A Survey on Quantum Channel Capacities

Laszlo Gyongyosi,[1,2,3,*] *Member, IEEE*, Sandor Imre,[2] *Senior Member, IEEE*, and Hung Viet Nguyen,[1] *Member, IEEE*

[1]School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, UK
[2]Department of Networked Systems and Services, Budapest University of Technology and Economics, Budapest, H-1117 Hungary
[3]MTA-BME Information Systems Research Group, Hungarian Academy of Sciences, Budapest, H-1051 Hungary

***Abstract*—Quantum information processing exploits the quantum nature of information. It offers fundamentally new solutions in the field of computer science and extends the possibilities to a level that cannot be imagined in classical communication systems. For quantum communication channels, many new capacity definitions were developed in comparison to classical counterparts. A quantum channel can be used to realize classical information transmission or to deliver quantum information, such as quantum entanglement. Here we review the properties of the quantum communication channel, the various capacity measures and the fundamental differences between the classical and quantum channels.**

***Index Terms*—Quantum communication, quantum channels, quantum information, quantum entanglement, quantum Shannon theory.**

I. Introduction

According to Moore's Law [326], the physical limitations of classical semiconductor-based technologies could be reached within the next few years. We will then step into the age of quantum information. When first quantum computers become available on the shelf, today's encrypted information will not remain secure. Classical computational complexity will no longer guard this information. Quantum communication systems exploit the quantum nature of information offering new possibilities and limitations for engineers when designing protocols. Quantum communication systems face two major challenges.

First, available point-to-point communication link should be connected on one hand to cover large distances an on the other hand to reach huge number of users in the form of a network. Thus, the quantum Internet [267], [304] requires quantum repeaters and quantum switches/routers. Because of the so called *no-cloning theorem* [551], which is the simple consequence of the postulates of the quantum mechanics, the construction of these network entities proves to be very hard [523].

The other challenge – this paper focuses on – is the amount of information which can be transmitted over quantum channels, i.e. the capacity. The capacity of a communication channel describes the capability of the channel for delivering information from the sender to the receiver, in a faithful and recoverable way. Thanks to Shannon we can calculate the capacity of classical channels within the frames of classical information theory[1] [477]. However, the different capacities of quantum channels have been discovered just in the '90s, and there are still many open questions about the different capacity measures.

Many new capacity definitions exist for quantum channels in comparison to a classical communication channel. In the case of a classical channel, we can send only classical information while quantum channels extend the possibilities, and besides the classical information we can deliver entanglement-assisted classical information, private classical information, and of course, quantum information [54], [136]. On the other hand, the elements of classical information theory cannot be applied in general for quantum information –in other words, they can be used only in some special cases. There is no general formula to describe the capacity of every quantum channel model, but one of the main results of the recent researches was a simplified picture in which various capacities of a quantum channel (i.e., the classical, private, quantum) are all non-additive [245].

In possession of admitted capacity definitions they have to be calculated for various channel models. Channels behave in very different ways in free-space or in optical fibers and these two main categories divides into many subclasses and special cases [178], [181], [567].

Since capacity shows only the theoretically achievable transmission rate and gives no construction rules how to reach or near them, therefore quantum channel/error correction coding has similar importance from practical implementation point of view as in case of classical information theory [171].

This paper is organized as follows. In Section II, preliminaries are summarized. In Section III, we study the classical information transmission capability of quantum channels. In Section IV, we discuss the quantum capacity. Numerical examples are included in Section V. Section VI focuses on the practical implementations of quantum channels. Finally, Section VII concludes the paper. Supplementary material is included in the Appendix.

This work was partially supported by the European Research Council through the Advanced Fellow Grant, in part by the Royal Societys Wolfson Research Merit Award, in part by the Engineering and Physical Sciences Research Council under Grant EP/L018659/1, by the Hungarian Scientific Research Fund - OTKA K-112125, and by the National Research Development and Innovation Office of Hungary (Project No. 2017-1.2.1-NKP-2017-00001).

*Email: l.gyongyosi@soton.ac.uk

[1]Quantum Shannon theory has deep relevance concerning the information transmission and storage in quantum systems. It can be regarded as a natural generalization of classical Shannon theory. Classical information theory represents an orthogonality-restricted case of quantum information theory.

II. Preliminaries

A. Applications and Gains of Quantum Communications

Before discussing the modeling, characteristics and capacities of quantum channels we present their potential to improve state-of the-art communication and computing systems.

We highlight the fact that from application point of view the concept of channel can represent any medium possessing an input to receive information and an output to give back a modified version of this information. This simplified definition highlights the fact that not only an optical fiber, a copper cable or a free-space link can be regarded as channel but a computer memory, too.

Quantum communication systems are capable of providing absolute randomness, absolute security, of improving transmission quality as well as of bearing much more information in comparison to the current classical binary based systems. Moreover, when the benefits of quantum computing power are properly employed, the quantum based solutions are capable of supporting the execution of tasks much faster or beyond the capability of the current binary based systems [131]. The appealing gains and the associated application scenarios that we may expect from quantum communications are as follows.

The general existence of a qubit ψ in a superposition state (see the next sub-sections of Section II) of two pure quantum states $|0\rangle$ and $|1\rangle$ can be represented by

$$|\psi\rangle \quad = \quad \alpha|0\rangle + \beta|1\rangle, \tag{1}$$

where α and β are complex number. If a qubit ψ is measured by $|0\rangle$ and $|1\rangle$ bases, the measurement result is randomly obtained in the state of $|0\rangle$ or $|1\rangle$ with the corresponding probability of $|\alpha|^2$ or $|\beta|^2$. This random nature of quantum measure have been favourably used for providing high quality random number generator [249, 265], [316]. It is important to note that along with the measurement randomness, no-cloning theorem [551] of qubit says that it is not possible to clone a qubit. This characteristics allow quantum based solutions to support absolute security, to which there have been abundant examples of quantum based solutions [176], [300], [302], [569], [553] where a popular example of mature applications is quantum key distribution (QKD) [53], [68].

Quantum entanglement is a unique characteristic of quantum mechanics, which is another valuable foundation for provisioning the absolute secure communication. Let us consider a two qubit system σ represented by

$$|\sigma\rangle \quad = \quad \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle, \tag{2}$$

where $\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11}$ are complex numbers having $|\alpha_{00}|^2+|\alpha_{01}|^2+|\alpha_{10}|+|\alpha_{11}|^2= 1$. If the system σ is prepared in one of the four states (see Appendix), for example

$$|\sigma\rangle \quad = \quad \alpha_{00}|0\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle, \tag{3}$$

where $|\alpha_{00}|^2+|\alpha_{11}|^2= 1$, the measurement result of the two qubits is in either $|00\rangle$ or $|11\rangle$ state. In this state, the two qubits are entangled, meaning that having the measurement result of either of the two is sufficient to know the measurement result of the other. As a result, if the two entangled qubits are separated in the distance, for example 144 km terrestial distance [158] or earth-station to satellite 1200 km distance [561], information can be secretly transmitted over two locations, where there exists entanglement between the two locations. The entanglement based transmission can be employed for transmitting classical bits by using the superdense coding protocol [1], [33], [242] or for transmitting qubits using the quantum teleportation protocol [55], [226].

Classical channels handle classical information i.e. orthogonal (distinguishable) basis states while quantum channels may deliver superposition states (linear combination of basis states). Of course, since quantum mechanic is more complete than classical information theory classical information and classical channels can be regarded as special cases of quantum information and channels. Keeping in mind the application scenarios, there is a major difference between classical and quantum information. Human beings due to their limited senses can perceive only classical information; therefore measurement is needed to perform conversion between the quantum and classical world.

From the above considerations, quantum channels can be applied in several different ways for information transmission. If classical information is encoded to quantum states, the quantum channel delivers this information between its input and output and finally a measurement device converts the information back to the classical world. In many practical settings, quantum channels are used to transfer classical information only.

The most discussed practical application of this approach is QKD. Optical fiber based [243], [255], [282], [511] ground-ground [565] and ground-space [301] systems have already been demonstrated. These protocols independently whether they are first-generation single photon systems or second-generation multi photon solutions exchange classical sequences between Alice and Bob over the quantum channel being encoded in non-orthogonal quantum states. Since the no-cloning theorem [244], [551] makes no possible to copy (to eavesdrop) the quantum states without error, symmetric ciphering keys can be established for both parties. In this case quantum channel is used to create a new quality instead of improving the performance of classical communication.

Furthermore, quantum encoding can improve the transmission rates of certain channels. For example the well-known bit-flip channel inverts the incoming bit value by probability p and leaves it unchanged by $(1-p)$. Classically this type of channel can not transmit any information at all if $p = 0.5$ even if we apply redundancy for error correction. However, if classical bits are encoded into appropriate quantum bits one-by-one, i.e., no redundancy is used, the information will be delivered without error. This means that quantum communication improves the classical information transmission capability of the bit-flip channel form 0 to the maximum 1. The different models of classical information transmission over a quantum channel will be detailed in Section III (particulary in Section III-C-Section III-G).

The second approach applies quantum channels to deliver quantum information and this information is used to improve the performance of classical communication systems. The

detailed discussion of the transmission of quantum information is the subject of Section IV. These protocols exploit over-quantum-channel-shared entangled states, i.e. entanglement assisted communications is considered. In case of quantum superdense coding [58], [70], [244] we assume that Alice and Bob have already shared an entangled Bell-pair, such as $|\beta_{00}\rangle$ (see Appendix), expressed as

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle \right). \tag{4}$$

When Alice wants to communicate with Bob, she encodes two classical bits into the half pair she possesses and sends this quantum bit to Bob over the quantum channel. Finally, Bob leads his own qubit together the received one to a measuring device which decodes the original two classical bits. Practically 2 classical bits have been transferred at the expense of 1 quantum bit, i.e., the entanglement assisted quantum channels can outperform classical ones.

Another practical example of this approach is distributed medium access control. In this case a classical communication channel is supported by pre-shared entanglement. It is well-known that WiFi and other systems can be derived from the Slotted Aloha protocol [2] widely used as a reference. Slotted Aloha can deliver $[0.5/e, 1/e]$ packets in average in each timeslot if the number of nodes is known for everyone, and optimal access strategy is used by everyone. This is because of collisions and unused timeslots. Practically the size of the population can be only estimated which decreases the efficiency. However, if special entangled $|w_n\rangle$ states are generated as

$$|w_n\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |2^{(n-i)}\rangle. \tag{5}$$

and used to coordinate the channel access in a distributed way the timeslot usage will improve to 100% and there is no need to know the number of users.

Further important application scenarios are related to quantum computers where quantum information has to be delivered between modules over quantum connections. Similarly quantum memories are practically quantum channels of course with different characteristics compared to communication channels which store and read back quantum information.

B. Privacy and Performance Gains of Quantum Channels

Due to the inherent no-cloning theory of quantum mechanics, the random nature of quantum measurement as well as to the unique entanglement phenomenon of quantum mechanics, secure communications can be guaranteed by quantum communications. The private classical capacity of a quantum channel is detailed in Section III-C.

Moreover, quantum communications using quantum channels is capable of carrying much more information in comparison to the current classical binary based systems. Let us have a closer look at Eq. (1), where obviously one qubit contains superpositioned 2^1 distinct states or values, which is equivalent to at least 2 bits. In the case of using two qubits in Eq. (3), 2^2 distinct states or values are simultaneously conveyed by two qubits, meaning at least $2^2 \times 2$ bits are carried by 2 qubits. Generally, n qubits can carry up to 2^n states, which corresponds to $2^n \times n$ bits. The superposition nature of qubits leads to the advent of powerful quantum computing, which is in some cases proved be 100 millions times faster than the classical computer [131]. Moreover, in theory quantum computer is capable of providing the computing power that is beyond the capability of its classical counterpart. Importantly, in order to realise such supreme computing power, the crucial part is quantum communications, which has to be used for transmitting qubits within the quantum processor as well as between distributed quantum processors.

Additionally, quantum receivers [49] relying on quantum communications principle has proved to outperform classical homodyne or heterodyne receiver in the context of optical communications. For the sake of brevity, please allow us to refer interested readers to the references [49], [516].

C. Communication over a Quantum Channel

Communication through a quantum channel cannot be described by the results of classical information theory; it requires the generalization of classical information theory by quantum perception of the world. In the general model of communication over a quantum channel $\mathcal{N}$, the encoder encodes the message in some coded form, and the receiver decodes it, however in this case, the whole communication is realized through a quantum system.

The information sent through quantum channels is carried by quantum states, hence the encoding is fundamentally different from any classical encoder scheme. The encoding here means the preparation of a quantum system, according to the probability distribution of the classical message being encoded. Similarly, the decoding process is also different: here it means the measurement of the received quantum state. The properties of quantum communication channel, and the fundamental differences between the classical and quantum communication channel cannot be described without the elements of quantum information theory.

The model of the quantum channel represents the physically allowed transformations which can occur on the sent quantum system. The result of the channel transformation is another quantum system, while the quantum states are represented by matrices. The physically allowed channel transformations could be very different; nevertheless they are always *Completely Positive Trace Preserving* (CPTP) transformations (trace: the sum of the elements on the main diagonal of a matrix). The trace preserving property therefore means that the corresponding density matrices (density matrix: mathematical description of a quantum system) at the input and output of the channel have the same trace.

The input of a quantum channel is a quantum state, which encodes information into a physical property. The quantum state is sent through a quantum communication channel, which in practice can be implemented e.g. by an optical-fiber channel, or by a wireless quantum communication channel. To extract any information from the quantum state, it has to be measured at the receiver's side. The outcome of the measurement of the quantum state (which might be perturbed)

depends on the transformation of the quantum channel, since it can be either totally probabilistic or deterministic. In contrast to classical channels, a quantum channel transforms the information coded into quantum states, which can be e.g. the spin state of the particle, the ground and excited state of an atom, or several other physical approaches. The classical capacity of a quantum channel has relevance if the goal is transmit classical information in a quantum state, or would like to send classical information privately via quantum systems (private classical capacity). The quantum capacity has relevance if one would like to transmit quantum information such as superposed quantum states or quantum entanglement.

First, we discuss the process of transmission of information over a quantum channel. Then, the interaction between quantum channel output and environment will be described.

1) The Quantum Channel Map: From algebraic point of view, quantum channels are linear CPTP maps, while from a geometrical viewpoint, the quantum channel $\mathcal{N}$ is an affine transformation. While, from the algebraic view the transformations are defined on density matrices, in the geometrical approach, the qubit transformations are also interpretable via the Bloch sphere (a geometrical representation of the pure state space of a qubit system) as Bloch vectors (vectors in the Bloch sphere representation). Since, density matrices can be expressed in terms of Bloch vectors, hence the map of a quantum channel $\mathcal{N}$ also can be analyzed in the geometrical picture.

To preserve the condition for a density matrix ρ, the noise on the quantum channel $\mathcal{N}$ must be trace-preserving (TP), i.e.,

$$Tr\left(\rho\right)=Tr\left(\mathcal{N}\left(\rho\right)\right), \tag{6}$$

and it must be Completely Positive (CP), i.e., for any identity map I, the map $I\otimes\mathcal{N}$ maps a semi-positive Hermitian matrix to a semi-positive Hermitian matrix.

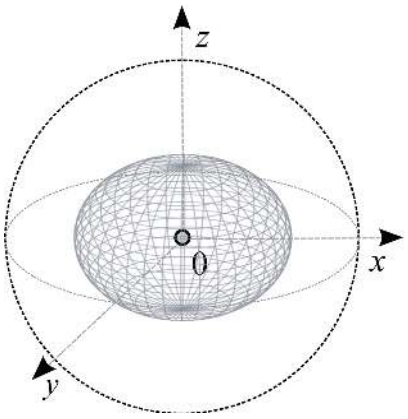

Fig. 1: Geometrical picture of a noisy qubit quantum channel on the Bloch sphere [Imre13].

For a unital quantum channel $\mathcal{N}$, the channel map transforms the I identity transformation to the I identity transformation, while this condition does not hold for a non-unital channel. To express it, for a unital quantum channel, we have

$$\mathcal{N}\left(I\right)=I, \tag{7}$$

while for a non-unital quantum channel,

$$\mathcal{N}\left(I\right)\neq I. \tag{8}$$

Focusing on a qubit channel, the image of the quantum channel's linear transform is an *ellipsoid* on the Bloch sphere, as it is depicted in Fig. 1. For a unital quantum channel, the center of the geometrical interpretation of the channel ellipsoid is equal to the center of the Bloch sphere. This means that a unital quantum channel preserves the average of the system states. On the other hand, for a non-unital quantum channel, the center of the channel ellipsoid will differ from the center of the Bloch sphere. The main difference between unital and non-unital channels is that the non-unital channels do not preserve the average state in the center of the Bloch sphere. It follows from this that the numerical and algebraic analysis of non-unital quantum channels is more complicated than in the case of unital ones. While unital channels shrink the Bloch sphere in different directions with the center preserved, non-unital quantum channels shrink both the original Bloch sphere and move the center from the origin of the Bloch sphere. This fact makes our analysis more complex, however, in many cases, the physical systems cannot be described with unital quantum channel maps. Since the unital channel maps can be expressed as the convex combination of the basic unitary transformations, the unital channel maps can be represented in the Bloch sphere as different rotations with shrinking parameters. On the other hand, for a non-unital quantum map, the map cannot be decomposed into a convex combination of unitary rotations [245].

2) Steps of the Communication: The transmission of information through classical channels and quantum channels differs in many ways. If we would like to describe the process of information transmission through a quantum communication channel, we have to introduce the three main phases of quantum communication. In the first phase, the sender, Alice, has to encode her information to compensate the noise of the channel $\mathcal{N}$ (i.e., for error correction), according to properties of the physical channel - this step is called *channel coding*. After the sender has encoded the information into the appropriate form, it has to be put on the quantum channel, which transforms it according to its channel map - this second phase is called the *channel evolution*. The quantum channel $\mathcal{N}$ conveys the quantum state to the receiver, Bob; however this state is still a superposed and probably *mixed* (according to the noise of the channel) quantum state. To extract the information which is encoded in the state, the receiver has to make a measurement - this *decoding process* (with the error correction procedure) is the third phase of the communication over a quantum channel.

The channel transformation represents the noise of the quantum channel. Physically, the quantum channel is the medium, which moves the particle from the sender to the receiver. The noise disturbs the state of the particle, in the case of a half-spin particle, it causes spin precession. The channel evolution phase is illustrated in Fig. 2.

Finally, the measurement process responsible for the decoding and the extraction of the encoded information. The

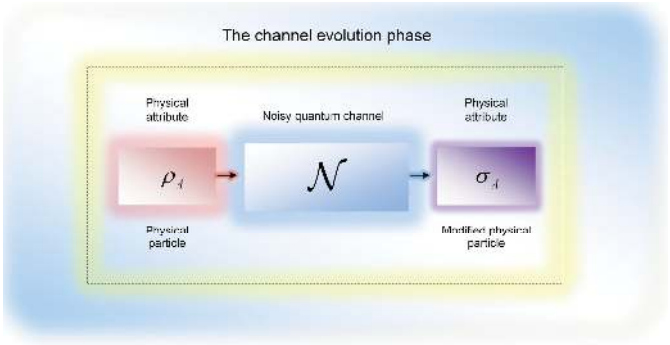

Fig. 2: The channel evolution phase.

previous phase determines the success probability of the recovery of the original information. If the channel $\mathcal{N}$ is completely noisy, then the receiver will get a maximally mixed quantum state. The output of the measurement of a maximally mixed state is completely undeterministic: it tells us nothing about the original information encoded by the sender. On the other hand, if the quantum channel $\mathcal{N}$ is completely noiseless, then the information which was encoded by the sender can be recovered with probability 1: the result of the measurement will be completely deterministic and completely correlated with the original message. In practice, a quantum channel realizes a map which is in between these two extreme cases. A general quantum channel transforms the original pure quantum state into a mixed quantum state, - but not into a maximally mixed state - which makes it possible to recover the original message with a high - or low - probability, depending on the level of the noise of the quantum channel $\mathcal{N}$.

D. Formal Model

As shown in Fig. 3, the information transmission through the quantum channel $\mathcal{N}$ is defined by the ρ_{in} input quantum state and the initial state of the environment $\rho_E = |0\rangle\langle 0|$. In the initial phase, the environment is assumed to be in the pure state $|0\rangle$. The system state which consist of the input quantum state ρ_{in} and the environment $\rho_E = |0\rangle\langle 0|$, is called the *composite state* $\rho_{in} \otimes \rho_E$.

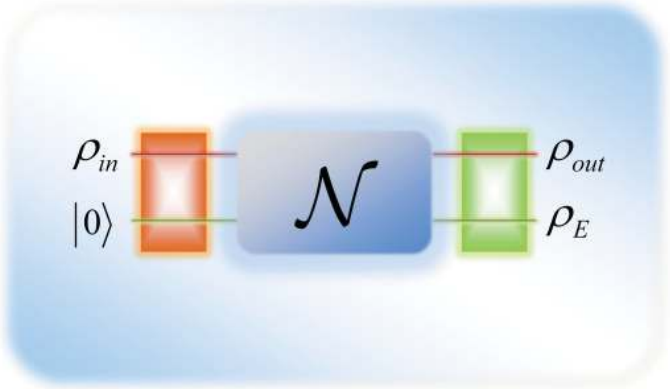

Fig. 3: The general model of transmission of information over a noisy quantum channel.

If the quantum channel $\mathcal{N}$ is used for information transmission, then the state of the composite system changes unitarily, as follows:

$$U\left(\rho_{in} \otimes \rho_E\right) U^{\dagger}, \tag{9}$$

where U is a unitary transformation, and $U^{\dagger}U = I$. After the quantum state has been sent over the quantum channel $\mathcal{N}$, the ρ_{out} output state can be expressed as:

$$\mathcal{N}\left(\rho_{in}\right) = \rho_{out} = Tr_E\left[U\left(\rho_{in} \otimes \rho_E\right) U^{\dagger}\right], \tag{10}$$

where Tr_E traces out the environment E from the joint state. Assuming the environment E in the pure state $|0\rangle$, $\rho_E = |0\rangle\langle 0|$, the $\mathcal{N}\left(\rho_{in}\right)$ noisy evolution of the channel $\mathcal{N}$ can be expressed as:

$$\mathcal{N}\left(\rho_{in}\right) = \rho_{out} = Tr_E U \rho_{in} \otimes |0\rangle\langle 0| U^{\dagger}, \tag{11}$$

while the post-state ρ_E of the environment after the transmission is

$$\rho_E = Tr_B U \rho_{in} \otimes |0\rangle\langle 0| U^{\dagger}, \tag{12}$$

where Tr_B traces out the output system B. In general, the i-th input quantum state ρ_i is prepared with probability p_i, which describes the ensemble $\{p_i, \rho_i\}$. The average of the *input* quantum system is

$$\sigma_{in} = \sum_i p_i \rho_i, \tag{13}$$

The average (or the mixture) of the *output* of the quantum channel is denoted by

$$\sigma_{out} = \mathcal{N}\left(\sigma_{in}\right) = \sum_i p_i \mathcal{N}\left(\rho_i\right). \tag{14}$$

E. Quantum Channel Capacity

The capacity of a communication channel describes the capability of the channel for sending information from the sender to the receiver, in a faithful and recoverable way. The perfect ideal communication channel realizes an identity map. For a quantum communication channel, it means that the channel can transmit the quantum states perfectly. Clearly speaking, the capacity of the quantum channel measures the closeness to the ideal identity transformation *I*.

To describe the information transmission capability of the quantum channel $\mathcal{N}$, we have to make a distinction between the various capacities of a quantum channel. The encoded quantum states can carry classical messages or quantum messages. In the case of classical messages, the quantum states encode the output from a *classical information source*, while in the latter the source is a *quantum information source*.

On one hand for classical communication channel *N*, only one type of capacity measure can be defined, on the other hand for a quantum communication channel $\mathcal{N}$ a number of different types of quantum channel capacities can be applied, with different characteristics. There are plenty of open questions regarding these various capacities. In general, the *single-use* capacity of a quantum channel is not equal to the *asymptotic* capacity of the quantum channel (As we will see later, it also depends on the type of the quantum channel). The asymptotic capacity gives us the amount of information

which can be transmitted in a reliable form using the quantum channel infinitely many times. The encoding and the decoding functions mathematically can be described by the operators $\mathcal{E}$ and $\mathcal{D}$, realized on the blocks of quantum states. These superoperators describe unitary transformations on the input states together with the environment of the quantum system. The model of communication through noisy quantum channel $\mathcal{N}$ with encoding, delivery and decoding phases is illustrated in Fig. 4.

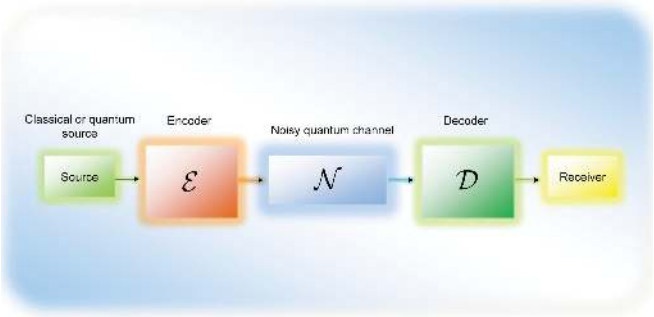

Fig. 4: Communication over a noisy quantum channel.

We note, in our paper we will use the terms *classical quantity* and *quantum quantity* with relation to the quantum channel $\mathcal{N}$ as follows:

1) *classical quantity*: it is a measure of the classical transmission capabilities of a quantum channel. (See later: Holevo information, quantum mutual information, etc., in Section III)
2) *quantum quantity*: it is a measure of the quantum transmission capabilities of a quantum channel (See later: quantum coherent information,etc., in Section IV)

If we mention classical quantity we will do this with relation to the quantum channel $\mathcal{N}$, i.e., for example the Holevo information is also not a typical' classical quantity since it is describes a quantum system not a classical one, but with relation to the quantum channel we can use the *classical* mark. The historical background with the description of the most relevant works can be found in the Related Work part of each section. For detailed information see [245].

F. Definitions

Quantum information theory also has relevance to the discussion of the capacity of quantum channels and to information transmission and storage in quantum systems. As we will see in this section, while the transmission of product states can be described similar to classical information, on the other hand, the properties of quantum entanglement cannot be handled by the elements of classical information theory. Of course, the elements of classical information theory can be viewed as a subset of the larger and more complex quantum information theory [568].

First, we summarize the basic definitions and formulas of quantum information theory. We introduce the reader to the description of a noisy quantum channel, purification, isometric extension, Kraus representation and the von Neumann entropy. Next, we describe the encoding of quantum states and the meaning of Holevo information, the quantum mutual information and quantum conditional entropy.

1) Discussion: Before starting the discussion on various capacities of quantum channels and the related consequences we summarize the basic definitions and formulas of quantum information theory intended to represent the information stored in quantum states. Those readers who are familiar with density matrices, entropies etc. may run through this section.

The world of quantum information processing (QIP) is describable with the help of quantum information theory (QIT), which is the main subject of this section. We will provide an overview of the most important differences between the compressibility of classical bits and quantum bits, and between the capacities of classical and quantum communication channels. To represent classical information with quantum states, we might use pure orthogonal states. In this case there is no difference between the compressibility of classical and quantum bits.

Similarly, a quantum channel can be used with pure orthogonal states to realize classical information transmission, or it can be used to transmit non-orthogonal states or even quantum entanglement. Information transmission also can be approached using the question, whether the input consists of unentangled or entangled quantum states. This leads us to say that for quantum channels many new capacity definitions exist in comparison to a classical communication channel.

Quantum information theory also has relevance to the discussion of the capacity of quantum channels and to information transmission and storage in quantum systems. While the transmission of product states can be described similar to classical information, on the other hand, the properties of quantum entanglement cannot be handled by the elements of classical information theory. Of course, the elements of classical information theory can be viewed as a subset of the larger and more complex quantum information theory.

Before we would start to our introduction to quantum information theory, we have to make a clear distinction between quantum information theory and quantum information processing. Quantum information theory is rather a generalization of the elements and functions of classical information theory to describe the properties of quantum systems, storage of information in quantum systems and the various quantum phenomena of quantum mechanics. While quantum information theory aims to provide a stable theoretical background, quantum information processing is a more general and rather experimental field: it answers what can be achieved in engineering with the help of quantum information. Quantum information processing includes the computing, error-correcting schemes, quantum communication protocols, field of communication complexity, etc.

The character of classical information and quantum information is significantly different. There are many phenomena in quantum systems which cannot be described classically, such as entanglement, which makes it possible to store quantum information in the correlation of quantum states. Entangled quantum states are named to EPR states after Einstein, Podolsky and Rosen, or Bell states, after J. Bell. Quantum entanglement was discovered in the 1930s, and it may still

yield many surprises in the future. Currently it is clear that entanglement has many classically indescribable properties and many new communication approaches based on it. Quantum entanglement plays a fundamental role in advanced quantum communications, such as teleportation, quantum cryptography etc.

The elements of quantum information theory are based on the laws of quantum mechanics. The main results of quantum information processing were laid down during the end of the twentieth century, the most important results being stated by Feynman, Bennett, DiVincenzo, Devetak, Deutsch, Holevo, Lloyd, Schumacher, Shor and many more. After the basic concepts of quantum information processing had been stated, researchers started to look for efficient quantum error correction schemes and codes, and started to develop the theoretical background of fault-tolerant quantum computation. The main results from this field were presented by Bennett, Schumacher, Gottesman, Calderbank, Preskill, Knill, and Kerckhoff. On the other hand, there are still many open questions about quantum computation. The theoretical limits of quantum computers were discovered by Bennett, Bernstein, Brassard and Vazirani: quantum computers can provide at best a quadratic reduction in the complexity of search-based problems, hence if we give an NP-complete problem to quantum computer, it still cannot solve it. Recently, the complexity classes of quantum information processing have been investigated, and many new classes and lower bounds have been found.

By the end of the twentieth century, many advanced and interesting properties of quantum information theory had been discovered, and many possible applications of these results in future communication had been developed. One of the most interesting revealed connections was that between quantum information theory and the elements of geometry. The space of quantum states can be modeled as a convex set which contains points with different probability distributions, and the geometrical distance between these probability distributions can be measured by the elementary functions of quantum information theory, such as the von Neumann entropy or the quantum relative entropy function. The connection between the elements of quantum information theory and geometry leads us to the application of advanced computational geometrical algorithms to quantum space, to reveal the still undiscovered properties of quantum information processing, such as the open questions on the capacities of the quantum channels or their additivity properties. The connection between the Hilbert space of quantum states and the geometrical distance can help us to reveal the fantastic properties of quantum bits and quantum state space.

Several functions have been defined in quantum information theory to describe the statistical distances between the states in the quantum space: one of the most important is the quantum relative entropy function which plays a key role in the description of entanglement, too. This function has many different applications, and maybe this function plays the most important role in the questions regarding the capacity of quantum channels. The possible applications of the quantum relative entropy function have been studied by Schumacher and Westmoreland and by Vedral.

Quantum information theory plays fundamental role in the description of the data transmission through quantum communication channels. At the dawn of this millennium new problems have arisen, whose solutions are still not known, and which have opened the door to many new promising results such as the superactivation of zero-capacity quantum channels in 2008, and then the superactivation of the zero-error capacities of the quantum channels in 2009 and 2010. One of the earliest works on the capacities of quantum communication channels was published in the early 1970s. Along with other researchers, Holevo was showed that there are many differences between the properties of classical and quantum communication channels, and illustrated this with the benefits of using entangled input states. Later, he also stated that quantum communication channels can be used to transmit both classical and quantum information. Next, many new quantum protocols were developed, such as teleportation or superdense coding. After Alexander Holevo published his work, about thirty years later, he, with Benjamin Schumacher and Michael Westmoreland presented one of the most important result in quantum information theory, called the *Holevo-Schumacher-Westmoreland* (HSW) theorem [233], [469]. The HSW-theorem is a generalization of the classical noisy channel coding theorem from classical information theory to a noisy quantum channel. The HSW theorem is also called the *product-state* classical channel capacity theorem of a noisy quantum channel. The understanding of the classical capacity of a quantum channel was completed by 1997 by Schumacher and Westmoreland, and by 1998 by Holevo, and it has tremendous relevance in quantum information theory, since it was the first to give a mathematical proof that a noisy quantum channel can be used to transmit classical information in a reliable form. The HSW theorem was a very important result in the history of quantum information theory, on the other hand it raised a lot of questions regarding the transmission of classical information over general quantum channels.

The quantum capacity of a quantum channel was firstly formulated by Seth Lloyd in 1996, then by Peter Shor in 2002, finally it was completed by Igor Devetak in 2003, - the result is known as the *LSD channel capacity* [134], [303], [487]. While the classical capacity of a quantum channel is described by the maximum of quantum mutual information and the Holevo information, the quantum capacity of the quantum channels is described by a completely different correlation measure: called the *quantum coherent information*. The concept of quantum coherent information plays a fundamental role in the computation of the quantum capacity which measures the asymptotic quantum capacity of the quantum capacity in general. For the complete historical background with the references see the Related Works.

2) Density Matrix and Trace Operator: In this section we introduce a basic concept of quantum information theory, called the *density matrix*.

Before we start to discuss the density matrix, we introduce some terms. An $n \times n$ square matrix A is called *positive-semidefinite* if $\langle\psi| A |\psi\rangle$ is a non-negative real number for every vector $|\psi\rangle$. If $A{=}A^{\dagger}$, i.e., A has Hermitian matrix and the $\{\lambda_1, \lambda_2, \ldots \lambda_n\}$ eigenvalues of A are all non-negative real

numbers then it is positive-semidefinite. This definition has important role in quantum information theory, since *every density matrix is positive-semidefinite.* It means, for any vector $|\varphi\rangle$ the positive-semidefinite property says that

$$\langle\varphi|\,\rho\,|\varphi\rangle=\sum_{i=1}^{n}p_i\,\langle\varphi\mid\psi_i\rangle\,\langle\psi_i\mid\varphi\rangle=\sum_{i=1}^{n}p_i|\langle\varphi\mid\psi_i\rangle|^2\geq 0. \tag{15}$$

In (15) we used, the density matrix is denoted by ρ, and it describes the system by the classical probability weighted sum of possible states

$$\rho=\sum_i p_i\,|\psi_i\rangle\,\langle\psi_i|\,, \tag{16}$$

where $|\psi_i\rangle$ is the *i*-th system state occurring with classical probability p_i. As can be seen, this density matrix describes the system as a probabilistic mixture of the possible known states the so called *pure states*. For pure state $|\psi\rangle$ the density matrix is $\rho=|\psi\rangle\,\langle\psi|$ and the rank of the matrix is equal to one. Trivially, classical states e.g. $|0\rangle$ and $|1\rangle$ are pure, however, if we know that our system is prepared to the *superposition* $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ then this state is pure, too. Clearly speaking, while superposition is a quantum linear combination of orthonormal basis states weighted by probability amplitudes, mixed states are classical linear combination of pure superpositions (quantum states) weighted by classical probabilities.

The density matrix contains all the possible information that can be extracted from the quantum system. It is possible that two quantum systems possess the same density matrices: in this case, these quantum systems are called indistinguishable, since it is not possible to construct a measurement setting, which can distinguish between the two systems.

The density matrix ρ of a simple pure quantum system which can be given in the state vector representation $|\psi\rangle=\alpha\,|0\rangle+\beta\,|1\rangle$ can be expressed as the outer product of the *ket* and *bra* vectors, where bra is the transposed complex conjugate of ket, hence for $|\psi\rangle=\begin{bmatrix}\alpha\\ \beta\end{bmatrix}, \langle\psi|=\begin{bmatrix}\alpha^* & \beta^*\end{bmatrix}$ the density matrix is

$$\begin{aligned}\rho=|\psi\rangle\,\langle\psi|&=\begin{bmatrix}\alpha\\ \beta\end{bmatrix}\begin{bmatrix}\alpha^* & \beta^*\end{bmatrix}\\ &=\begin{bmatrix}\alpha\alpha^* & \alpha\beta^*\\ \alpha^*\beta & \beta\beta^*\end{bmatrix}=\begin{bmatrix}|\alpha|^2 & \alpha\beta^*\\ \alpha^*\beta & |\beta|^2\end{bmatrix}.\end{aligned} \tag{17}$$

The density matrix $\rho=\sum_{i=1}^{n}p_i\,|\psi_i\rangle\,\langle\psi_i|$ contains the probabilistic mixture of different pure states, which representation is based on the fact that the mixed states can be decomposed into weighted sum of pure states [530].

To reveal important properties of the density matrix, we introduce the concept of the *trace operation*. The trace of a density matrix is equal to the sum of its diagonal entries. For an $n\times n$ square matrix A, the Tr trace operator is defined as

$$Tr\,(A)=a_{11}+a_{22}+\cdots+a_{nn}=\sum_{i=1}^{n}a_{ii}, \tag{18}$$

where a_{ii} are the elements of the main diagonal. The trace of the matrix *A* is also equal to the sum of the *eigenvalues* of its matrix. The eigenvalue is the factor by which the *eigenvector* changes if it is multiplied by the matrix *A*, for each eigenvectors. The *eigenvectors* of the square matrix *A* are those non-zero vectors, whose direction remain the same to the original vector after multiplied by the matrix *A*. It means, the eigenvectors remain proportional to the original vector. For square matrix *A*, the non-zero vector $\boldsymbol{v}$ is called *eigenvector* of *A*, if there is a scalar λ for which

$$A\boldsymbol{v}=\lambda\boldsymbol{v}, \tag{19}$$

where λ is the *eigenvalue* of *A* corresponding to the eigenvector $\boldsymbol{v}$.

The trace operation gives us the sum of the eigenvalues of positive-semidefinite *A*, for each eigenvectors, hence $Tr\,(A)=\sum_{i=1}^{n}\lambda_i$, and $Tr\left(A^k\right)=\sum_{i=1}^{n}\lambda_i^k$. Using the eigenvalues, the *spectral decomposition* of density matrix ρ can be expressed as

$$\rho=\sum_i \lambda_i\,|\varphi_i\rangle\,\langle\varphi_i|\,, \tag{20}$$

where $|\varphi_i\rangle$ are orthonormal vectors.

The trace is a linear map, hence for square matrices *A* and *B*

$$Tr\,(A+B)=Tr\,(A)+Tr\,(B)\,, \tag{21}$$

and

$$Tr\,(sA)=sTr\,(A)\,, \tag{22}$$

where *s* is a scalar. Another useful formula, that for $m\times n$ matrix *A* and $n\times m$ matrix *B*,

$$Tr\,(AB)=Tr\,(BA)\,, \tag{23}$$

which holds for any matrices *A* and *B* for which the product matrix *AB* is a square matrix, since

$$Tr\,(AB)=\sum_{i=1}^{m}\sum_{j=1}^{n}A_{ij}B_{ji}=Tr\,(BA)\,. \tag{24}$$

Finally, we mention that the trace of a matrix *A* and the trace of its transpose A^T are equal, hence

$$Tr\,(A)=Tr\left(A^T\right). \tag{25}$$

If we take the conjugate transpose A^* of the $m\times n$ matrix *A*, then we will find that

$$Tr\,(A^*A)\geq 0, \tag{26}$$

which will be denoted by $\langle A,A\rangle$ and it is called the *inner product*. For matrices *A* and *B*, the inner product $\langle A,B\rangle=Tr\,(B^*A)$, which can be used to define the angle between the two vectors. The inner product of two vectors will be zero if and only if the vectors are orthogonal.

As we have seen, the trace operation gives the sum of the eigenvalues of matrix *A*, this property can be extended to the density matrix, hence for each eigenvectors λ_i of density matrix ρ

$$Tr\,(\rho)=\sum_{i=1}^{n}\lambda_i. \tag{27}$$

Now, having introduced the *trace* operation, we apply it to a density matrix. If we have an *n*-qubit system being in the state $\rho=\sum_{i=1}^{n} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$, then

$$\begin{aligned} Tr\left(\sum_{i=1}^{n} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|\right) &= \sum_{i=1}^{n} p_i Tr\left(\left|\psi_i\right\rangle \left\langle\psi_i\right|\right) \\ &= \sum_{i=1}^{n} p_i \left(\left\langle\psi_i|\psi_i\right\rangle\right) = 1, \end{aligned} \tag{28}$$

where we exploited the relation for unit-length vectors $\left|\psi_i\right\rangle$

$$\left\langle\psi_i|\psi_i\right\rangle \equiv 1. \tag{29}$$

Thus the trace of any density matrix is equal to one

$$Tr\left(\rho\right) = 1. \tag{30}$$

The trace operation can help to distinguish *pure* and *mixed* states since for a given *pure* state ρ

$$Tr\left(\rho^2\right) = 1, \tag{31}$$

while for a *mixed* state σ,

$$Tr\left(\sigma^2\right) < 1. \tag{32}$$

where $Tr\left(\rho^2\right)=\sum_{i=1}^{n} \lambda_i^2$ and $Tr\left(\sigma^2\right)=\sum_{i=1}^{n} \omega_i^2$, where ω_i are the eigenvalues of density matrix σ.

