal to the zero-error capacity $(\mathcal{S}_3, \mathcal{M}_3)$ which is, for $n = 1$, equal to $C_S^{(0)}(\mathcal{E}_3) = \log 3$ bits per symbol per channel use.

(a) $(\mathcal{S}_3, \mathcal{M}_3)$ (b) $(\mathcal{S}_3^{'}, \mathcal{M}_3^{'})$

Fig. 9: Characteristic graphs for $(\mathcal{S}_3, \mathcal{M}_3)$ and $(\mathcal{S}_3^{'}, \mathcal{M}_3^{'})$.

Despite the previous examples in which ZESC is $C_S^{(0)}(\mathcal{E}) = C_S(\mathcal{E}) = C^{(0)}(\mathcal{E})$, there are other situations to consider. The graph in Figure 10a shows a channel $\mathcal{E}_4$ which characteristic graph is shown in Figure 10b. The ZESC of this channel is $C_S^{(0)}(\mathcal{E}_4) = \min\left\{C^{(0)}(\mathcal{E}_4), C_S(\mathcal{E}_4), \right\} = \left\{\frac{1}{2}\log 5, \frac{1}{1}\log 2\right\} = 1$ bit per symbol per channel use.



(a) Channel $\mathcal{E}_4$ (b) Characteristic graph for $\mathcal{E}_4$

Fig. 10: Non-trivial example of ZESC.

VI. Related Work

Until the work of Guedes and de Assis [6], [7], many works exploring the use of DFS in communications did not consider its ability to send messages with unconditional security. All of the works investigated [20]–[22] consist of protocols for quantum secure direct communication and deterministic secure quantum communications where redundancy and eavesdropping check are performed, increasing significantly the number of messages exchanges essentially necessary to carry out the communication with security.

So far, very few contributions to the characterization of wiretap codes have been found in the literature. The code proposed by Hamada [23], [24] is based on the Calderbank-Shor-Steane codes that are suitable for practical implementation, since they do not demand the use of entanglement. However, the rate achieved by such codes is below the secrecy capacity of the quantum channel in use. The work of Wilde and Guha [25] also presents a proposition of quantum wiretap codes, based on polar codes. Despite that, as argued by the own authors, the code proposed may be restricted to some types of quantum channels. Regarding the proposition of wiretap codes from DFS and error-free quantum codes as proposed by our work, no similar strategy was found in the literature.

Braunstein et al. [26] show the relation between DFS and zero-error subspaces, showing that the former is an instance of the latter. Besides that clarifying this relation, they also propose a method for searching DFS within zero-error subspaces. This method seems to have some similarities with the one proposed by Medeiros et al. [10]. We opted to use the latter method because it is guaranteed optimum and also because provides a more intuitive approach to find DFS given a quantum error-free code. It is a key component in the characterization of the codes proposed by us.

Regarding the capacity, Watanabe [27] characterizes a class of *more capable quantum channels* in which the private and quantum capacities are equal. However, he argues that the conditions such that a certain channel belongs to this class are hard to verify in general. The channel considered in our work is more capable in this sense since such equality can be verified, as shown in Section V.

VII. Final Remarks

In this paper, we presented the *quantum zero-error secrecy capacity*, the maximum rate in which one can send information through a wiretapped quantum channel without decoding error not information leakage out to the wiretapper. This capacity can be achieved with decoherence-free subspaces and subsystems that may rely in the inner structure of some error-free quantum codes.

The use of the codes defined in this paper provides unconditional security in the classical information conveying through quantum channels with an additional advantage that are no decoding errors. It is possible since the wiretapper has access only to the environment to which no accessible information about the secret message is leaked out. The maximum rate in which information can be conveyed can reach the HSW capacity of the quantum channel. A formulation in terms of

graphs appropriated from the zero-error quantum codes was also presented.

To illustrate the concepts regarding ZESC, detailed examples were shown in Section V-B. In all examples it was shown how to obtain a QEAC from an error-free quantum code, and latter how to determine the ZESC for such case. In some cases, simulations were necessary to determine the Holevo quantity.

This paper contributes in the understanding of the relation between noise and decoherence in quantum channels and their impacts in information leakage out to an wiretapper. In first instance, secrecy was reached by avoiding decoherence with the use of DFS in the work of Guedes and de Assis [6], [7]. However, with the recent results of Braunstein et al. [26] pointing out that DFS are instances of zero-error subspaces, fight decoherence also implied also in fight decoding errors. Thus, this work unifies both ideas creating secure codes based on DFS and on error-free quantum codes. This contributes to the characterization of an unconditional secure way to exchange messages without the use of classical channels nor private keys neither previous communications.

Due to the technical difficulties to build completely closed quantum system [4], the results shown here can be applied to build devices that perform unconditional secure message exchange even in the presence of noise and decoherence. It is very promising in practical applications especially considering already existing results regarding the use of DFS in communications [28]–[30], particularly in long-distance [31]. The same is true for the zero-error scenario in practical applications using optical quantum channels as reported recently by Gyongyosi and Imre [32].

In future work, we suggest the investigation of more general conditions to the existence of perfect secrecy in quantum systems.

REFERENCES

[1] C. H. Bennett and P. W. Shor, "Quantum information theory," *IEEE Trans. Info. Theory*, vol. 44, no. 6, pp. 2724–2755, 1998.