Similarly, for a pure *entangled* system ρ_{EPR}

$$Tr\left(\rho_{EPR}^2\right) = 1, \tag{33}$$

while for any mixed subsystem σ_{EPR} of the entangled state (i.e., for a half-pair of the entangled state), we will have

$$Tr\left(\sigma_{EPR}^2\right) < 1. \tag{34}$$

The density matrix also can be used to describe the effect of a unitary transform on the probability distribution of the system. The probability that the whole quantum system is in $\left|\psi_i\right\rangle$ can be calculated by the trace operation. If we apply unitary transform U to the state $\rho=\sum_{i=1}^{n} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$, the effect can be expressed as follows:

$$\sum_{i=1}^{n} p_i \left(U\left|\psi_i\right\rangle\right)\left(\left\langle\psi_i\right| U^{\dagger}\right) = U\left(\sum_{i=1}^{n} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|\right) U^{\dagger} = U\rho U^{\dagger}. \tag{35}$$

If the applied transformation is not unitary, a more general operator denoted by G is introduced, and with the help of this operator the transform can be written as

$$G\left(\rho\right) = \sum_{i=1}^{n} A_i \rho A_i^{\dagger} = \sum_{i=1}^{n} A_i \left(p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|\right) A_i^{\dagger}, \tag{36}$$

where $\sum_{i=1}^{n} A_i A_i^{\dagger}=I$, for every matrices A_i. In this sense, operator G describes the physically admissible or *Completely Positive Trace Preserving* (CPTP) operations. The application of a CPTP operator G on density matrix ρ will result in a matrix $G\left(\rho\right)$, which in this case is still a density matrix.

Now we can summarize the two most important properties of density matrices:

1) *The density matrix ρ is a positive-semidefinite matrix, see* (15).
2) *The trace of any density matrix ρ is equal to 1, see* (28).

The properties of a quantum measurement are as follows.

3) Quantum Measurement: Now, let us turn to measurements and their relation to density matrices. Assuming a projective measurement device, defined by measurement operators - i.e., projectors $\{P_j\}$. The projector P_j is a Hermitian matrix, for which $P_j=P_j^{\dagger}$ and $P_j^2=P_j$. According to the *3rd Postulate of Quantum Mechanic*s the trace operator can be used to give the probability of outcome *j* belonging to the operator P_j in the following way

$$\Pr\left[j|\, P_j\rho\right] = Tr\left(P_j \rho P_j^{\dagger}\right) = Tr\left(P_j^{\dagger} P_j \rho\right) = Tr\left(P_j\rho\right). \tag{37}$$

After the measurement, the measurement operator P_j leaves the system in a post measurement state

$$\rho_j = \frac{P_j\left[\sum_{i=1}^{n} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|\right] P_j}{Tr\left(P_j\left[\sum_{i=1}^{n} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|\right] P_j\right)} = \frac{P_j\rho P_j}{Tr\left(P_j\rho P_j\right)} = \frac{P_j\rho P_j}{Tr\left(P_j\rho\right)}. \tag{38}$$

If we have a pure quantum state $\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$, where $\alpha=\left\langle 0 \mid \psi\right\rangle$ and $\beta=\left\langle 1 \mid \psi\right\rangle$. Using the trace operator, the measurement probabilities of $\left|0\right\rangle$ and $\left|1\right\rangle$ can be expressed as

$$\begin{aligned} &\Pr\left[j=0|\,\psi\right] = Tr\left(P_j\rho\right) = Tr\left(\left|0\right\rangle \underbrace{\left\langle 0\right| \left|\psi\right\rangle}_{\left\langle 0|\psi\right\rangle} \left\langle\psi\right|\right) \\ &= \left\langle 0 \mid \psi\right\rangle Tr\left(\left|0\right\rangle \left\langle\psi\right|\right) = \left\langle 0 \mid \psi\right\rangle \left\langle\psi \mid 0\right\rangle \\ &= \left\langle 0 \mid \psi\right\rangle \left(\left\langle 0 \mid \psi\right\rangle\right)^{*} = \alpha\cdot\alpha^{*} = \left|\alpha\right|^2, \end{aligned} \tag{39}$$

and

$$\begin{aligned} &\Pr\left[j=1|\,\psi\right] = Tr\left(P_j\rho\right) = Tr\left(\left|1\right\rangle \underbrace{\left\langle 1\right| \left|\psi\right\rangle}_{\left\langle 1|\psi\right\rangle} \left\langle\psi\right|\right) \\ &= \left\langle 1 \mid \psi\right\rangle Tr\left(\left|1\right\rangle \left\langle\psi\right|\right) = \left\langle 1 \mid \psi\right\rangle \left\langle\psi \mid 1\right\rangle \\ &= \left\langle 1 \mid \psi\right\rangle \left(\left\langle 1 \mid \psi\right\rangle\right)^{*} = \beta\cdot\beta^{*} = \left|\beta\right|^2, \end{aligned} \tag{40}$$

in accordance with our expectations. Let us assume we have an *orthonormal* basis $M=\{\left|x_1\right\rangle \left\langle x_1\right|, \ldots, \left|x_n\right\rangle \left\langle x_n\right|\}$ and an arbitrary (i.e., non-diagonal) density matrix ρ. The set of Hermitian operators $P_i=\{\left|x_i\right\rangle \left\langle x_i\right|\}$ satisfies the *completeness relation*, where $P_i=\left|x_i\right\rangle \left\langle x_i\right|$ is the projector over $\left|x_i\right\rangle$, i.e., quantum measurement operator $M_i=\left|x_i\right\rangle \left\langle x_i\right|$ is a valid measurement operator. The measurement operator M_i projects the input quantum system $\left|\psi\right\rangle$ to the pure state $\left|x_i\right\rangle$ from the orthonormal basis $M=\{\left|x_1\right\rangle \left\langle x_1\right|, \ldots, \left|x_n\right\rangle \left\langle x_n\right|\}$. Now, the probability that the quantum state $\left|\psi\right\rangle$ is after the measurement in basis state $\left|x_i\right\rangle$ can be expressed as

$$\begin{aligned} &\left\langle \psi\right| M_i^{\dagger} M_i \left|\, \psi\right\rangle = \left\langle\psi\right| P_i \left|\, \psi\right\rangle \\ &= \left(\sum_{j=1}^{n} x_j^{*} \left\langle x_j\right|\right) \left|x_i\right\rangle \left\langle x_i\right| \left(\sum_{l=1}^{n} \left|x_l\right\rangle x_l\right) = \left|x_i\right|^2. \end{aligned} \tag{41}$$

In the computational basis $\{\left|x_1\right\rangle, \ldots, \left|x_n\right\rangle\}$, the state of the quantum system after the measurement can be expressed as

$$\rho' = \sum_{i=1}^{n} p_i \left|x_i\right\rangle \left\langle x_i\right|, \tag{42}$$

and the matrix of the quantum state ρ' will be *diagonal* in the computational basis $\{|x_i\rangle\}$, and can be given by

$$\rho'=\begin{bmatrix} p_1 & 0 & \dots & 0 \\ 0 & p_2 & 0 & \vdots \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & p_n \end{bmatrix}. \tag{43}$$

To illustrate it, let assume we have an initial (not diagonal) density matrix in the computational basis $\{|0\rangle, |1\rangle\}$ e.g. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $p{=}|\alpha|^2$ and $1{-}p{=}|\beta|^2$ as

$$\rho{=}|\psi\rangle\langle\psi| = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix}, \tag{44}$$

and we have orthonormal basis $M{=}\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. In this case, the after-measurement state can be expressed as

$$\rho'{=}p|0\rangle\langle 0| + (1{-}p)|1\rangle\langle 1| = \begin{bmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{bmatrix} = \begin{bmatrix} p & 0 \\ 0 & 1{-}p \end{bmatrix}. \tag{45}$$

As it can be seen, the matrix of ρ' is a diagonal matrix in the computational basis $\{|0\rangle, |1\rangle\}$. Eq. (44) and (45) highlights the difference between quantum superpositions (probability amplitude weighted sum) and classical probabilistic mixtures of quantum states.

Now, let us see the result of the measurement on the input quantum system ρ

$$M(\rho) = \sum_{j=0}^{1} M_j \rho M_j^\dagger = M_0 \rho M_0^\dagger + M_1 \rho M_1^\dagger. \tag{46}$$

For the measurement operators $M_0{=}|0\rangle\langle 0|$ and $M_1{=}|1\rangle\langle 1|$ the completeness relation holds

$$\begin{aligned} &\textstyle\sum_{j=0}^{1} M_j M_j^\dagger = |0\rangle\langle 0|0\rangle\langle 0| + |1\rangle\langle 1|1\rangle\langle 1| \\ &= |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I. \end{aligned} \tag{47}$$

Using input system $\rho{=}|\psi\rangle\langle\psi|$, where $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, the state after the measurement operation is

$$\begin{aligned} &M(\rho) = \textstyle\sum_{j=0}^{1} M_j \rho M_j^\dagger \\ &= |0\rangle\langle 0|\rho|0\rangle\langle 0| + |1\rangle\langle 1|\rho|1\rangle\langle 1| \\ &= |0\rangle\langle 0|\psi\rangle\langle\psi|0\rangle\langle 0| + |1\rangle\langle 1|\psi\rangle\langle\psi|1\rangle\langle 1| \\ &= |0\rangle\langle 0|\psi\rangle\langle 0|\psi\rangle\langle 0| + |1\rangle\langle 1|\psi\rangle\langle 1|\psi\rangle\langle 1| \\ &= |\langle 0|\psi\rangle|^2 |0\rangle\langle 0| + |\langle 1|\psi\rangle|^2 |1\rangle\langle 1| \\ &= |\alpha|^2 |0\rangle\langle 0| + |\beta|^2 |1\rangle\langle 1| = p|0\rangle\langle 0| + 1{-}p|1\rangle\langle 1|. \end{aligned} \tag{48}$$

As we have found, after the measurement operation $M(\rho)$, the *off-diagonal* entries will have zero values, and they *have no relevance*. As follows, the initial input system $\rho{=}|\psi\rangle\langle\psi|$ after operation *M* becomes

$$\rho{=}\begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix} \xrightarrow{M} \rho'{=}\begin{bmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{bmatrix}. \tag{49}$$

a) Orthonormal Basis Decomposition: Let assume we have orthonormal basis $\{|b_1\rangle, |b_2\rangle, \dots, |b_n\rangle\}$, which basis can be used to rewrite the quantum system $|\psi\rangle$ in a unique decomposition

$$|\psi\rangle = b_1|b_1\rangle + b_2|b_2\rangle + \dots + b_n|b_n\rangle = \sum_{i=1}^{n} b_i|b_i\rangle, \tag{50}$$

with complex b_i. Since $\langle\psi \mid \psi\rangle = 1$, we can express it in the form

$$\langle\psi \mid \psi\rangle = \sum_{i=1}^{n}\sum_{j=1}^{n} b_i^* b_j \langle b_i \mid b_j\rangle = \sum_{i=1}^{n} |b_i|^2 = 1, \tag{51}$$

where b_i^* is the complex conjugate of *probability amplitude* b_i, thus $|b_i|^2$ is the *probability* p_i of measuring the quantum system $|\psi\rangle$ in the given basis state $|b_i\rangle$, i.e.,

$$p_i{=}|b_i|^2. \tag{52}$$

Using (16), (50) and (51) the density matrix of quantum system $|\psi\rangle$ can be expressed as

$$\begin{aligned} &\rho{=}|b_1|^2|b_1\rangle\langle b_1| + |b_2|^2|b_2\rangle\langle b_2| + \dots + |b_n|^2|b_n\rangle\langle b_n| \\ &= \textstyle\sum_{i=1}^{n} |b_i|^2 |b_i\rangle\langle b_i| = \sum_{i=1}^{n} p_i |b_i\rangle\langle b_i|. \end{aligned} \tag{53}$$

This density matrix is a diagonal matrix with the probabilities in the diagonal entries

$$\rho{=}\begin{bmatrix} p_1 & \cdots & 0 & 0 \\ 0 & p_2 & 0 & \vdots \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & p_n \end{bmatrix}. \tag{54}$$

The diagonal property of density matrix (53) in (54) can be checked, since the elements of the matrix can be expressed as

$$\begin{aligned} \rho_{ij} &= \langle b_i|\rho|b_j\rangle \\ &= \langle b_i| \left(\sum_{l=1}^{n} p_i |b_i\rangle\langle b_i| \right) |b_j\rangle = \sum_{l=1}^{n} p_l \langle b_i|b_l\rangle\langle b_l|b_j\rangle, \end{aligned} \tag{55}$$

where $\sum_{l=1}^{n} p_i = 1$.

b) The Projective and POVM Measurement: The *projective measurement* is also known as the *von Neumann measurement* is formally can be described by the Hermitian operator $\mathcal{Z}$, which has the spectral decomposition

$$\mathcal{Z}{=}\sum_m \lambda_m P_m. \tag{56}$$

where P_m is a projector to the eigenspace of $\mathcal{Z}$ with eigenvalue λ_m. For the projectors

$$\sum_m P_m{=}I, \tag{57}$$

and they are pairwise orthogonal. The measurement outcome *m* corresponds to the eigenvalue λ_m, with measurement probability

$$\Pr[m|\psi\rangle] = \langle\psi|P_m|\psi\rangle. \tag{58}$$

When a quantum system is measured in an orthonormal basis $|m\rangle$, then we make a projective measurement with projector $P_m=|m\rangle\langle m|$, thus (56) can be rewritten as

$$\mathcal{Z}=\sum_m mP_m. \tag{59}$$

The $\mathcal{P}$ *POVM* (Positive Operator Valued Measurement) is intended to select among the non-orthogonal states $\{|\psi_i\rangle\}_{i=1}^{m}$ and defined by a *set* of POVM operators $\{\mathcal{M}_i\}_{i=1}^{m+1}$, where

$$\mathcal{M}_i=\mathcal{Q}_i^{\dagger}\mathcal{Q}_i, \tag{60}$$

and since we are not interested in the post-measurement state the exact knowledge about measurement operator $\mathcal{Q}_i$ is not required. For POVM operators $\mathcal{M}_i$ the completeness relation holds,

$$\sum_i \mathcal{M}_i=I. \tag{61}$$

For the POVM the probability of a given outcome *n* for the state $|\psi\rangle$ can be expressed as

$$\Pr\left[i\,|\psi\rangle\right]=\langle\psi|\mathcal{M}_i|\,\psi\rangle\,. \tag{62}$$

The POVM also can be imagined as a 'black-box', which outputs a number from 1 to *m* for the given input quantum state ψ, using the set of operators

$$\{\mathcal{M}_1,\ldots,\mathcal{M}_m,\mathcal{M}_{m+1}\}, \tag{63}$$

where $\{\mathcal{M}_1,\ldots,\mathcal{M}_m\}$ are responsible to distinguish *m* different typically non-orthogonal states i.e., if we observe $i\in[1,m]$ on the display of the measurement device we can be sure, that the result is correct. However, because unknown non-orthogonal states can not be distinguished with probability 1, we have to introduce an extra measurement operator, $\mathcal{M}_{m+1}$, as the price of the distinguishability of the *m* different states and if we obtain *m*+1 as measurement results we can say nothing about $|\psi\rangle$. This operator can be expressed as

$$\mathcal{M}_{m+1}=I-\sum_{i=1}^{m}\mathcal{M}_i. \tag{64}$$

Such $\mathcal{M}_{m+1}$ can be always constructed if the states in $\{|\psi_n\rangle\}_{n=1}^{m}$ are linearly independent. We note, we will omit listing operator $\mathcal{M}_{m+1}$ in further parts of the paper. The POVM measurement apparatus will be a key ingredient to distinguish quantum codewords with zero-error, and to reach the zero-error capacity of quantum channels.

The POVM can be viewed as the most general formula from among of any possible measurements in quantum mechanics. Therefore the effect of a projective measurement can be described by POVM operators, too. Or with other words, the projective measurements are the special case POVM measurement [244]. The elements of the POVM are not necessarily orthogonal, and the number of the elements can be larger than the dimension of the Hilbert space which they are originally used in.

G. Geometrical Interpretation of the Density Matrices

While the *wavefunction* representation is the full physical description of a quantum system in the space-time, the tensor product of multiple copies of two dimensional Hilbert spaces is its discrete version, with discrete finite-dimensional Hilbert spaces. The geometrical representation also can be extended to analyze the geometrical structure of the transmission of information though a quantum channel, and it also provides a very useful tool to analyze the capacities of different quantum channel models.

As it has been mentioned, the Bloch sphere is a geometrical conception, constructed to represent two-level quantum systems in a more expressive way than is possible with algebraic tools. The Bloch sphere has unit radius and is defined in a three-dimensional real vector space. The pure states are on the surface of the Bloch sphere, while the mixed states are in the interior of the original sphere. In the Bloch sphere representation, the state of a single qubit $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ can be expressed as

$$|\psi\rangle=e^{i\delta}\left(\cos\frac{\theta}{2}|0\rangle+e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right), \tag{65}$$

where δ is the global phase factor, which can be ignored from the computations, hence the state $|\psi\rangle$ in the terms of the angle θ and φ can be expressed as

$$|\psi\rangle=\cos\frac{\theta}{2}|0\rangle+e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\,. \tag{66}$$

The Bloch sphere is a very useful tool, since it makes possible to describe various, physically realized one-qubit quantum systems, such as the photon polarization, spins or the energy levels of an atom. Moreover, if we would like to compute the various channel capacities of the quantum channel, the geometrical expression of the channel capacity also can be represented by the Bloch sphere. Before we would introduce the geometrical calculation of the channel capacities, we have to start from the geometrical interpretation of density matrices. The density matrix ρ can then be expressed using the Pauli matrices (a set of three complex matrices which are Hermitian and unitary) $\sigma_X=\begin{bmatrix}0&1\\1&0\end{bmatrix}$, $\sigma_Y=\begin{bmatrix}0&-i\\i&0\end{bmatrix}$ and $\sigma_Z=\begin{bmatrix}1&0\\0&-1\end{bmatrix}$ as

$$\rho=\frac{1+r_X\sigma_X+r_Y\sigma_Y+r_Z\sigma_Z}{2}, \tag{67}$$

where $\boldsymbol{r}=(r_X,r_Y,r_Z)=(\sin\theta\cos\phi,\sin\theta\sin\phi,\cos\theta)$ is the Bloch vector, $\|(r_X,r_Z,r_Y)\|\leq 1$, and $\sigma=(\sigma_X,\sigma_Y,\sigma_Z)^T$. In the vector representation, the previously shown formula can be expressed as

$$\rho=\frac{1+\boldsymbol{r}\sigma}{2}. \tag{68}$$

In conclusion, every state can be expressed as linear combinations of the Pauli matrices and according to these Pauli matrices every state can be interpreted as a point in the three-dimensional real vector space. If we apply a unitary

transformation U to the density matrix ρ, then it can be expressed as

$$\rho \rightarrow \rho' = U\rho U^{\dagger} = \frac{1+U\boldsymbol{r}\sigma U^{\dagger}}{2} = \frac{1+U\boldsymbol{r}U^{\dagger}\sigma}{2}, \tag{69}$$

and $\boldsymbol{r}' = U\boldsymbol{r}U^{\dagger}$ realizes a unitary transformation on $\boldsymbol{r}$ as a rotation.

A density matrix ρ can be expressed in a 'weighted form' of density matrices ρ_1 and ρ_2 as follows:

$$\rho = \gamma\rho_1 + (1-\gamma)\,\rho_2, \tag{70}$$

where $0 \leq \gamma \leq 1$, and ρ_1 and ρ_2 are pure states, and lie on a line segment connecting the density matrices in the Bloch sphere representation. Using probabilistic mixtures of the pure density matrices, any quantum state which lies between the two states can be expressed as a convex combination

$$\rho = p\rho_1 + (1-p)\,\rho_2, 0 \leq p \leq 1. \tag{71}$$

This remains true for an arbitrary number of quantum states, hence this result can be expressed for arbitrary number of density matrices. Mixed quantum states can be represented as *statistical mixtures* of pure quantum states. The statistical representation of a pure state is unique. On the other hand we note that the decomposition of a mixed quantum state is not unique. In the geometrical interpretation a pure state ρ is on the surface of the Bloch sphere, while the mixed state σ is inside. A maximally mixed quantum state, $\sigma = \frac{1}{2}I$, can be found in the center of the Bloch sphere. The mixed state can be expressed as probabilistic mixture of pure states $\{\rho_1, \rho_2\}$ and $\{\rho_3, \rho_4\}$. As it has been stated by von Neumann, the *decomposition of a mixed state is not unique*, since it can be expressed as a mixture of $\{\rho_1, \rho_2\}$ or equivalently of $\{\rho_3, \rho_4\}$.

One can use a pure state ρ to recover mixed state σ from it, after the effects of environment (E) are traced out. With the help of the partial trace operator, Bob, the receiver, can decouple the environment from his mixed state, and the original state can be recovered by discarding the effects of the environment. If Bob's state is a *probabilistic mixture* $\sigma = \sum_i p_i \left|\varphi_i\right\rangle \left\langle\varphi_i\right|$, then a global pure *purification* state $\left|\Psi\right\rangle$ exists, which from Bob's state can be expressed as

$$\sigma = Tr_E \left|\Psi\right\rangle \left\langle\Psi\right|. \tag{72}$$

Note, density matrix σ can be recovered from $\left|\Psi\right\rangle$ after discarding the environment. The decoupling of the environment can be achieved with the Tr_E operator. For any unitary transformation of the environment, the pure state $\left|\Psi\right\rangle$ is a unique state.

We have seen, that the decomposition of mixed quantum states into pure quantum states is not unique, hence for example, it can be easily verified by the reader, that the decomposition of a mixed state $\sigma = \frac{1}{2}\left(\left|0\right\rangle\left\langle 0\right| + \left|1\right\rangle\left\langle 1\right|\right)$ can be made with pure states $\{\left|0\right\rangle, \left|1\right\rangle\}$, and also can be given with pure states $\left\{\frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right), \frac{1}{\sqrt{2}}\left(\left|0\right\rangle - \left|1\right\rangle\right)\right\}$. Here, we have just changed the basis from rectilinear to diagonal, and we have used just pure states - and it resulted in the same mixed quantum state.

H. Channel System Description

If we are interested in the origin of noise (randomness) in the quantum channel the model should be refined in the following way: Alice's register *X*, the purification state *P*, channel input *A*, channel output *B*, and the environment state *E*. The input system *A* is described by a quantum system ρ_x, which occurs on the input with probability $p_X(x)$. They together form an ensemble denoted by $\{p_X(x), \rho_x\}_{x\in X}$, where *x* is a classical variable from the register *X*. In the preparation process, Alice generates pure states ρ_x according to random variable *x*, i.e., the input density operator can be expressed as $\rho_x = \left|x\right\rangle\left\langle x\right|$, where the classical states $\{\left|x\right\rangle\}_{x\in X}$ form an orthonormal basis. According to the elements of Alice's register *X*, the input system can be characterized by the quantum system

$$\rho_A = \sum_{x\in X} p_X(x)\,\rho_x = \sum_{x\in X} p_X(x)\left|x\right\rangle\left\langle x\right|. \tag{73}$$

The system description is illustrated in Fig. 5.

The system state ρ_x with the corresponding probability distribution $p_X(x)$ can be indentified by a set of measurement operators $M = \{\left|x\right\rangle\left\langle x\right|\}_{x\in X}$. If the density operators ρ_x in ρ_A are mixed, the probability distribution $p_X(x)$ and the classical variable *x* from the register *X* cannot be indentified by the measurement operators $M = \{\left|x\right\rangle\left\langle x\right|\}_{x\in X}$, since the system state ρ_x is assumed to be a mixed or in a non-orthonormal state. Alice's register *X* and the quantum system *A* can be viewed as a tensor product system as

$$\{p_X(x), \left|x\right\rangle\left\langle x\right|_X \otimes \rho_A^x\}_{x\in X}, \tag{74}$$

where the classical variable *x* is correlated with the quantum system ρ_x, using orthonormal basis $\{\left|x\right\rangle\}_{x\in X}$. Alice's register *X* represents a classical variable, the channel input system is generated corresponding to the register *X* in the form of a quantum state, and it is described by the density operator ρ_A^x. The input system *A* with respect to the register *X*, is described by the density operator

$$\rho_{XA} = \sum_{x\in X} p_X(x)\left|x\right\rangle\left\langle x\right|_X \otimes \rho_A^x, \tag{75}$$

where $\rho_A^x = \left|\psi_x\right\rangle\left\langle\psi_x\right|_A$ is the density matrix representation of Alice's input state $\left|\psi_x\right\rangle_A$.

1) Purification: The *purification* gives us a new viewpoint on the noise of the quantum channel. Assuming Alice's side *A* and Alice's register *X*, the spectral decomposition of the density operator ρ_A can be expressed as

$$\rho_A = \sum_x p_X(x)\left|x\right\rangle\left\langle x\right|_A, \tag{76}$$

where $p_X(x)$ is the probability of variable *x* in Alice's register *X*. The $\{p_X(x), \left|x\right\rangle\}$ together is called an ensemble, where $\left|x\right\rangle$ is a quantum state according to classical variable *x*. Using the set of orthonormal basis vectors $\{\left|x\right\rangle_P\}_{x\in X}$ of the purification system *P*, the purification of (76) can be given in the following way:

$$\left|\varphi\right\rangle_{PA} = \sum_x \sqrt{p_X(x)}\left|x\right\rangle_P\left|x\right\rangle_A. \tag{77}$$

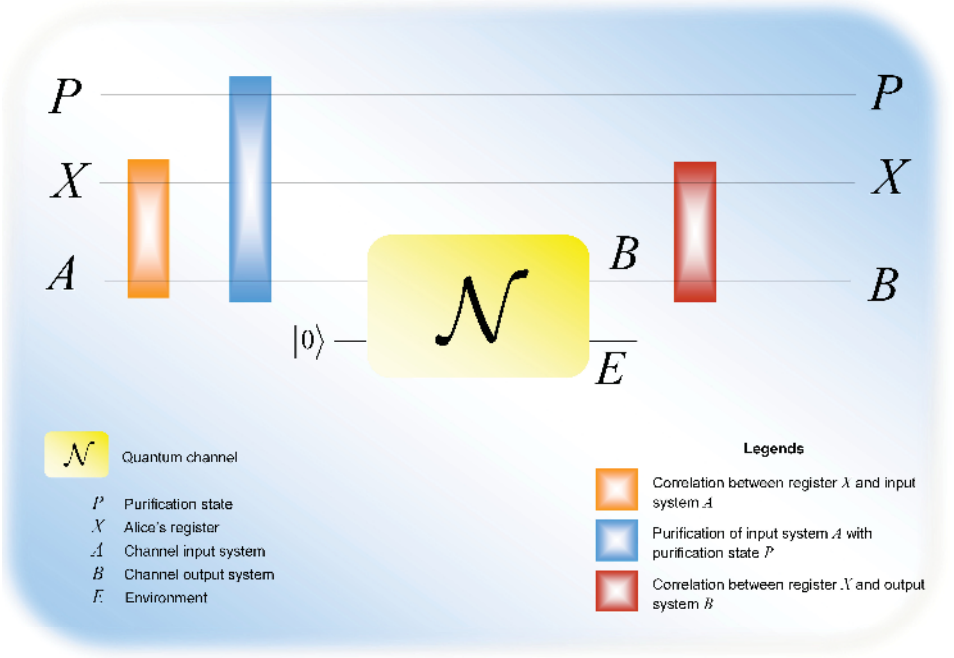

Fig. 5: Detailed model of a quantum communication channel exposing the interaction with the environment. Alice's register is denoted by *X*, the input system is *A* while *P* is the purification state. The environment of the channel is denoted by *E*, the output of the channel is *B*. The quantum channel has positive classical capacity if and only if the channel output system *B* will be correlated with Alice's register *X*.

From the purified system state $|\varphi\rangle_{PA}$, the original system state ρ_A can be expressed with the partial trace operator (see Appendix) $Tr_P(\cdot)$, which operator traces out the purification state from the system

$$\rho_A = Tr_P\left(|\varphi\rangle\langle\varphi|_{PA}\right). \tag{78}$$

From joint system (77) and the purified state (78), one can introduce a new definition. The *extension* of ρ_A can be given as

$$\rho_A = Tr_P\left(\omega_{PA}\right), \tag{79}$$

where ω_{PA} is the joint system of purification state *P* and channel input *A* [538], which represents a noisy state.

2) Isometric Extension: *Isometric extension* has utmost importance, because it helps us to understand what happens between the quantum channel and its environment whenever a quantum state is transmitted from Alice to Bob. Since the channel and the environment together form a closed physical system the isometric extension of the quantum channel $\mathcal{N}$ is the *unitary representation* of the channel

$$\mathcal{N}: U_{A\to BE}, \tag{80}$$

enabling the 'one-sender and two-receiver' view: beside Alice the sender, both Bob and the environment of the channel are playing the receivers. In other words, the output of the noisy quantum channel $\mathcal{N}$ can be described only after the environment of the channel is traced out

$$\rho_B = Tr_E\left(U_{A\to BE}\left(\rho_A\right)\right) = \mathcal{N}\left(\rho_A\right). \tag{81}$$

3) Kraus Representation: The map of the quantum channel can also be expressed by means of a special tool called the *Kraus Representation*. For a given input system ρ_A and quantum channel $\mathcal{N}$, this representation can be expressed as

$$\mathcal{N}\left(\rho_A\right) = \sum_i N_i \rho_A N_i^\dagger, \tag{82}$$

where N_i are the Kraus operators, and $\sum_i N_i^\dagger N_i = I$. The isometric extension of $\mathcal{N}$ by means of the *Kraus Representation* can be expressed as

$$\rho_B = \mathcal{N}\left(\rho_A\right) = \sum_i N_i \rho_A N_i^\dagger \to U_{A\to BE}\left(\rho_A\right) = \sum_i N_i \otimes |i\rangle_E. \tag{83}$$

The action of the quantum channel $\mathcal{N}$ on an operator $|k\rangle\langle l|$, where $\{|k\rangle\}$ form an orthonormal basis also can be given in operator form using the Kraus operator $N_{kl} = \mathcal{N}\left(|k\rangle\langle l|\right)$. By exploiting the property $UU^\dagger = P_{BE}$, for the input quantum system ρ_A

$$\begin{aligned} \rho_B &= U_{A\to BE}\left(\rho_A\right) = U\rho_A U^\dagger \\ &= \left(\textstyle\sum_i N_i \otimes |i\rangle_E\right) \rho_A \left(\sum_j N_j^\dagger \otimes \langle j|_E\right) \\ &= \textstyle\sum_{i,j} N_i \rho_A N_j^\dagger \otimes |i\rangle\langle j|_E. \end{aligned} \tag{84}$$

If we trace out the environment, we get the equivalence of the two representations

$$\rho_B = Tr_E\left(U_{A\to BE}\left(\rho_A\right)\right) = \sum_i N_i \rho_A N_i^\dagger. \tag{85}$$

4) The von Neumann Entropy: Quantum information processing exploits the quantum nature of information. It offers fundamentally new solutions in the field of computer science

and extends the possibilities to a level that cannot be imagined in classical communication systems. On the other hand, it requires the generalization of classical information theory through a quantum perception of the world. As Shannon entropy plays fundamental role in classical information theory, the von Neumann entropy does the same for quantum information. The von Neumann entropy $\mathrm{S}(\rho)$ of quantum state ρ can be viewed as an extension of classical entropy for quantum systems. It measures the information of the quantum states in the form of the uncertainty of a quantum state. The classical Shannon entropy $H(X)$ of a variable *X* with probability distribution $p(X)$ can be defined as

$$H(X) = -\sum_{x \in X} p(x) \log(p(x)), \tag{86}$$

with $1 \leq H(X) \leq \log(|X|)$, where $|X|$ is the cardinality of the set *X*.

The von Neumann entropy

$$\mathrm{S}(\rho) = -Tr(\rho \log(\rho)) \tag{87}$$

measures the information contained in the quantum system ρ. Furthermore $\mathrm{S}(\rho)$ can be expressed by means of the Shannon entropy for the eigenvalue distribution

$$\mathrm{S}(\rho) = H(\lambda) = -\sum_{i=1}^{d} \lambda_i \log(\lambda_i), \tag{88}$$

where *d* is the level of the quantum system and λ_i are the eigenvalues of density matrix ρ.

5) The Holevo Quantity: The *Holevo bound* determines the amount of information that can be extracted from a single qubit state. If Alice sends a quantum state ρ_i with probability p_i over an ideal quantum channel, then at Bob's receiver a mixed state

$$\rho_B = \rho_A = \sum_i p_i \rho_i \tag{89}$$

appears. Bob constructs a measurement $\{M_i\}$ to extract the information encoded in the quantum states. If he applies the measurement to ρ_A, the probability distribution of Bob's classical symbol *B* will be $\Pr[b|\rho_A] = Tr\left(M_b^\dagger M_b \rho_A\right)$. As had been shown by Holevo [231], the bound for the maximal classical mutual information between Alice and Bob is

$$I(A{:}B) \leq \mathrm{S}(\rho_A) - \sum_i p_i \mathrm{S}(\rho_i) \equiv \chi, \tag{90}$$

where χ is called the *Holevo quantity, and* (90) known as the *Holevo bound*.

In classical information theory and classical communication systems, the mutual information $I(A{:}B)$ is bounded only by the classical entropy of $H(A)$, hence $I(A{:}B) \leq H(A)$. The mutual information $I(A{:}B)$ is bounded by the classical entropy of $H(A)$, hence $I(A{:}B) \leq H(A)$. On the other hand, for mixed states and pure non-orthogonal states the Holevo quantity χ can be greater than the mutual information $I(A{:}B)$, however, it is still bounded by $H(A)$, which is the bound for the pure orthogonal states

$$I(A{:}B) \leq \chi \leq H(A). \tag{91}$$

The *Holevo bound* highlights the important fact that one qubit can contain at most one classical bit i.e., cbit of information.

6) Quantum Conditional Entropy: While the classical conditional entropy function is always takes a non negative value, the *quantum conditional entropy can be negative*. The quantum conditional entropy between quantum systems *A* and *B* is given by

$$\mathrm{S}(A|B) = \mathrm{S}(\rho_{AB}) - \mathrm{S}(\rho_B). \tag{92}$$

If we have two uncorrelated subsystems ρ_A and ρ_B, then the information of the quantum system ρ_A does not contain any information about ρ_B, or reversely, thus

$$\mathrm{S}(\rho_{AB}) = \mathrm{S}(\rho_A) + \mathrm{S}(\rho_B), \tag{93}$$

hence we get $\mathrm{S}(A|B) = \mathrm{S}(\rho_A)$, and similarly $\mathrm{S}(B|A) = \mathrm{S}(\rho_B)$. The negative property of conditional entropy $\mathrm{S}(A|B)$ can be demonstrated with an *entangled* state, since in this case, the joint quantum entropy of the joint state less than the sum of the von Neumann entropies of its individual components. For a pure entangled state, $\mathrm{S}(\rho_{AB}) = 0$, while $\mathrm{S}(\rho_A) = \mathrm{S}(\rho_B) = 1$ since the two qubits are in *maximally mixed* $\frac{1}{2}I$ state, which is classically totally unimaginable. Thus, in this case

$$\mathrm{S}(A|B) = -\mathrm{S}(\rho_B) \leq 0, \tag{94}$$

and $\mathrm{S}(B|A) = -\mathrm{S}(\rho_A) \leq 0$ and $\mathrm{S}(\rho_A) = \mathrm{S}(\rho_B)$.

7) Quantum Mutual Information: The classical mutual information $I(\cdot)$ measures the information correlation between random variables *A* and *B*. In analogue to classical information theory, $I(A{:}B)$ can be described by the quantum entropies of individual states and the von Neumann entropy of the joint state as follows:

$$I(A{:}B) = \mathrm{S}(\rho_A) + \mathrm{S}(\rho_B) - \mathrm{S}(\rho_{AB}) \geq 0, \tag{95}$$

i.e., the quantum mutual information is always a non negative function. However, there is a distinction between classical and quantum systems, since the quantum mutual information can take its value above the maximum of the classical mutual information. This statement can be confirmed, if we take into account that for an pure entangled quantum system, the quantum mutual information is

$$I(A{:}B) = \mathrm{S}(\rho_A) + \mathrm{S}(\rho_B) - \mathrm{S}(\rho_{AB}) = 1 + 1 - 0 = 2, \tag{96}$$

and we can rewrite this equation as

$$I(A{:}B) = 2\mathrm{S}(\rho_A) = 2\mathrm{S}(\rho_B). \tag{97}$$

For some pure joint system ρ_{AB}, the equation (97) can be satisfied such that $\mathrm{S}(\rho_A) = \mathrm{S}(\rho_B)$ and $\mathrm{S}(\rho_{AB}) = 0$.

If we use entangled states, the quantum mutual information could be 2, while the quantum conditional entropies could be 2. In classical information theory, negative entropies can be obtained only in the case of mutual information of three or more systems. An important property of maximized quantum mutual information: *it is always additive for a quantum channel*.

The character of classical information and quantum information is significantly different. There are many phenomena in quantum systems which cannot be described classically, such as entanglement, which makes it possible to store quantum information in the correlation of quantum states. Similarly, a

quantum channel can be used with pure orthogonal states to realize classical information transmission, or it can be used to transmit non-orthogonal states or even quantum entanglement. Information transmission also can be approached using the question, whether the input consists of unentangled or entangled quantum states. This leads us to say that for quantum channels many new capacity definitions exist in comparison to a classical communication channel. In possession of the general communication model and the quantities which are able to represent information content of quantum states we can begin to investigate the possibilities and limitations of information transmission through quantum channels [304].

8) Quantum Relative Entropy: The *quantum relative entropy* measures the informational distance between quantum states, and introduces a deeper characterization of the quantum states than the von Neumann entropy. Similarly to the classical relative entropy, this quantity measures the distinguishability of the quantum states, in practice it can be realized by POVM measurements. The relative entropy classically is a measure that quantifies how close a probability distribution *p* is to a model or candidate probability distribution *q*. For probability distributions *p* and *q,* the classical relative entropy is given by

$$D\left(p\|\,q\right)=\sum_{i}p_{i}\log\left(\frac{p_{i}}{q_{i}}\right), \tag{98}$$

while the quantum relative entropy between quantum states ρ and σ is

$$\begin{aligned} D\left(\rho\|\,\sigma\right) &= Tr\left(\rho\log\left(\rho\right)\right)-Tr\left(\rho\log\left(\sigma\right)\right) \\ &= Tr\left[\rho\left(\log\left(\rho\right)-\log\left(\sigma\right)\right)\right]. \end{aligned} \tag{99}$$

In the definition above, the term $Tr\left(\rho\log\left(\sigma\right)\right)$ is finite only if $\rho\log\left(\sigma\right)\geq 0$ for all diagonal matrix elements. If this condition is not satisfied, then $D\left(\rho\|\,\sigma\right)$ could be infinite, since the trace of the second term could go to infinity.

The *quantum informational distance* (i.e., quantum relative entropy) has some distance-like properties (for example, the quantum relative entropy function between a maximally mixed state and an arbitrary quantum state is symmetric, hence in this case it is not just a pseudo distance), however it is *not commutative*, thus $D\left(\rho\,\|\sigma\right)\neq D\left(\sigma\,\|\rho\right)$, and $D\left(\rho\,\|\sigma\right)\geq 0$ iff $\rho\neq\sigma$, and $D\left(\rho\,\|\sigma\right)=0$ iff $\rho=\sigma$. Note, if σ has zero eigenvalues, $D\left(\rho\,\|\sigma\right)$ may diverge, otherwise it is a finite and continuous function. Furthermore, the quantum relative entropy function has another interesting property, since if we have two density matrices ρ and σ, then the following property holds for the traces used in the expression of $D\left(\rho\,\|\sigma\right)$

$$Tr\left(\rho\log\left(\rho\right)\right)\geq Tr\left(\rho\log\left(\sigma\right)\right). \tag{100}$$

The symmetric Kullback-Leibler distance is widely used in classical systems, for example in computer vision and sound processing. Quantum relative entropy reduces to the classical Kullback-Leibler relative entropy for simultaneously diagonalizable matrices.

We note, the quantum mutual information can be defined by quantum relative entropy $D\left(\cdot\|\,\cdot\right)$. This quantity can be regarded as the informational distance between the tensor product of the individual subsystems $\rho_A\otimes\rho_B$, and the joint state ρ_{AB} as follows:

$$I\left(A{:}B\right)=D\left(\rho_{AB}\|\,\rho_A\otimes\rho_B\right)=\mathrm{S}\left(\rho_A\right)+\mathrm{S}\left(\rho_B\right)-\mathrm{S}\left(\rho_{AB}\right). \tag{101}$$

9) Quantum Rényi-Entropy: As we have seen, the quantum informational entropy can be defined by the $\mathrm{S}\left(\rho\right)$ von Neumann entropy function. On the other hand, another entropy function can also be defined in the quantum domain, it is called the Rényi-entropy and denoted by $\mathrm{R}\left(\rho\right)$. This function has relevance mainly in the description of quantum entanglement. The Rényi-entropy function is defined as follows

$$\mathrm{R}\left(\rho\right)=\frac{1}{1-r}Tr(\rho^{r}), \tag{102}$$

where $r\geq 0$, while $\mathrm{R}\left(\rho\right)$ is equal to the von Neumann entropy function $\mathrm{S}\left(\rho\right)$ if

$$\lim_{r\to 1}\mathrm{R}\left(\rho\right)=\mathrm{S}\left(\rho\right). \tag{103}$$

If parameter *r* converges to infinity, then we have

$$\lim_{r\to\infty}\mathrm{R}\left(\rho\right)=-\log\left(\|\rho\|\right). \tag{104}$$

On the other hand if $r=0$ then $\mathrm{R}\left(\rho\right)$ can be expressed from the rank of the density matrix

$$\mathrm{R}\left(\rho\right)=\log\left(rank\left(\rho\right)\right). \tag{105}$$

I. Related Work

The field of quantum information processing is a rapidly growing field of science, however there are still many challenging questions and problems. These most important results will be discussed in further sections, but these questions cannot be exposited without a knowledge of the fundamental results of quantum information theory.

1) Early Years of quantum information theory: quantum information theory extends the possibilities of classical information theory, however for some questions, it gives extremely different answers. The advanced communications and quantum networking technologies offered by quantum information processing will revolutionize traditional communication and networking methods. Classical information theory— was founded by Claude Shannon in 1948 [209], [477]. In Shannon's paper the mathematical framework of communication was invented, and the main definitions and theorems of classical information theory were laid down. On the other hand, classical information theory is just one part of quantum information theory. The other, missing part is the Quantum Theory, which was completely finalized in 1926.

The results of quantum information theory are mainly based on the results of von Neumann, who constructed the mathematical background of quantum mechanics [395]. An interesting—and less well known—historical fact is that quantum entropy was discovered by Neumann before the classical information theoretic concept of entropy. Quantum entropy was discovered in the 1930s, based on the older idea of entropy in classical Statistical Mechanics, while the classical information theoretic concept was discovered by Shannon only later, in 1948. It is an interesting note, since the reader might have thought that

quantum entropy is an extension of the classical one, however it is not true. Classical entropy, in the context of Information Theory, is a special case of von Neumann's quantum entropy. Moreover, the name of Shannon's formula was proposed by von Neumann. Further details about the history of Quantum Theory, and the main results of physicists from the first half of the twentieth century——such as Planck, Einstein, Schrödinger, Heisenberg, or Dirac——can be found in the works of Misner et al. [325], McEvoy [318], Sakurai [454], Griffiths [190] or Bohm [76].

'*Is quantum mechanics useful*'— asked by Landauer in 1995 [291]. Well, having the results of this paper in our hands, we can give an affirmative answer: *definitely yes*. An interesting work about the importance of quantum mechanical processes was published by Dowling [144]. Some fundamental results from the very early days of Quantum Mechanics can be found in [92], [141], [152], [153], [175], [225], [441], [458], [459], [512]. About the early days of Information Theory see the work of Pierce [440]. A good introduction to Information Theory can be found in the work of Yeung [560]. More information about the connection of Information Theory and statistical mechanics can be found in work of Aspect from 1981 [23], in the book of Jaynes [251] or Petz [428]. The elements of classical information theory and its mathematical background were summarized in a very good book by Cover [116]. On matrix analysis a great work was published by Horn and Johnson [234].

A very good introduction to quantum information theory was published by Bennett and Shor [65]. The idea that the results of quantum information theory can be used to solve computational problems was first claimed by Deutsch in 1985 [133].

Later in the 90s, the answers to the most important questions of quantum information theory were answered, and the main elements and the fundamentals of this field were discovered. Details about the simulation of quantum systems and the possibility of encoding quantum information in physical particles can be found in Feynman's work from 1982 [160]. Further information on quantum simulators and continuous-time automata can be found in the work of Vollbrecht and Cirac [526].

2) Quantum Coding and Quantum Compression: The next milestone in quantum information theory is Schumacher's work from 1995 [466] in which he introduced the term, '*qubit*.' In [465, 466, 467, 468] the main theories of quantum source coding and the quantum compression were presented. The details of quantum data compression and quantum typical subspaces can be found in [466]. In this paper, Schumacher extended those results which had been presented a year before, in 1994 by Schumacher and Jozsa on a new proof of quantum noiseless coding, for details see [464]. Schumacher in 1995 also defined the quantum coding of pure quantum states; in the same year, Lo published a paper in which he extended these result to mixed quantum states, and he also defined an encoding scheme for it [306]. Schumacher's results from 1995 on the compression of quantum information [466] were the first main results on the encoding of quantum information—— *its importance and significance in quantum information theory is similar to Shannon's noiseless channel coding theorem in classical information theory*. In this work, Schumacher also gives upper and lower bounds on the rate of quantum compression. We note, that the mathematical background of Schumacher proof is very similar to Shannon's proof, as the reader can check in [466] and in Shannon's proof [477].

The method of sending classical bits via quantum bits was firstly completed by Schumacher et al. in their famous paper form 1995, see [465]. In the same year, an important paper on the encoding of information into physical particles was published by Schumacher [465, 466]. The fundaments of noiseless quantum coding were laid down by Schumacher, one year later, in 1996 [467, 468]. In 1996, many important results were published by Schumacher and his colleges. These works cover the discussion of the relation of entropy exchange and coherent quantum information, which was completely unknown before 1996. The theory of processing of quantum information, the transmission of entanglement over a noisy quantum channel, the error-correction schemes with the achievable fidelity limits, or the classical information capacity of a quantum channel with the limits on the amount of accessible information in a quantum channel were all published in the same year. For further information on the fidelity limits and communication capabilities of a noisy quantum channel, see the work of Barnum et al. also from 1996 [45]. In 1997, Schumacher and Westmoreland completed their proof on the classical capacity of a quantum channel, and they published in their famous work, for details see [469]. These results were extended in their works from 1998, see [470-472]. On the experimental side of fidelity testing see the work of Radmark et al. [446].

About the limits for compression of quantum information carried by ensembles of mixed states, see the work of Horodecki [240]. An interesting paper about the quantum coding of mixed quantum states was presented by Barnum et al. [42]. Universal quantum compression makes it possible to compress quantum information without the knowledge about the information source itself which emits the quantum states. Universal quantum information compression was also investigated by Jozsa et al. [258], and an extended version of Jozsa and Presnell [256]. Further information about the technique of universal quantum data compression can be found in the article of Bennett et al. [56]. The similarity of the two schemes follows from the fact that in both cases we compress quantum information, however in the case of Schumacher's method we do not compress entanglement. The two compression schemes are not equal to each other, however in some cases——if running one of the two schemes fails——they can be used to correct the errors of the other, hence they can be viewed as auxiliary protocols of each other. Further information about the mathematical background of the processes applied in the compression of quantum information can be found in Elias's work [155].

A good introduction to quantum error-correction can be found in the work of Gottesman, for details see [188]. A paper about classical data compression with quantum side information was published by Devetak and Winter [134]. We note that there is a connection between the compression of quantum information and the concentration of entanglement,

however the working method of Schumacher's encoding and the process of entanglement concentrating are completely different. Benjamin Schumacher and Richard Jozsa published a very important paper in 1994 [464]. Here, the authors were the first to give an explicit proof of the quantum noiseless coding theorem, which was a milestone in the history of quantum computation. Further information on Schumacher's noiseless quantum channel coding can be found in [464].

The basic coding theorems of quantum information theory were summarized by Winter in 1999 [547]. In this work, he also analyzed the possibilities of compressing quantum information. A random coding based proof for the quantum coding theorem was shown by Klesse in 2008 [277]. A very interesting article was presented by Horodecki in 1998 [240], about the limits for the compression of quantum information into mixed states. On the properties of indeterminate-length quantum coding see the work of Schumacher and Westmoreland [461].

The quantum version of the well-known Huffman coding can be found in the work of Braunstein et al. from 2000 [88]. Further information about the compression of quantum information and the subspaces can be found in [169], [223], and [224]. The details of quantum coding for mixed states can be found in the work of Barnum et al. [42].

3) Quantum Entanglement: Entanglement is one of the most important differences between the classical and the quantum worlds. An interesting paper on communication via one- and two-particle operators on Einstein-Podolsky-Rosen states was published in 1992, by Bennett [58]. About the history of entanglement see the paper of Einstein, Podolsky and Rosen from 1935 [153]. In this manuscript, we did not give a complete mathematical background of quantum entanglement—further details on this topic can be found in Nielsen's book [403] or by Hayashi [220], or in an very good article published by the four Horodeckis in 2009 [239]. We have seen that entanglement concentration can be applied to generate maximally mixed entangled states. We also gave the asymptotic rate at which entanglement concentration can be made, it is called the entropy of entanglement and we expressed it in an explicit form. A very important paper on the communication cost of entanglement transformations was published by Hayden and Winter, for details see [221]. The method of entanglement concentration was among the first quantum protocols, for details see the work of Bennett et al. from 1996 [63]. The method of Bennett's was improved by Nielsen in 1999, [405]. A very important work on variable length universal entanglement concentration by local operations and its application to teleportation and dense coding was published by Hayashi and Matsumoto [217]. The entanglement cost of antisymmetric states was studied by [317].

The calculation of entanglement-assisted classical capacity requires a superdense protocol-like encoding and decoding strategy,——we did not explain its working mechanism in detail, further information can be found in the work of Bennett et al. [54]. A paper about the compression of quantum-measurement operations was published by Winter and Massar in 2001 [543]. Later, in 2004, Winter extended these results [544]. Here we note, these results are based on the work of Ahlswede and Winter [8].

The definition of a conditionally typical subspace in quantum information was given by Schumacher and Westmoreland in 1997 [469]. Holevo also introduced it in 1998 [233].

We did not explain in detail entanglement concentrating [63], entanglement transformations [405], or entanglement generation, entanglement distribution and quantum broadcasting,——further information can be found in [217], [221], [241], [542], [555], [556]. About the classical communication cost of entanglement manipulation see the work of Lo and Popescu from 1999 [307]. The fact that noncommuting mixed states cannot be broadcast was shown by Barnum et al. in 1995, see [44].

Lo and Popescu also published a work on concentrating entanglement by local actions in 2001, for details see [305]. About the purification of noisy entanglement see the article of Bennett et al. from 1996 [62]. The entanglement purification protocol was a very important result, since it will have great importance in the quantum capacity of a quantum channel. (However, when the authors have developed the entanglement purification scheme, this connection was still not completely cleared.)

About the quantum networks for concentrating entanglement and the distortion-free entanglement concentration, further information can be found in the paper of Kaye and Mosca from 2001 [262]. In 2005, Devetak and Winter have shown, that there is a connection between the entanglement distillation and the quantum coherent information, which measure has tremendous relevance in the quantum capacity of the quantum channels, for details see [137, 137]. An interesting paper about distortion-free entanglement concentration was published by Kohout et al. in 2009 [281]. The method presented in that paper gives an answer to streaming universal. We did not mentioned the inverse protocol of entanglement concentration which is called entanglement dilution, for further details see the works of Lo and Popescu from 1999 [307] and 2001 [305], and Harrow and Lo's work from 2004 [213]. Harrow and Lo have also given an explicit solution of the communication cost of the problem of entanglement dilution, which was an open question until 2004. Their results are based on the previous work of Hayden and Winter from 2003, for details see [221]. The typical entanglement in stabilizer states was studied by Smith and Leung, see [495]. The teleportation-based realization of a two-qubit entangling gate was shown by Gao et al. [173].

4) Quantum Channels: About the statistical properties of the HSW theory and the general HSW capacity, a very interesting paper was published by Hayashi and Nagaoka in 2003 [218]. As we have seen, some results of quantum information theory are similar to the results of classical information theory, however many things have no classical analogue. As we have found in this section, the Holevo theorem gives an information-theoretic meaning to the von Neumann entropy, however it does not make it possible to use it in the case of the interpretation of von Neumann entropy of physical macrosystems. Further properties of the von Neumann entropy function was studied by Audenaert in 2007 [25].

The concept of quantum mutual information measures the

classical information which can be transmitted through a noisy quantum channel (originally introduced by Adami and Cerf [4]) however it cannot be used to measure the maximal transmittable quantum information. The maximized quantum mutual information is always additive, however this is not true for the Holevo information. In this case, the entanglement makes non-additive the Holevo information, but it has no effect on the quantum mutual information. Further information about the mathematical background of these 'strange' phenomena can be found in the work of Adami from 1996 [4] or in the book of Hayashi from 2006 [220]. A very good book on these topics was published by Petz in 2008 [428].

For the properties of Holevo information and on the capacity of quantum channels see the works of Holevo [231], [233], Schumacher and Westmoreland [464, 465, 466, 467, 468, 469], Horodecki [237], Datta [127], Arimoto [18]. On the geometrical interpretation of the maps of a quantum channel see the works of Cortese [114], Petz [427-433], [435], Hiai [229].

On physical properties of quantum communication channels the work of Levitin [295], on the capacities of quantum communication channels see Bennett [64], DiVincenzo [142], Schumacher [469], Fuchs [165]. In 1997, Barnum, Smolin and Terhal also summarized the actual results on quantum channel, see [47].

The mathematical background of distinguishing arbitrary multipartite basis unambiguously was shown by Duan et al. [146].)

In 2010, Dupis et al. [148] published a paper in which they described a protocol for quantum broadcast quantum channel, then Jon Yard et al. published a paper on quantum broadcast channels [557]. Before these results, in 2007, an important practical result on broadcasting was shown by Guha et al. [192], [193], who demonstrated the classical capacity of practical (bosonic) quantum channels. General quantum protocols—such as super-dense coding and teleportation—are not described in this article. Further information about these basic quantum protocols can be found in the book of Hayashi from 2006 [220], in the book of Nielsen and Chuang [403], or in the paper of Bennett and Wiesner [58], and [59], (both papers from 1992),, and Bennett's paper from 1993 [60].

A very good overview of the capacity of quantum channels was presented by Smith in 2010, see [504]. About the information tradeoff relations for finite-strength quantum measurements, see the works of [163]. On the mathematical background of quantum communication see the works of [435], Ruskai et al. [451], and [219], [525]. The generalized Pauli channels are summarized by Ohno and Petz in [408].

The relative entropy function was introduced by Solomon Kullback and Richard Leibler in 1951 [285]. Another interpretation of the relative entropy function was introduced by Bregman, known as the class of Bregman divergences [89]. A very important paper about the role of relative entropy in quantum information theory was published by Schumacher and Westmoreland in 2000 [463]. The quantum relative entropy function was originally introduced by Umegaki, and later modified versions have been defined by Ohya, Petz and Watanbe [409]. Some possible applications of quantum relative entropy in quantum information processing were introduced by Vedral [524].

About the negativity of quantum information see the works of Horodecki et al. [237], [238]. About the use of entanglement in quantum information theory, see the work of Li et al. from 2010, [297], [299]. A method for measuring two-qubit entanglement by local operations and classical communication was shown by Bai et al. in 2005 [40]. About the additivity of the capacity of quantum channels see [167], [274] and [488]. A very good paper on the Holevo capacity of finite dimensional quantum channels and the role of additivity problem in quantum information theory was published by Shirokov [486]. A great summary of classical and quantum information theory can be found in the book of Desurvire from 2009 [132]. The bounds for the quantity of information transmittable by a quantum communication channel was analyzed by Holevo in 1973, see [231]. About sending classical information via noisy quantum channels, see the works of Schumacher and Jozsa [464], Schumacher from 1996 [467, 468], and Schumacher and Westmoreland from 1997 [469] and Smith's summarize [504]. The mathematical background of classical relative entropy function can be found in the works of Kullback and Leibler [285], [286], and [288]. For the details of Bregman distance see [89] and [41]. Further information about the Kraft-McMillan inequality can be found in [284], [319] and [116].

For research on satellite quantum communications, see [35, 36, 37, 38], [172]. For research results on quantum repeaters see [32], [74], [90], [150], [254], [289], [309], [330-332], [455], [520, 521, 522, 523], and [563]. For some further research topic on quantum channels see [34], [419, 420], [194-197,198-199, 200, 201, 202-205, 206], [246].

5) Comprehensive Surveys: A reader who is interested in the complete mathematical background of quantum information theory can find the details for example in Nielsen and Chuang's book [403]. For a general introduction to the quantum information theory and its applications see the excellent book of Hayashi [220]. We also suggest the book of Imre from 2005, see [244]. A very good introduction to quantum information theory was published by Bennett and Shor, for details see [65]. Also in 1998, Preskill summarized the actual state of quantum information theory in the form of lecture notes [443]. Preskill also summarized the conditions of reliable quantum computers, for details see [444]. Also in 1998, a1998, a good work on the basics of quantum computations and the mathematical formalism was published by Vedral and Plenio [525] and by Nielsen [404]. On the mathematical background of quantum information processing, see the works of Shor [491, 492, 493], [494], [487], and [489]. The description of classical data compression can be found in the very good book of Cover and Thomas [116], or in the book of Berger [71]. We also suggest the work of Stinespring [510]. A very important result regarding the compression of classical information was published by Csiszár and Körner in 1978 [117], and later the authors published a great book about coding theorems for discrete memoryless systems [118]. A work on the non-additivity of Renyi entropy was published by Aubrun et al. [24]. On the connection of quantum entanglement and classi-

cal communication through a depolarizing channel see [93]. Regarding the results of quantum Shannon theory, we suggest the great textbook of Wilde [538]. The structure of random quantum channels, eigenvalue statistics and entanglement of random subspaces are discussed in [110], [111]. Finally, for an interesting viewpoint on 'topsy turvy world of quantum computing' see [329].

III. Classical Capacities of a Quantum Channel

Communication over quantum channels is bounded by the corresponding capacities. Now, we lay down the fundamental theoretic results on *classical capacities of quantum channel*s. These results are all required to analyze the advanced and more promising properties of quantum communications.

This section is organized as follows. In the first part, we introduce the reader to formal description of a noisy quantum channel. Then we start to discuss the classical capacity of a quantum channel. Next, we show the various encoder and decoder settings for transmission of classical information. We define the exact formula for the measure of maximal transmittable classical information. Finally, we discuss some important channel maps.

The most relevant works are included in the Related Work subsection.

A. Extended Formal Model

The discussed model is general enough to analyze the limitations for information transfer over quantum channels. However, later we will investigate special quantum channels which models specific physical environment. Each quantum channel can be represented as a CPTP map (*Completely Positive Trace Preserving*), hence the process of information transmission through a quantum communication channel can be described as a quantum operation.

The general model of a quantum channel describes the transmission of an input quantum bit, and its interaction with the environment (see Fig. 6. Assuming Alice sends quantum state ρ_A into the channel this state becomes entangled with the environment ρ_E, which is initially in a pure state $|0\rangle$. For a mixed input state a so called *purification state P* can be defined, from which the original mixed state can be restored by a partial trace (see Appendix) of the pure system $\rho_A P$. The unitary operation U_{AE} of a quantum channel $\mathcal{N}$ entangles $\rho_A P$ with the environment ρ_E, and outputs Bob's mixed state as ρ_B (and the purification state as P). The purification state is a reference system, it cannot be accessed, it remains the same after the transmission.

The output of the noisy quantum channel is denoted by ρ_B, the post state of the environment by ρ_E, while the post-purification state after the output realized on the channel output is depicted by P.

B. Capacity of Classical Channels

Before we start to investigate quantum channels, we survey the results of transmitting information over classical noisy channels. In order to achieve reliable (error-free) information transfer we use the so called *channel codin*g which extends the payload (useful) information bits with redundancy bits so that at the receiver side Bob will be able to correct some amount of error by means of this redundancy.

The channel is given an input *A,* and maps it probabilistically (it is a *stochastic* mapping, not a unitary or deterministic transformation) to an output *B,* and the probability of this mapping is denoted by $p(B|A)$.

The *channel capacity* $C(N)$ of a *classical* memoryless communication channel *N* gives an upper bound on the number of classical bits which can be transmitted per channel use, in reliable manner, i.e., with arbitrarily small error at the receiver. As it has been proven by Shannon the capacity $C(N)$ of a noisy classical memoryless communication channel *N*, can be expressed by means of the maximum of the mutual information $I(A{:}B)$ over all possible input distributions $p(x)$ of random variable *X*

$$C(N) = \max_{p(x)} I(A{:}B). \tag{106}$$

In order to make the capacity definition more plausible let us consider Fig. 7. Here, the effect of environment *E* is represented by the classical conditional entropies $H(A{:}E|B) > 0$ and $H(B{:}E|A) > 0$.

Shannon's noisy coding theorem claims that forming *K* different codewords $m = \log K$ of length from the source bits and transmitting each of them using the channel *n* times (*m* to *n* coding) the rate at which information can be transmitted through the channel is

$$R = \frac{\log(K)}{n}, \tag{107}$$

and exponentially small probability of error at this rate can be achieved only if $R \leq C(N)$, otherwise the probability of the successful decoding exponentially tends to zero, as the number of channel uses increases. Now, having introduced the capacity of classical channel it is important to highlight the following distinction. The asymptotic capacity of any channel describes that rate, which can be achieved if the channel can be used *n* times (denoted by $N^{\otimes n}$), where where $n \to \infty$. Without loss of generality, in case of $n = 1$ we speak about single-use capacity. Multiple channel uses can be implemented in consecutive or parallel ways, however from practical reasons we will prefer the latter one.

C. Transmission of Classical Information over Noisy Quantum Channels

As the next step during our journey towards the quantum information transfer through quantum channels (which is the most general case) we are leaving the well-known classical (macro) world and just entering into the border zone. Similar to the ancient Romans - who deployed a sophisticated wide border defense system (called *the limes* which consisted of walls, towers, rivers, etc.), instead of drawing simply a red line between themselves and the barbarians – we remain classical in terms of inputs and outputs but allow the channel operating in a quantum manner.

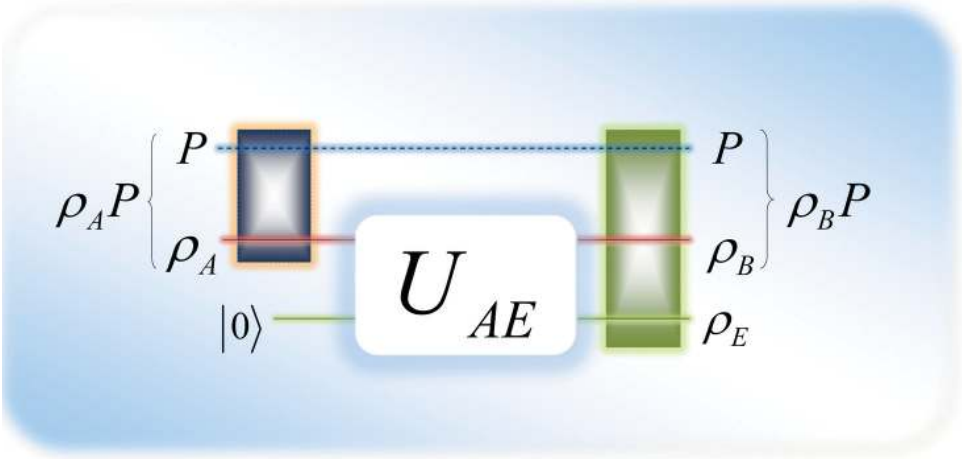

Fig. 6: The formal model of a noisy quantum communication channel. The output of the channel is a mixed state.

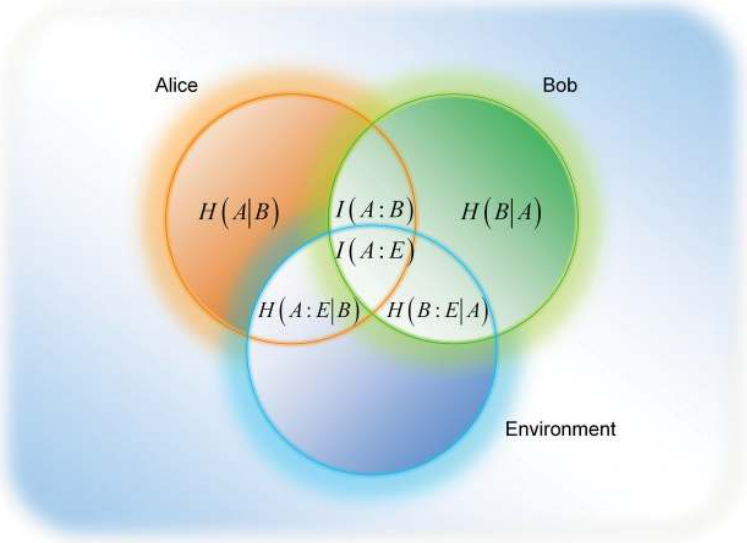

Fig. 7: The effects of the environment on the transmittable information and on the receiver's uncertainty.

Quantum channels can be used in many different ways to transmit information from Alice to Bob. Alice can send classical bits to Bob, but she also has the capability of transmitting quantum bits. In the first case, we talk about the classical capacity of the quantum channel, while in the latter case, we have a different measure - the quantum capacity. The map of the channel is denoted by $\mathcal{N}$, which is trace preserving if

$$Tr\left(\mathcal{N}\left(\rho\right)\right) = Tr\left(\rho\right) \tag{108}$$

for all density matrices ρ, and positive if the eigenvalues of $\mathcal{N}\left(\rho\right)$ are non-negative whenever the eigenvalues of ρ are non-negative.

Compared to classical channels – which have only one definition for capacity – the transmittable classical information and thus the corresponding capacity definition can be different when one considers quantum channels. This fact splits the classical capacity of quantum channels into three categories, namely the (*unentangled*) *classical (*also known as the *product-state* classical capacity, or the HSW (Holevo-Schumacher-Westmoreland) capacity*) capacity* $C\left(\mathcal{N}\right)$, *private classical capacity* $P\left(\mathcal{N}\right)$ and *entanglement-assisted classical capacity* $C_E\left(\mathcal{N}\right)$.

The (*unentangled*) *classical capacity* $C\left(\mathcal{N}\right)$ is a natural extension of the capacity definition from classical channels to the quantum world. For the sake of simplicity the term *classical capacity* will refer to the *unentangled* version in the forthcoming pages of this paper. (The entangled version will be referred as the entanglement-assisted classical capacity. As we will see, the HSW capacity is defined for product state inputs; however it is possible to extend it for entangled input states)

The *private classical capacity* $P\left(\mathcal{N}\right)$ has deep relevance in secret quantum communications and quantum cryptography. It describes the rate at which Alice is able to send classical information through the channel in secure manner. Security here means that an eavesdropper will not be able to access

the encoded information without revealing her/himself.

The *entanglement-assisted classical capacity* $C_E(\mathcal{N})$ measures the classical information which can be transmitted through the channel, if Alice and Bob have already shared entanglement before the transmission. A well-known example of such protocols is '*superdense coding*' [244]. Next, we discuss the above listed various classical capacities of quantum channels in detail.

As the first obvious generalization of classical channel capacity definition is if we maximize the quantum mutual information over all possible input ensembles

$$C(\mathcal{N}) = \max_{allp_i,\rho_i} I(A{:}B). \tag{109}$$

Next, we start to discuss the classical information transmission capability of a noisy quantum channel.

1) The Holevo-Schumacher-Westmoreland Capacity: The HSW (Holevo-Schumacher-Westmoreland) theorem defines the maximum of classical information which can be transmitted through a noisy quantum channel $\mathcal{N}$ if the input contains product states (i.e., entanglement is not allowed, also known as the product-state classical capacity) and the output is measured by joint measurement setting (see the *second* measurement setting in subsection 3.3.2.1). In this setting, for the quantum noisy communication channel $\mathcal{N}$, the classical capacity can be expressed as follows

$$\begin{aligned} C(\mathcal{N}) &= \max_{allp_i,\rho_i} \chi = \max_{allp_i,\rho_i} \left[\mathrm{S}(\sigma_{out}) - \sum_i p_i \mathrm{S}(\sigma_i) \right] \\ &= \max_{allp_i,\rho_i} \left[\mathrm{S}\left(\mathcal{N}\left(\sum_i p_i \rho_i \right) \right) - \sum_i p_i \mathrm{S}(\mathcal{N}(\rho_i)) \right] \\ &= \chi(\mathcal{N}), \end{aligned} \tag{110}$$

where the maximum is taken over all ensembles $\{p_i, \rho_i\}$ of input quantum states, while for σ_{out} see (14), while $\chi(\mathcal{N})$ is the Holevo capacity of $\mathcal{N}$. Trivially follows, that the $\chi(\mathcal{N})$ capacity reaches its maximum for a perfect noiseless quantum channel $\mathcal{N} = I$.

If Alice chooses among a set of quantum codewords, then is it possible to transmit these codewords through the noisy quantum channel $\mathcal{N}$ to Bob with arbitrary small error, if

$$R < C(\mathcal{N}) = \max_{allp_i,\rho_i} \left[\mathrm{S}\left(\mathcal{N}\left(\sum_i p_i \rho_i \right) \right) - \sum_i p_i \mathrm{S}(\mathcal{N}(\rho_i)) \right]; \tag{111}$$

if Alice adjusts *R* to be under $\max_{allp_i,\rho_i} \chi$, then she can transmit her codewords with arbitrarily small error. If Alice chooses $R > C(\mathcal{N})$,then she cannot select a quantum code of arbitrary size, which was needed for her to realize an error-free communication. The HSW channel capacity guarantees an error-free quantum communication only if $R < C(\mathcal{N}) = \max_{allp_i,\rho_i} \chi$ is satisfied for her code rate *R*.

2) Various Classical Capacities of a Quantum Channel: The asymptotic channel capacity is the 'true measure' of the various channel capacities, instead of the single-use capacity, which characterizes the capacity only in a very special case. The three classical capacities of the quantum channel of quantum channels will be discussed next.

In the regularization step, the channel capacity is computed as a limit. In possession of this limit, we will use the following lower bounds for the single-use capacities. In Section 3.3.1 we have also seen, the *Holevo-Schumacher-Westmoreland* theorem gives an explicit answer to the maximal transmittable classical information over the quantum channel. Next, we show the connection between these results. As we will see in subsection 3.3.2.1, four different measurement settings can be defined for the measurement of the *classical* capacity of the quantum channel. Here we call the attention of the reader that Holevo bound (90) limits the classical information stored in a quantum bit. HSW theorem can be regarded a similar scenario but a quantum channel deployed between Alice and Bob introduces further uncertainty before extracting the classical information. Obviously if we assume an ideal channel the two scenarios become the same.

Now, we present an example allowing the comparison of classical capacity of a simple channel model in classical and quantum context. The binary symmetric channel inverts the input cbits with probability *p* and leaves it unchanged with (1-*p*). The equivalent quantum bit flip channel (see Section V) applies the Pauli *X* and the identity transforms *I*.

Considering the worst case $p = 0.5$ all the sent information vanishes in the classical channel $C(N) = 1 - H(p) = 0$. However, the HSW theorem enables the optimization not only over the input probabilities but over input ensembles $\{p_i, \rho_i\}$. If we set ρ_i to the eigenvectors of Pauli *X* deriving them from its spectral decomposition

$$X = 1 \left|+\right\rangle \left\langle+\right| + (-1) \left|-\right\rangle \left\langle-\right|, \tag{112}$$

where $\left|\pm\right\rangle = \frac{\left|0\right\rangle \pm \left|1\right\rangle}{\sqrt{2}}$, $C(\mathcal{N}) = 1$ can be achieved. This results is more than surprising, encoding into quantum states in certain cases may improve the transfer of classical information between distant points i.e., the increased degree of freedom enables reducing the uncertainty introduced by the channel.

a) Measurement Settings: Similar to classical channel encoding, the quantum states can be transmitted in codewords *n* qubit of length using the quantum channel consecutively *n*-times or equivalently we can send codewords over *n* copies of quantum channel $\mathcal{N}$ denoted by $\mathcal{N}^{\otimes n}$. For the sake of simplicity we use $n = 2$ in the figures belonging to the following explanation. In order to make the transient smoother between the single-shot and the asymptotic approaches we depicted the scenario using *product input states* and *single* (or independent) measurement devices at the output of the channel in Fig. 8. In that case the $C(\mathcal{N})$ classical capacity of quantum channel $\mathcal{N}$ with input *A* and output *B* can be expressed by the maximization of the $I(A{:}B)$ quantum mutual information as follows:

$$C(\mathcal{N}) = \max_{allp_i,\rho_i} I(A{:}B). \tag{113}$$

From (113) also follows that for this setting the single-use $C^{(1)}(N)$ and the asymptotic $C(\mathcal{N})$ classical capacities are equal:

$$C^{(1)}(N) = C(\mathcal{N}) = \max_{allp_i,\rho_i} I(A{:}B). \tag{114}$$

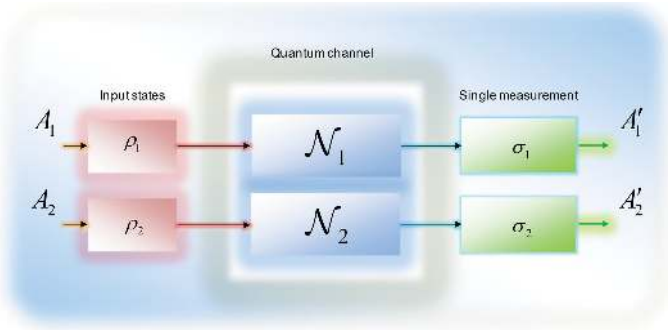

Fig. 8: Transmission of classical information over quantum channel with product state inputs and single measurements. Environment is not depicted.

On the other hand, if we have *product state inputs* but we change the measurement setting from the single measurement setting to *joint measurement* setting, then the classical channel capacity cannot be given by (113), hence

$$C(\mathcal{N}) \neq \max_{allp_i,\rho_i} I(A{:}B). \tag{115}$$

If we would like to step forward, we have to accept the fact, that the quantum mutual information cannot be used to express the asymptotic version: the *maximized* quantum mutual information is *always additive* (see Section II) - but not the Holevo information. As follows, if we would take the regularized form of quantum mutual information to express the capacity, we will find that the asymptotic version is equal to the single-use version, since:

$$\lim_{n\to\infty} \frac{1}{n} \max_{allp_i,\rho_i} I(A{:}B) = \max_{allp_i,\rho_i} I(A{:}B). \tag{116}$$

From (116) follows, that if we have *product inputs* and *joint measurement* at the outputs, we cannot use the $\max_{allp_i,\rho_i} I(A{:}B)$ maximized quantum mutual information function to express $C(\mathcal{N})$. If we would like to compute the classical capacity $C(\mathcal{N})$ for that case, we have to leave the quantum mutual information function, and instead of it we have to use the maximized Holevo information $\max_{allp_i,\rho_i} \chi$.

This new $C(\mathcal{N})$ capacity (according to the *Holevo-Schumacher-Westmoreland* theorem) can be expressed by the Holevo capacity $\chi(\mathcal{N})$, which will be equal to the maximization of Holevo information of channel $\mathcal{N}$:

$$C(\mathcal{N}) = \chi(\mathcal{N}) = \max_{allp_i,\rho_i} \chi. \tag{117}$$

The Holevo capacity and the asymptotic channel capacity will be equal in this case.

The HSW theorem gives an explicit answer for the classical capacity of the *product state input* with *joint measurement* setting, and expresses $C(\mathcal{N})$ as follows:

$$C(\mathcal{N}) = \chi(\mathcal{N}) = \max_{allp_i,\rho_i} \left[\mathrm{S}\left(\mathcal{N}\left(\sum_i p_i \rho_i \right) \right) - \sum_i p_i \mathrm{S}\left(\mathcal{N}(\rho_i) \right) \right]. \tag{118}$$

The relation discussed above holds for the restricted channel setting illustrated in Fig. 9, where the input consists of product states, and the output is measured by a joint measurement setting.

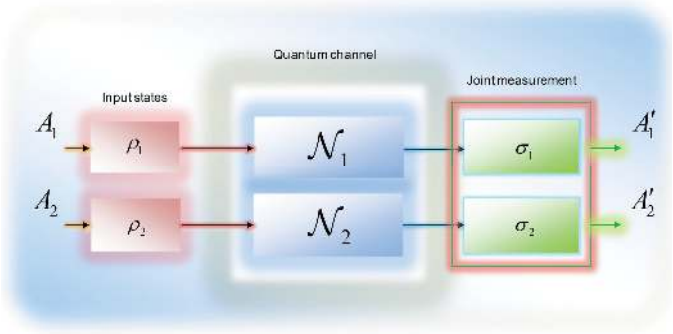

Fig. 9: Transmission of classical information over quantum channel with product state inputs and joint measurements. Environment is not depicted.

However, if *entangled inputs* are allowed with the *joint measurement setting* - then this equality does not hold anymore. As a conclusion, the relation between the maximized Holevo information $\chi(\mathcal{N})$ of the channel of the channel and the asymptotic classical channel capacity $C(\mathcal{N})$:

$$\chi(\mathcal{N}) \leq C(\mathcal{N}). \tag{119}$$

This means that we have to redefine the asymptotic formula of $C(\mathcal{N})$ for entangled inputs and joint measurement setting, to measure the maximum transmittable classical information through a quantum channel.

In the 1990s, it was conjectured that the formula of (118) can be applied to describe the channel capacity for entangled inputs with the *single measurement* setting; however it was an open question for a long time. Single measurement *destroys* the possible benefits arising from the entangled inputs, and joint measurement is required to achieve the benefits of entangled inputs [275].

In 2009 Hastings have used *entangled input states* and showed that the entangled inputs (with the *joint measurement*) can increase the amount of classical information which can be transmitted over a noisy quantum channel. In this case, $C(\mathcal{N}) \neq \chi(\mathcal{N})$ and the $C(\mathcal{N})$ can be expressed with the help of Holevo capacity as follows, using the asymptotic formula of $\chi(\mathcal{N})$:

$$C(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \chi\left(\mathcal{N}^{\otimes n}\right). \tag{120}$$

The channel construction for this relation is illustrated in Fig. 10. The entangled input is formally denoted by Ψ_{12}.

We also show the channel construction of the fourth possible construction to measure the classical capacity of a quantum channel. In this case, we have entangled input states, however we use a single measurement setting instead of a joint measurement setting.

To our knowledge, currently there is no quantum channel model where the channel capacity can be increased with this setting, since in this case the benefits of entanglement vanish

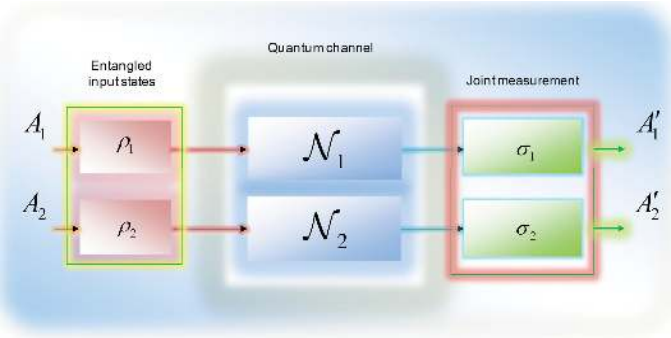

Fig. 10: Transmission of classical information over quantum channel with entangled inputs Ψ_{12} and joint measurements. Environment is not depicted.

because of the joint measurement setting has been changed into the single measurement setting. We illustrated this setting in Fig. 11.

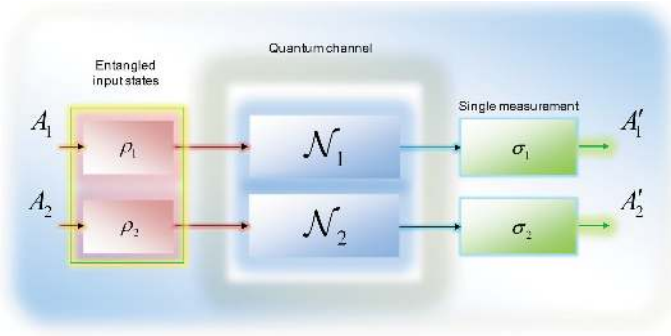

Fig. 11: Transmission of classical information over quantum channel with entangled inputs and single measurements. Environment is not depicted.

We have seen in (118), that if we have *product input states* and we change from a single to a *joint measurement* setting, then the classical capacity of $\mathcal{N}$ cannot be expressed by the maximized quantum mutual information function, because it is always additive, hence

$$C(\mathcal{N}) \neq \lim_{n\to\infty} \frac{1}{n} \max_{all p_i,\rho_i} I(A{:}B). \tag{121}$$

If we allow *entangled input states* and *joint measurement* (see (120)), then we have to use the $C(\mathcal{N})$ asymptotic formula of the previously derived Holevo capacity, $\chi(\mathcal{N})$ which yields

$$C(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \chi\left(\mathcal{N}^{\otimes n}\right) \neq \chi(\mathcal{N}). \tag{122}$$

3) Brief Summary: The Holevo quantity measures the classical information, which remains in the encoded quantum states after they have transmitted through a noisy quantum channel. During the transmission, some information passes to the environment from the quantum state, which results in the increased entropy of the sent quantum state. The HSW theorem states very similar to Holevo's previous result. As in the case of the Holevo quantity, the HSW capacity measures the classical capacity of a noisy quantum channel - however, as we will see in Section IV, the Holevo quantity also can be used to express the quantum capacity of the quantum channel, which is a not trivial fact. The HSW capacity maximizes the Holevo quantity over a set of possible input states, and expresses the classical information, which can be sent through *reliably* in the form of *product input states* over the noisy quantum channel, hence HSW capacity is also known as *product state channel capacity*. In this case, the input states are not entangled; hence there is no entanglement between the multiple uses of the quantum channel. As we have seen in this section, if the input of the channel consists of product states and we use *single measurement* setting, then the classical capacity can be expressed as the maximized of the quantum mutual information. On the other hand, if the single measurement has been changed to *joint measurement*, this statement is not true anymore; - this capacity will be equal to HSW capacity, see (118). Moreover, if we step forward, and we allow *entanglement* among the input states, then we cannot use anymore the HSW capacity, which was defined in (110). In this case we have to take its asymptotic formula, which was shown in (120).

Next we discuss the private classical capacity of quantum channels.

D. The Private Classical Capacity

The private classical capacity $P(\mathcal{N})$ of a quantum channel $\mathcal{N}$ describes the maximum rate at which the channel is able to send *classical information* through the channel reliably and *privately* (i.e., without any information leaked about the original message to an eavesdropper). Privately here means that an eavesdropper will not be able to access the encoded information without revealing her/himself i.e., the private classical capacity describes the maximal secure information that can be obtained by Bob on an eavesdropped quantum communication channel.