[2] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Problems of Information Transmission*, vol. 40, pp. 318–336, 2004.

[3] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Th.*, vol. 51, no. 1, pp. 44 –55, 2005.

[4] M. S. Byrd, L.-A. Wu, and D. A. Lidar, "Overview of quantum error prevention and leakage elimination," *Journal of Modern Optics*, vol. 51, no. 16-18, pp. 2449–2460, 2004.

[5] D. A. Lidar and K. B. Whaley, "Decoherence-free subspaces and subsystems," arXiv:quant-ph/0301032v1, pp. 83–120, 2003.

[6] E. B. Guedes and F. M. de Assis, "Unconditional security with decoherence-free subspaces," arXiv:quant-ph/1204.3000, pp. 1–6, 2012.

[7] ——, "Utilização de subespaços livres de descoerência em comunicações quânticas incondicionalmente seguras," in *XXX Simpósio Brasileiro de Telecomunicações – SBrT'12*, 2012.

[8] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Info. Theory*, vol. 4, no. 1, pp. 269–273, 1998.

[9] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A*, vol. 56, pp. 131–138, 1997.

[10] R. A. C. Medeiros, R. Alléaume, G. Cohen, and F. M. de Assis, "Zero-error capacity of quantum channels and noiseless subsystems," in *IEEE International Telecommunications Symposium*, 2006, pp. 900–905.

[11] M.-D. Choi and D. W. Kribs, "A method to find quantum noiseless subsystems," *Phys. Rev. Lett.*, vol. 96, p. 050501, 2006.

[12] R. A. C. Medeiros and F. M. de Assis, "Quantum zero-error capacity," *International Journal of Quantum Information*, vol. 3, no. 1, pp. 135–139, 2005.

[13] A. Shabani and D. A. Lidar, "Theory of initialization-free decoherence-free subspaces and subsystems," *Phys. Rev. A*, vol. 72, p. 042303, 2005.

[14] E. Knill, R. Laflamme, and L. Viola, "Theory of quantum error correction for general noise," *Phys. Rev. Lett.*, vol. 84, p. 2525, 2000.

[15] D. M. Bacon, "Decoherence, control, and symmetry in quantum computers," Ph.D. dissertation, University of California at Berkeley, 2001.

[16] C. E. Shannon, "The zero error capacity of a noisy channel," *IRE Transactions on Information Theory*, vol. 2, no. 3, pp. 8–19, 1956.

[17] R. A. C. Medeiros, "Zero-error capacity of quantum channels," Ph.D. dissertation, Universidade Federal de Campina Grande – TELECOM Paris Tech, 2008.

[18] R. Medeiros, R. Alleaume, G. Cohen, and F. M. de Assis, "Quantum states characterization for the zero-error capacity," arxiv:quant-ph/0611042, 2006.

[19] B. Schumacher and M. Westmoreland, "Quantum privacy and quantum coherence," *Physical Review Letters*, vol. 80, no. 25, pp. 5695–5697, 1998.

[20] G. Bin, P. ShiXin, S. Biao, and Z. Kun, "Deterministic secure quantum communication over a collective-noise channel," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 52, no. 12, pp. 1913–1918, 2009.

[21] S. Qin, Q. Wen, L. Meng, and F. Zhu, "Quantum secure direct communication over the collective amplitude damping channel," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 52, no. 8, pp. 1208–1212, 2009.

[22] H.-K. Dong, L. Dong, X.-M. Xiu, and Y.-J. Gao, "A deterministic secure quantum communication protocol through a collective rotation noise channel," *Int. J. of Quantum Inf.*, vol. 8, no. 8, pp. 1389–1395, 2010.

[23] M. Hamada, "Algebraic and quantum theoretical approach to coding on wiretap channels," in *ISCCP*, 2008.

[24] ——, "Constructive codes for classical and quantum wiretap channels," In Cryptography and Research Perspectives, Nova Science Publishers Inc., 2008, chapter 1, pgs. 1-48.

[25] M. M. Wilde and S. Guha, "Polar codes for degradable quantum channels," arxiv/quantum-ph:1109.5346, 2011.

[26] S. L. Braunstein, D. W. Kribs, and M. K. Patra, "Zero-error subspaces of quantum channels," in *IEEE International Symposyum on Information Theory*, 2011, pp. 104–108.

[27] S. Watanabe, "Private and quantum capacities of more capable and less noisy quantum channels," *Phys. Rev. A*, vol. 85, p. 012326, 2012.

[28] U. Dorner, A. Klein, and D. Jaksch, "A quantum repeater based on decoherence free subspaces," *Quant. Inf. Comp.*, vol. 8, p. 468, 2008.

[29] G. Jaeger and A. Sergienko, "Constructing four-photon states for quantum communication and information processing," *Int. J. Theor. Phys.*, vol. 47, p. 2120, 2008.

[30] Y. Xia, J. Song, Z.-B. Yang, and S.-B. Zheng, "Generation of four-photon polarization-entangled decoherence-free states within a network," *Appl. Phys. B*, vol. 99, pp. 651–656, 2010.

[31] P. Xue, "Long-distance quantum communication in a decoherence-free subspace," *Phys. Lett. A*, vol. 372, pp. 6859–6866, 2008.

[32] L. Gyongyosi and S. Imre, "Long-distance quantum communications with superactivated gaussian optical quantum channels," *Optical Engineering*, vol. 51, no. 1, 2012.