The generalized model of the private communication over quantum channels is illustrated in Fig. 12. The first output of the channel is denoted by $\sigma_B{=}\mathcal{N}(\rho_A)$, the second 'receiver' is the eavesdropper *E*, with state σ_E. The single-use private classical capacity from these quantities can be expressed as the maximum of the difference between two mutual information quantities. The eavesdropper, Eve, attacks the quantum channel, and she steals $I(A{:}E)$ from the information $I(A{:}B)$ sent by Alice to Bob, therefore the *single-use* private classical capacity (or *private information*) of $\mathcal{N}$ can be determined asl

$$P^{(1)}(\mathcal{N}) = \max_{all p_i,\rho_i} \left(I(A{:}B) - I(A{:}E)\right). \tag{123}$$

while the *asymptotic* private classical capacity is

$$\begin{aligned} P(\mathcal{N}) &= \lim_{n\to\infty} \frac{1}{n} P^{(1)}\left(\mathcal{N}^{\otimes n}\right) \\ &= \lim_{n\to\infty} \frac{1}{n} \max_{all\ p_i,\rho_i} \left(I(A:B) - I(A:E)\right). \end{aligned} \tag{124}$$

The private classical capacity can be expressed as the difference of two quantum mutual information functions, see (124). Here, we give an equivalent definition for private classical

capacity $P(\mathcal{N})$ and show, that it also can be rewritten using the Holevo quantity $\mathcal{X}$, as follows:

$$P(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \max_{all p_i,\rho_i} (\mathcal{X}_{AB} - \mathcal{X}_{AE}), \tag{125}$$

where

$$\mathcal{X}_{AB} = \mathrm{S}(\mathcal{N}_{AB}(\rho_{AB})) - \sum_i p_i \mathrm{S}(\mathcal{N}_{AB}(\rho_i)) \tag{126}$$

and

$$\mathcal{X}_{AE} = \mathrm{S}(\mathcal{N}_{AE}(\rho_{AE})) - \sum_i p_i \mathrm{S}(\mathcal{N}_{AE}(\rho_i)) \tag{127}$$

measure the Holevo quantities between Alice and Bob, and Alice and the eavesdropper Eve, respectively, while $\rho_{AB} = \sum_i p_i \rho_i$ and $\rho_{AE} = \sum_i p_i \rho_i$. An important corollary from (124), while the quantum mutual information itself is additive (see the properties of quantum mutual information function in Section II), the difference of two quantum mutual information functions is not (i.e., we need the asymptotic version to compute the 'true' private classical capacity of a quantum channel.)

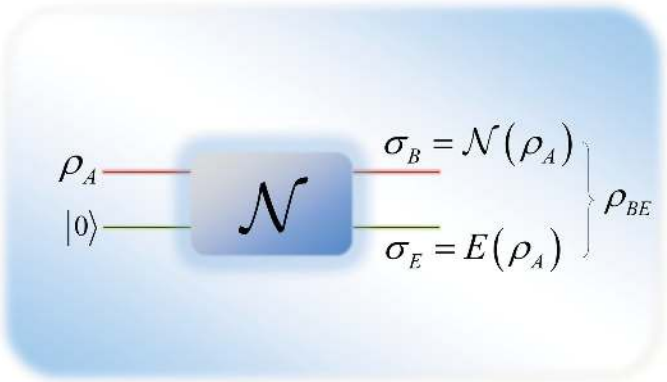

Fig. 12: The model of private classical communication of a quantum channel.

E. The Entanglement-assisted Classical Capacity

The last capacity regarding classical communication over quantum channels is called *entanglement-assisted classical capacity* $C_E(\mathcal{N})$, which measures the classical information which can be transmitted through the channel, if Alice and Bob have shared entanglement before the transmission i.e., entanglement is applied not between the input states like in case of the HSW (i.e., the product-state capacity) theorem. This capacity measures classical information, and it can be expressed with the help of the *quantum mutual information function* (see Section II) as

$$C_E(\mathcal{N}) = \max_{all p_i,\rho_i} I(A{:}B). \tag{128}$$

The main difference between the classical capacity $C(\mathcal{N})$ and the entanglement-assisted classical capacity $C_E(\mathcal{N})$, is that in the latter case the maximum of the transmittable classical information is equal to the maximized quantum mutual information, - hence the entanglement-assisted classical capacity $C_E(\mathcal{N})$ can be derived from the *single-use* version $C_E^{(1)}(\mathcal{N})$. From (128) the reader can conclude, there is no need for the asymptotic version to express the entanglement-assisted classical capacity, i.e.:

$$C_E(\mathcal{N}) = C_E^{(1)}(\mathcal{N}) = \max_{all p_i,\rho_i} I(A{:}B). \tag{129}$$

It also can be concluded, that shared entanglement does not change the additivity of maximized quantum mutual information - or with other words, it remains true if the parties use shared entanglement for the transmission of classical information over $\mathcal{N}$. In Fig. 13 we illustrate the general model of entanglement-assisted classical capacity $C_E(\mathcal{N})$.

We note an important property of shared entanglement: while it does not provide any benefits in the improving of the classical capacity of the quantum channel, (see (128)), it can be used to increase the single-use classical capacity. It was shown, that with the help of shared entanglement the transmission of a single quantum bit can be realized with higher success probability, - this strategy is known as the CHSH (*Clauser-Horne-Shimony-Holt*) game, for details see [244].

a) Brief Summary of Classical Capacities: Here, we give a brief summarization on the classical capacities. For the *asymptotic* capacity of a quantum channel, we have

$$C(\mathcal{N}) \geq \chi(\mathcal{N}). \tag{130}$$

According to the results of Holevo-Schumacher-Westmoreland, the asymptotic classical capacity is not equal to the single-use classical capacity. The *asymptotic* formula of the classical capacity $C(\mathcal{N})$ can be expressed by the help of the Holevo capacity $\chi(\mathcal{N})$ as

$$C(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \chi\left(\mathcal{N}^{\otimes n}\right). \tag{131}$$

The difference between the single-use formula and the asymptotic formula holds for the private capacity $P(\mathcal{N})$. Unlike these capacities, in the case of entanglement-assisted classical capacity $C_E(\mathcal{N})$, we will find something else in the expression. In this case, we have

$$C_E(\mathcal{N}) = C_E^{(1)}(\mathcal{N}) = \max_{all p_i,\rho_i} I(A{:}B), \tag{132}$$

and so we can conclude, *there is no regularization*. Since there is no regularization needed, it also means that the entanglement-assisted classical capacity $C_E(\mathcal{N})$ will always be additive. This makes it easier to compute the entanglement-assisted capacity than the other formulas, in which regularization is needed.

Originally, it was conjectured that in the general case, the Holevo information χ is additive too, for the same channels. Later, a counterexample was found by Hastings. As has been shown, in this case the additivity of the Holevo information fails.

Similarly, for the $P(\mathcal{N})$ private classical capacity, - which also measures classical information we have

$$P(\mathcal{N}) \geq \max_{all p_i,\rho_i} (I(A{:}B) - I(A{:}E)), \tag{133}$$

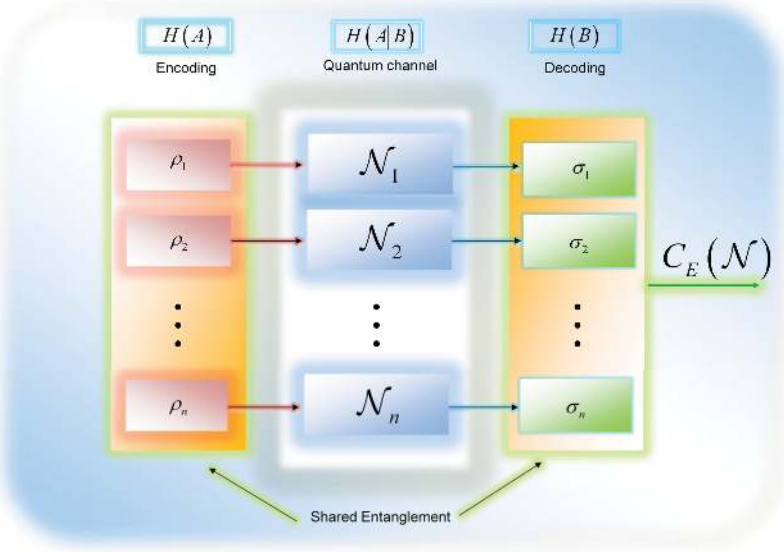

Fig. 13: The entanglement-assisted capacity of a quantum channel. This capacity measures the maximum of transmittable classical information through a quantum channel, if shared a priori entanglement between the parties is allowed.

and finally, for the classical capacity $C(\mathcal{N})$ of $\mathcal{N}$

$$\max_{all p_i,\rho_i} I(A{:}B) \leq C(\mathcal{N}) \leq \lim_{n\to\infty} \frac{1}{n}\chi\left(\mathcal{N}^{\otimes n}\right). \tag{134}$$

As can be seen, in case of the classical and private classical capacities the regularization is needed, since the asymptotic and the single-use formulas are not equal.

F. The Classical Zero-Error Capacity

Shannon's results on capacity [477] guarantees transmission rate only in average when using multiple times of the channel. The zero-error capacity of the quantum channel describes the amount of (classical or quantum) information which can be transmitted *perfectly* (*zero probability of error*) through a noisy quantum channel. The zero-error capacity of the quantum channel could have an overriding importance in future quantum communication networks.

The zero-error capacity stands a very strong requirement in comparison to the standard capacity where the information transmission can be realized with asymptotically small *but non-vanishing* error probability, since in the case of zero-error communication the *error probability of the communication has to be zero*, hence the transmission of information has to be perfect and no errors are allowed. While in the case of classical non zero-error capacity for an *n*-length code the error probabilities after the decoding process are $\Pr[error]\to 0$ as $n\to\infty$, in case of an *n*-length zero-error code, $\Pr[error]=0$.

In this subsection we give the exact definitions which required for the characterization of a quantum zero-error communication system. We will discuss the classical and quantum zero-error capacities and give the connection between zero-error quantum codes and the elements of graph theory.

1) Classical Zero-Error Capacities of Quantum Channels: In this section we review the background of zero-error capacity $C_0(\mathcal{N})$ of a quantum channel $\mathcal{N}$. Let us assume that Alice has information source $\{X_i\}$ encoded into quantum states $\{\rho_i\}$ which will be transmitted through a quantum channel $\mathcal{N}$ (see Fig. 14). The quantum states will be measured by a set of POVM operators $\mathcal{P}=\{\mathcal{M}_1,\ldots,\mathcal{M}_k\}$ at the receiver (see Section II). The classical zero-error quantum capacity $C_0(\mathcal{N})$ for product input states can be reached if and only if the input states are *pure* states, similarly to the HSW capacity $C(\mathcal{N})$.

The zero-error transmission of quantum states requires perfect distinguishability. To achieve this perfect distinguishability of the zero-error quantum codewords, they have to be *pairwise orthogonal*. *Non-adjacent codewords can be distinguished perfectly*. Two inputs are called *adjacent* if they can result in the same output. The number of possible non-adjacent codewords determines the rate of maximal transmittable classical information through $\mathcal{N}$.

In the *d* dimensional Hilbert space (e.g. *d*=2 for qubits) at most *d* pairwise distinguishable quantum states exist, thus for a quantum system which consist of *n* pieces of *d* dimensional quantum states at most d^n pairwise distinguishable *n*-length quantum codewords are available. Obviously if two quantum codewords are not orthogonal, then they cannot be distinguished perfectly. We note, if we would like to distinguish between *K pairwise orthogonal* quantum codewords (the length of each codewords is *n*) in the d^n dimensional Hilbert space, then we have to define the POVM set

$$\mathcal{P}=\left\{\mathcal{M}^{(1)},\ldots,\mathcal{M}^{(K)}\right\}, \tag{135}$$

where $\mathcal{M}^{(i)}$ are set of *d*-dimensional projectors on the individual quantum systems (e.g. qubits) which distinguish the *n*-length codewords

$$\mathcal{M}^{(i)}=\{\mathcal{M}_1,\ldots,\mathcal{M}_m\} \tag{136}$$

where $m{=}d^n$. The probability that Bob gives measurement outcome *j* from quantum state ρ_i is

$$\Pr[j|\,\rho_i]=Tr\left(\mathcal{M}_j\mathcal{N}(\rho_i)\right). \tag{137}$$

The *i*-th *codeword* $|\psi_{X_i}\rangle$ encodes the *n*-length classical codeword $X_i=\{x_{i,1}, x_{i,2}, \ldots, x_{i,n}\}$ consisting of *n* product input quantum states:

$$|\psi_{X_i}\rangle = [|\psi_{i,1}\rangle \otimes |\psi_{i,2}\rangle \otimes |\psi_{i,3}\rangle \cdots \otimes |\psi_{i,n}\rangle], \; i=1..K, \tag{138}$$

where $\rho_i=|\psi_{X_i}\rangle \langle\psi_{X_i}|$.

The quantum block code consist of codewords

$$\begin{aligned} |\psi_{X_1}\rangle &= [|\psi_{1,1}\rangle \otimes |\psi_{1,2}\rangle \otimes |\psi_{1,3}\rangle \cdots \otimes |\psi_{1,n}\rangle] \\ &\vdots \\ |\psi_{X_K}\rangle &= [|\psi_{K,1}\rangle \otimes |\psi_{K,2}\rangle \otimes |\psi_{K,3}\rangle \cdots \otimes |\psi_{K,n}\rangle], \end{aligned} \tag{139}$$

where *K* is the number of classical (*n* length) messages.

The decoder will produce the output codeword $X_i' = \{x_{i,1}', x_{i,2}', \ldots, x_{i,n}'\}$ generated by the POVM measurement operators, where the POVM $\mathcal{M}^{(i)}$ can distinguish *m* messages $\{X_1', X_2', \ldots X_m'\}$ (*n*-length) at the output. Bob would like to determine each message $i\in[1,K]$ with unit probability. The zero probability of error means that for the input code $|\psi_{X_i}\rangle$ the decoder has to identify the classical output codeword X'_i with classical input codeword X_i perfectly for each possible *i*, otherwise the quantum channel has no zero-error capacity; that is, for the zero-error quantum communication system

$$\Pr[X_i'|X_i] = 1. \tag{140}$$

2) Formal Definitions of Quantum Zero-Error Communication: In this subsection we review the most important definitions of quantum zero-error communication systems.

The *non-adjacent* elements are important for zero-error capacity, since *only non-adjacent codewords can be distinguished perfectly*. Two inputs are called *adjacent* if they can result in the same output, while for *non-adjacent* inputs, the output of the encoder is unique. The number of possible non-adjacent codewords determines the rate of maximal transmittable classical information through quantum channels.

Formally, the *non-adjacent* property of two quantum states ρ_1 and ρ_2 can be given as

$$Set_1 \cap Set_2 = \emptyset, \tag{141}$$

where $Set_i = \left\{\Pr\left[X_j'|\, X_i\right] = Tr\left(\mathcal{M}_j \mathcal{N}\left(|\psi_{X_i}\rangle \langle\psi_{X_i}|\right)\right) > 0\right\}$, $j \in \{1,\ldots,m\}, i = 1,2$, and $\mathcal{P}=\{\mathcal{M}_1,\ldots,\mathcal{M}_m\}$ is a POVM measurement operator. In a relation of a noisy quantum channel $\mathcal{N}$, the non-adjacent property can be rephrased as follows. Two input quantum states ρ_1 and ρ_2 are non-adjacent with relation to $\mathcal{N}$, if $\mathcal{N}(\rho_1)$ and $\mathcal{N}(\rho_2)$ are *perfectly distinguishable*. The notation $\rho_1 \underset{N}{\perp} \rho_2$ also can be used to denote the non-adjacent inputs of quantum channel $\mathcal{N}$.

A quantum channel $\mathcal{N}$ has greater than zero zero-error capacity if and only if a subset of quantum states $\Omega=\{\rho_i\}_{i=1}^{l}$ and POVM $\mathcal{P}=\{\mathcal{M}_1,\ldots,\mathcal{M}_m\}$ exists where for at *least two states* ρ_1 and ρ_2 from subset Ω, the relation (141) holds; that is, the non-adjacent property with relation to the POVM measurement is satisfied. For the quantum channel $\mathcal{N}$, the two inputs ρ_1 and ρ_2 are non-adjacent if and only if the quantum channel takes the input states ρ_1 and ρ_2 into orthogonal subspaces

$$\mathcal{N}(\rho_1) \underset{\mathcal{N}}{\perp} \mathcal{N}(\rho_2); \tag{142}$$

that is, the quantum channel has positive classical zero-error capacity $C_0(\mathcal{N})$ if and only if this property holds for the output of the channel for a given POVM $\mathcal{P}=\{\mathcal{M}_1,\ldots,\mathcal{M}_m\}$. The previous result can be rephrased as follows. Using the trace preserving property of the quantum channe, the two quantum states ρ_1 and ρ_2 are non-adjacent if and only if for the channel output states $\mathcal{N}(\rho_1), \mathcal{N}(\rho_2)$,

$$Tr(\mathcal{N}(\rho_1)\mathcal{N}(\rho_2)) = 0, \tag{143}$$

and if ρ_1 and ρ_2 are non-adjacent input states then

$$Tr(\rho_1\rho_2) = 0. \tag{144}$$

Let the two *non-adjacent* input codewords of the $\mathcal{N}$ be denoted by $|\psi_{X_1}\rangle$ and $|\psi_{X_2}\rangle$. These quantum codewords encode messages $X_1=\{x_{1,1}, x_{1,2}, \ldots, x_{1,n}\}$ and $X_2=\{x_{2,1}, x_{2,2}, \ldots, x_{2,n}\}$. For this setting, we construct the following POVM operators for the given complete set of POVM $\mathcal{P}=\{\mathcal{M}_1,\ldots,\mathcal{M}_m\}$ and the two input codewords $|\psi_{X_1}\rangle$ and $|\psi_{X_2}\rangle$ as follows

$$\mathcal{M}^{(1)}=\{\mathcal{M}_1,\ldots,\mathcal{M}_k\} \tag{145}$$

and

$$\mathcal{M}^{(2)}=\{\mathcal{M}_{k+1},\ldots,\mathcal{M}_m\}. \tag{146}$$

The groups of operators, $\mathcal{M}^{(1)}$ and $\mathcal{M}^{(2)}$, will identify and distinguish the input codewords $|\psi_{X_1}\rangle$ and $|\psi_{X_2}\rangle$. Using this setting the two non-adjacent codewords $|\psi_{X_1}\rangle$ and $|\psi_{X_2}\rangle$ can be distinguished with probability one at the output since

$$\begin{aligned} &\Pr[X_i'|X_1] = 1,\ i=1,\ldots,k, \\ &\Pr[X_i'|X_2] = 1,\ i=k+1,\ldots,m, \end{aligned} \tag{147}$$

where X_i' is a number between 1 and *m*, (according to the possible number of POVM operators) which identifies the measured unknown quantum codeword and consequently

$$\begin{aligned} &\Pr[X_i'|X_1] = 0,\ i=k+1,\ldots,m, \\ &\Pr[X_i'|X_2] = 0,\ i=1,\ldots,k. \end{aligned} \tag{148}$$

For input message $|\psi_{X_1}\rangle$ and $|\psi_{X_2}\rangle$ with the help of set $\mathcal{M}^{(1)}$ and $\mathcal{M}^{(2)}$ these probabilities are

$$\begin{aligned} &\Pr[X_1'|X_1] = Tr\left(\mathcal{M}^{(1)}\mathcal{N}\left(|\psi_{X_1}\rangle \langle\psi_{X_1}|\right)\right) = 1, \\ &\Pr[X_2'|X_2] = Tr\left(\mathcal{M}^{(2)}\mathcal{N}\left(|\psi_{X_2}\rangle \langle\psi_{X_2}|\right)\right) = 1, \end{aligned} \tag{149}$$

where $\mathcal{M}^{(1)}$ and $\mathcal{M}^{(2)}$ are orthogonal projectors, $\mathcal{M}^{(1)}$ and $\mathcal{M}^{(2)}$ are defined in (145) and (146)), and $\mathcal{M}^{(1)}+\mathcal{M}^{(2)}+\mathcal{M}^{(2+1)}=I$, to make it possible for the quantum channel to take the input states into orthogonal subspaces; that is, $\mathcal{N}(|\psi_{X_1}\rangle \langle\psi_{X_1}|) \perp \mathcal{N}(|\psi_{X_2}\rangle \langle\psi_{X_2}|)$ has to be satisfied. The POVM measurement has to be restricted to projective measurement. As follows, the $\mathcal{P}=\{\mathcal{M}^{(1)}, \mathcal{M}^{(2)}\}$ POVM measurement can be replaced with the set of *von Neumann* operators, $\mathcal{Z}=\{\mathcal{P}^{(1)}, \mathcal{P}^{(2)}\}$, where $\mathcal{P}^{(1)}+\mathcal{P}^{(2)}=I$. This result also can be extended for arbitrarily number of operators, depending on the actual system. The non-adjacent property also can be interpreted for arbitrary length of

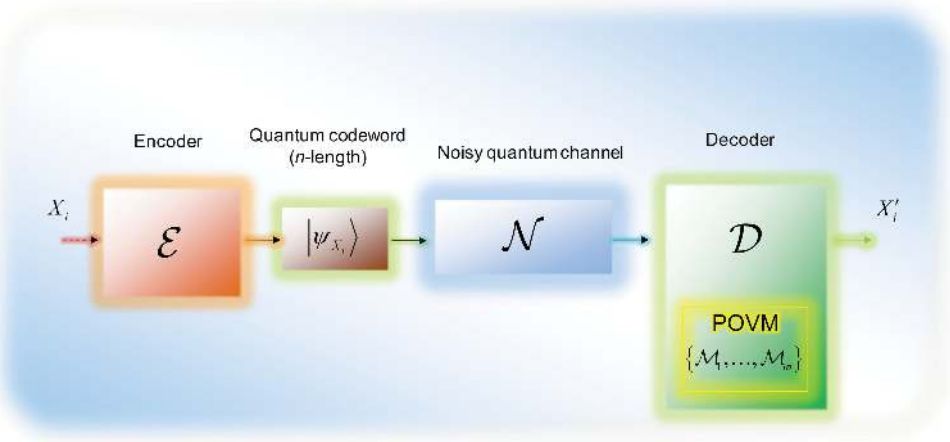

Fig. 14: A quantum zero-error communication system.

quantum codewords. For a given quantum channel $\mathcal{N}$, the two *n*-length input quantum codewords $|\psi_{X_1}\rangle$ and $|\psi_{X_2}\rangle$, which are tensor products of *n* quantum states, then *input* codewords $|\psi_{X_1}\rangle$ and $|\psi_{X_2}\rangle$ are non-adjacent in relation with $\mathcal{N}$ if and only if *at least one* pair of quantum states $\{|\psi_{1,i}\rangle, |\psi_{2,i}\rangle\}$ from the two *n*-length sequences is perfectly distinguishable. Formally, at least one *input* quantum state pair $\{|\psi_{1,i}\rangle, |\psi_{2,i}\rangle\}$ with i, $1 \leq i \leq n$, exists in $|\psi_{X_1}\rangle$ and $|\psi_{X_2}\rangle$, for which $\mathcal{N}(|\psi_{1,i}\rangle\langle\psi_{1,i}|)$ is non-adjacent to $\mathcal{N}(|\psi_{2,i}\rangle\langle\psi_{2,i}|)$. Because we have stated that the two codewords can be distinguished at the channel output, the following relation has to be hold for their trace, according to (143), and their non-adjacency can be verified as follows:

$$\begin{aligned} &Tr\left(\mathcal{N}\left(|\psi_{X_1}\rangle\langle\psi_{X_1}|\right)\mathcal{N}\left(|\psi_{X_2}\rangle\langle\psi_{X_2}|\right)\right) \\ &= Tr\left(\left(\overset{n}{\underset{i=1}{\otimes}}\mathcal{N}\left(|\psi_{1,i}\rangle\langle\psi_{1,i}|\right)\right)\left(\overset{n}{\underset{i=1}{\otimes}}\mathcal{N}\left(|\psi_{2,i}\rangle\langle\psi_{2,i}|\right)\right)\right) \\ &= \prod_{i=1}^{n} Tr\left(\mathcal{N}\left(|\psi_{1,i}\rangle\langle\psi_{1,i}|\right)\mathcal{N}\left(|\psi_{2,i}\rangle\langle\psi_{2,i}|\right)\right) = 0. \end{aligned} \tag{150}$$

As follows from (150), a quantum channel $\mathcal{N}$ has non-zero zero-error capacity if and only if there exists at least two non-adjacent input quantum states ρ_1 and ρ_2. These two non-adjacent quantum states make distinguishable the two, *n*-length quantum codewords at the output of quantum channel $\mathcal{N}$, and these input codewords will be called as *non-adjacent quantum codewords*. The joint measurement of the quantum states of an output codeword is *necessary* and *sufficient* to distinguish the input codewords with zero-error. *Necessary*, because the joint measurement is required to distinguish orthogonal general (i.e., non zero-error code) tensor product states [67]. Sufficient, because the non-adjacent quantum states have orthogonal *supports* at the output of the noisy quantum channel, i.e., $Tr(\rho_i\rho_j) = 0$ [320]. (The *support* of a matrix *A* is the orthogonal complement of the kernel of the matrix. The *kernel* of *A* is the set of all vectors *v*, for which $Av = 0$.) In the joint measurement, the $\{\mathcal{M}_i\}, i = 1,\ldots,m$ projectors are $d^n \times d^n$ matrices, while if we were to use a single measurement then the size of these matrices would be $d \times d$.

In Fig. 15 we compared the difference between single and joint measurement settings for a given *n*-length quantum codeword $|\psi_X\rangle = [|\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle \cdots \otimes |\psi_n\rangle]$. In the case of single measurement Bob measures each of the *n* quantum states of the *i*-th codeword states individually. In case of the joint measurement Bob waits until he receives the *n* quantum states, then measures them together.

Next we study the achievable rates for zero error classical communication over quantum channels.

3) Achievable Zero-Error Rates in Quantum Systems: Theoretically (without making any assumptions about the physical attributes of the transmission), the *classical single-use zero-error capacity* $C_0^{(1)}(\mathcal{N})$ of the noisy quantum channel can be expressed as

$$C_0^{(1)}(\mathcal{N}) = \log\left(K(\mathcal{N})\right), \tag{151}$$

where $K(\mathcal{N})$ is the maximum number of different messages which can be sent over the channel with a *single use* of $\mathcal{N}$ (or in other words the maximum size of the set of *mutually non-adjacent* inputs).

The asymptotic *zero-error capacity* of the noisy quantum channel $\mathcal{N}$ can be expressed as

$$C_0(\mathcal{N}) = \lim_{n\to\infty}\frac{1}{n}\log\left(K\left(\mathcal{N}^{\otimes n}\right)\right), \tag{152}$$

where $K(\mathcal{N}^{\otimes n})$ is the maximum number of *n*-length classical messages that the quantum channel can transmit with zero error and $\mathcal{N}^{\otimes n}$ denotes the *n*-uses of the channel.

The $C_0(\mathcal{N})$ asymptotic classical zero-error capacity of a quantum channel is *upper bounded* by the HSW capacity, that is,

$$C_0^{(1)}(\mathcal{N}) \leq C_0(\mathcal{N}) \leq C(\mathcal{N}). \tag{153}$$

Next, we study the connection of zero-error quantum codes and graph theory.

4) Connection with Graph Theory: The problem of finding *non-adjacent* codewords for the zero-error information transmission can be rephrased in terms of graph theory. The adjacent codewords are also called *confusable*, since these codewords can generate the same output with a given non-zero

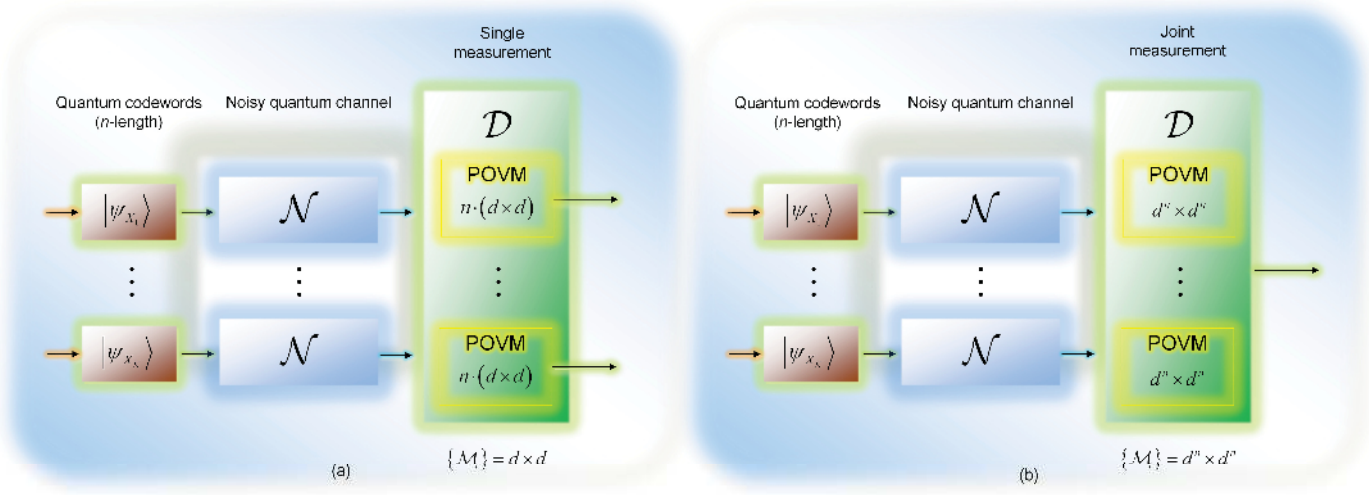

Fig. 15: Comparison of single (a) and joint (b) measurement settings. The joint measurement is necessary to attain the quantum zero-error communication.

probability. Since we know that two input codewords $|\psi_{X_1}\rangle$ and $|\psi_{X_2}\rangle$ are *adjacent* if there is a channel output codeword $|\psi_{X'}\rangle$ which can be resulted by either of these two, that is $\Pr[X'|X_1] > 0$ and $\Pr[X'|X_2] > 0$.

The non-adjacent property of two quantum codewords can be analyzed by the *confusability graph* $\mathcal{G}_n$, where *n* denotes the *length of the block code*.

Let us take as many vertices as the number of input messages *K*, and connect two vertices if these input messages are adjacent. For example, using the quantum version of the famous *pentagon graph* we show how the classical zero-error capacity $C_0(\mathcal{N})$ of the quantum channel $\mathcal{N}$ changes if we use block codes of length *n*=1 and *n*=2. In the pentagon graph an input codeword from the set of non-orthogonal qubits $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle, |4\rangle\}$ is connected with two other adjacent input codewords, and the number of total codewords is 5 [311].

The $\mathcal{G}_1$ *confusability* graph of the pentagon structure for block codes of length *n*=1 is shown in Fig. 16. The vertices of the graph are the possible input messages, where *K* = 5. The *adjacent* input messages are connected by a line. The non-adjacent inputs $|2\rangle$ and $|4\rangle$ are denoted by gray circles, and there is no connection between these two input codewords.

For the block codes of length *n*=1, the maximal transmittable classical information with zero error is

$$C_0(\mathcal{N}) = \log(2) = 1, \tag{154}$$

since only two non-adjacent vertices can be found in the graph. We note, other possible codeword combinations also can be used to realize the zero-error transmission, in comparison with the confusability graph, for example $|1\rangle$ and $|3\rangle$ also non-adjacent, etc. On the other hand, the maximum number of non-adjacent vertices (two, in this case) cannot be exceeded, thus $C_0(\mathcal{N}) = 1$ remains in all other possible cases, too.

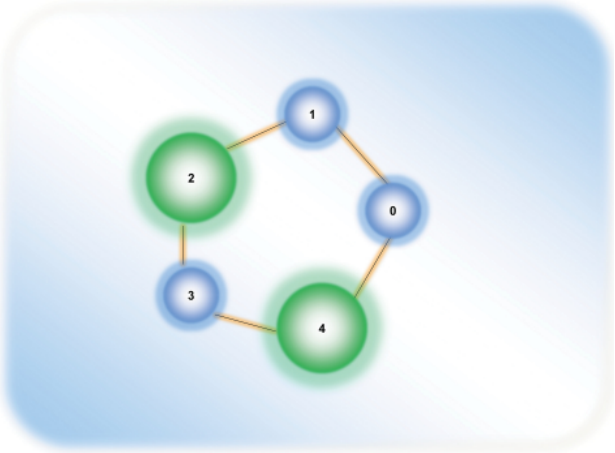

Fig. 16: The confusability graph of a zero-error code for one channel use. The two possible non-adjacent codewords are denoted by the large shaded circles.

Let assume that we use $n = 2$ length of block codes. First, let us see how the graph changes. The non-adjacent inputs are denoted by the large gray shaded circles. The connections between the possible codewords (which can be used as a block code) are denoted by the thick line and the dashed circle. The confusability graph $\mathcal{G}_2$ for $n = 2$ length of block codes is shown in Fig. 17. The two half-circles together on the left and right sides represent one circle and the two half circles at the top and bottom of the figure also represent one circle; thus there are five dashed circles in the figure.

It can be seen that the complexity of the structure of the graph has changed, although we have made only a small modification: we increased the lengths of the block codes from $n = 1$ to $n = 2$. The five two-length codewords and zero-error quantum block codes which can realize the zero-error

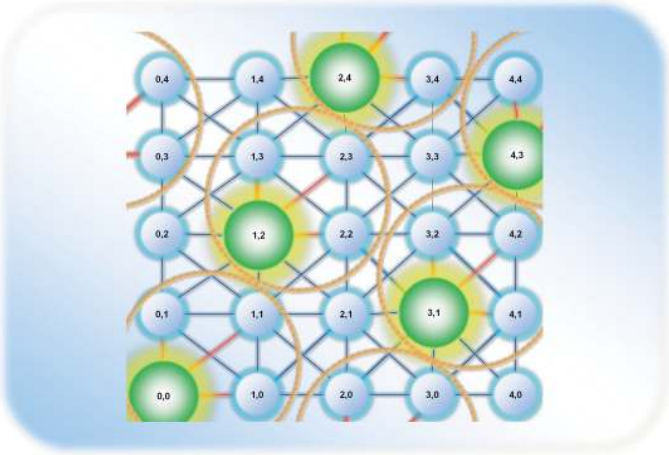

Fig. 17: The graph of a zero-error code for two channel uses of a quantum channel. The possible zero-error codewords are depicted by the thick lines and dashed circles.

transmission can be defined using the computational basis $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle, |4\rangle\}$. The classical zero-error capacity which can be achieved by $n=2$ length block codes is

$$C_0\left(\mathcal{N}^{\otimes 2}\right) = \frac{1}{2}\log(5) = 1.1609. \tag{155}$$

From an engineering point of view this result means, that for the pentagon graph, the maximum rate at which classical information can be transmitted over a noisy quantum channel $\mathcal{N}$ with a zero error probability, can be achieved with quantum block code length of two.

For the classical zero-error capacities of some typical quantum channels see Section V.

G. Entanglement-assisted Classical Zero-Error Capacity

In the previous subsection we discussed the main properties of zero-error capacity using product input states. Now, we add the entanglement to the picture. Here we discuss how the encoding and the decoding setting will change if we bring entanglement to the system and how it affects the classical zero-error capacity of a quantum channel.

If entanglement allowed between the communicating parties then the single-use and asymptotic *entanglement-assisted* classical zero-error capacities are defined as

$$C_0^{E(1)}(\mathcal{N}) = \log\left(K^E(\mathcal{N})\right) \tag{156}$$

and

$$C_0^E(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\log\left(K^E\left(\mathcal{N}^{\otimes n}\right)\right). \tag{157}$$

where $K^E(\mathcal{N}^{\otimes n})$ is the maximum number of n-length mutually non-adjacent classical messages that the quantum channel can transmit with zero error using *shared entanglement*.

Before we start to discuss the properties of the entanglement-assisted zero-error quantum communication, we introduce a new type of graph, called the *hypergraph* $\mathcal{G}_H$. The hypergraph is very similar to our previously shown *confusability* graph $\mathcal{G}_n$. The hypergraph contains a set of vertices and hyperedges. The vertices represent the *inputs* of the quantum channel $\mathcal{N}$, while the hyperedges contain all the channel inputs which could cause the same channel output with non-zero probability.

We will use some new terms from graph theory in this subsection; hence we briefly summarize these definitions:

1) *maximum independent set of* $\mathcal{G}_n$: the maximum number of non-adjacent inputs (K),
2) *clique of* $\mathcal{G}_n$: κ_i, the set of possible inputs of a given output in a confusability graph (which inputs could result in the same output with non-zero probability),
3) *complete graph*: if all the vertices are connected with one another in the graph; in this case there are no non-adjacent inputs; i.e., the channel has no zero-error capacity.

In Fig. 18(a) we show a hypergraph $\mathcal{G}_H$, where the inputs of the channel are the vertices and the hyperedges represent the channel outputs. Two inputs are non-adjacent if they are in a different loop. The two non-adjacent inputs are depicted by the greater grey shaded vertices. In Fig. 18(b) we give the confusability graph $\mathcal{G}_n$ for a single channel use ($n=1$), for the same input set. The cliques in the $\mathcal{G}_n$ confusability graph are depicted by κ_i.

Both the hypergraph and the confusability graph can be used to determine the non-adjacent inputs. However, if the number of inputs starts to increase, the number of hyperedges in the hypergraph will be significantly lower than the number of edges in the confusability graph of the same system. In short, the entanglement-assisted zero-error quantum communication protocol works as follows according to Fig. 19 [123]. Before the communication, Alice and Bob share entanglement between themselves. The d-dimensional shared system between Alice and Bob will be denoted by $\rho_{AB} = |\Phi_{AB}\rangle\langle\Phi_{AB}|$, where

$$|\Phi_{AB}\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1} |i\rangle_A |i\rangle_B \tag{158}$$

is a rank-d maximally entangled qudit state (also called as *edit*). If Alice would like to send a message $q\in\{1,\ldots,K\}$,

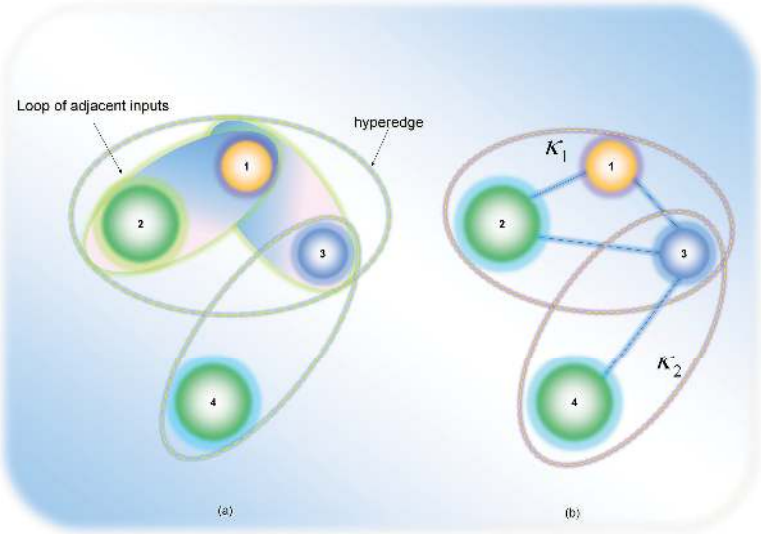

Fig. 18: The hypergraph and the confusability graph of a given input system with four inputs. The hyperedges of the hypergraph are labeled by the output. The number of non-adjacent inputs is two.

where *K* is the number of messages, to Bob, she has to measure her half of the entangled system using a complete orthogonal basis $B_q = \{|\psi_{x'}\rangle\}$, $x' \in \kappa_q$, where x' is a vertice in the hypergraph $\mathcal{G}_H$ from clique κ_q. The *orthonormal representation of a graph is a map:* the vertice x' represents the unit vector $|\psi_{x'}\rangle$ such that if $x$and x' are *adjacent* then $\langle\psi_x \mid \psi_{x'}\rangle = 0$ (*i.e., they are orthogonal in the orthonormal representation*) and κ_q is the clique corresponding to message *q* in the hypergraph $\mathcal{G}_H$. The hypergraph has *K* cliques of size *d*, $\{\kappa_1, \ldots, \kappa_K\}$ (i.e., each message $q \in \{1, \ldots, K\}$ is represented by a *d*-size clique in the hypergraph $\mathcal{G}_H$.) After the measurement, Bob's state will collapse to $|\psi_x\rangle^*$. Bob will measure his state in $B_q = \{|\psi_x\rangle\}$ to get the final state $|\psi_{x'}\rangle^*$. Bob's output is denoted by *y*. Bob's possible states are determined by those vertices x', for which $p(y|x') > 0$, and these *adjacent* states are *mutually orthogonal*; i.e., for any two x'_1 and x'_2, $\langle\psi_{x'_1}|\psi_{x'_2}\rangle = 0$. Finally, Alice makes her measurement using $B_q = \{|\psi_{x'}\rangle\}$, then Bob measures his state $|\psi_x\rangle^*$ in $B_q = \{|\psi_{x'}\rangle\}$ to produce $|\psi_{x'}\rangle^*$.

In order to make the above explanations more plausible, let us provide an example. Supposed Alice's set contains $K = 6$ codewords and she shares a rank-four (*i.e., d*=4) maximally entangled qudit state with Bob

$$\Phi_{AB} = \frac{1}{\sqrt{4}} \sum_{i=0}^{3} |i\rangle_A |i\rangle_B, \tag{159}$$

however, in the general case *d* can be chosen as large as Alice and Bob would like to use. Alice measures her system from the maximally entangled state, and she chooses a basis among the *K* possible states, according to which message *q* she wants to send Bob. Alice's measurement outcome is depicted by *x*, which is a random value. Alice sends *q* and *x* to the classical channel *N*. In the next phase, Bob performs a projective measurement to decide which *x* value was made to the classical channel by Alice. After Bob has determined it, he can answer which one of the possible *K* messages had been sent by Alice with the help of the maximally entangled system. Alice makes her measurement on her side using one of the six possible bases $B_q = \{|\psi_{x'}\rangle\}$ on her half of the state ρ_{AB}. Her system collapses to $|\psi_x\rangle \in B_q$, while Bob's system collapses to $|\psi_x\rangle^*$, conditioned on *x*. Alice makes *x* to the classical channel *N*; Bob will receive classical message *y*. From the channel output $y = N(x)$, where *N* is the classical channel between Alice and Bob, Bob can determine the mutually adjacent inputs (i.e., those inputs which could produce the given output). If Bob makes a measurement in basis $B_q = \{|\psi_x\rangle\}$, then he will get $|\psi_{x'}\rangle^*$, where these states for a given set of x' corresponding to possible x are *orthogonal states*, so he can determine *x* and the original message *q*. The channel output gives Bob the information that some set of mutually adjacent inputs were used on Alice's side. On his half of the entangled system, the states will be mutually orthogonal. A measurement on these mutually orthogonal states will determine Bob's state and he can tell Alice's input with certainty.

Using this protocol, the number of mutually non-adjacent input messages is

$$K^E \geq 6, \tag{160}$$

while if Alice and Bob would like to communicate with zero-error but without shared entanglement, then $K = 5$. As follows, for the single-use classical zero-error capacities we get

$$C_0^{(1)} = \log(5) \tag{161}$$

and

$$C_0^{E(1)} = \log\left(K^E\right) = \log(6), \tag{162}$$

while for the asymptotic entanglement-assisted classical zero-error capacity,

$$C_0^E \geq \log\left(K^E\right) = \log(6). \tag{163}$$

According to Alice's $K^E = 6$ messages, the hypergraph can be partitioned into six cliques of size $d = 4$. The adjacent vertices

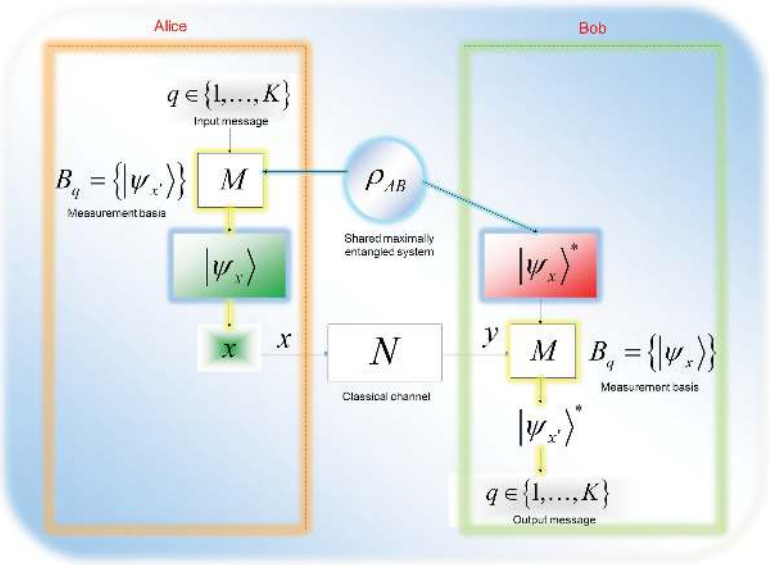

Fig. 19: The steps of the entanglement-assisted zero-error quantum communication protocol.

are denoted by a common loop. The overall system contains $6 \times 4 = 24$ basis vectors. These vectors are grouped into $K^E = 6$ orthogonal bases. Two input vectors are connected in the graph if they are adjacent vectors; i.e., they can produce the same output. The hypergraph $\mathcal{G}_H$ of this system is shown in Fig. 20. The mutually non-adjacent inputs are denoted by the great shaded circles. An important property of the entanglement-assisted classical zero-error capacity is that the number of maximally transmittable messages is not equal to the number of non-adjacent inputs. While the hypergraph has five independent vertices, the maximally transmittable messages are greater than or equal to six. The confusability graph of this system for a single use of quantum channel $\mathcal{N}$ would consist of $6 \times 4 \times 9 = 216$ connections, while the hypergraph has a significantly lower number ($6 \times 6 = 36$) of hyperedges. The adjacent vertices are depicted by the loops connected by the thick lines. The six possible messages are denoted by the six, four dimensional (i.e., each contains four vertices) cliques $\{\kappa_1, \ldots, \kappa_K\}$. The cliques (dashed circles) show the set of those input messages which could result in the same output with a given probability $p > 0$.

We note, the cliques are defined in the $\mathcal{G}_n$ confusability graph representation, but we also included them on the hypergraph $\mathcal{G}_H$. The adjacent vertices which share a loop represent mutually orthogonal input states. For these mutually orthogonal inputs the output will be the same.

The complete theoretical background of this example, i.e., the proof of the fact, that entanglement can increase the asymptotic classical zero-error capacity $C_0(\mathcal{N})$ of a quantum channel was described in [123].

We have seen in this subsection that shared entanglement between Alice and Bob can help to increase the maximally transmittable classical messages using noisy quantum channels with zero error probability. According to the *Cubitt-Leung-Matthews-Winter* theorem (CLMW theorem) [123] there exist entanglement-assisted quantum communication protocol which can send one of *K* messages with *zero error*; hence for the entanglement-assisted asymptotic classical zero-error capacity

$$\begin{aligned} \log(K) \leq C_0 &= \lim_{n\to\infty} \frac{1}{n} \log\left(K\left(\mathcal{N}^{\otimes n}\right)\right) \\ &< C_0^E = \lim_{n\to\infty} \frac{1}{n} \log K^E\left(\mathcal{N}^{\otimes n}\right) \geq \log\left(K^E\right). \end{aligned} \tag{164}$$

Entanglement is very useful in zero-error quantum communication, since with the help of entanglement the maximum amount of perfectly transmittable information can be achieved.

As was show by Leung et al. [294], using special input codewords (based on a special Pauli graph), entanglement can help to increase the classical zero-error capacity to the maximum achievable HSW capacity; that is, there exists a special combination for which the entanglement-assisted classical zero-error capacity $C_0^E(\mathcal{N})$ is

$$C_0^E(\mathcal{N}) = \log(9), \tag{165}$$

while the classical zero-error capacity is

$$C_0(\mathcal{N}) = \log(7), \tag{166}$$

i.e., with the help of entanglement-assistance the number of possible input messages (*K*) can be increased.

Another important discovery is that for this special input system the entanglement-assisted classical zero-error capacity, $C_0^E(\mathcal{N})$, is equal to the maximal transmittable classical information over $\mathcal{N}$; that is

$$C_0^E(\mathcal{N}) = C(\mathcal{N}) = \log(9). \tag{167}$$

In the asymptotic setting the maximum achievable capacities as functions of block code length are summarized in Fig. 21.

The maximal amount of transmittable classical information which can be sent through a noisy quantum channel $\mathcal{N}$ without

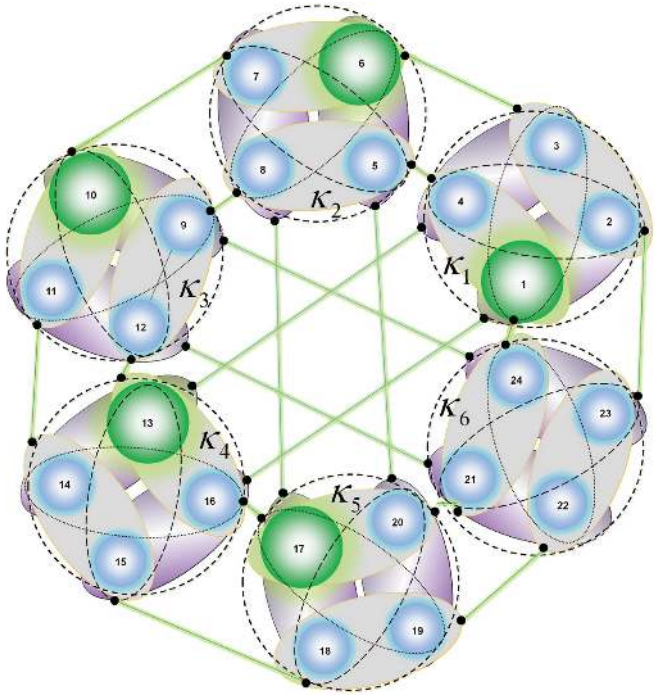

Fig. 20: The hypergraph of an entanglement-assisted zero-error quantum code. The non-adjacent inputs are depicted by the great shaded circles. The adjacent vertices are depicted by loops connected by the thick lines.

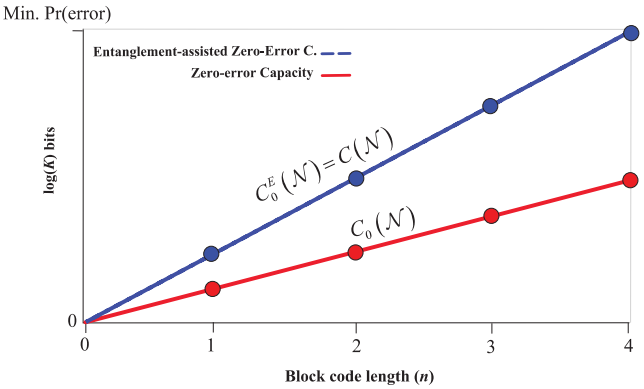

Fig. 21: The asymptotic classical zero-error capacities without entanglement and with entanglement assistance using a special Pauli graph.

error increases with the length of the input block code, and with the help of EPR input states (for this special Pauli graph-based code) the classical HSW capacity can be reached, which is also the upper bound of the classical zero-error capacity.

H. Related Work

The classical world with the classical communication channel can be viewed as a special case of a quantum channel, since classical information can be encoded into the qubits—just as into classical bits. Classical information can also be encoded in quantum states. In this section we summarize the most important works related to the classical capacity of the quantum channels.

a) The Early Days: At the end of the twentieth century, the capacities of a quantum channel were still an open problem in quantum information theory. Before the several, and rather different, capacities of the quantum channel were recognized, the 'academic' opinion was that quantum channels could be used only for the transmission of classical information encoded in the form of quantum states [231], [232]. As has been found later, the classical capacity of the quantum channel can be measured in several different settings. It was shown that the classical capacity depends on whether the input states are entangled or not, or whether the output is measured by single or by joint measurement setting [64], [163], [274]. In a specified manner, the classical capacity has been defined for measuring the maximal asymptotic rate at which classical information can be transmitted through the quantum channel, with an arbitrarily high reliability [46], [469].

The first proposed capacity measure was the *classical capacity* of a quantum channel—denoted by $C(\mathcal{N})$—measures the maximum transmittable classical information—in the form of product or entangled quantum states. The idea of transmitting classical information through a quantum channel was formulated in the 1970s. The Holevo bound was introduced by Holevo in 1973, however the theorem which describes the classical capacity of the quantum channel in an explicit way appeared just about *three decades later*, in the mid 1990s.

The maximal accessible classical information from a quantum source firstly has been characterized by Levitin [295] and Holevo [231], [232] in the early days, which were some of the first and most important results in quantum information theory regarding the classical capacity of quantum channels. More information about the connection between the Holevo bound and the accessible information (which quantifies the

information of the receiver after the measurement) can be found in [231], [232]. Later this result was developed and generalized by Holevo, Schumacher, and Westmoreland, and became known in quantum information theory as the *HSW channel capacity* [233], [469]. The HSW theorem uses the Holevo information to describe the amount of classical information which can be transmitted through a noisy quantum channel, and it makes possible to apply different measurement constructions on the sender and on the receiver's side. The proofs of the HSW theorem, such as the direct coding theorem and the converse theorem, with the complete mathematical background can be found in the work of Holevo [233] and of Schumacher and Westmoreland [469]. About the efficiency problems of implementation and construction of joint POVM (Positive Operator Valued Measure) measurement setting, as it was shown in the same works of the authors.

One of the most important result on the mechanism of the encoding of quantum information into physical particles was discovered by Glauber in the very early years of quantum information processing [183] and a great summarize from more than four-decades later [182]. Also from this era and field, important results on the encoding and decoding processes of quantum information were shown in the works of Gordon [185] and Helstrom [227]. About detection of quantum information and the process of measurement see [157], or the work of Helstrom from 1976 [227], or Herbert's work from 1982 [228]. Before their results, Levitin published a paper about the quantum measure of the amount of information in 1969 [295], which was a very important basis for further work.

b) Classical Capacity of a Quantum Channel: The amount of classical information which can be transmitted through a noisy quantum channel in a reliable form with product input states, using the quantum channel many times, was determined by the HSW theorem [233], [469]. This coding theorem is an analogue to Shannon's classical channel coding theorem, however it extends its possibilities. The inventors of the HSW theorem—Holevo, Schumacher and Westmoreland—proved and concluded independently the same result. Holevo's result from 1998 can be found in [233], Schumacher and Westmoreland's results can be found in [469]. They, with Hausladen et al. in 1995 [215], and in 1996 [216], have also confirmed that the maximal classical information which can be transmitted via pure quantum states is bounded by the Holevo information.

A different approach to the proof of the HSW theorem was presented by Nielsen and Chuang in 2000 [403]. An interesting connection between the mathematical background of the compressibility of quantum states and the HSW theorem was shown by Devetak in 2003 [134], who proved that a part of the mathematical background constructed for the compression of quantum information can be used to prove the HSW theorem. Another interesting approach for proving the HSW theorem and bounds on the error probability was presented by Hayashi and Nagaoka in 2003 [218]. The additivity property of qubit channels which require four inputs to achieve capacity was analyzed by Hayashi et al. in [219].

Very important connections regarding the transmission of classical information over noisy quantum channels was derived in the work of Schumacher and Westmoreland in 1997 [469], and two years later, a very important work was published on the relevance of optimal signal ensembles in the classical capacity of a noisy quantum channels [473]. (We also suggest their work on the characterizations of classical and quantum communication processes [474].) The classical information capacity of a class of most important practical quantum channels (Gaussian quantum channels) was shown by Wolf and Eisert [548] or the work of Lupo et al. [313]. The generalized minimal output entropy conjecture for Gaussian channels was studied by Giovannetti et al. [180].

About the role of feedback in quantum communication, we suggest the works of Bowen [79] and 2005 [80], the article of Bowen et al. [81], and the work of Harrow [213]. The works of Bowen provide a great introduction to the role of quantum feedback on the classical capacity of the quantum channel, it was still an open question before. As he concluded, the classical capacity of a quantum channel using quantum feedback is equal to the entanglement-assisted classical capacity, the proof was given in Bowen and Nagarajan's paper [81].

We have also seen that the noise of a quantum channel can be viewed as a result of the entanglement between the output and the reference system called the purification state (see purification in (77)). Some information leaks to the environment, and to the purification state, which purification state cannot be accessed. As is implicitly woven into this section, a noisy quantum channel can be viewed as a special case of an ideal quantum communication channel. The properties of the general quantum channel model and the quantum mutual information function can be found in the work of Adami and Cerf [4].

A great analysis of completely-positive trace preserving (CPTP) maps was published by Ruskai et al. [451]. Further information on the classical capacity of a quantum channel can be found in [65], [233], [274], [403].

c) Entanglement-assisted Classical Capacity: In the early 1970s, it was also established that the classical capacity of a quantum channel can be higher with *shared entanglement*—this capacity is known as the *entanglement-assisted classical capacity* of a quantum channel, which was completely defined by Bennett et al. just in 1999 [66], and is denoted by $C_E(\mathcal{N})$. The preliminaries of the definition of this quantity were laid down by Bennett and Wiesner in 1992 [58]. Later, in 2002 Holevo published a review paper about the entanglement-assisted classical capacity of a quantum channel [230].

Entanglement-assisted classical communication requires a super-dense protocol-like encoding and decoding strategy [54]. About the classical capacity of a noiseless quantum channel assisted by noisy entanglement, an interesting paper was published by Horodecki et al. in 2001 [235]. In the same work the authors have defined the 'noisy version' of the well-known superdense coding protocol, which originally was defined by Bennett in 1992 [58] for ideal (hence noiseless) quantum channels. As can be found in the works of Bennett et al. from 1999 [66] and from 2002 [54], the *entanglement-assisted classical capacity* opened the possibility to transmit more classical information using shared entanglement (in case of single-use

capacity). As can be checked by the reader, the treatment of entanglement-assisted classical capacity is based on the working mechanism of the well-known superdense coding protocol—however, classical entanglement-assisted classical capacity used a noisy quantum channel instead of an ideal one.

Bennett, in two papers from 1999 [66] and 2002 [54] showed that the *quantum mutual information* function (see Adami and Cerf's work [4]) can be used to describe the classical entanglement-assisted capacity of the quantum channel i.e., the *maximized quantum mutual information of a quantum channel and the entanglement-assisted classical capacity are equal.* The connection between the quantum mutual information and the entanglement-assisted capacity can be found in the works of Bennett et al. [54] and [66]. In the latter work, the formula of the quantum-version of the well-known classical Shannon formula was generalized for the classical capacity of the quantum channel. In these two papers the authors also proved that the entanglement-assisted classical capacity is an upper bound of the HSW channel capacity. Holevo gave an explicit upper bound on the classical information which can be transmitted through a noisy quantum channel, it is known as the Holevo-bound. The Holevo-bound states that the most classical information which can be transmitted in a qubit (i.e., two level quantum system) through a noiseless quantum channel in a reliable form, is one bit. However, as was shown later by Bennett et al. in 1999 [66], the picture changes, if the parties use shared entanglement (known as the *Bennett-Shor-Smolin-Thapliyal, or the BSST-* theorem). As follows, the BSST-theorem gives a closer approximation to the maximal transmittable classical information (i.e., to the 'single-use' capacity) over quantum channels, hence it can be viewed as the *true 'quantum version' of the well known classical Shannon capacity formula* (since it is a maximization formula), instead of the 'non entanglement-assisted' classical capacity. Moreover, the inventors of the BSST-theorem have also found a very important property of the entanglement-assisted classical capacity: *its single-use version is equal to the asymptotic version*, which implies the fact that no regularization is needed. (As we have seen in this section, we are not so lucky in the case of general classical and private classical capacities. As we will show in Section IV, we are 'unlucky' in the case of quantum capacity, too.) They have also found that no classical feedback channel can increase the entanglement-assisted classical capacity of a quantum channel, and this is also true for the classical (i.e., the not entanglement-assisted one) capacity of a quantum channel. These results were also confirmed by Holevo in 2002 [230]. It was a very important discovery in the history of the classical capacity of the quantum channel, and due to the BSST-theorem, the analogue with classical Shannon's formula *has been finally completed*. Later, it was discovered that in special cases the entanglement-assisted capacity of a quantum channel can be improved [211], [422]. The Holevo information can be attained even with pure input states, and the concavity of the Holevo information also shown. The concavity can be used to compute the classical HSW capacity of quantum channels, since the maximum of the transmittable information can be computed by a local maximum among the input states. Moreover, as was shown by Bennett et al. in 2002, the concavity holds for the entanglement-assisted classical capacity, too [54], [57]— the concavity, along with the non-necessity of any computation of an asymptotic formula, and the use of classical feedback channels to improve the capacity, *makes the entanglement-assisted classical capacity the most generalized classical capacity*—and it has the same role as Shannon's formula in classical information theory [57]. The fact that the classical feedback channel does not increase the classical capacity and the entanglement-assisted classical capacity of the quantum channel, follows from the work of Bennett et al., and the proof of the BSST-theorem [54]. Wang and Renner's work [529] introduces the reader to the connection between the single-use classical capacity and hypothesis testing.

d) The Private Classical Capacity: The third classical capacity of the quantum channel is the *private classical capacity*, denoted by $P(\mathcal{N})$. The concept of private classical capacity was introduced by Devetak in 2003 [134], and one year later by Cai et al. in 2004 [98]. Private classical capacity measures classical information, and it is always at least as large as the single-use quantum capacity (or the quantum coherent information) of any quantum channel. As shown in [138], for a degradable quantum channel the coherent information (see Section IV) is additive [138],—however for a general quantum channel these statements do not hold. The additivity of private information would also imply the fact that shared entanglement cannot help to enhance the private classical capacity for degradable quantum channels. The complete proof of the private classical capacity of the quantum channel was made by Devetak [134], who also cleared up the connection between private classical capacity and the quantum capacity. As was shown by Smith et al. [501], the private classical capacity of a quantum channel is additive for degradable quantum channels, and closely related to the quantum capacity of a quantum channel (moreover, Smith has shown that the private classical capacity is equal to the quantum coherent information for degradable channels), since in both cases we have to 'protect' the quantum states: in the case of private classical capacity the enemy is called Eve (the eavesdropper), while in the latter case the name of the enemy is 'environment.' As was shown in [134], the eavesdropper in private coding acts as the environment in quantum coding of the quantum state, and vice-versa. This 'gateway' or 'dictionary' between the classical capacity and the quantum capacity of the quantum channel was also used by Devetak [134], by Devetak and Shor [138] and by Smith and Smolin [501], using a different interpretation.

About the coherent communication with continuous quantum variables over the quantum channels a work was published Wilde et al. in [536] and [537]. On the noisy processing of private quantum states, see the work of Renes et al. [448]. A further application of private classical information in communicating over adversarial quantum channels was shown by Leung et al. [292]. Further information about the private classical capacity can be found in [83], [134], [137], [296], [501], [502], [503]. Another important work on non-additive quantum codes was shown by Smolin et al. [506]. A great

summary on the main results of Quantum Shannon Theory was published by Wilde [538]. For further information on quantum channel capacities and advanced quantum communications see the book of Imre and Gyongyosi [245], and also [200]. We also suggest the great work of Bennett et al. on the quantum reverse Shannon theorem [57]. A work on the connection of secure communication and Gaussian-state quantum Illumination was published by Shapiro [481].

e) The Zero-Error Classical Capacity: The properties of *zero-error* communication systems are discussed in Shannon's famous paper on the zero-error capacity of a noisy channel [478], in the work of Körner and Orlitsky on zero-error information theory [283], and in the work of Bollobás on modern graph theory [77]. We also suggest the famous proof of Lovász on the Shannon capacity of a graph [311]. The proof of the classical zero-error capacity of quantum channel can be found in Medeiros's work [320]. Here, he has shown, that the classical zero-error capacity of the quantum channel is also bounded above by the classical HSW capacity. The important definitions of quantum zero-error communication and the characterization of quantum states for the zero-error capacity were given by Medeiros et al., in [321]. On the complexity of computation of zero-error capacity of quantum channels see the work of Beigi and Shor [50]. The fact, that the zero-error classical capacity of the quantum channel can be increased with entanglement, was shown by Cubitt et al. in 2010 [123]. The role of entanglement in the asymptotic rate of zero-error classical communication over quantum channels was shown by Leung et al. in 2010 [294]. For further information about the theoretical background of entanglement-assisted zero-error quantum communication see [123] and for the properties of entanglement, the proof of the Bell-Kochen-Specker theorem in [51], [280].

IV. The Quantum Capacity of a Quantum Channel

Having discussed the general model of quantum channels and introduced various classical capacities in this section we focus on the *quantum information* transfer over quantum channels. Two new quantities will be explained. By means of *fidelity F* one can describe the differences between two quantum states e.g. between the input and output states of a quantum channel. On the other hand *quantum coherent information* represents the quantum information loss to the environment during quantum communication similarly as mutual information did for a classical channel *N*. Exploiting this latter quantity we can define the maximal quantum information transmission rate through quantum channels – the quantum capacity $Q(\mathcal{N})$ analogously to Shannon's noisy channel theorem. As we have seen Section III, the classical capacity of a quantum channel is described by the maximum of quantum mutual information and the Holevo information. The quantum capacity of the quantum channels is described by the maximum of *quantum coherent information*. The concept of quantum coherent information plays a fundamental role in the computation of the *LSD (Lloyd-Shor-Devetak)* channel capacity [134], [303], [487] which measures the asymptotic quantum capacity of the quantum capacity in general.

This section is organized as follows. First, we discuss the transmission of quantum information over a nosy quantum channel. Next, we define the quantum coherent information and overview its main properties. Finally the formula for the measure of maximal transmittable quantum information over a quantum channel will be introduced. The description of the most relevant works can be found in the Related Work subsection.

A. Preserving Quantum Information

The encoding and decoding quantum information have many similarities to the classical case, however, there exist some fundamental differences, as we will reveal in this section. In the case of quantum communication, the source is a quantum information source and the *quantum information* is encoded into quantum states. When transmitting quantum information, the information is encoded into non-orthogonal superposed or entangled quantum states chosen from the ensemble $\{\rho_k\}$ according to a given probability $\{p_k\}$. If the states $\{\rho_k\}$ are pure and mutually orthogonal, we talk about classical information; that is, in this case the quantum information reduces to classical.

Formulating the process more precisely (see Fig. 22) the encoding and the decoding mathematically can be described by the operators $\mathcal{E}$ and $\mathcal{D}$ realized on the blocks of quantum states. The input of the encoder consists of *m* pure quantum states, and the encoder maps the *m* quantum states into the joint state of *n* intermediate systems. Each of them is sent through an independent instance of the quantum channel $\mathcal{N}$ and decoded by the decoder $\mathcal{D}$, which results in *m* quantum states again. The output of the decoder $\mathcal{D}$ is typically mixed, according to the noise of the quantum channel. The rate of the code is equal to *m*/*n*.

Theoretically quantum states have to preserve their original superposition during the whole transmission, without the disturbance of their actual properties. Practically, quantum channels are entangled with the environment which results in mixed states at the output. Mixed states are classical probability weighted sum of pure states where these probabilities appear due to the interaction with the environment (i.e., noise). Therefore, we introduce a new quantity, which is able to describe the quality of the transmission of the superposed states through the quantum channel. The fidelity (see Appendix) for two pure quantum states is defined as

$$F(|\varphi\rangle, |\psi\rangle) = |\langle\varphi \mid \psi\rangle|^2. \tag{168}$$

The fidelity of quantum states can describe the relation of Alice pure channel input state $|\psi\rangle$ and the received mixed quantum system $\sigma = \sum_{i=0}^{n-1} p_i \rho_i = \sum_{i=0}^{n-1} p_i |\psi_i\rangle \langle\psi_i|$ at the channel output as

$$F(|\psi\rangle, \sigma) = \langle\psi|\sigma|\psi\rangle = \sum_{i=0}^{n-1} p_i |\langle\psi|\psi_i\rangle|^2. \tag{169}$$

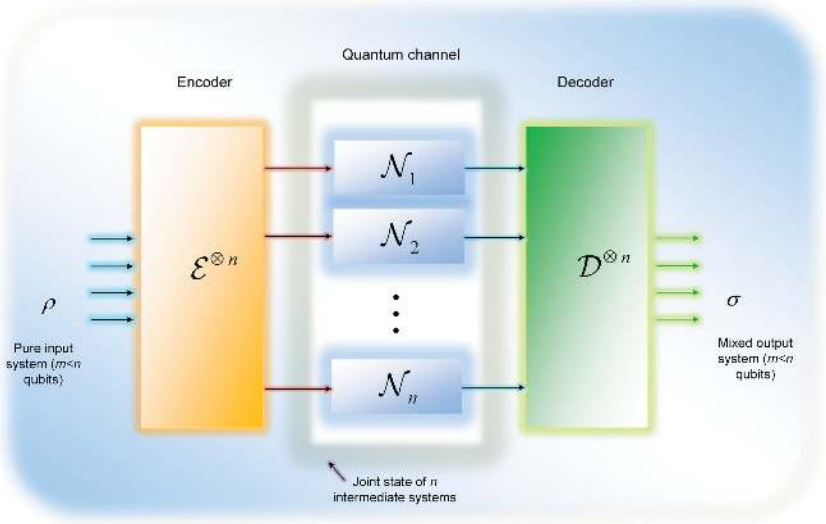

Fig. 22: Transmission of quantum information through the quantum channel. The encoder produces a joint state of *n* intermediate systems. The encoded qubits are passed through the independent instances of the quantum channel.

Fidelity can also be defined for *mixed* states σ and ρ

$$F(\rho,\sigma)=\left[Tr\left(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right)\right]^2=\sum_i p_i\left[Tr\left(\sqrt{\sqrt{\sigma_i}\rho_i\sqrt{\sigma_i}}\right)\right]^2. \tag{170}$$

Let us assume that we have a quantum system denoted by *A* and a reference system *P*. Initially, the quantum system *A* and the reference system *P* are in a *pure entangled* state, denoted by $\left|\psi^{PA}\right\rangle$. The density matrix ρ_A of system *A* can be expressed by a partial trace over *P*, as follows

$$\rho_A=Tr_P\left(\left|\psi^{PA}\right\rangle\left\langle\psi^{PA}\right|\right). \tag{171}$$

The entanglement between the initial quantum system and the reference state is illustrated in Fig. 23.

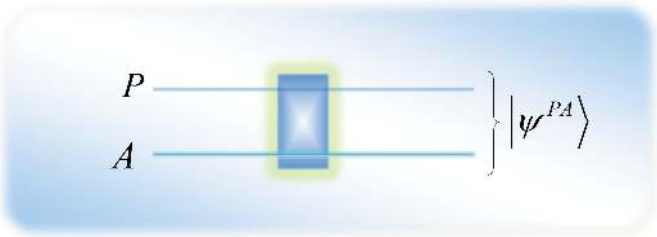

Fig. 23: Initially, the quantum system and the reference system are in a pure entangled state.

In the next step, ρ_A will be transmitted through the quantum channel $\mathcal{N}$, while the reference state *P* is *isolated from the environment* (see Section II), hence it has not been not modified during the transmission. After the quantum system ρ_A is transmitted through the quantum channel, the final state will be

$$\rho^{PB}=\left(\mathcal{I}^P\otimes\mathcal{N}^A\right)\left(\left|\psi^{PA}\right\rangle\left\langle\psi^{PA}\right|\right), \tag{172}$$

where $\mathcal{I}^P$ is the identity transformation realized on the reference system *P*. After the system *A* is sent through the quantum channel, both the quantum system *A* and the entanglement between *A* and *P* are affected, as we illustrated in Fig. 24. The resultant output system is denoted by B.

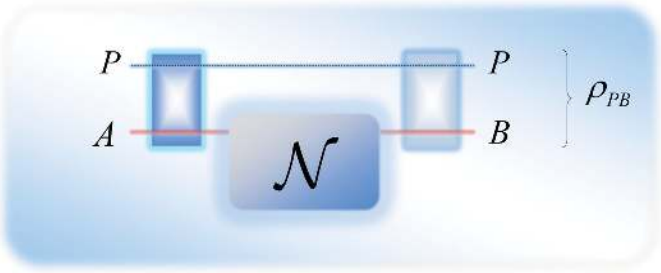

Fig. 24: After system *A* is sent through the quantum channel $\mathcal{N}$, both the quantum system *A* and the entanglement between *A* and *P* are affected.

Now, we can study the preserved entanglement between the two systems *A* and *P*. Entanglement fidelity F_E measures the fidelity between the initial pure system $\left|\psi^{PA}\right\rangle$ and the mixed output quantum system ρ_{PB} as follows

$$\begin{aligned}F_E&=F_E(\rho_A,\mathcal{N})=F\left(\left|\psi^{PA}\right\rangle,\rho_{PB}\right)\\&=\left\langle\psi^{PA}\right|\left(\mathcal{I}^P\otimes\mathcal{N}^A\right)\left(\left|\psi^{PA}\right\rangle\left\langle\psi^{PA}\right|\right)\left|\psi^{PA}\right\rangle.\end{aligned} \tag{173}$$

It is important to highlight the fact that F_E depends on $\left|\psi^{PA}\right\rangle$ i.e., on the reference system. The sender's goal is to transmit quantum information, i.e., to preserve entanglement between *A* and the inaccessible reference system *P*. Alice can apply many independent channel uses of the same noisy quantum channel $\mathcal{N}$ to transmit the quantum information. Similar to encoding classical information into the quantum states, the quantum messages can be transmitted over copies of a quantum channel. In this case, we have *n* copies of a quantum channel $\mathcal{N}$.

B. Quantum Coherent Information

In case of the classical capacity $C(\mathcal{N})$, the correlation between the input and the output is measured by the Holevo information and the quantum mutual information function. In case of the quantum capacity $Q(\mathcal{N})$, we have a completely different correlation measure with completely different behaviors: it is called the *quantum coherent information*. There is a *very important distinction* between the maximized quantum mutual information and maximized quantum coherent information: *the maximized quantum mutual information of a quantum channel $\mathcal{N}$ is always additive* (see Section II)*, but the quantum coherent information is not.*

The S_E *entropy exchange* between the initial system PA and the output system PB is defined as follows. The entropy that is acquired by PA when input system *A* is transmitted through the quantum channel $\mathcal{N}$ can be expressed with the help of the von Neumann entropy function as follows

$$\mathrm{S}_E = \mathrm{S}_E\left(\rho_A : \mathcal{N}\left(\rho_A\right)\right) = \mathrm{S}\left(\rho_{PB}\right), \tag{174}$$

or in other words the von Neumann entropy of the output system ρ_{PB}. As can be observed, the value of entropy exchange depends on ρ_A and $\mathcal{N}$ and is independent from the purification system *P*. Now, we introduce the environment state *E*, and we will describe the map of the quantum channel as a unitary transformation. The environment is initially in a pure state $|0\rangle$. After the unitary transformation $U_{A\to BE}$ has been applied to the initial system $A|0\rangle$, it becomes

$$U_{A\to BE}\left(A|0\rangle\right) = BE. \tag{175}$$

From the entropy of the *final state* of the environment ρ_E, the *entropy exchange* S_E can be expressed as

$$\mathrm{S}\left(\rho_{PB}\right) = \mathrm{S}\left(\rho_E\right) = \mathrm{S}_E. \tag{176}$$

S_E measures the increase of entropy of the environment *E*, or with other words, the entanglement between PA and *E,* after the unitary transformation $U_{A\to BE}$ had been applied to the system. This entropy exchange S_E is analogous to the classical conditional entropy; however in this case we talk about quantum instead of classical information.

Using the notations of Fig. 24, the quantum coherent information can be expressed as

$$\begin{aligned} I_{coh}\left(\rho_A : \mathcal{N}\left(\rho_A\right)\right) &= \mathrm{S}\left(\mathcal{N}\left(\rho_A\right)\right) - \mathrm{S}_E\left(\rho_A : \mathcal{N}\left(\rho_A\right)\right) \\ &= \mathrm{S}\left(\rho_B\right) - \mathrm{S}\left(\rho_{PB}\right) \\ &= \mathrm{S}\left(\rho_B\right) - \mathrm{S}\left(\rho_E\right), \end{aligned} \tag{177}$$

where $\mathrm{S}_E\left(\rho_A : \mathcal{N}\left(\rho_A\right)\right)$ is the entropy exchange as defined in (174).

Using the definition of quantum coherent information (177), it can be verified that quantum coherent information takes its maximum if systems *A* and *P* are *maximally entangled* and the quantum channel $\mathcal{N}$ is *completely noiseless*. This can be presented easily

$$\mathrm{S}\left(\rho_B\right) = \mathrm{S}\left(\rho_A\right), \tag{178}$$

since the input state ρ_A is maximally mixed, and

$$\mathrm{S}\left(\rho_{PB}\right) = 0, \tag{179}$$

because $\left|\psi^{PA}\right\rangle\left\langle\psi^{PA}\right|$ will remain pure after the state has been transmitted through the ideal quantum channel. If the input system $\left|\psi^{PA}\right\rangle\left\langle\psi^{PA}\right|$ is not a maximally entangled state, or the quantum channel $\mathcal{N}$ is not ideal, then the value of quantum coherent information will decrease.

Considering another expressive picture, quantum coherent information measures the quantum capacity as the difference between the von Neumann entropies of two channel output states. The first state is received by Bob, while the second one is received by a 'second receiver' - called the environment. If we express the transformation of a quantum channel as the partial trace of the overall system, then

$$\mathcal{N}\left(\rho_A\right) = Tr_E\left(U\rho_A U^\dagger\right), \tag{180}$$

and similarly, for the 'effect' of the environment *E*, we will get

$$E\left(\rho_A\right) = \rho_E = Tr_B\left(U\rho_A U^\dagger\right). \tag{181}$$

The results of (180) and (181) are summarized in Fig. 25.

It can be concluded that the quantum coherent information measures the capability of transmission of entanglement over a quantum channel. For the exact value of quantum coherent information of some important quantum channels see Section V.

C. Connection between Classical and Quantum Information

As it has been shown by Schumacher and Westmoreland [463], the I_{coh} quantum coherent information also can be expressed with the help of Holevo information, as follows

$$I_{coh}\left(\rho_A : \mathcal{N}\left(\rho_A\right)\right) = \left(\mathcal{X}_{AB} - \mathcal{X}_{AE}\right), \tag{182}$$

where

$$\mathcal{X}_{AB} = \mathrm{S}\left(\mathcal{N}_{AB}\left(\rho_{AB}\right)\right) - \sum_i p_i \mathrm{S}\left(\mathcal{N}_{AB}\left(\rho_i\right)\right) \tag{183}$$

and

$$\mathcal{X}_{AE} = \mathrm{S}\left(\mathcal{N}_{AE}\left(\rho_{AE}\right)\right) - \sum_i p_i \mathrm{S}\left(\mathcal{N}_{AE}\left(\rho_i\right)\right) \tag{184}$$

measure the Holevo quantities between Alice and Bob, and between Alice and environment *E*, where $\rho_{AB} = \sum_i p_i \rho_i$ and $\rho_{AE} = \sum_i p_i \rho_i$ are the average states. The definition of (182) also draws a very important connection: *the amount of transmittable quantum information can be derived by the Holevo information*, which measures classical information.

As follows, the *single-use* quantum capacity $Q^{(1)}(\mathcal{N})$ can be expressed as

$$\begin{aligned} Q^{(1)}(\mathcal{N}) &= \max_{all p_i, \rho_i} \left(\mathcal{X}_{AB} - \mathcal{X}_{AE}\right) \\ &= \max_{all p_i, \rho_i} \mathrm{S}\left(\mathcal{N}_{AB}\left(\sum_{i=1}^{n} p_i\left(\rho_i\right)\right)\right) - \sum_{i=1}^{n} p_i \mathrm{S}\left(\mathcal{N}_{AB}\left(\rho_i\right)\right) \\ &\quad - \mathrm{S}\left(\mathcal{N}_{AE}\left(\sum_{i=1}^{n} p_i\left(\rho_i\right)\right)\right) + \sum_{i=1}^{n} p_i \mathrm{S}\left(\mathcal{N}_{AE}\left(\rho_i\right)\right), \end{aligned} \tag{185}$$

where $\mathcal{N}\left(\rho_i\right)$ represents the *i*-th output density matrix obtained from the quantum channel input density matrix ρ_i.

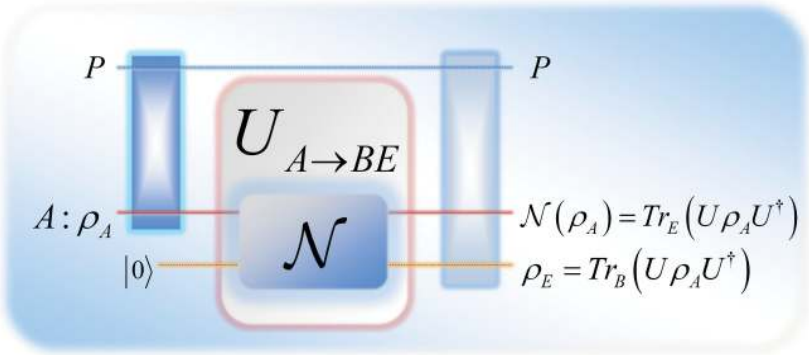

Fig. 25: The conceptional meaning of quantum coherent information. The unitary transformation represents the channel and the environment. The first receiver is Bob, the second is the environment. The state of the environment belonging to the unitary transformation is represented by dashed line. The outputs can be computed as the partial traces of the joint system.

The *asymptotic* quantum capacity $Q(\mathcal{N})$ can be expressed by

$$\begin{aligned} Q(\mathcal{N}) &= \lim_{n\to\infty}\frac{1}{n}Q^{(1)}\left(\mathcal{N}^{\otimes n}\right) \\ &= \lim_{n\to\infty}\frac{1}{n}\max_{all p_i,\rho_i} I_{coh}\left(\rho_A{:}\mathcal{N}^{\otimes n}(\rho_A)\right) \\ &= \lim_{n\to\infty}\frac{1}{n}\max_{all p_i,\rho_i}\left(\mathcal{X}_{AB}-\mathcal{X}_{AE}\right). \end{aligned} \tag{186}$$

The quantum capacity $Q(\mathcal{N})$ of a quantum channel $\mathcal{N}$ can also be expressed by $\mathcal{X}_{AB}$, the *Holevo quantity* of Bob's output and by $\mathcal{X}_{AE}$, the information leaked to the environment during the transmission.

1) Quantum Coherent Information and Quantum Mutual Information: Finally let us make an interesting comparison between quantum coherent information and quantum mutual information. For classical information transmission, the *quantum mutual information* can be expressed according to Section 2

$$I(A{:}B)=\mathrm{S}(\rho_A)+\mathrm{S}(\rho_B)-\mathrm{S}(\rho_{AB}). \tag{187}$$

However, in case of *quantum coherent information* (177) the term $\mathrm{S}(\rho_A)$ vanishes. The channel transformation $\mathcal{N}$ modifies Alice's original state ρ_A, hence Alice's original density matrix cannot be used to express $\mathrm{S}(\rho_A)$, *after Alice's qubit has been sent through* the quantum channel $\mathcal{N}$. After the channel has modified Alice's quantum state, the initially sent qubit vanishes from the system, and we will have a different density matrix, denoted by $\rho_B{=}\mathcal{N}(\rho_A)$. The coherent information can expressed as $\mathrm{S}(\rho_B)-\mathrm{S}(\rho_{AB})$, where ρ_B is the transformed state of Bob, and $\mathrm{S}(\rho_{AB})$ is the joint von Neumann entropy.

As follows, we will have $\mathrm{S}(\rho_B)-\mathrm{S}(\rho_{AB})$, which is equal to the *negative conditional entropy* $\mathrm{S}(A|B)$, (see Section II) thus

$$I_{coh}(\rho_A{:}\mathcal{N}(\rho_A))=\mathrm{S}(\rho_B)-\mathrm{S}(\rho_{AB})=-\mathrm{S}(A|B). \tag{188}$$

This imporatnt result is summarized in Fig. 26.

As we have seen in this section, there is a *very important difference* between the maximized quantum *mutual information* and the maximized *quantum coherent information* of a quantum channel. While the former is always additive, it does not remain true for the latter. *The quantum coherent information* is defined as follows

$$I_{coh}(\mathcal{N})=\mathrm{S}(\rho_B)-\mathrm{S}(\rho_E), \tag{189}$$

where ρ_B refers to the output of the quantum channel $\mathcal{N}$, while ρ_E is the state of the environment. The term $\mathrm{S}(\rho_B)$ measures how much information Bob has, while $\mathrm{S}(\rho_E)$ measures how much information environment has. As follows, the quantum coherent information $I_{coh}(\mathcal{N})$ measures that '*how much more information Bob has than the environment*' about the original input quantum state.

2) Quantum Coherent Information of an Ideal Channel: Now, we have arrived at the question of whether the $Q(\mathcal{N})$ quantum capacity of $\mathcal{N}$, as defined previously by the I_{coh} quantum coherent information, is an appropriate measure to describe the whole quantum capacity of a quantum channel. The answer is yes for an ideal channel. If we have a completely noiseless channel, then channel $\mathcal{N}_{AB}{=}I$ leads us to coherent information

$$\begin{aligned} Q(I) &= I_{coh}(I) \\ &= \mathrm{S}(\mathcal{N}_{AB}(\rho))-\mathrm{S}(\mathcal{N}_E(|0\rangle\langle 0|)) \\ &= \mathrm{S}(\rho). \end{aligned} \tag{190}$$

This equation can be used to calculate the $Q(\mathcal{N}_{AB})$ quantum capacity of a quantum channel (i.e., without maximization) only when we have a completely noiseless idealistic channel $\mathcal{N}_{AB}{=}I$. It also implies the following: to achieve the maximal coherent information for an idealistic quantum channel $\mathcal{N}_{AB}{=}I$, the input quantum states have to be maximally mixed states or one half of an EPR state, since in these cases, the von Neumann entropies will be maximal.

On the other hand, if the environment of the communication system interacts with the quantum state, the quantum capacity could vanish, but not the classical capacity of the channel. In this case, the quantum channel $\mathcal{N}_{AB}{=}I$ can transmit pure orthogonal states faithfully, but it cannot transmit the superposed or entangled states. Furthermore, if the interaction is more significant, it could result in an extremely noisy quantum channel for which the $C(\mathcal{N}_{AB})$ classical capacity of $\mathcal{N}_{AB}$ could also vanish.

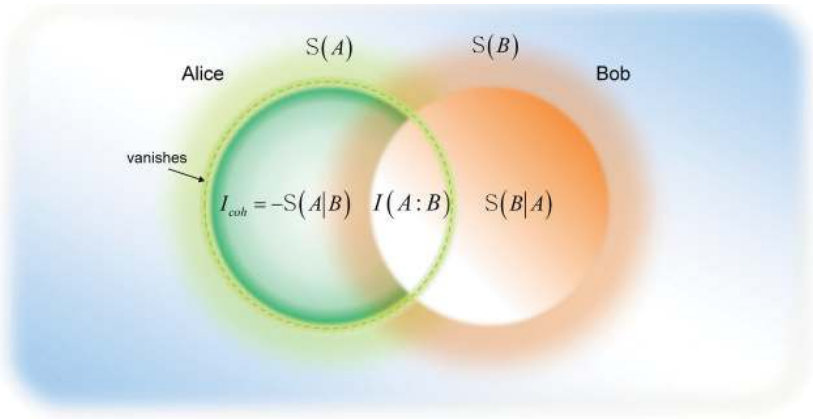

Fig. 26: The expression of quantum coherent information. The source entropy of Alice's state vanishes after the state is passed to Bob.

D. The Lloyd-Shor-Devetak Formula

The concept of quantum coherent information can be used to express the *asymptotic* quantum capacity $Q(\mathcal{N})$ of quantum channel $\mathcal{N}$ called the *Lloyd-Shor-Devetak (LSD)* capacity as follows

$$\begin{aligned} Q(\mathcal{N}) &= \lim_{n\to\infty} \frac{1}{n} Q^{(1)}\left(\mathcal{N}^{\otimes n}\right) \\ &= \lim_{n\to\infty} \frac{1}{n} \max_{all p_i,\rho_i} I_{coh}\left(\rho_A : \mathcal{N}^{\otimes n}(\rho_A)\right) \\ &= \lim_{n\to\infty} \frac{1}{n} \max_{all p_i,\rho_i} \left(S(\rho_B) - S(\rho_E)\right), \end{aligned} \tag{191}$$

where $Q^{(1)}(\mathcal{N})$ represents the *single-use* quantum capacity.

The asymptotic quantum capacity can also be expressed using the Holevo information, since as we have seen previously, the quantum coherent information can be derived from the Holevo information

$$Q(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \max_{all p_i,\rho_i} \left(\mathcal{X}_{AB} - \mathcal{X}_{AE}\right), \tag{192}$$

where $\mathcal{X}_{AB}$ denotes the classical information sent from Alice to Bob, and $\mathcal{X}_{AE}$ describes the classical information passed from Alice to the environment during the transmission.

Quantum coherent information plays a fundamental role in describing the maximal amount of transmittable quantum information through a quantum channel $\mathcal{N}$, and - as the Holevo quantity has deep relevance in the classical HSW capacity of a quantum channel - the quantum coherent information will play a crucial role in the LSD capacity of $\mathcal{N}$.

E. The Assisted Quantum Capacity

There is another important quantum capacity called *assisted capacity* which measures the quantum capacity for a channel pair that contains different channel models – and it will have relevance in the *superactivation* of quantum channels [497]. If we have a quantum channel $\mathcal{N}$, then we can find a symmetric channel $\mathcal{A}$, that results in the following assisted quantum capacity

$$Q_{\mathcal{A}}(\mathcal{N}) = Q(\mathcal{N} \otimes \mathcal{A}). \tag{193}$$

We note, that the symmetric channel has unbounded dimension in the strongest case, and this quantity cannot be evaluated in general. $Q_{\mathcal{A}}(\mathcal{N})$ makes it possible to realize the superactivation of zero-capacity (in terms of LSD capacity) quantum channels. For example if we have a zero-capacity *Horodecki channel* and a zero-capacity symmetric channel, then their combination can result in positive joint capacity [497].

F. The Zero-Error Quantum Capacity

Finally, let us shortly summarize the quantum counterpart of classical zero-error capacity. In the case of quantum zero-error capacities $Q_0^{(1)}(\mathcal{N})$ and $Q_0(\mathcal{N})$, the encoding and decoding process differs from the classical zero-error capacity: the encoding and decoding are carried out by the *coherent* encoder and *coherent* POVM decoder, whose special techniques make it possible to preserve the quantum information during the transmission [211], [241].

The *single-use* and *asymptotic* quantum zero-error capacity is defined in a similar way

$$Q_0^{(1)}(\mathcal{N}) = \log\left(K(\mathcal{N})\right), \tag{194}$$

and

$$Q_0(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \log\left(K\left(\mathcal{N}^{\otimes n}\right)\right), \tag{195}$$

where $K(\mathcal{N}^{\otimes n})$ is the maximum number of n-length mutually non-adjacent quantum messages that the quantum channel can transmit with zero error. The quantum zero-error capacity is upper bounded by LSD channel capacity $Q(\mathcal{N})$; that is, the following relation holds between the quantum zero-error capacities:

$$Q_0(\mathcal{N}) \leq Q(\mathcal{N}). \tag{196}$$

G. Relation between Classical and Quantum Capacities of Quantum Channels

Before introducing some typical quantum channel maps let us summarize the main properties of various capacities in conjunction with a quantum channels. First of all, the quantum capacity of $\mathcal{N}$ cannot exceed the maximal classical capacity that can be measured with entangled inputs and joint

measurement; at least, it is not possible in general. On the other hand, for some quantum channels, it is conjectured that the maximal *single-use* classical capacity - hence the capacity that can be reached with *product* inputs and a *single* measurement setting - is lower than the *quantum capacity* for the same quantum channel.

For all quantum channels

$$C(\mathcal{N}) \geq Q(\mathcal{N}), \tag{197}$$

where $C(\mathcal{N})$ is the classical capacity of the quantum channel that can be achieved with entangled input states and a joint measurement setting.

On the other hand, it is conjectured that for some quantum channels,

$$C(\mathcal{N}) < Q(\mathcal{N}) \tag{198}$$

holds as long as the classical capacity $C(\mathcal{N})$ of the quantum channel is measured by a classical encoder and a single measurement setting. (As we have seen in Section III, the classical capacities of a quantum channel can be measured in different settings, and the strongest version can be achieved with the combination of entangled inputs and joint measurement decoding.)

The fundamental differences between classical and quantum capacities are summarized in Table I.

It can be concluded from the table that in case of a quantum communication channel we have to count with so many capacities. Each of these capacities is based on different correlation measures: the *classical correlation* between the input and the output is measured by the quantum mutual information and the Holevo information. The private classical capacity is measured by the private information, which is the *maximization of the difference of two quantum mutual information functions.* For entanglement assisted capacity the correlation between input and output is also measured by the *maximized quantum mutual information*, however in this case we do not have to compute the asymptotic version to get the true capacity. Finally, the *quantum correlation* between the input and output is measured by the *quantum coherent information*.

H. Related Work

In this section we summarize the most important works regarding on the quantum capacity of the quantum channels.

The quantum capacity is one of the most important result of quantum information theory. The classical capacity of quantum channels was discovered in early years, in the beginning of the 1970s, and the researchers from this era —such as Holevo and Levitin—suggested that physical particles can encode only classical information [295], [231], [232]. The first step in the encoding of quantum information into a physical particle was made by Feynman, in his famous work from 1982 [160]. However, the researchers did not see clearly and did not understand completely the importance of quantum capacity until the late 1990s. As we have shown in Section III, a quantum channel can be used to transmit classical information and the amount of maximal transmittable information depends on the properties of the encoder and decoder setting, or whether the input quantum states are mixed or pure. Up to this point, we have mentioned just the transmission of classical information through the quantum channel—here we had broken this picture. The HSW theorem was a very useful tool to describe the amount of maximal transmittable classical information over a noisy quantum channel, however we cannot use it to describe the amount of maximal transmittable *quantum information.*

1) Quantum Coherent Information: The computation of quantum capacity is based on the concept of *quantum coherent information*, which measures the ability of a quantum channel to preserve a quantum state. The definition of quantum coherent information (in an exact form) was originally introduced by Schumacher and Nielsen in 1996 [468]. This paper is a very important milestone in the history of the quantum capacity, since here the authors were firstly shown that the concept of quantum coherent information can be used to measure the quantum information (hence not the classical information) which can be transmitted through a quantum channel. The first,—but yet not complete—definitions of the quantum capacity of the quantum channel can be found in Shor's work from 1995 [491], in which Shor has introduced a scheme for reducing decoherence in quantum computer memory, and in Schumacher's articles from one year later [467, 468]. Shor's paper from 1995 mainly discusses the problem of implementation of quantum error correcting schemes - the main focus was not on the exact definition of quantum capacity. Later, Shor published an extended version with a completed proof in 2002 [487]. To transmit quantum information the parties have to encode and decode coherently. An interesting engineering problem is how the receiver could decode quantum states in superposition without the destruction of the original superposition [536]. The quantum capacity of a quantum channel finally was formulated completely by the *LSD-theorem*, named after Lloyd, Shor and Devetak [134], [303], [487], and they have shown that the rate of quantum communication can be expressed by the quantum coherent information. The LSD-channel capacity states that the asymptotic quantum capacity of the quantum channel is greater than (or equal to in some special cases) the single-use capacity; hence it is not equal to the quantum coherent information.

More information about the properties of fidelity and about the connection with other distance measures can be found in Fuch's works [164], [166]. An important article regarding the fidelity of mixed quantum states was published by Jozsa in 1994 [257]. Fidelity also can be measured between entangled quantum states—a method to compute the fidelity of entanglement was published by Schumacher in 1996 [467]. Here, the upper bound of the quantum capacity was also mentioned, in the terms of quantum coherent information. Nielsen in 2002 [396] defined a connection between the different fidelity measures.

2) Proofs on Quantum Capacity: The exact measure of quantum capacity was an open question for a long time. The fact that the quantum capacity cannot be increased by classical communication was formally proven by Bennett et al. [62], who discussed the mixed state entanglement and quantum error correction. Barnum, in 2000 [43], defined the connection between the fidelity and the capacity of a quantum channel,

Capacity	Type of information	Correlation measure	Capacity formula
Classical	Classical information	Holevo information	HSW formula
Private Classical	Private information	Private information	Li-Winter-Zou-Guo, Smith-Smolin formula
Entanglement Assisted Classical	Classical information	Quantum mutual information	Bennett-Shor-Smolin-Thapliyal formula
Quantum	Quantum information	Quantum Coherent Information	LSD formula

TABLE I: The measure of classical and quantum capacities.

and here he also showed the same result as Bennett et al. did in 1996, namely that the quantum capacity cannot increased by classical communication [62]. The works of Barnum et al. [43] and Schumacher et al. [470] from the late 1990s gave very important results to the field of quantum information theory, since these works helped to clarify exactly the maximum amount of transmittable quantum information over very noisy quantum channels [538].

Seth Lloyd gave the first proof in 1997 on the quantum capacity of a noisy quantum channel. The details of Lloyd's proof can be found in [303], while Shor's results in detail can be found in [487]. On the basis of Shor's results, a proof on the quantum capacity was given by Hayden et al. in 2008 [224]. The next step in the history of the quantum capacity of the quantum channel was made by Devetak [134]. Devetak also gave a proof for the quantum capacity using the private classical capacity of the quantum channel, and he gave a clear connection between the quantum capacity and the private classical capacity of the quantum channel. As in the case of the discoverers of the HSW-theorem, the discoverers gave different proofs. The quantum capacity of a quantum channel is generally lower than the classical one, since in this case the quantum states encode quantum information. The quantum capacity requires the transmission of arbitrary quantum states, hence not just 'special' orthogonal states—which is just a subset of a more generalized case, in which the states can be arbitrary quantum states. On the several different encoder, decoder and measurement settings for quantum capacity see the work of Devetak and Winter [137], Devetak and Shor's work [138], and the paper of Hsieh et al. [241]. In this paper we have not mentioned the definition of unit resource capacity region and private unit resource capacity region, which can be found in detail in the works of Hsieh and Wilde [242], and Wilde and Hsieh [537]. In 2005, Devetak and Shor published a work which analyzes the simultaneous transmission of classical and quantum information [138].

On the quantum capacities of bosonic channels a work was published by Wolf, Garcia and Giedke, see [549]. In 2007, Wolf and Pérez-García published a paper on the quantum capacities of channels with small environment, the details can be found in [550]. They have also determined the quantum capacity of an amplitude damping quantum channel (for the description of amplitude damping channel, see Section V), for details see the same paper from 2007 [550]. The properties of quantum coherent information and reverse coherent information were studied by Patrón in 2009 [422].

The proofs of the LSD channel capacity can be found in [134], [303], [487]. The quantum communication protocols based on the transmission of quantum information were intensively studied by Devetak [135], and the work of the same authors on the generalized framework for quantum Shannon theory, from 2008 [139].

V. Quantum Channel Maps and Capacities

Here, we give a brief survey of some important quantum channel maps and study some capacity formulas. For the corresponding definitions related to the state-vector description we advise to the reader to [245].

A. Channel Maps

1) The Pauli Channel: The Pauli channel model having an input state ρ can be formulated [456] as

$$\rho \to C_P(\rho) = (1-p)\rho + p_x X\rho X + p_y Y\rho Y + p_x Z\rho Z, \quad (199)$$

where that X, Y and Z are single-qubit Pauli determined by

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad (200)$$

$$X = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad (201)$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (202)$$

Note that the depolarizing probability $p = p_x + p_y + p_z$ is the sum of p_x, p_y and p_z representing the depolarizing probability of Pauli X, Y and Z errors, respectively. The probabilities of the errors at time instant t are dependent to relaxation time T_1 and dephasing time T_2 as

$$\begin{aligned} p_x = p_y &= \frac{1}{4}\left(1 - \mathrm{e}^{-t/T_2}\right), \\ p_z &= \frac{1}{4}\left(1 + \mathrm{e}^{-t/T_1} - 2\mathrm{e}^{-t/T_2}\right). \end{aligned} \quad (203)$$

2) The Depolarizing Channel: The last discussed unital channel model is the *depolarizing* channel which performs the following transformation

$$\mathcal{N}(\rho_i) = p\frac{I}{2} + (1-p)\rho_i, \quad (204)$$

where p is the *depolarizing parameter* of the channel, and if Alice uses two orthogonal states ρ_0 and ρ_1 for the encoding then the mixed input state is

$$\rho = \left(\sum_i p_i\rho_i\right) = p_0\rho_0 + (1-p_0)\rho_1. \quad (205)$$

After the unital channel has realized the transformation $\mathcal{N}$ on state ρ, we will get the following result

$$\begin{aligned} \mathcal{N}\left(\sum_i p_i\rho_i\right) &= \mathcal{N}\left(p_0\rho_0 + (1-p_0)\rho_1\right) \\ &= p\frac{1}{2}I + (1-p)\left(p_0\rho_0 + (1-p_0)\rho_1\right). \end{aligned} \quad (206)$$

3) The Damping Channel: Let us consider the influences of an environment to a single qubit of a quantum system, where for example the qubit is realised by using a two-level atom having the ground state $|0\rangle$ and the excited state $|1\rangle$. The atom may have a spontaneous dissipation/absorption of energy to/from the environment, which makes the atom change its state from the ground state $|0\rangle$ to the excited state $|1\rangle$ or vice versa. The transition of the state is refered to as the decoherence process. As a result, the state of the qubit when there is no interaction with the environment is as follows [445]

$$\begin{aligned} |0\rangle|0\rangle_E &\rightarrow |0\rangle|0\rangle_E, \\ |0\rangle|1\rangle_E &\rightarrow |0\rangle|1\rangle_E, \\ |1\rangle|0\rangle_E &\rightarrow |1\rangle|0\rangle_E, \\ |1\rangle|1\rangle_E &\rightarrow |1\rangle|1\rangle_E, \end{aligned} \tag{207}$$

where $|0\rangle_E$ and $|1\rangle_E$ represent the low and high basis states of the environment. Accordingly, if the dissipation/absorption occurs, we have

$$\begin{aligned} |1\rangle|0\rangle_E &\rightarrow |0\rangle|1\rangle_E, \\ |0\rangle|1\rangle_E &\rightarrow |1\rangle|0\rangle_E. \end{aligned} \tag{208}$$

The transition represented by Eq. (208) is may be formulated as:

$$\begin{aligned} |1\rangle|0\rangle_E &\rightarrow \sqrt{1-p_l}|1\rangle|0\rangle_E + \sqrt{p_l}|0\rangle|1\rangle_E, \\ |0\rangle|1\rangle_E &\rightarrow \sqrt{1-p_o}|0\rangle|1\rangle_E + \sqrt{p_o}|1\rangle|0\rangle_E, \end{aligned} \tag{209}$$

where p_l and p_o is the probability of the atom losing its energy to the environment or obtaining its energy from the environment, respectively. We may generalise the channel model of Eq. (209) by alternating the basis states by the superposition states to lead to

$$\begin{aligned} &(\alpha|0\rangle + \beta|1\rangle)\,|0\rangle_E \rightarrow \\ &\qquad \left(\alpha|0\rangle + \beta\sqrt{1-p_l}|1\rangle\right)|0\rangle_E + \beta\sqrt{p_l}|0\rangle|1\rangle_E, \\ &(\alpha|0\rangle + \beta|1\rangle)\,|1\rangle_E \rightarrow \\ &\qquad \alpha\sqrt{p_o}|1\rangle|0\rangle_E + \left(\alpha\sqrt{1-p_o}|0\rangle + \beta|1\rangle\right)|1\rangle_E. \end{aligned}$$

It should be noted that the coefficient α and β may be used representing the $(N-1)$ qubit states orthogonal to the states $|0\rangle$ and $|1\rangle$ of the considered qubit. Moreover, if it can be assumed that each qubit interacts independently with the environment, the associated decoherence process in the N-qubit system may be considered as temporally and spatially uncorrelated. Accordingly, the process where the qubit loses its energy can be modelled by an amplitude damping channel C_{AD} having an input state ρ [177]:

$$\rho \rightarrow C_{AD}(\rho) = E_{AD1}\ \rho\ E_{AD1}^{\dagger} + E_{AD2}\ \rho\ E_{AD2}^{\dagger}, \tag{210}$$

where Kraus matrices E_{AD} used for characterising the amplitude damping channel are as follows:

$$E_{AD1} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p_l} \end{pmatrix}, \tag{211}$$

$$E_{AD2} = \begin{pmatrix} 0 & \sqrt{p_l} \\ 0 & 0 \end{pmatrix}. \tag{212}$$

Influences from the environment may results in random phase kicks on a single qubit. In such scenario, the decoherence process reflecting phase changes of the qubit is modelled as the phase damping channel $C_{PD}(\rho)$ as

$$\rho \rightarrow C_{PD}(\rho) = E_{PD1}\ \rho\ E_{PD1}^{\dagger} + E_{PD2}\ \rho\ E_{PD2}^{\dagger}, \tag{213}$$

where we have the corresponding Kraus matrices as

$$E_{AD1} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p_l} \end{pmatrix}, \tag{214}$$

$$E_{AD2} = \begin{pmatrix} 0 & \sqrt{p_l} \\ 0 & 0 \end{pmatrix}. \tag{215}$$

In order to reflect changes of the qubit in both phase and amplitude, the combination of amplitude and phase damping channel may be used. However, in general it is not affordable to classically simulate N-qubit combined channel, which requires to have a $2N$-dimensional Hilbert space. For the sake of facilitating efficient classical simulations, the combined amplitude and phase damping channel may be approximated using a Pauli channel model.

4) The Dephasing Channel Model: The second type of decoherence map discussed is unitary and results in relative phase differences between the computational basis states: the channel map which realizes it is called the *dephasing* map. In contrast to the amplitude damping map, it realizes a unitary transformation. The unitary representation of the dephasing quantum channel for a given input $\rho = \sum_{i,j} \rho_{ij}\,|\,i\rangle\,\langle\,j|$ can be expressed as

$$\mathcal{N}(\rho) = \sum_i \rho_{ii}\,|\,E_i\rangle\,\langle\,E_i|\,, \tag{216}$$

where $|\,E_i\rangle$ are the environment states. The dephasing quantum channel acts on the density operator ρ as follows

$$\mathcal{N}(\rho_i) = p\sigma_Z\rho\sigma_Z + (1-p)\,\rho_i, \tag{217}$$

where σ_Z is the Pauli Z-operator. The image of the dephasing channel map is similar to that of the phase flip channel map, however, the shrinkage of the original Bloch sphere is greater. The dephasing channel transforms an arbitrary superposed pure quantum state $\alpha\,|\,0\rangle + \beta\,|\,1\rangle$ into a mixture

$$\mathcal{N}(\rho) \rightarrow \rho' = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* e^{-\gamma(t)} \\ \alpha^*\beta e^{-\gamma(t)} & |\beta|^2 \end{bmatrix}, \tag{218}$$

where $\gamma(t)$ is a positive real parameter, which characterizes the coupling to the environment, using the time parameter *t*.

5) The Pancake Map: To give an example for physically not allowed (nonphysical, non-CP) transformations, we discuss the *pancake map*. The non-CP property means, that there exists no Completely Positive Trace Preserving map, which preserves some information along the equatorial spanned by the *x* and *y* axes of the Bloch sphere, while it completely demolishes any information along the *z* axis. This map is called the pancake map, and it realizes a physically not allowed (non-CP) transformation. The effect of the pancake map is similar to the bit-phase flip channel, however, this channel defines a non-CP transform: it 'smears' the original Bloch sphere along the equatorial spanned by the *x* and *y* axes. On

the other hand, the pancake map—besibdes the fact that is a non-physical map—can be used theoretically to transfer some information, and some information can be transmitted through these kinds of channel maps. The reason behind decoherence is Nature. She cannot be perfectly eliminated from quantum systems in practice. The reduction of decoherence is also a very complex task, hence it brings us on the engineering side of the problem: the quantum systems have to be designed in such a way that the unwanted interaction between the quantum states and the environment has to be minimal [491], [492]. Currently - despite the efficiency of these schemes - the most important tools to reduce decoherence are quantum error-correcting codes and decoupling methods.

B. Capacities

Next, we study the classical and quantum capacities of the following quantum channels:

1) *erasure quantum channel,*
2) *phase-erasure quantum channel,*
3) *mixed erasure/phase-erasure quantum channel,*
4) *amplitude damping channel.*

First we derive the classical capacities of these channels in closed forms. Then we give the quantum capacities and compare them.

1) Erasure Quantum Channel: The *erasure* quantum channel $\mathcal{N}_p$ erases the input state ρ with probability p or transmits the state unchanged with probability $(1-p)$

$$\mathcal{N}_p(\rho) \to (1-p)\,\rho + (p\,|e\rangle\,\langle e|)\,, \tag{219}$$

where $|e\rangle$ is the erasure state. The classical capacity of the erasure quantum channel $\mathcal{N}_p$ can be expressed as

$$C(\mathcal{N}_p) = (1-p)\log(d)\,, \tag{220}$$

where d is the dimension of the input system ρ. As follows from (220), the classical capacity of $\mathcal{N}_p$ vanishes at $p=1$, while if $0 \leq p < 1$ then the channel $\mathcal{N}_p$ can transmit some classical information.

The quantum capacity of the erasure quantum channel $\mathcal{N}_p$ is

$$Q(\mathcal{N}_p) = (1-2p)\log(d)\,. \tag{221}$$

$Q(\mathcal{N}_p)$ vanishes at $p=1/2$, but it can transmit some quantum information if $0 \leq p < 1/2$.

In Fig. 27, the classical (dashed line) and quantum capacity (solid line) of the erasure quantum channel as a function of erasure probability are shown.

2) Phase-Erasure Quantum Channel: The *phase-erasure* quantum channel $\mathcal{N}_\delta$ erases the phase of the input quantum state with probability p without causing any disturbance in the amplitude. Using input density matrix ρ, the map of the phase-erasure quantum channel can be expressed as

$$\mathcal{N}(\rho) \to (1-p)\,\rho \otimes |0\rangle\,\langle 0| + p\frac{\rho + Z\rho Z^\dagger}{2} \otimes |1\rangle\,\langle 1|\,, \tag{222}$$

where Z realizes the phase transformation on the input quantum system ρ, while the second qubit is used as a flag qubit.

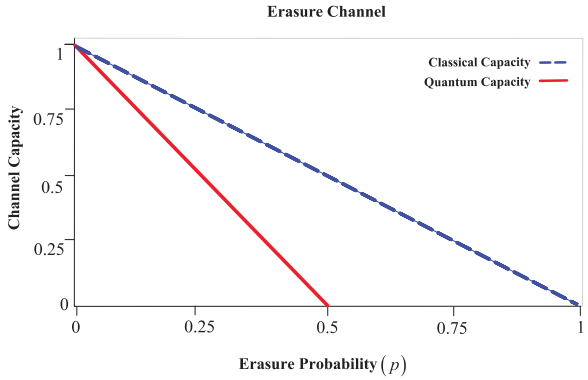

Fig. 27: The classical and quantum capacities of the erasure quantum channel as a function of erasure probability [Imre13].

The classical capacity of the $\mathcal{N}_\delta$ phase-erasure quantum channel using phase erasing probability q is

$$C(\mathcal{N}_\delta) = 1, \tag{223}$$

since the phase error has no effect on the distinguishability of orthogonal input quantum states $|0\rangle$ and $|1\rangle$. On the other hand, if we talk about quantum capacity $Q(\mathcal{N}_\delta)$ of $\mathcal{N}_\delta$ the picture changes:

$$Q(\mathcal{N}_\delta) = (1-q)\log(d)\,. \tag{224}$$

3) Mixed Erasure/Phase-Erasure Quantum Channel: From the erasure quantum channel and the phase-erasure quantum channel a third type of quantum channel can be constructed – the *mixed erasure/phase-erasure quantum channel*. This channel erases the input quantum system with probability p, erases the phase with probability q, and leaves the input unchanged with probability $1-p-q \geq 0$. Using (220) and (223), the classical capacity of the mixed erasure/phase-erasure quantum channel, $\mathcal{N}_{p+q}$, can be expressed as

$$C(\mathcal{N}_{p+q}) = (1-p)\log(d) = C(\mathcal{N}_p)\,. \tag{225}$$

Furthermore, combining (221) and (224), the quantum capacity of the mixed erasure/phase-erasure quantum channel, $\mathcal{N}_{p+q}$, we get

$$Q(\mathcal{N}_{p+q}) = (1-q-2p)\log(d)\,. \tag{226}$$

The classical (dashed line) and quantum capacities (solid line) of the mixed erasure/phase-erasure quantum channel as a function of total erasure probability $p+q$ are illustrated in Fig. 28.

4) Amplitude damping Quantum Channel: Finally, we give the quantum capacity of the amplitude damping channel. The classical capacity of the amplitude damping quantum channel can be expressed as

$$C(A_\gamma) = \max_\tau H(\tau) + [-H(\tau(\gamma)) + H(\tau(1-\gamma))]\,, \tag{227}$$

where $\tau \in [0,1]$ is a special parameter called the *population* parameter, and H is the Shannon entropy function, and

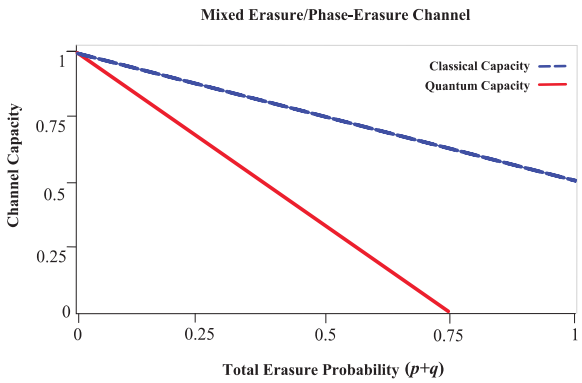

Fig. 28: The classical and quantum capacities of the mixed erasure/phase-erasure quantum channel as a function of total erasure probability [Imre13].

$H(\tau) = -\tau\log(\tau) - (1-\tau)\log(1-\tau)$. As follows from (227) the classical capacity $C(A_\gamma)$ of the amplitude damping channel completely vanishes if $\gamma = 1$, otherwise (if $0 \leq \gamma < 1$) the channel can transmit classical information. On the other hand for the quantum capacity $Q(A_\gamma)$ the capacity behaves differ.

The quantum capacity of this channel can be expressed as a maximization:

$$Q(A_\gamma) = \max_\tau \left[H(\tau(\gamma)) - H(\tau(1-\gamma))\right]. \tag{228}$$

The classical (dashed line) and the quantum capacity (solid line) of the amplitude damping quantum channel as a function of the damping parameter γ are shown in Fig. 29.

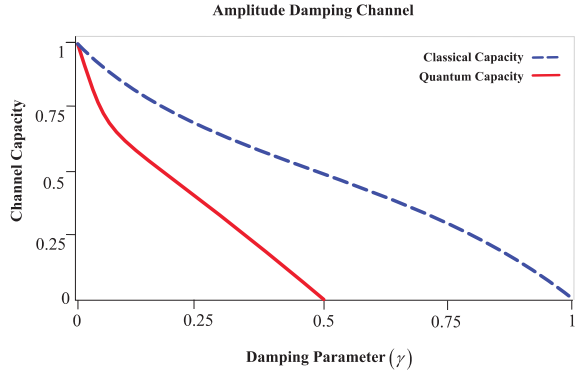

Fig. 29: The classical and quantum capacities of the amplitude damping quantum channel as a function of the damping parameter [Imre13].

It can be concluded that the working mechanism of the amplitude damping channel is similar to the erasure channel (see (220) and (221)), since if the damping parameter value is equal to or greater than 0.5, the quantum capacity of the channel completely vanishes. We obtained the same result for the erasure channel; however in that case the erasure probability p was the channel parameter.

VI. Practical Implementations of Quantum Channels

In this section, we focus on the physical and experimental implications of quantum channels in different scenarios.

A. Realistic Material: Asymmetric Depolarising Channel

A quantum depolarizing channel characterised by the probability p_x, p_y and p_z can be directly used for modelling quantum systems employing diverse materials. In other words, the quantum depolarizing channel can be used for modelling the imperfections in quantum hardware, namely, qubit flips resulting from quantum decoherence and quantum gates. Furthermore, a quantum depolarizing channel can also be invoked for modelling quantum-state flips imposed by the real transmission medium, including free-space wireless channels and optical fiber links, when qubits are transmitted across these media. For the sake of simpliciy, most recent studies of the quantum channel capacity [54], [66], [85], [539] as well as of quantum error correction (QEC) schemes considered the symmetric polarizing channel [34], [442], [540], where the constituent flip probabilities obey $p_x = p_y = p_z = p/3$. By contrast, popular materials invoked for producing quantum devices often exhibit asymmetric behaviour, where a phase flip is orders of magnitude more likely than a bit flip [308], which can be modelled by an asymmetric quantum depolarizing channel [75], [259], [426], [517], [519]. In such asymmetric depolarizing channels, an extra parameter α termed as the channel's ratio of asymmetry is introduced for reflecting the ratio of the phase flip probability p_z and the bit flip probability p_x as [156], [456]

$$\alpha = \frac{p_z}{p_x} = 1 + 2\frac{e^{\frac{-t}{T_1}} - e^{\left(\frac{-t}{2T_1} - \frac{2t}{T_2}\right)}}{1 - e^{\frac{-t}{T_1}}}. \tag{229}$$

Note that the bit flip probability p_x as well as the simultaneous bit-and-phase flip probability p_y may be considered to be equal [156], [456] while time instant t may be interpreted as the coherent operation duration of a physical quantum gate [541]. If the coherent operation duration t is relatively short, formulated as $t << T_1$, we can invoke the approximation of $\alpha \approx 2T_2/T_1 - 1$ [426]. As a result, the phase flip probability p_z can be directly determined from the values of α and p_x. Note that in the case of having $\alpha = 1$, the depolarising channel is the symmetric depolarizing channel, where the condition of having $p_x = p_y = p_z = p/3$ is satisfied. In practice the channel's ratio of asymmetry has popular values of $\alpha = 10^2, 10^4, 10^6$ [34], [442], [540], which correspond to the typical materials of Table II, which are used for producing quantum devices.

B. Acting Time in Asymmetric Channels

In the asymmtric depolarizing chanel, when the acting time [2] t of the channels under investigation is small, the value of α in Eq. (229) may be calculated by

$$\alpha = 1 + 2\frac{1 - e^{t/T_1(1 - T_1/T_2)}}{e^{t/(T_1 - 1)}}, \tag{230}$$

[2] t is the evolution time of the quantum system with the presence of decoherence, which can be considered to be equal to the duration of a physical quantum gate.

System (Material)	T_1	T_2	α
P:Si [517]	1 hour	1ms	10^6
GaAs Quantum Dots [426]	10ms	$> 1\mu$s	10^4
Super conducting (flux qubits) [75]	1μs	100 ns	10^2
Trapped ions [259]	100 ms	1 ms	10^2
Solid State NMR [519]	> 1 min	> 1 s	10^2

TABLE II: Estimated asymmetric ratio α representing various quantum depolarizing channels associated with various quantum devices.

Then, the bit flip probability p_x is calculated upon the asymmetric level α and the depolarizing probability of p as:

$$p_x = \frac{p}{\alpha+2}. \quad (231)$$

As a result, the phase flip probability p_z can be determined from the values of α and p_x. Since, the phase flip probability dominates over the bit flip one, the bit flip probability p_x and the bit-and-phase flip probability p_y may be considered to be equal.

We may use the precalculated α values in Table II for characterising the quantum channel. Since this way does not take in consideration the absolute values of t, T_1, T_2, it may not closely characterise different systems manufactured by different materials in Table II that are associated with the same value of α. The absolute values of t, T_1, T_2 may be used for calculating the depolarizing probabilities of p_x, p_z and p_y as follows [156]:

$$p_z(t) = \frac{1}{4\left[1+e^{\frac{-t}{T_1}}-2e^{\left(\frac{-t}{2T_1}-\frac{-2t}{T_2}\right)}\right]}, \quad (232)$$

$$\begin{aligned} p_x(t) &= p_y(t), \quad (233)\\ &= \frac{1}{4(1-e^{\frac{-t}{T_1}})}. \end{aligned}$$

Accordingly, the encoding and decoding gate operation times pertaining to different materials are listed in Table III.

C. Implementation of Quantum Channel in FSO-based Quantum Key Distribution

Depending on the specific form of the electromagnetic plane wave pertaining to the monochromatic laser signal generating photons, photons may be linearly polarized (LP) or elliptically polarized (EP) [417]. In the context of considering Quantum Key Distribution (QKD) systems, we only consider LP photons having polarizations of say $0^0, 90^0, -45^0, 45^0$ [564]. Accordingly, the basis associated with the polarization of $0^0, 90^0$ can be characterised by:

$$|0^0\rangle = 1|0^0\rangle + 0i|90^0\rangle, \quad (234)$$

$$|90^0\rangle = 0|0^0\rangle + i|90^0\rangle. \quad (235)$$

The relationship between the two bases can also be expressed by:

$$|0^0\rangle = \frac{1}{\sqrt{2}}|45^0\rangle + \frac{i}{\sqrt{2}}|-45^0\rangle, \quad (236)$$

$$|90^0\rangle = \frac{1}{\sqrt{2}}|45^0\rangle - \frac{i}{\sqrt{2}}|-45^0\rangle. \quad (237)$$

An FSO quantum transmission channel is used for carrying the photon stream to from the source (S) to the destination (D). Since the FSO channel imposes deleterious effects, such as diffraction, atmospheric turbulence and extinction [515], only a certain fraction γ of the photon stream transmitted by S arrives at D. In other words, the term γ invoked for characterising the power transfer properties of the FSO channel over a distance L imposed on the QKD system's performance is approximated by [170], [453], [480]

$$\gamma = \mu e^{-\alpha L}, \quad (238)$$

where μ represents the diffraction losses or the normalised version of the fraction γ, while α is the extinction coefficient.

The value of μ depends on the Fresnel number of

$$D_f^0 = \left(\frac{\pi d_1 d_2}{4\lambda L}\right)^2, \quad (239)$$

where d_1 is the transmit aperture diameter and d_2 is the receiver's aperture diameter, while λ is the wavelength of the optical signal.

In the near-field region having $D_f^0 >> 1$, the parameter μ is bounded by [479], [480]

$$\mu_{NF,LB} \leq \mu \leq \mu_{NF,UB}, \quad (240)$$

where the upper bound $\mu_{NF,UB}$ can be calculated by [480]

$$\mu_{NF,UB} = \min(D_f^0, 1), \quad (241)$$

while the lower bound $\mu_{NF,LB}$ is given by [480]

$$\begin{aligned} \mu_{NF,LB} &= \frac{8\sqrt{D_f^0}}{\pi}\int_0^1 \exp\left(\frac{-D(d_2 x)}{2}\right) \quad (242)\\ &\times\left(\arccos(x) - x\sqrt{1-x^2}\right) J_1\left(4x\sqrt{D_f^0}\right) dx, \end{aligned}$$

where $J_1(.)$ is the first-order Bessel function. The spherical-wave structure function $D(\rho)$ of Eq. (242) is calculated for the worse-case scenario of having $d_1 = d_2$ as [480]:

$$D(\rho) = 51\sigma_R^2 \left(D_f^0\right)^{5/12} \rho^{5/3}, \quad (243)$$

where σ_R^2 is the Rytov variance [261] of

$$\sigma_R^2 = 1.24\left(\frac{2\pi}{\lambda}\right)^{7/6} C_n^2 L^{11/6}, \quad (244)$$

with C_n^2 ranging from 10^{-13} to 10^{-17} representing the altitude-dependent index of the refractive structure parameter [566].

By contrast, in the far-field region having $D_f^0 << 1$, the value of μ can be calculated by [479]

$$\begin{aligned} \mu_{FF} &= \frac{8\sqrt{D_f^0}}{\pi}\int_0^1 \exp\left(\frac{-D(d_2 x)}{2}\right) \quad (245)\\ &\times\left(\arccos^{-1}(x) - x\sqrt{1-x^2}\right) J_1\left(4x\sqrt{D_f^0}\right) dx, \end{aligned}$$

Quantum Systems	Time per gate Operation (sec)	Coherence time	Maximal number of coherence steps
Electrons from a gold atom	10^{-14}	10^{-8}	10^{6}
Trapped indium atoms	10^{-14}	10^{-1}	10^{13}
Optical micro cavity	10^{-14}	10^{-5}	10^{9}
Electron spin	10^{-7}	10^{-3}	10^{4}
Electron quantum dot	10^{-6}	10^{-3}	10^{3}
Nuclear spin	10^{-3}	10^{4}	10^{7}

TABLE III: Maximal number of computational steps that can be performed without losing coherence

where the spherical-wave structure function $D(\rho)$ of Eq. (245) can be calculated by

$$D(\rho) \quad = \quad 1.09 \left(\frac{2\pi}{\lambda}\right)^2 C_n^2 L \rho^{5/3}. \tag{246}$$

As a result, when a more accurate value range of γ is sought, the following bounds should be used (see Fig. 30)

$$\gamma_{LB} \quad \leq \quad \gamma \leq \gamma_{UB}, \tag{247}$$

where the upper bound γ_{UB} is determined by:

$$\gamma_{UB} = \begin{cases} \gamma_{NF,UB} & : \text{ if } D_f^0 > T_{near} \\ (\gamma_{NF,UB} + \gamma_{FF})/2 & : \text{ if } T_{far} \leq D_f^0 \leq T_{near} \\ \gamma_{FF} & : \text{ if } D_f^0 < T_{far} \end{cases}, \tag{248}$$

while the lower bound γ_{LB} is calculated by:

$$\gamma_{LB} = \begin{cases} \gamma_{NF,LB} & : \text{ if } D_f^0 > T_{near} \\ (\gamma_{NF,LB} + \gamma_{FF})/2 & : \text{ if } T_{far} \leq D_f^0 \leq T_{near} \\ \gamma_{FF} & : \text{ if } D_f^0 < T_{far} \end{cases}, \tag{249}$$

where the region having $T_{far} \leq D_f^0 \leq T_{near}$ is the transition region between the near-field and far-field regimes.

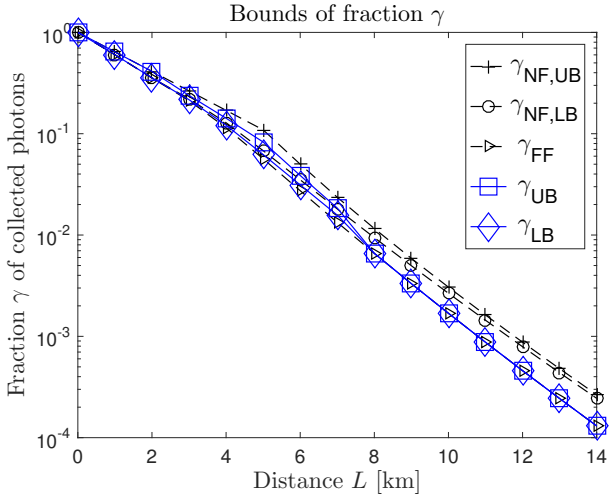

Fig. 30: Bounds of γ characterised by Eq. (247) for a transition region of ($T_{far} = 0.5 \leq D_f^0 \leq T_{near} = 5$).

D. Quantum Channel Codes for Approaching Quantum Channel Capacity

The appealing parallelism of quantum computing relying on quantum bits has inspired researchers to consider various quantum-related applications in the area of quantum communications [143], [263], [313], [314], [421], [457]. However, a crucial obstacle to the practical realisation of quantum communications systems is the presence of quantum perturbations. Their deleterious effects can be mitigated by Quantum Error Correction Codes [54]. It was suggested that the employment of entanglement assistance is capable of further improving the performance of QECCs [442], [540] in the context of the so-called symmetric depolarizing channel, which has been routinely used in theoretical studies. In the symmetric depolarizing channel characterised by the gross depolarizing probability p, each transmitted qubit may independently experience either a bit flip (X), a phase flip (Z), or both (Y) at a probability of $p_x = p_y = p_z = p/3$. By contrast, the materials considered at the time of writing for building quantum devices, including trapped ions [460] and solid state Nuclear Magnetic Resonance [519], exhibit asymmetric depolarization property defined as the ratio of the phase flip probability over the bit flip probability, where the grade of asymmetry is in the range spanning from $\alpha = 10^2$ to $\alpha = 10^6$ [333-337]. QECCs designed for the asymmetric depolarizing channel were termed as asymmetric QECCs in [338-343], where a limited range of α values was assumed and no entanglement assistance was addressed. In [344], a more general framework covering both symmetric and asymmetric depolarizing channels was proposed for Entanglement Assisted QECCs (EAQECCs).

To benchmark the design of the EAQECCs, the Entanglement Assisted Quantum Channel's (EAQC) capacity was investigated in [85], [539]. Accordingly, the so-called Hashing bound is advocated for setting a lower limit on the achievable quantum depolarizing channel capacity, which has been used for benchmarking the performance of various QECC schemes in [34], [345], [540]. Furthermore, the powerful Extrinsic Information Transfer (EXIT) chart technique [346-350] that was originally introduced for analysing the convergence behaviour of iterative decoding and detection in conventional communication systems was recently further developed for analysing the iterative decoding convergence of QECCs [345]. In [344], entanglement assisted quantum coding schemes and the associated quantum depolarizing channel capacity were considered for both asymmetric and symmetric quantum depolarizing channels.

E. Quantum Network Coding for Entanglement Distribution

In the classical domain, network coding [351, 352] is capable of increasing the throughput, while minimising the amount of energy required per packet as well as the delay of packets travelling through the network [353, 354]. This is

achieved by allowing the intermediate nodes of the network to combine multiple data packets received via the incoming links before transmission to the destination [355]. Due to its merits, the concept of the network coding has been applied in diverse disciplines [356].

Inspired by its classical counterpart [352, 357, 358], the question arises if the quantum version of network coding exists. Due to the inherent nature of quantum communications, namely that cloning is impossible, negative answers to this cardinal question were suggested in [359, 360]. However, further studies of Quantum Network Coding (QNC) confirm that given the availability of extra resources, such as preshared entanglement [361-368] or the abundance of low-cost classical communications [360, 369-371], QNC can indeed be made feasible.

Entanglement consitutes a valuable enabler of various quantum protocols that are essential for various applications of quantum communications, such as quantum teleportation [372], remote state preparation [373], quantum remote measuring [374] and secret sharing [375]. Entanglement refers to the fact that two or more photons have a very special connection, whereby changing for example the spin of a photon will instantaneously change that of its entangled couterpart. Anecdotally, this phenomenon is referred to as a "spooky action at a distance" by Einstein [153] due to the fact that unlike in electromagnetism, interactions between entangled photons occur instantaneously, regardless of how far apart the photons are. By contrast, electromagnetic interactions are bounded by the speed of light [246].

In such quantum protocols, the entangled qubits have to be distributed to distant nodes. A particularly popular application of the entanglement distribution is QKD [376], which has been gradually finding its way into different practical scenarios, such as satellite communications [377, 378], terrestrial communications [379, 380] and over handheld communication [381, 382]. These advances lay the foundations of the quantum Internet [383-385]. Entanglement distribution over a large-scale network consisting of multiple-hops and multiple-nodes can be realised by Entanglement Swapping (ES) [386-388] or by QNC [363, 365, 389]. ES may be deemed to be similar to the classic Decode-and-Forward (DF) techniques, which is outperformed by the classical Network Coding (NC) in a number of practical scenarios [390-392]. This leads to another intriguing and crucial question, namely whether the QNC is similarly capable of providing a better performance than ES. In order to answer the second question, Satoh *et al.* [363] provided quantitative comparisons between the QNC and the ES. Explicitly, it was shown that the fidelity-performance of the ES-based system is superior to that of the QNC-based system in a quantum communication network having $M = 2$ pairs of source-to-target users that are connected via a backbone link having $N = 1$ hop. However, Nguyen *et al.* [393] generalised the QNC of [363, 365] to large-scale quantum communication networks, in order to demonstrate the benefits of large-scale QNC over ES.

VII. Conclusions

Quantum channels extend the possibilities of classical communication channels allowing us to transmit classical information, entanglement assisted classical information, private classical information and quantum information. Contrary to classical channels, quantum channels can be used to construct more advanced communication primitives. Quantum entanglement or the superposed states carry quantum information, which cannot be described classically. Quantum channels can be implemented in practice easily e.g. via optical fiber networks or by wireless optical channels, and make it possible to send various types of information. The errors are a natural interference from the noisy environment, and the can be much diverse due to the extended set of quantum channel models. In the near future, advanced quantum communication and networking technologies driven by quantum information processing will revolutionize the traditional methods. Quantum information will help to resolve still open scientific and technical problems, as well as expand the boundaries of classical computation and communication systems.

References

[1] A. Abeyesinghe, P. Hayden, G. Smith, and A. J.Winter, "Optimal superdense coding of entangled states," *IEEE Transactions on Information Theory*, vol. 52, pp. 3635–3641, (2006).

[2] Abramson, N.: The Aloha system-another alternative for computer communications. *AFIPS Conf. Proc*. 36, pp. 295-298, (1970).

[3] M. Ackermann, J. Blömer, and C. Sohler. Clustering for metric and non-metric distance measures. In *Proceedings of the 19th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA '08),* pages 799–808. Society for Industrial and Applied Mathematics, (2008).

[4] C. Adami and N. J. Cerf, On the von Neumann capacity of noisy quantum channels, *arXiv:quant-ph/9609024v3* (1996).

[5] P. Agarwal. Range searching. In J. E. Goodman and J. O'Rourke, editors, *Handbook of Discrete and Computational Geometry*, 2nd edition., chapter 36. Chapman & Hall/CRC, (2004).

[6] P. Agarwal, J. Pach, and M. Sharir. State of the union (of geometric objects): A review. In J. Goodman, J. Pach, and R. Pollack, editors, *Computational Geometry*: Twenty Years Later. American Mathematical Society, (2007).

[7] D. Aharonov and M. Ben-Or, Fault-tolerant quantum computation with constant error. In *STOC '97: Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*, pp 176-188, New York, NY, USA, ACM, (1997).

[8] R. Ahlswede and A. J. Winter. Strong converse for identication via quantum channels. *IEEE Transactions in Information Theory*, 48(3):569-579, arXiv:quant-ph/0012127, (2002).

[9] R. Alicki and M. Fannes, "Note on multiple additivity of minimal entropy output of extreme SU(d)-covariant channels", *Open Systems and Information Dynamics* 11, 339 - 342 (2004).

[10] S. Aluru. Quadtrees and octrees. In D. Metha and S. Sahni, editors, *Handbook of Data Structures and Applications*, chapter 19. Chapman & Hall/CRC, (2005).

[11] S. Amari and H. Nagaoka: Methods of Information Geometry. *Translations of Mathematical Monographs*, 191. AMS, Oxford University Press, Oxford, (2000).

[12] S. Amari and H. Nagaoka: Methods of Information Geometry. Translated from the 1993 Japanese original by Daishi Harada. *Translations of Mathematical Monographs*, 191. AMS, Oxford University Press, Oxford, (2000).

[13] N. Amato, M. T. Goodrich, and E. A. Ramos. A randomized algorithm for triangulating a simple polygon in linear time. *Discrete Comput. Geom.*, 26:245– 265, 2001.

[14] G. Amosov. Remark on the additivity conjecture for the quantum depolarizing channel, http://arxiv.org/abs/quant-ph/0408004, (2004).

[15] G. Amosov, "The strong superadditivity conjecture holds for the quantum depolarizing channel in any dimension", *Phys. Rev. A* 75, 2104 - 2117 (2007).

[16] G. Amosov, A. S. Holevo and R. F. Werner, "On some additivity problems in quantum information theory", *Problems in Information Transmission* 36, 305 - 313 (2000).

[17] L. Arge, G. Brodal, and L. Georgiadis. Improved dynamic planar point location. In Proc. 47th Annu. *IEEE Sympos. Found. Comput. Sci*., pages 305–314, (2006).

[18] S. Arimoto. An algorithm for calculating the capacity of an arbitrary discrete memoryless channel. *IEEE Trans. Inf. Theory*, 18:14–20, (1972).

[19] P. Arrighi, V. Nesme, & R. Werner, Unitarity plus causality implies localizability, *Proceedings of the Quantum Information Processing* 2010 conference (QIP2010). (2010).

[20] T. Asano, N. Katoh, N. Tamaki, and T. Tokuyama. Angular Voronoi diagram with applications. In *Proceedings of 3rd International Symposium on Voronoi Diagram in Science and Engineering*, pages 32–39, Banff, Canada, (2006).

[21] T. Asano, N. Katoh, N. Tamaki, and T. Tokuyama. Voronoi diagram with respect to criteria on vision information. In *Proceedings of 4th International Symposium on Voronoi Diagram in Science and Engineering*, pages 25–32, Wales, UK, (2007).

[22] T. Asano. Aspect-ratio voronoi diagram and its complexity bounds. *Information Processing Letters*, 105(1. 31):26–31, (2007).

[23] A. Aspect, P. Grangier, and G. Roger. Experimental tests of realistic local theories via Bell's theorem, *Physical Review Letters*, 47(7):460-463, (1981).

[24] G. Aubrun, S. Szarek, and E. Werner, "Hastings' additivity counterexample via Dvoretzky's theorem," ArXiv e-prints*, arXiv:1003.4925*. (2010).

[25] K. M. R. Audenaert. A sharp continuity estimate for the von Neumann entropy. *Journal of Physics A: Mathematical and Theoretical*, 40(28):8127, (2007).

[26] F. Aurenhammer and R. Klein. Voronoi Diagrams. In J. Sack and G. Urrutia (Eds), *Handbook of Computational Geometry,* Chapter V, pp. 201–290. Elsevier *Science* Publishing, (2000).

[27] F. Aurenhammer and H. Edelsbrunner. An optimal algorithm for constructing the weighted Voronoi diagram in the plane. *Pattern Recogn*., 17:251–257, (1984).

[28] F. Aurenhammer, "Power diagrams: properties, algorithms and applications," *SIAM J. Comput*., vol. 16, no. 1, pp. 78–96, (1987).

[29] F. Aurenhammer. Voronoi diagrams: A survey of a fundamental geometric data structure. *ACM Comput. Surv*., 23:345–405, (1991).

[30] F. Aurenhammer and O. Schwarzkopf. A simple on-line randomized incremental algorithm for computing higher order Voronoi diagrams. *Internat. J. Comput. Geom. Appl.*, 2:363–381, (1992).

[31] F. Aurenhammer, F. Hoffmann, and B. Aronov. Minkowski-type theorems and least-squares clustering. *Algorithmica*, 20:61–76, (1998).

[32] K. Azuma, N. Sota, R. Namiki, S. Kaya Ozdemir, T. Yamamoto, M. Koashi, Optimal entanglement generation for efficient hybrid quantum repeaters, *Physical Review A* 80, 060303(R) (2009).

[33] Z. Babar, S. X. Ng, and L. Hanzo, "Near-capacity code design for entanglement-assisted classical communication over quantum depolarizing channels," *IEEE Transactions on Communications*, vol. 61, pp. 4801–4807, (2013).

[34] Z. Babar, S. X. Ng, and L. Hanzo, "Exit-chart-aided near-capacity quantum turbo code design," *IEEE Transactions on Vehicular Technology*, vol. 64, pp. 866–875 (2015).

[35] L. Bacsardi, Using Quantum Computing Algorithms in Future Satellite Communication, *ACTA ASTRONAUTICA* 57: pp. 224-229. (2005)

[36] L. Bacsardi, Satellite Communication Over Quantum Channel, *ACTA ASTRONAUTICA* 61:(1-6) pp. 151-159. (2007)

[37] L. Bacsardi, S. Imre, Quantum Based Information Transfer in Satellite Communication, *Satellite Communications*, SCIYO, 2010. pp. 421-436.

[38] L. Bacsardi, On the Way to Quantum-Based Satellite Communication, *IEEE COMMUNICATIONS MAGAZINE* 51:(08) pp. 50-55. (2013)

[39] M. Badoiu, S. Har-Peled, and P. Indyk. Approximate clustering via core-sets. In *Proceedings 34th ACM Symposium on Theory of Computing*, pages 250–257, (2002).

[40] Y-K. Bai, S. Li and H. Zheng, "Method for measuring two-qubit entanglement of formation by local operations and classical communication", *J. Phys. A*: Math. Gen. 38 8633, doi: 10.1088/0305-4470/38/40/010 (2005).

[41] Banerjee, Arindam; Merugu, Srujana; Dhillon, Inderjit S.; Ghosh, Joydeep "Clustering with Bregman divergences". *Journal of Machine Learning Research* 6: 1705–1749. (2005).

[42] H. Barnum, C. Caves, C. Fuchs, R. Jozsa, and B. Schumacher. On quantum coding for ensembles of mixed states. *Journal of Physics A: Mathematical and General*, 34(35):6767, (2001).

[43] H. Barnum, Emanuel Knill, and Michael A. Nielsen. On quantum fidelities and channel capacities. *IEEE Transactions on Information Theory*, 46:1317-1329, (2000).

[44] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, "Noncommuting mixed states cannot be broadcast," *Phys. Rev. Lett*., vol. 76, pp. 2818–2821, eprint quant-ph/9511010, (1996).

[45] H. Barnum, C. A. Fuchs, R. Jozsa, and B. Schumacher, "A general fidelity limit for quantum channels," eprint *quant-ph/9603014,* (1996).

[46] H. Barnum, M. A. Nielsen, and B. Schumacher, "Information transmission through noisy quantum channels," *eprint quant-ph/9702049*, (1997).

[47] H. Barnum, J. Smolin, and B. Terhal, "Results on quantum channel capacity," submitted to Phys. Rev A (eprint *quant-ph/9711032*). (1997).

[48] S. D. Barrett, T. M. Stace, Fault tolerant quantum computation with very high threshold for loss errors, *Physical Review Letters*, DOI:10.1103/PhysRevLett.105.200502, http://arxiv.org/abs/1005.2456. (2010).

[49] F. E. Becerra, J. Fan, and A. Migdall, "Photon number resolution enables quantum receiver for realistic coherent optical communications," *Nature Photonics*, vol. 9, p. 48, (2014).

[50] S. Beigi and P. W. Shor, On the Complexity of Computing Zero-Error and Holevo Capacity of Quantum Channels, *arXiv:0709.2090* [quant-ph] (2007).

[51] J. Bell, "On the Problem of Hidden Variables in Quantum Mechanics", *Rev. Mod. Phys*. 38: 447-452 (1966).

[52] P. Benioff, The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*, 22:563–591. (1980).

[53] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, (2014).

[54] C. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement assisted capacity of a quantum channel and the reverse shannon theorem," *IEEE Trans. Inf. Theory*, vol. 48, pp. 2637–2655, (2002).

[55] C. H. Bennett, P. Hayden, D. W. Leung, P. W. Shor, and A. Winter, "Remote preparation of quantum states," *IEEE Transactions on Information Theory*, vol. 51, pp. 56–74, (2005).

[56] C. Bennett, A. Harrow, and S. Lloyd. Universal quantum data compression via nondestructive tomography. *Physical Review A*, 73(3):032336, (2006).

[57] C. Bennett, I. Devetak, A. Harrow, P. Shor, A. Winter, Quantum Reverse Shannon Theorem, (2009), *arXiv:0912.5537*

[58] C. Bennett and S. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states.*Phys.Rev.Lett*.,69:2881-2884, (1992).

[59] Charles H. Bennett, Gilles Brassard, Claude Crepeau, and Marie-Helene Skubiszewska, Practical Quantum Oblivious Transfer" in Advances in Cryptology. *Lecture Notes in Computer Science, 576*., 351-366 (1992).

[60] C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895-1899, (1993).

[61] C. Bennett. *Quantum Information and Computation*. *Physics Today*, 48(10):24-30, (1995).

[62] C. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed state entanglement and quantum error correction". *Phys. Rev. A*, 54(5):3824– 3851, (1996).

[63] C. Bennett, H. Bernstein, S. Popescu, and B. Schumacher. Concentrating partial entanglement by local operations. *Physical Review A*, 53(4):2046-2052, (1996).

[64] C. Bennett, D. P. DiVincenzo, and J. A. Smolin, "Capacities of quantum erasure channels," *Phys. Rev. Lett*., vol. 78, no. 16, pp. 3217–3220, (1997).

[65] C. Bennett and P. W. Shor, "quantum information theory", *IEEE Trans. Info. Theory* 44, 2724 - 2742 (1998).

[66] C. Bennett, P. Shor, J. Smolin, and A. Thapliyal, "Entanglement-assisted classical capacity of noisy quantum channels," *Physical Review Letters*, vol. 83, pp. 3081–3084, Oct. 11 (1999).

[67] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters. Quantum nonlocality without entanglement. *Phys.Rev. A*, 59(2):1070–1091, (1999).

[68] C. H. Bennett and G. Brassard, "Quantum cryptography and its application to provably secure key expansion, public-key distribution, and coin-tossing," 1983 *IEEE International Symposium on Information Theory,* pp. 91–91 (1983).

[69] I. Bengtsson, K. Zyczkowski, *Entanglement & geometry of quantum states*, Cambridge University Press, Cambridge, United Kingdom, (2006).

[70] Berces M, Imre S.:Extension and analysis of modifiedsuperdensecodinginmulti-userenvironment, *IEEE 19th International Conference on Intelligent Engineering Systems* (INES2015), pp. 291-294. (2015).

[71] T. Berger. Rate distortion theory: *A mathematical basis for data compression*. Prentice-Hall, Englewood Cliffs, New Jersey, USA, (1971).

[72] M. Bern. *Triangulation and mesh generation*. In J. E. Goodman and J. O'Rourke, editors, *Handbook of Discrete and Computational Geometry*, 2nd edn., chapter 25. Chapman & Hall/CRC, (2004).

[73] M. Bern and P. Plasman. Mesh generation. In J.-R. Sack and J. Urrutia, editors, *Handbook of Computational Geometry*, 2nd edn., chapter 6. Elsevier, (1999).

[74] N. K. Bernardes, L. Praxmeyer, P. van Loock, Rate analysis for a hybrid quantum repeater, arXiv:1010.0106v1, (2010).

[75] P. Bertet, I. Chiorescu, G. Burkard, K. Semba, C. J. P. M. Harmans, D. P. DiVincenzo, and J. E. Mooij, "Dephasing of a superconducting qubit induced by photon noise," *Physical Review Lettes*, vol. 95 (2005).

[76] D. Bohm. *Quantum Theory*. Courier Dover Publications, (1989).

[77] B. Bollobas, *Modern graph theory*. Springer-Verlag New York, Inc., New York, (1998).

[78] C. Bonato, S. Bonora, A. Chiuri, P. Mataloni, G. Milani, G. Vallone, and P. Villoresi, Phase control of a path-entangled photon state by a deformable membrane mirror, *JOSA B,* Vol. 27, Issue 6, pp. A175-A180, doi:10.1364/JOSAB.27.00A175, (2010).

[79] G. Bowen. Quantum feedback channels. *IEEE Transactions in Information Theory*,50(10):2429-2434, *arXiv:quant-ph/0209076*, (2004).

[80] G. Bowen. Feedback in quantum communication. International Journal of Quantum Information, 3(1):123-127*, arXiv:quant-ph/0410191*, (2005).

[81] G. Bowen and R. Nagarajan. On feedback and the classical capacity of a noisy quantum channel. *IEEE Transactions in Information Theory*, 51(1):320-324, *arXiv:quant-ph/0305176*, (2005).

[82] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, The Edinburgh Building, Cambridge, CB2 8RU, UK, (2004).

[83] K. Bradler, P. Hayden, and P. Panangaden. Private information via the Unruh effect, *Journal of High Energy Physics* 08, 074 (2009).

[84] K. Bradler, An infinite sequence of additive channels: the classical capacity of cloning channels. *arXiv:0903.1638*, (2009).

[85] K. Bradler, P. Hayden, D. Touchette, and M. M. Wilde, Trade-off capacities of the quantum Hadamard channels, *arXiv:1001.1732v2*, (2010).

[86] F. Brandao and J. Oppenheim, "Public Quantum Communication and Superactivation," *arXiv:1005.1975*. (2010).

[87] F. Brandao, J. Oppenheim and S. Strelchuk, "When does noise increase the quantum capacity?", *arXiv:1107.4385v1* [quant-ph] (2011).

[88] S. Braunstein, C. Fuchs, D. Gottesman, and H. Lo. A quantum analog of Huffman coding. *IEEE Transactions in Information Theory*, 46(4):1644-1649, (2000).

[89] L. Bregman, "The relaxation method of finding the common points of convex sets and its application to the solution of problems in convex programming". *USSR Computational Mathematics and Mathematical Physics* 7: 200–217. doi:10.1016/0041 5553(67)90040-7. (1967).

[90] H.-J. Briegel, W. Dür, J.I. Cirac, and P. Zoller, Quantum repeaters: the role of imperfect local operations in quantum communication. *Physical Review Letters*, 81:5932 5935, (1998).

[91] G. Brodal and R. Jacob. Dynamic planar convex hull. In Proc. 43rd Annu. *IEEE Sympos. Found. Comput. Sci*., pages 617–626, (2002).

[92] L. de Broglie. Recherches sur la théorie des quanta. PhD thesis, Paris, (1924).

[93] D. Bruss, L. Faoro, C. Macchiavello and M. Palma, "Quantum entanglement and classical communication through a depolarizing channel", *J. Mod. Opt*. 47 325 (2000).

[94] B. Buckley, G. Fuchs, L. Bassett, and D. Awschalom, Spin-Light Coherence for Single-Spin Measurement and Control in Diamond. *Science*, Online October 14 2010 DOI: 10.1126/*Science*.1196436. (2010).

[95] C. Buckley. A divide-and-conquer algorithm for computing 4-dimensional convex hulls. In Lecture Note in Computer *Science*, volume 333, pages 113–135. Berlin: Springer-Verlag, (1988).

[96] J. Burbea and C. Rao, "On the convexity of some divergence measures based on entropy functions," *IEEE Transactions on Information Theory*, vol. 28, no. 3, pp. 489–495, (1982).

[97] D. Bures, "An extension of kakutani's theorem on infinite product measures to the tensor product of semifinite w*-algebras," *Transactions on American Mathematical Society*, vol. 135, pp. 199–212, (1969).

[98] N. Cai, A. Winter, and R. Yeung, "Quantum privacy and quantum wiretap channels," *Problems of Information Transmission*, vol. 40, no. 4, pp. 318–336, (2004).

[99] R. Calderbank and P. Shor, Good quantum error-correcting codes exist, *Physical Review A*, 54:1098, (1996).

[100] R. Calderbank, E. Rains, P. Shor, and N. J. A. Sloane, Quantum error correction and orthogonal geometry. *Physical Review Letters*, 78(3):405-408, (1997).

[101] A. R. Calderbank, E. Rains, P. Shor, and N. J. A. Sloane, Quantum error correction via codes over GF(4). *IEEE Transactions on Information Theory*, 44:1369-1387, (1998).

[102] N. Cerf and C. Adami. Negative entropy and information in quantum mechanics. *Physical Review Letters*, 79:5194-5197, (1997).

[103] J. Chan. Dynamic planar convex hull operations in near-logarithmaic amortized time. *J. ACM*, 48:1–12, (2001).

[104] K. Chen. On k-median clustering in high dimensions. In Proceedings of the *17th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA '06),* pages 1177–1185, (2006).

[105] Chen, Shuai, Chen, Yu-Ao, Strassel, Thorsten, Yuan, Zhen-Sheng, Zhao, Bo, Schmiedmayer, Jorg, and Pan, Jian-Wei, Deterministic and Storable Single-Photon Source Based on a Quantum Memory, *Physical Review Letters* 97, 173004 (2006).

[106] K. Chen. On k-median and k-means clustering in metric and Euclidean spaces and their applications. Manuscript, available at:http://ews.uiuc.edu/∼kechen/, (2007).

[107] K. Clarkson and P. Shor. Applications of random sampling in computational geometry, II. *Discrete Comput. Geom*., 4:387–421, (1989).

[108] K. Clarkson, R. E. Tarjan, and C. J. Van Wyk. A fast Las Vegas algorithm for triangulating a simple polygon. *Discrete Comput. Geom*., 4:423–432, (1989).

[109] B. Collins and I. Nechita, „Random quantum channels I: graphical calculus and the Bell state phenomenon*", arXiv:0905.2313*, (2009).

[110] B. Collins and I. Nechita, „Random quantum channels II: Entanglement of random subspaces, Renyi entropy estimates and additivity problems", arXiv:0906.1877, (2009).

[111] B. Collins and I. Nechita, „Gaussianization and eigenvalue statistics for Random quantum channels (III*)", arXiv:0910.1768*, (2009).

[112] T. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. Introduction to Algorithms, 2nd edn. MIT Press, Cambridge, MA, (2001).

[113] B. Cornwell, *Group Theory In Physics*: An Introduction, Academic Press, (1997).

[114] J. Cortese, "The Holevo-Schumacher-Westmoreland Channel Capacity for a Class of Qudit Unital Channels", LANL ArXiV e-print *quant-ph/0211093*, (2002).

[115] J. Cortese, "*Classical Communication over Quantum Channels*". PhD Thesis by. John A. Cortese. California Institute of Technology (2003).

[116] T. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley and Sons, New York, (1991).

[117] I. Csiszar, and J. Korner, *IEEE Trans. Inf. Theory* 24, 339. (1978).

[118] I. Csiszar and J. Korner. *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Probability and mathematical statistics. Akademiai Kiado, Budapest, (1981).

[119] T. Cubitt, M. Beth Ruskai and G. Smith, The Structure of Degradable Quantum Channels *J. Math. Phys*. 49, 102104 (2008).

[120] T. Cubitt and J. Cirac, Engineering Correlation and Entanglement Dynamics in Spin Systems *Physical Review Letters* 100, 180406 (2008).

[121] T. Cubitt, J. X. Chen, and A. Harrow, Superactivation of the Asymptotic Zero-Error Classical Capacity of a Quantum Channel, *arXiv: 0906.2547*. (2009).

[122] T. Cubitt, G. Smith, Super-Duper-Activation of Quantum Zero-Error Capacities, *arXiv:0912.2737v1*. (2009).

[123] T. Cubitt, D. Leung, W. Matthews and A. Winter, Improving Zero-Error Classical Communication with Entanglement, *Phys. Rev. Lett*. 104, 230503, arXiv:0911.5300, (2010).

[124] L. Czekaj and P. Horodecki. Nonadditivity effects in classical capacities of quantum multiple-access channels. *arXiv:0807.3977*, (2008).

[125] L. Czekaj and P. Horodecki. Nonadditivity effects in classical capacities of quantum multiple-access channels. *arXiv:0807.3977*, (2008).

[126] N. Datta, A. S. Holevo, Yu. M. Sukhov, On a Sufficient Additivity Condition in quantum information theory, *Probl. Peredachi Inf*., Volume 41. Issue 2, Pages 9–25 (2004).

[127] N. Datta, A. S. Holevo, and Y. Suhov, A quantum channel with additive minimum output entropy, http://arxiv.org/abs/quant-ph/0403072, (2004).

[128] N. Datta, A. S. Holevo, and Y. Suhov. Additivity for transpose

depolarizing channels, http://arxiv.org/abs/quant-ph/0412034, (2004).
[129] N. Datta and M. B. Ruskai, ,,Maximal output purity and capacity for asymmetric unital qudit channels", *J. Phys. A*: Math. Gen. 38, 9785 – 9802 (2005).
[130] N. Datta, M. Fukuda and A. S. Holevo, ,,Complementarity and additivity for covariant channels", *Quant. Info. Proc*. 5, 179 - 207 (2006).
[131] V. S. Denchev, S. Boixo, S. V. Isakov, N. Ding, R. Babbush, V. Smelyanskiy, J. Martinis, and H. Neven, "What is the computational value of finite-range tunneling?," *Phys. Rev. X*, vol. 6, p. 031015, (2016).
[132] E. Desurvire, *Classical and quantum information theory,* Cambridge University Press, The Edinburgh Building, Cambridge CB2 8RU, UK, (2009).
[133] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A*, 400(1818):97-117, July (1985).
[134] I. Devetak and A. Winter. Classical data compression with quantum side information. *Physical Review A*, 68(4):042301, (2003).
[135] I. Devetak, A. W. Harrow, and A. J. Winter. A family of quantum protocols. *Physical Review Letters*, 93:239503, (2004).
[136] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Theory*, vol. 51, pp. 44–55, arXiv:quant-ph/0304127, (2005).
[137] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A*, 461:207-235, (2005).
[138] I. Devetak and P. Shor. The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Communications in Mathematical Physics*, 256:287-303, (2005).
[139] I. Devetak, A. W. Harrow, and A. Winter. A resource framework for quantum Shannon theory. *IEEE Transactions on Information Theory*, 54(10):4587- 4618, (2008).
[140] S. J. Devitt, W. J. Munro, K. Nemoto, High Performance Quantum Computing, *arXiv:0810.2444* (2008).
[141] P. A. M. Dirac. *The Principles of Quantum Mechanics* (International Series of Monographs on Physics). Oxford University Press, USA, (1982).
[142] D. DiVincenzo, P. Shor, and J. Smolin, "Quantum-channel capacity of very noisy channels," *Phys. Rev. A*., vol. 57, pp. 830–839, eprint quant-ph/9706061, (1998).
[143] I. Djordjevic, "Quantum LDPC Codes from Balanced Incomplete Block Designs," *IEEE Communications Letters*, vol. 12, pp. 389–391 (2008).
[144] J. P. Dowling and G. J. Milburn. Quantum technology: The second quantum revolution. *Philosophical Transactions of The Royal Society of London Series A*, 361(1809):1655-1674, (2003).
[145] L. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Long-distance quantum communication with atomic ensembles and linear optics, *Nature* 414, 413 (2001).
[146] R. Duan, Y. Feng, Z. F. Ji, and M. S. Ying, "Distinguishing Arbitrary Multipartite Basis Unambiguously Using Local Operations and Classical Communication", *Phys. Rev. Lett*. 98, 230502 (2007).
[147] R. Duan, Superactivation of zero-error capacity of noisy quantum channels.*arXiv:0906.2527*, (2009).
[148] F. Dupuis, P. Hayden, and K. Li. A father protocol for quantum broadcast channels. *IEEE Transactions on Information Theory*, 56(6):2946-2956, arXiv:quant ph/0612155. (2010).
[149] W. Dür and H.J. Briegel, Entanglement purification and quantum error correction. *Rep. Prog. Phys*, 70:1381–1424, (2007).
[150] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Quantum repeaters based on entanglement purification. *Physical Review A*, 59(1):169–181, (1999).
[151] Electronic Engineering Times Portal, MEMS shown to enable quantum computing, http://www.eetimes.com/electronics-news/4211424/MEMS-enables-quantum computing, Mark Saffman's group at University of Wisconsin-Madison, (2010).
[152] A. Einstein. Über einen die erzeugung und verwandlung des lichtes betreenden heuristischen gesichtspunkt. *Annalen der Physik*, 17:132-148, (1905).
[153] A. Einstein, B. Podolsky, N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Physical Review* 47(10). 777-780. (1935).
[154] J. Eisert and M. M. Wolf, "Gaussian quantum channels,", arXiv:quant-ph/0505151. (2005).
[155] P. Elias. The efficient construction of an unbiased random sequence. *Annals of Mathematical Statistics*, 43(3):865-870, (1972).
[156] Z. W. E. Evans, A. M. Stephens, J. H. Cole, L. C. L. Hollenberg, "Error correction optimisation in the presence of X/Z asymmetry," *ArXiv*, (2007).
[157] M. Fannes. A continuity property of the entropy density for spin lattices. *Communications in Mathematical Physics*, 31:291, (1973).
[158] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, and A. Zeilinger, "High-fidelity transmission of entanglement over a high-loss free-space channel," *Nature Physics*, vol. 5, pp. 389–392, (2009).
[159] D. Feldman, M. Monemizadeh, and C. Sohler. A PTAS for k-means clustering based on weak coresets. In *Proceedings of the 23rd ACM Symposium on Computational Geometry (SCG'07),* pages 11–18, (2007).
[160] R. Feynman, Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488. (1982).
[161] K. Fischer and B. Gartner. The smallest enclosing ball of balls: combinatorial structure and algorithms. *International Journal of Computational Geometry & Application*, 14(4-5):341–378, (2004).
[162] G. Frahling and C. Sohler. Coresets in dynamic geometric data streams. In *Proceedings of the 27th Annual ACM Symposium on Theory of Computing (STOC'05),* pages 209–217, New York, NY, USA, ACM, (2005).
[163] C. Fuchs, "Information Tradeoff Relations for Finite-Strength Quantum Measurements", LANL ArXiV e-print *quant-ph/0009101*. (2000).
[164] C. Fuchs. *Distinguishability and Accessible Information in Quantum Theory*. PhD thesis, University of New Mexico, December 1996. arXiv:quant-ph/9601020, (1996).
[165] C. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, *Phys. Rev. A* 56, 1163. (1997).
[166] C. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216-1227,. arXiv:quant-ph/9712042, (1998).
[167] T. Fujiwara and T. Hashizume, "Additivity of the capacity of depolarizing channels". *Phys. Lett. A*, 299:469–475, (2002).
[168] M. Fukuda, C. King, D. K. Moser, Comments on Hastings' Additivity Counterexamples, *Communications in Mathematical Physics*, DOI 10.1007/s00220-010-0996-9, (2010).
[169] M. Fukuda and C. King. Entanglement of random subspaces via the Hastings bound. *Journal of Mathematical Physics*, 51(4):042201, (2010).
[170] M. Gabay and S. Arnon, "Quantum key distribution by a free-space MIMO system," *Journal of Lightwave Technology*, vol. 24, pp. 3114–3120 (2006).
[171] F. Gaitan, *Quantum Error Correction and Fault Tolerant Quantum Computing*, CRC Press, ISBN 9780849371998, p.312 (2008).
[172] M. Galambos, L. Bacsardi, S. Imre, Modeling the superdense coding in satellite-satellite and ground-satellite communications, *Proc of 10th Asian Conference on Quantum Information Science*, Tokyo, Japán, .08.27-2010.08.31.pp. 205-206 (2010).
[173] W. Gao, et al. "Teleportation-based realization of an optical quantum two-qubit entangling gate." *PNAS* Early Edition.DOI:10.1073/pnas.1005720107, (2010).
[174] M. Gardner, Mathematical Games: The fantastic combinations of John Conway's new solitaire game "Life", *Scientific American* 223: 120–123. (1970).
[175] W. Gerlach and Otto Stern. Das magnetische moment des silberatoms. Zeitschrift für Physik, 9:353-355, (1922).
[176] A. Ghilen, M. Azizi, and R. Bouallegue, "Enhancing the Security of IEEE 802.11i Standard by Integrating a Quantum Scheme for Authentication and Encryption Key Distribution," *Wireless Personal Communications*, vol. 95, pp. 1655–1675, (2017).
[177] J. Ghosh, A. G. Fowler, and M. R. Geller, "Surface code with decoherence: An analysis of three superconducting architectures," *Phys. Rev. A*, vol. 86, p. 062318 (2012).
[178] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J H. Shapiro, B J. Yen, H P. Yuen, Classical capacity of free-space optical communication, *Quantum Information & Computation*, Volume 4 Issue 6, Dec Pages 489-499 (2004).
[179] V. Giovannetti and R. Fazio. Information-capacity description of spin-chain correlations. *Physical Review A*, 71(3):032314, (2005).
[180] V. Giovannetti, A. S. Holevo, S. Lloyd, L. Maccone, Generalized minimal output entropy conjecture for one-mode Gaussian channels: definitions and some exact results, *J. Phys. A: Math. Theor. 43 415305*, 8, 796–800, (2010).
[181] V. Giovannetti, R. García-Patrón, N. J. Cerf, A. S. Holevo, Ultimate classical communication rates of quantum optical channels, *Nature Photonics*, 8, 796–800, (2014).

[182] R. J. Glauber. *One hundred years of light quanta.* In Karl Grandin, editor, Les Prix Nobel. The Nobel Prizes 2005, pages 90-91. Nobel Foundation, (2005).

[183] R. J. Glauber. The quantum theory of optical coherence. *Physical Review*, 130(6):2529-2539, (1963).

[184] J. Goodman and J. O'Rourke, editors. *Handbook of Discrete and Computational Geometry*, 2nd edn. Chapman & Hall/CRC, 2004.

[185] J. P. Gordon. *Noise at optical frequencies; information theory*. In P. A. Miles, editor, Quantum Electronics and Coherent Light; Proceedings of the International School of Physics Enrico Fermi, Course XXXI, pages 156-181, Academic Press New York, (1964).

[186] D. Gottesman, Class of quantum error-correcting codes saturating the quantum Hamming bound. *Physical Review A*, 54(3):1862-1868, (1996).

[187] D. Gottesman, *Stabilizer Codes and Quantum Error Correction*. PhD thesis, California Institute of Technology (arXiv:quant-ph/9705052), (1997).

[188] D. Gottesman*, An Introduction to Quantum Error Correction, Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium*, ed. S. J. Lomonaco, Jr., pp. 221-235, (2002).

[189] M. Grassl, T. Beth, and T. Pellizzari. Codes for the quantum erasure channel. *Phys.Rev.A*,56:33-38, quant-ph/9610042. (1997).

[190] D. Griffiths. Introduction to Quantum Mechanics. Prentice-Hall, Inc., (1995).

[191] G. Grössing, A. Zeilinger, Quantum cellular automata. *Complex Syst*., 2:197–208. (1988).

[192] S. Guha, J. Shapiro. Classical information capacity of the Bosonic broadcast channel. In *Proceedings of the IEEE International Symposium on Information Theory*, pages 1896-1900, Nice, France, (2007).

[193] S. Guha, J. Shapiro, B. Erkmen. Classical capacity of bosonic broadcast communication and a minimum output entropy conjecture. *Physical Review A*, 76(3):032303, (2007).

[194] L. Gyongyosi, S. Imre: Information Geometric Superactivation of Classical Zero-Error Capacity of Quantum Channels, *Progress in Informatics*, Quantum Information Technology, Quantum Information Science Theory Group, National Institute of Informatics, Tokyo, Japan, Print ISSN : 1349-8614, Online ISSN : 1349-8606; (2011.)

[195] L. Gyongyosi, S. Imre: Algorithmic Superactivation of Asymptotic Quantum Capacity of Zero-Capacity Quantum Channels, *Information Sciences*, ELSEVIER, ISSN: 0020-0255. (2011).

[196] L. Gyongyosi, S. Imre*: Quantum Cryptographic Protocols and Quantum Security*, in "Cryptography: Protocols, Design and Applications", Nova Science Publishers, USA. (2011).

[197] L. Gyongyosi, S. Imre: *Quantum Cellular Automata Controlled Self-Organizing Networks*, in "Cellular Automata", Book Chapter, INTECH, New York, USA, ISBN 978-953-7619-X-X; (2011).

[198] L. Gyongyosi, S. Imre: Quasi-Superactivation of Classical Capacity of Zero-Capacity Quantum Channels, *Journal of Modern Optics*, Taylor & Francis, 0950-0340 (Print), 1362-3044 (Online). 2012.

[199] L. Gyongyosi, S. Imre: Superactivation of Quantum Channels is Limited by the Quantum Relative Entropy Function, *Quantum Information Processing*, Springer, ISSN: 1570-0755 (print version), ISSN: 1573-1332 (electronic version). 2012.

[200] L. Gyongyosi, *Information Geometric Superactivation of Asymptotic Quantum Capacity and Classical Zero-Error Capacity of Zero-Capacity Quantum Channels*, PhD Thesis, Budapest University of Technology and Economics, 2013.

[201] L. Gyongyosi, The Correlation Conversion Property of Quantum Channels, *Quantum Information Processing*, Springer, ISSN: 1570-0755 (print version), ISSN: 1573-1332 (electronic version). (2013).

[202] L. Gyongyosi, A Statistical Model of Information Evaporation of Perfectly Reflecting Black Holes*, International Journal of Quantum Information* (IJQI), ISSN 0219-7499 (print), 1793-6918 (online), 2014.

[203] L. Gyongyosi: The Private Classical Capacity of a Partially Degradable Quantum Channel, *Physica Scripta - Special Issue on Quantum Information*, Institute of Physics (IOP), Online ISSN: 1402-4896 Print ISSN: 0031-8949, 2014.

[204] L. Gyongyosi: The Structure and Quantum Capacity of a Partially Degradable Quantum Channel, *IEEE Access*, ISSN: 2169-3536, 2014.

[205] L. Gyongyosi: Quantum Information Transmission over a Partially Degradable Channel, *IEEE Access*, ISSN: 2169-3536 (2014).

[206] Quantum Imaging of High-Dimensional Hilbert Spaces with Radon Transform, *International Journal of Circuit Theory and Applications* (IJCTA), Special Issue on Quantum Circuits (Wiley), 2017.

[207] A. Hagar, "Quantum Computing", The Stanford Encyclopedia of Philosophy (Spring 2011 Edition), Edward N. Zalta (ed.), http://plato.stanford.edu/archives/spr2011/entries/qt-quantcomp, (2011).

[208] M. Hamada. Information rates achievable with algebraic codes on quantum discrete memoryless channels. *IEEE Transactions in Information Theory*, 51(12):4263–4277, arXiv:quant-ph/0207113, (2005).

[209] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, L. Gyongyosi. Wireless Myths, Realities, and Futures: From 3G/4G to Optical and Quantum Wireless, *Proceedings of the IEEE*, Volume: 100, Issue: Special Centennial Issue, pp. 1853-1888. (2012).

[210] S. Har-Peled and A. Kushal. Smaller coresets for k-median and k-means clustering. *In Proceedings of the 21st Annual Symposium on Computational Geometry (SCG'05),* pages 126–134, New York, NY, USA, ACM, (2005).

[211] A. Harrow. Coherent communication of classical messages. *Physical Review Letters*, 92:097902, (2004).

[212] A. Harrow and H. Lo. A tight lower bound on the classical communication cost of entanglement dilution. *IEEE Transactions on Information Theory*,

[213] A. Harrow and H. Lo. A tight lower bound on the classical communication cost of entanglement dilution. *IEEE Transactions on Information Theory*, 50(2):319-327, (2004).

[214] M. Hastings, "A Counterexample to Additivity of Minimum Output Entropy" *Nature Physics* 5, 255, arXiv:0809.3972, (2009).

[215] P. Hausladen, B. Schumacher, M. Westmoreland, and W. Wootters. Sending classical bits via quantum its. *Annals of the New York Academy of Sciences*, 755:698-705, (1995).

[216] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters. Classical information capacity of a quantum channel. *Physical Review A*, 54(3):1869-1876, (1996).

[217] M. Hayashi and K. Matsumoto. Variable length universal entanglement concentration by local operations and its application to teleportation and dense coding. *arXiv:quant-ph/0109028*, (2001).

[218] M. Hayashi and H. Nagaoka, "General formulas for capacity of classical-quantum channels," *IEEE Transactions on Information Theory*, Vol.49, No.7, pp.1753-1768 (2003).

[219] M. Hayashi, H. Imai, K. Matsumoto, M. B. Ruskai, and T. Shimono. Qubit channels which require four inputs to achieve capacity: Implications for additivity conjectures. *QUANTUM INF.COMPUT*., 5:13, http://arxiv.org/abs/quant-ph/0403176, (2005).

[220] M. Hayashi. *Quantum Information: An Introduction*. Springer-Verlag, (2006).

[221] P. Hayden and A. Winter. Communication cost of entanglement transformations. *Physical Review A*, 67(1):012326, (2003).

[222] P. Hayden and A. Winter, „Counterexamples to the maximal p-norm multiplicativity conjecture for all p $>$ 1", *Commun. Math. Phys*. 284, 263 – 280 (2008).

[223] P. Hayden, M. Horodecki, J. Yard, and A. Winter, "A decoupling approach to the quantum capacity," *Open Syst. Inf. Dyn*., vol. 15, pp. 7–19, arXiv:quant-ph/0702005. (2008).

[224] P. Hayden, P. Shor, and A. Winter. Random quantum codes from Gaussian ensembles and an uncertainty relation. *Open Systems & Information Dynamics*, 15:71-89, (2008).

[225] W. Heisenberg. Über quantentheoretische umdeutung kinematischer und mechanischer beziehungen. *Zeitschrift fur Physik*, 33:879-893, (1925).

[226] A. Hellemans, "Teleporting what matters," *IEEE Spectrum*, vol. 41, pp. 18, 20–, (2004).

[227] C. Helstrom, *Quantum Detection and Estimation Theory* "Academic, New York". (1976).

[228] N. Herbert. Flash - a superluminal communicator based upon a new kind of quantum measurement. *Foundations of Physics*, 12(12):1171-1179, (1982).

[229] F. Hiai and D. Petz. The proper formula for relative entropy and its asymptotics in quantum probability. *Communications in Mathematical Physics*, 143(1):99–114, (1991).

[230] A. Holevo. On entanglement assisted classical capacity. *Journal of Mathematical Physics*, 43(9):4326-4333, (2002).

[231] A. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. Problemly Peredachi Informatsii, 9(3):3–11, (1973). English Translation: *Probl. Inform. Transm*., 9, 177–183, (1975).

[232] A. Holevo, Information theoretical aspects of quantum measurements. *Probl. Info. Transm*., 9(2):31–42, (1973).

[233] A. Holevo, "The capacity of the quantum channel with general signal states", *IEEE Trans. Info. Theory* 44, 269 - 273 (1998).

[234] R. Horn and C. Johnson, *Matrix Analysis*, Cambridge University Press, (1986).

[235] M. Horodecki, P. Horodecki, R. Horodecki, D. Leung, and B. Terhal. Classical capacity of a noiseless quantum channel assisted by noisy entanglement. *Quantum Information and Computation*, 1(3):70-78, arXiv:quant-ph/0106080, (2001).

[236] M. Horodecki, P. Shor, and M. Ruskai. Entanglement breaking channels. *Reviews in Mathematical Physics*, 15(6):629-641, arXiv:quant-ph/0302031, (2003).

[237] M. Horodecki, J. Oppenheim and A. Winter, "Partial quantum information", *Nature* 436, 673-676 | doi:10.1038/nature03909. (2005).

[238] M. Horodecki, Jonathan Oppenheim, and Andreas Winter. Quantum state merging and negative information. *Communications in Mathematical Physics*, 269:107-136, (2007).

[239] R. Horodecki, P. Horodecki, M. Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865-942, (2009).

[240] M. Horodecki. Limits for compression of quantum information carried by ensembles of mixed states. *Physical Review A*, 57(5):3364-3369, (1998).

[241] M.Hsieh, I. Devetak, and A. Winter. Entanglement-assisted capacity of quantum multiple-access channels. *IEEE Transactions on Information Theory*, 54(7):3078-3090, (2008).

[242] M. Hsieh and M. Wilde. Trading classical communication, quantum communication, and entanglement in quantum Shannon theory. *IEEE Transactions on Information Theory*, 56(9):4705-4730, (2010).

[243] https://www.idquantique.com

[244] S. Imre, F. Balázs: *Quantum Computing and Communications – An Engineering Approach*, Published by John Wiley and Sons Ltd, (2005).

[245] S. Imre, L. Gyongyosi: *Advanced Quantum Communications – An Engineering Approach*, Published by Wiley-IEEE Press, (2013).

[246] S. Imre, Quantum communications: explained for communication engineers, *IEEE COMMUNICATIONS MAGAZINE* 51:(08) (2013).

[247] M. Isenburg, Y. Liu, J. Shewchuk, and J. Snoeyink. Streaming computation of delaunay triangulations. In SIGGRAPH '06: ACM SIGGRAPH 2006 Papers, pages 1049 1056, New York, NY, USA, ACM, (2006).

[248] C. Isham, *Modern Differential Geometry for Physicists*, World Scientific, Second Edition, Page 187, (1999).

[249] A. E. Ivanova, S. A. Chivilikhin, and A. V. Gleim, "Quantum random number generator based on homodyne detection," *Nanosystems-Physics Chemistry Mathematics*, vol. 8, pp. 239–242, (2017).

[250] R. Janardan and T. C. Woo. Design and manufacturing. In J. E. Goodman and J. O'Rourke, editors, *Handbook of Discrete and Computational Geometry*, 2nd edn., chapter 55. Chapman & Hall/CRC, (2004).

[251] E. T. Jaynes. *Probability Theory: The Logic* of *Science*. Cambridge University Press, (2003).

[252] E. T. Jaynes. Information theory and statistical mechanics. *Physical Review*, 106:620, (1957).

[253] E. T. Jaynes. Information theory and statistical mechanics II. *Physical Review*, 108:171, (1957).

[254] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, M. D. Lukin, Quantum Repeater with Encoding, *arXiv:0809.3629* (2008).

[255] Paul Jouguet, Sebastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, Eleni Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, *Nature Photonics* 7, 378-381 (2013).

[256] R. Jozsa and S. Presnell. Universal quantum information compression and degrees of prior knowledge. *Proceedings of the Royal Society A*: Mathematical, Physical and Engineering Sciences, 459(2040):3061-3077, (2003).

[257] R. Jozsa. Fidelity for mixed quantum states. Journal of Modern Optics, 41(12):2315-2323, (1994).

[258] R. Jozsa, M. Horodecki, P. Horodecki, and R. Horodecki. Universal quantum information compression. *Physical Review Letters*, 81(8):1714-1717, (1998).

[259] F. Schmidt-Kaler, S. Gulde, M. Riebe, T. Deuschle, A. Kreuter, G. Lancaster, C. Becher, J. Eschner, H. Hffner, and R. Blatt, "The coherence of qubits based on single Ca+ ions," *Journal of Physics B-Atomic Molecular and Optical Physics*, vol. 36, pp. 623–636 (2003).

[260] K. Kato, M. Oto, H. Imai, and K. Imai, "Voronoi diagrams for pure 1-qubit quantum states, quant-ph/0604101, (2006).

[261] Karp, S., Gagliardi, R.M., Moran, S.E., Stotts, L.B. (Eds.), *Optical channels: fibers, clouds, water and the atmosphere*. Plenum Press (1988).

[262] P. Kaye and M. Mosca. Quantum networks for concentrating entanglement. *Journal of Physics A: Mathematical and General*, 34(35):6939, (2001).

[263] J. Kelly, R. Barends, A. G. Fowler, A. Megrant, E. Jeffrey, T. C. White, D. Sank, J. Y. Mutus, B. Campbell, Yu Chen, Z. Chen, B. Chiaro, A. Dunsworth, I.-C. Hoi, C. Neill, P. J. J. O'Malley, C. Quintana, P. Roushan, A. Vainsencher, J. Wenner, A. N. Cleland, John M. Martinis, "State preservation by repetitive error detection in a superconducting quantum circuit," *Nature*, vol. 519, pp. 66–69 (2015).

[264] J. Kerckhoff, et al., Designing Quantum Memories with Embedded Control: Photonic Circuits for Autonomous Quantum Error Correction, *Physical Review Letters* 105, 040502 (2010).

[265] A. Khanmohammadi, R. Enne, M. Hofbauer, and H. Zimmermanna, "A monolithic silicon quantum random number generator based on measurement of photon detection time," *IEEE Photonics Journal*, vol. 7, pp. 1–13, (2015).

[266] G. Kimura. The Bloch vector for n-level systems. Physics Letter A, 314(339), (2003).

[267] Kimble, H. J. The quantum internet. *Nature* 453, 1023 - 1030 (2008).

[268] C. King and M. B. Ruskai, „Minimal entropy of states emerging from noisy quantum channels", *IEEE Trans. Info. Theory* 47, 192 - 209 (2001).

[269] C. King, M. Nathanson, and M. B. Ruskai, „Qubit Channels Can Require More Than Two Inputs to Achieve Capacity", LANL ArXiV e-print quant-ph/0109079, (2001).

[270] C. King. Additivity for unital qubit channels. *J. Math. Phys*., 43:4641–4653, (2002).

[271] C. King, „Maximal p-norms of entanglement breaking channels", *Quantum Info. and Comp*. 3, no.2, 186 - 190 (2003).

[272] C. King, „The capacity of the quantum depolarizing channel", *IEEE Trans. Info. Theory* 49, no.1, 221 - 229 (2003).

[273] C. King, K. Matsumoto, M. Nathanson, and M. B. Ruskai. Properties of conjugate channels with applications to additivity and multiplicativity. *Markov Processes and Related Fields*, 13(2):391-423, J. T. Lewis memorial issue, (2007).

[274] C. King, Remarks on the Additivity Conjectures for Quantum. Channels, www.mathphys.org/AZschool/material/AZ09-king.pdf, (2009).

[275] C. King and M. B. Ruskai, „Capacity of Quantum Channels Using Product Measurements", LANL ArXiV e-print quant-ph/0004062, (2000).

[276] A. Kitaev. U. Nauk., 52(53), (1997).

[277] R. Klesse. A random coding based proof for the quantum coding theorem. *Open Systems & Information Dynamics*, 15:21-45, (2008).

[278] E. Knill, Quantum computing with realistically noisy devices, *Nature*. March 3. (2005).

[279] E. H. Knill, R. Laflamme, and W. H. Zurek, Resilient quantum computation. *Science*, 279:342-345, *quant-ph/9610011*, (1998).

[280] S. Kochen and E. P. Specker, "The problem of hidden variables in quantum mechanics", *Journal of Mathematics and Mechanics* 17, 59{87 (1967).

[281] R. Kohout, Sarah Croke, and Daniel Gottesman. Streaming universal distortion-free entanglement concentration, *arXiv:0910.5952*, (2009).

[282] Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew and Hugo Zbinden, Provably secure and practical quantum key distribution over 307 km of optical fibre, *Nature Photonics* 9, 163-168 (2015)

[283] J. Körner and A. Orlitsky, Zero-error information theory. *IEEE Trans. Info. Theory*, 44(6):2207–2229, (1998).

[284] L. Kraft, "*A device for quantizing, grouping, and coding amplitude modulated pulses"*, Cambridge, MA: MS Thesis, Electrical Engineering Department, Massachusetts Institute of Technology. (1949).

[285] S. Kullback, R.A. Leibler, "On Information and Sufficiency". *Annals of Mathematical Statistics* 22 (1): 79–86. doi:10.1214/aoms/1177729694. MR39968. (1951).

[286] S. Kullback *Information theory and statistics* (John Wiley and Sons, NY). (1959).

[287] S. Kullback, "Letter to the Editor: The Kullback–Leibler distance". The *American Statistician* 41 (4): 340–341. JSTOR 2684769. (1987).

[288] S. Kullback, "Letter to the Editor: The Kullback–Leibler distance". The *American Statistician* 41 (4): 340–341. JSTOR 2684769. (1987).

[289] T. Ladd, P. van Loock, K. Nemoto, W. J. Munro, and Y. Yamamoto, Hybrid quantum repeater based on dispersive CQED interactions between matter qubits and bright coherent light, *New Journal of Physics* 8, 184 (2006).

[290] R.Laflamme, C. Miquel, J. Paz, and W. Zurek, Perfect quantum error correcting code. *Physical Review Letters*, 77(1):198-201, (1996).

[291] R. Landauer. Is quantum mechanics useful? *Philosophical Transactions of the Royal Society: Physical and Engineering Sciences*, 353(1703):367-376, (1995).

[292] D. Leung, G. Smith. Communicating over adversarial quantum chan-

nels using quantum list codes. *IEEE Trans. Info. Theory* 54, 2, 883-887 (2008).

[293] D. Leung and G. Smith. Continuity of quantum channel capacities, *Communications in Mathematical Physics* 292, 201-215 (November 2009).

[294] D. Leung, L. Mancinska, W. Matthews, M. Ozols, A. Roy, Entanglement can increase asymptotic rates of zero-error classical communication over classical channels, *arXiv:1009.1195v2* (2010).

[295] L. Levitin, „On the quantum measure of the amount of information", Proceedings of the Fourth all-union conference on Information Theory (in Russian), Tashkent, 111 - 115 (1969).

[296] K. Li, A. Winter, X. Zou, and G. Guo, "Private classical capacity of Quantum Channels is Not Additive," *Physical Review Letters*, vol. 103, no. 12, p. 120501, *arXiv:0903.4308*, (2009).

[297] M. Li, S-M. Fei and X. Li-Jost, "Quantum Entanglement: Separability, Measure, Fidelity of Teleportation, and Distillation", *Advances in Mathematical Physics*Volume 2010, Article ID 301072, 57 pages-doi:10.1155/2010/301072. (2010).

[298] J. Li, X.-B. Chen, G. Xu, Y.-X. Yang, and Z.-P. Li, "Perfect quantum network coding independent of classical network solutions," *IEEE Communications Letters*, vol. 19, pp. 115–118,(2015).

[299] Z. Li, G. Xu, X. Chen, X. Sun, and Y.-X. Yang, "Multi-User Quantum Wireless Network Communication Based on Multi-Qubit GHZ State", *IEEE Communications Letters*, vol. 20, no. 12, pp. 2470 - 2473, December 2016.

[300] J. Li, J. Xiong, Q. Zhang, L. Zhong, Y. Zhou, J. Li, and X. Lu, "A one-time pad encryption method combining full-phase image encryption and hiding," *Journal Of Optics*, vol. 19, (2017).

[301] Sheng-Kai Liao et al., Satellite-to-ground quantum key distribution, *Nature* 549, 43-47 (2017)

[302] Q. Liao, Y. Guo, and D. Huang, "Cancelable remote quantum fingerprint templates protection scheme," *Chinese Physics B*, vol. 26, (2017).

[303] S. Lloyd, "Capacity of the noisy quantum channel," *Phys. Rev. A*, vol. 55, pp. 1613–1622, (1997).

[304] S. Lloyd, J.H. Shapiro, F.N.C. Wong, P. Kumar, S.M. Shahriar, and H.P. Yuen. In-frastructure for the quantum Internet, *ACM SIGCOMM Computer Communication Review*, 34(5):9–20, (2004)

[305] H. Lo and S. Popescu. Concentrating entanglement by local actions: Beyond mean values. *Physical Review A*, 63(2):022301, (2001).

[306] H. Lo. Quantum coding theorem for mixed states. *Optics Communications*, 119(5-6):552-556, September (1995).

[307] H. Lo and Sandu Popescu. Classical communication cost of entanglement manipulation: Is entanglement an interconvertible resource? *Physical Review Letters*, 83(7):1459-1462, (1999).

[308] L. Loffe, and M. Mezard, "Asymmetric quantum error-correcting codes," *Physical Review A*, vol. 75, no. 3, p. 032345, PRA. (2007).

[309] P. van Loock, N. Lütkenhaus, W. J. Munro, and K. Nemoto, Quantum repeaters using coherent-state communication, *Physical Review A* 78, 062319 (2008).

[310] S. G. R. Louis, W. J.Munro, T. P. Spiller, and K. Nemoto, Loss in hybrid qubit-bus couplings and gates, *Physical Review A* 78, 022326 (2008).

[311] L . Lovász. On the Shannon capacity of a graph. *IEEE Trans. Info. Theory*, 25(1):1 – 7, (1979).

[312] M. Lukin, J. Taylor, Quantum physics: Quantum leaps in the solid state, *Nature* 467, 278–279 (16 September 2010) doi:10.1038/467278a. (2010).

[313] C. Lupo, S. Pirandola, P. Aniello, S. Mancini, On the classical capacity of quantum Gaussian channels, arXiv:1012.5965v2, (2011).

[314] L. Ma, A. Mink, H. Xu, O. Slattery, and X. Tang, "Experimental demonstration of an active quantum key distribution network with over GBPS clock synchronization," *IEEE Communications Letters*, vol. 11, pp. 1019–1021 (2007).

[315] L. Ma, T. Chang, A. Mink, O. Slattery, B. Hershman, and X. Tang, "Experimental demonstration of a detection-time-bin-shift polarization encoding quantum key distribution system," *IEEE Communications Letters*, vol. 12, pp. 459–461 (2008).

[316] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *Npj Quantum Information*, vol. 2, (2016).

[317] K. Matsumoto and F. Yura, Entanglement cost of antisymmetric states and additivity of capacity of some quantum channels. *Journal of Phys. A*, 37:L167–L171, (2004).

[318] J. P. McEvoy and Oscar Zarate. Introducing Quantum Theory. Totem Books, third edition, (2004).

[319] McMillan, Brockway, "Two inequalities implied by unique decipherability", *IEEE Trans. Information Theory* 2 (4): 115–116, doi:10.1109/TIT.1956.1056818. (1956).

[320] R. Medeiros and F. M. de Assis, "Quantum zero-error capacity", *Int. J. Quant. Inf.* 3, 135 (2005);

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

[322] D. Meyer, From quantum cellular automata to quantum lattice gases. *Journal of Statistical Physics*, 85:551–574. (1996).

[323] S. Michalakis, „Multiplicativity of the maximal output 2-norm for depolarized Werner-Holevo channels", *J. Math. Phys*. 48, no. 12, 122102, (2007).

[324] D. Miller, D. Maslov, & G. Dueck, Synthesis of quantum multiple-valued circuits, *Journal of Multiple-Valued Logic and Soft Computing*, vol. 12, no. 5-6, pp. 431–450. (2006).

[325] C. Misner, K. Thorne, and W. Zurek. J. Wheeler, Relativity, and quantum information. *Physics Today*, (2009).

[326] , Moore Gordon E. Cramming more components onto integrated circuits. *Electronics*. (1965).

[327] G. Morley, M. Warner, A. Stoneham, P. Greenland, J. van Tol, C. Kay & G. Aeppli, The initialization and manipulation of quantum information stored in silicon by bismuth dopants, *Nature Materials* 9, 725 (2010).

[328] M. Mosonyi and N. Datta. Generalized relative entropies and the capacity of classical-quantum channels. *Journal of Mathematical Physics*, 50(7):072104, (2009).

[329] J. Mullins. The topsy turvy world of quantum computing. *IEEE Spectrum*, 38(2):42-49, (2001).

[330] W. J. Munro, R. Van Meter, S. G. R. Louis, and K. Nemoto, High-Bandwidth Hybrid Quantum Repeater, *Physical Review Letters* 101, 040502 (2008).

[331] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, K. Nemoto, From quantum fusiliers to high-performance networks *arXiv:0910.4038* (2009).

[332] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto, From quantum multiplexing to high-performance quantum networking, *Nature Photonics*, 10.1038/nphoton.2010.213, (2010).

[333] M. Tyryshkin, J. J. L. Morton, S. C. Benjamin, A. Ardavan, G. A. D. Briggs, J. W. Ager, and S. A. Lyon, "Coherence of spin qubits in silicon," *Journal of Physics-Condensed Matter*, vol. 18, pp. S783–S794, May 31 2006.

[334] J. R. Petta, A. C. Johnson, J. M. Taylor, E. A. Laird, A. Yacoby, M. D. Lukin, C. M. Marcus, M. P. Hanson, and A. C. Gossard, "Coherent manipulation of coupled electron spins in semiconductor quantum dots," *SCIENCE*, vol. 309, pp. 2180–2184, Sep. 30 2005.

[335] P. Bertet, I. Chiorescu, G. Burkard, K. Semba, C. J. P. M. Harmans, D. P. DiVincenzo, and J. E. Mooij, "Dephasing of a superconducting qubit induced by photon noise," *Physical Review Letters*, vol. 95 2005.

[336] F. Schmidt-Kaler, S. Gulde, M. Riebe, T. Deuschle, A. Kreuter, G. Lancaster, C. Becher, J. Eschner, H. Hffner, and R. Blatt, "The coherence of qubits based on single Ca+ ions," *Journal of Physics B-Atomic Molecular and Optical Physics*, vol. 36, pp. 623–636, Feb. 14 2003.

[337] L. Vandersypen, M. Steffen, G. Breyta, C. Yannoni, M. Sherwood, and I. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature*, vol. 414, pp. 883–887, Dec. 20 2001.

[338] L. Loffe, and M. Mezard, "Asymmetric quantum error-correcting codes," *Physical Review A*, vol. 75, no. 3, p. 032345, 2007. PRA.

[339] Z. W. E. Evans, A. M. Stephens, J. H. Cole, L. C. L. Hollenberg, "Error correction optimisation in the presence of X/Z asymmetry," ArXiv, 2007.

[340] L. Wang, K. Feng, S. Ling, and C. Xing, "Asymmetric quantum codes: Characterization and constructions," *IEEE Transactions on Information Theory*, vol. 56, pp. 2938–2945, June 2010.

[341] M. Ezerman, S. Ling, and P. Sole, "Additive asymmetric quantum codes," *IEEE Transactions on Information Theory*, vol. 57, pp. 5536–5550, Aug 2011.

[342] M. Ezerman, S. Jitman, S. Ling, and D. Pasechnik, "CSS-like constructions of asymmetric quantum codes," *IEEE Transactions on Information Theory*, vol. 59, pp. 6732–6754, Oct 2013.

[343] G. PersonNameProductIDLa GuardiaLa Guardia, "On the construction of asymmetric quantum codes," *International Journal of Theoretical Physics*, vol. 53, no. 7, pp. 2312–2322, 2014.

[344] H. V. Nguyen, Z. Babar, D. Alanis, P. Botsinis, D. Chandra, S. X. Ng, and L. Hanzo, "Exit-chart aided quantum code design improves the normalised throughput of realistic quantum devices," *IEEE Access*.

[345] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "The road from classical to quantum codes: A hashing bound approaching design procedure," *IEEE Access*, vol. 3, pp. 146–176, 2015.

[346] S. ten Brink, "Convergence of iterative decoding," *Electronics Letters*, vol. 35, pp. 806–808, May 13, 1999.

[347] S. ten Brink and G. Kramer, "Design of repeat-accumulate codes for iterative detection and decoding," *IEEE Transactions on Signal Processing*, vol. 51, pp. 2764–2772, Nov 2003.

[348] S.-J. Lee, A. Singer, and N. Shanbhag, "Linear turbo equalization analysis via BER transfer and EXIT charts," *IEEE Transactions on Signal Processing*, vol. 53, pp. 2883–2897, Aug 2005.

[349] J. Karjalainen, M. Codreanu, A. Tolli, M. Juntti, and T. Matsumoto, "EXIT chart-based power allocation for iterative frequency domain MIMO detector," *IEEE Transactions on Signal Processing*, vol. 59, pp. 1624–1641, April 2011.

[350] F. Babich, A. Crismani, M. Driusso, and L. Hanzo, "Design criteria and genetic algorithm aided optimization of three-stage-concatenated spacetime shift keying systems," *Signal Processing Letters, IEEE,* vol. 19, pp. 543–546, Aug 2012.

[351] R. Ahlswede, N. Cai, and R. Yeung, "Network information flow theory," in *IEEE International Symposium on Information Theory*, 1998, p. 186, Aug. 1998.

[352] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, pp. 1204 –1216, July 2000.

[353] P. Chou and Y. Wu, "Network coding for the internet and wireless networks," *IEEE Signal Processing Magazine*, vol. 24, pp. 77 –85, Sept. 2007.

[354] E. Soljanin, "Network multicast with network coding [lecture notes]," *IEEE Signal Processing Magazine*, vol. 25, pp. 109 –112, Sept. 2008.

[355] Y. Chen and S. Kishore, "On the tradeoffs of implementing randomized network coding in multicast networks," *IEEE Transactions on Communications*, vol. 58, pp. 2107 –2115, July 2010.

[356] C. Fragouli and E. Soljanin, "Network coding fundamentals," *Foundation and Trends in Networking*, vol. 2, no. 1, pp. 1–133, 2007.

[357] R. W. Yeung and N. Cai, "Network error correction, Part I: Basic concepts and upper bounds," *Communications in Information and Systems*, vol. 6, no. 1, pp. 19–36, 2006.

[358] R. W. Yeung and N. Cai, "Network error correction, Part II: Lower bounds," *Communications in Information and Systems*, vol. 6, no. 1, pp. 37–54, 2006.

[359] M. Hayashi, K. Wama, H. Nishimura, R. Raymond, and S. Yamashita, Quantum network coding, vol. 4393 of *Lecture Notes in Computer Science*, pp. 610–621. Berlin: Springer-Verlag Berlin, 2007.

[360] D. Leung, J. Oppenheim, and A. Winter, "Quantum network communication-the butterfly and beyond," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3478–3490, 2010.

[361] M. Mahdian and R. Bayramzadeh, "Perfect k-pair quantum network coding using superconducting qubits," *Journal of Superconductivity and Novel Magnetism*, vol. 28, no. 2, pp. 345–348, 2015.

[362] L. Jing, C. Xiu-Bo, X. Gang, Y. Yi-Xian, and L. Zong-Peng, "Perfect quantum network coding independent of classical network solutions," *Communications Letters, IEEE*, vol. 19, no. 2, pp. 115–118, 2015.

[363] T. Satoh, K. Ishizaki, S. Nagayama, and R. Van Meter, "Analysis of quantum network coding for realistic repeater networks," *Phys. Rev. A*, vol. 93, p. 032302, Mar 2016.

[364] T. Shang, X.-J. Zhao, and J.-W. Liu, "Quantum network coding based on controlled teleportation," *IEEE Communications Letters*, vol. 18, no. 5, pp. 865–868, 2014.

[365] T. Satoh, F. Le Gall, and H. Imai, "Quantum network coding for quantum repeaters," *Physical Review A*, vol. 86, no. 3, 2012.

[366] A. Jain, M. Franceschetti, and D. A. Meyer, "On quantum network coding," *Journal of Mathematical Physics*, vol. 52, no. 3, 2011.

[367] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto, "From quantum multiplexing to high-performance quantum networking," *Nature Photonics*, vol. 4, no. 11, pp. 792–796, 2010.

[368] M. Hayashi, "Prior entanglement between senders enables perfect quantum network coding with modification," *Physical Review A*, vol. 76, no. 4, 2007.

[369] H. Kobayashi, F. Le Gall, H. Nishimura, and M. Rotteler, "Constructing quantum network coding schemes from classical nonlinear protocols," in *Information Theory Proceedings* (ISIT), 2011 IEEE International Symposium on, pp. 109–113.

[370] H. Kobayashi, F. L. Gall, H. Nishimura, and M. Rtteler, "Perfect quantum network communication protocol based on classical network coding," in 2010 *IEEE International Symposium on Information Theory*, pp. 2686–2690, June 2010.

[371] H. Kobayashi, F. Le Gall, H. Nishimura, and M. Roetteler, General Scheme for Perfect Quantum Network Coding with Free Classical Communication, vol. 5555 of *Lecture Notes in Computer Science*, pp. 622–633. 2009

[372] R. Pakniat, M. K. Tavassoly, and M. H. Zandi, "Entanglement swapping and teleportation based on cavity QED method using the nonlinear atom-field interaction: Cavities with a hybrid of coherent and number states," *OPTICS COMMUNICATIONS*, vol. 382, pp. 381–385, JAN 1 2017.

[373] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and W. K. Wootters, "Remote state preparation," *Phys. Rev. Lett*., vol. 87, p. 077902, Jul 2001.

[374] Y.-S. Ra, H.-T. Lim, and Y.-H. Kim, "Remote preparation of threephoton entangled states via single-photon measurement," *Phys. Rev. A*, vol. 94, p. 042329, Oct 2016.

[375] H. Lu, Z. Zhang, L.-K. Chen, Z.-D. Li, C. Liu, L. Li, N.-L. Liu, X. Ma, Y.-A. Chen, and J.-W. Pan, "Secret sharing of a quantum state," *Phys. Rev. Lett*., vol. 117, p. 030501, Jul 2016.

[376] H. P. Yuen, "Security of quantum key distribution," *IEEE Access*, vol. 4, pp. 724–749, 2016.

[377] J.-P. Bourgoin, B. L. Higgins, N. Gigov, C. Holloway, C. J. Pugh, S. Kaiser, M. Cranmer, and T. Jennewein, "Free-space quantum key distribution to a moving receiver," *Optics Express*, vol. 23, no. 26, pp. 33437–33447, 2015.

[378] M. T. Gruneisen, M. B. Flanagan, B. A. Sickmiller, J. P. Black, K. E. Stoltenberg, and A. W. Duchane, "Modeling daytime sky access for a satellite quantum key distribution downlink," *Optics Express*, vol. 23, no. 18, pp. 23924–23934, 2015.

[379] G. Vallone, D. G. Marangon, M. Canale, I. Savorgnan, D. Bacco, M. Barbieri, S. Calimani, C. Barbieri, N. Laurenti, and P. Villoresi, "Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels," *Physical Review A*, vol. 91, no. 4, 2015.

[380] A. Carrasco-Casado, N. Denisenko, and V. Fernandez, "Correction of beam wander for a free-space quantum key distribution system operating in urban environment," *Optical Engineering*, vol. 53, no. 8, 2014.

[381] G. Vest, M. Rau, L. Fuchs, G. Corrielli, H.Weier, S. Nauerth, A. Crespi, R. Osellame, and H. Weinfurter, "Design and evaluation of a handheld quantum key distribution sender module," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, pp. 131–137, May 2015.

[382] M. Rau, T. Heindel, S. Unsleber, T. Braun, J. Fischer, S. Frick, S. Nauerth, C. Schneider, G. Vest, S. Reitzenstein, M. Kamp, A. Forchel, S. Hoefling, and H. Weinfurter, "Free space quantum key distribution over 500 meters using electrically driven quantum dot single-photon sources-a proof of principle experiment," *New Journal of Physics*, vol. 16, 2014.

[383] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, "Inside quantum repeaters," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, pp. 78–90, May 2015.

[384] C. Y. Chen, G. J. Zeng, F. j. Lin, Y. H. Chou, and H. C. Chao, "Quantum cryptography and its applications over the internet," *IEEE Network*, vol. 29, pp. 64–69, September 2015.

[385] A. Hellemans, "Two steps closer to a quantum internet [news]," *IEEE Spectrum*, vol. 53, pp. 11–13, January 2016.

[386] N. L. Piparo and M. Razavi, "Long-distance trust-free quantum key distribution," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, pp. 123–130, May 2015.

[387] A. Delteil, Z. Sun, W.-b. Gao, E. Togan, S. Faelt, and A. Imamoglu, "Generation of heralded entanglement between distant hole spins," *NATURE PHYSICS*, vol. 12, pp. 218+, MAR 2016.

[388] B. T. Kirby, S. Santra, V. S. Malinovsky, and M. Brodsky, "Entanglement swapping of two arbitrarily degraded entangled states," *PHYSICAL REVIEW A*, vol. 94, JUL 20 2016.

[389] T. Shang, J. Li, Z. Pei, and J.-w. Liu, "Quantum network coding for general repeater networks," *Quantum Information Processing*, vol. 14, no. 9, pp. 3533–3552, 2015.

[390] H. V. Nguyen, S. X. Ng, and L. Hanzo, "Irregular convolution and unity-rate coded network-coding for cooperative multi-user communications,"*IEEE Transactions on Wireless Communications*, vol. 12,no. 3, pp. 1231–1243, 2013.

[391] Q. You, Y. Li, and Z. Chen, "Joint relay selection and network coding for error-prone two-way decode-and-forward relay networks," *IEEE Transactions on Communications*, vol. 62, pp. 3420–3433, Oct 2014.

[392] T. X. Vu, P. Duhamel, and M. D. Renzo, "On the diversity of networkcoded cooperation with decode-and-forward relay selection," *IEEE Transactions on Wireless Communications*, vol. 14, pp. 4369–4378, Aug 2015.

[393] H. Nguyen, Z. Babar, D. Alanis, P. Botsinis, D. Chandra, A. Izhar, S. Ng, and L. Hanzo, "Towards the quantum internet: Generalised

quantum network coding for large-scale quantum communication networks," *IEEE Access*, 8 2017.
[394] J. von Neumann, *Theory of Self-Reproducing Automata*. University of Illinois Press, Champaign, IL, USA. (1966).
[395] J. von Neumann. *Mathematical Foundations of Quantum Mechanics*. Princeton University Press, (1996).
[396] M. Nielsen. A simple formula for the average gate fidelity of a quantum dynamical operation. *Physics Letters A*, 303(4):249 - 252, (2002).
[397] F. Nielsen, J.-D. Boissonnat, and R. Nock. On Bregman Voronoi diagrams. *In Proceedings of the 18th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'07),* pages 746–755, Philadelphia, PA, USA, Society for Industrial and Applied Mathematics, (2007).
[398] F. Nielsen, J. D. Boissonnat, R. Nock, Bregman Voronoi Diagrams: Prop erties, *arXiv:0709.2196v1*, (2007).
[399] F. Nielsen, R. Nock: Bregman Sided and Symmetrized Centroids. ICPR 2008, ICPR'08, *(arXiv:0711.3242*), (2008).
[400] F. Nielsen, R. Nock: On the smallest enclosing information disk. *Inf. Process. Lett*. IPL'08, 105(3): 93-97 (2008).
[401] F. Nielsen, R. Nock: Quantum Voronoi Diagrams and Holevo Channel Capacity for 1-Qubit Quantum States, *ISIT 2008*, (2008).
[402] F. Nielsen, R. Nock: Approximating Smallest Enclosing Balls with Application to Machine Learning, *International Journal on Computational Geometry and Applications* (IJCGA'09), (2009).
[403] M. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, (2000).
[404] M. Nielsen. Quantum information theory. PhD thesis, University of New Mexico, quant-ph/0011036. (1998).
[405] M. Nielsen. Conditions for a class of entanglement transformations. *Physical Review Letters*, 83(2):436-439, (1999).
[406] R. Nock, F. Nielsen: Fitting the Smallest Enclosing Bregman Ball. ECML 2005, ECML'05, pages 649-656, (2005).
[407] T. Ogawa and Hiroshi Nagaoka. Making good codes for classical-quantum channel coding via quantum hypothesis testing. *IEEE Transactions on Information Theory*, 53(6):2261-2266, (2007).
[408] H. Ohno and D. Petz, Generalized Pauli channels, *Acta Math*. Hungary 124, 165-177. (2009).
[409] M. Ohya, D. Petz, and N. Watanabe. "On capacities of quantum channels". *Prob. Math. Stats*., 17:170–196, (1997).
[410] D. Oi, The Geometry of Single-Qubit Maps, *arXiv:quant-ph/0106035v1* (2001)
[411] K. Onishi and H. Imai: Voronoi Diagram in Statistical Parametric Space by Kullback-Leibler Divergence. *Proceedings of the 13th ACM Symposium on Computational Geometry*, pp.463–465, (1997).
[412] K. Onishi and H. Imai: Voronoi Diagram in Statistical Parametric Space by Kullback-Leibler Divergence. *Proceedings of the 13th ACM Symposium on Computational Geometry*, pp.463–465, (1997).
[413] K. Onishi and H. Imai: Voronoi Diagram in Statistical Parametric Space by Kullback-Leibler Divergence. *Proceedings of the 13th ACM Symposium on Computational Geometry*, pp.463–465, (1997).
[414] J. Oppenheim, For quantum information, two wrongs can make a right, *Science*, 321, 1783 (2008), arXiv:1004.0052v1 (2008).
[415] M. Oto, H. Imai and K. Imai: Computational Geometry on 1-qubit Quantum States. *Proc. International Symposium on Voronoi Diagrams in Science and Engineering* (VD 2004), Tokyo, pp.145–151, (2004).
[416] M. Ozawa. Quantum measuring processes of continuous observables. *Journal of Mathematical Physics*, 25(1):79-87, (1984).
[417] J. Pade. (auth.), *Quantum Mechanics for Pedestrians 1: Fundamentals. Undergraduate Lecture Notes in Physics*, Springer International Publishing, 1 ed., (2014).
[418] R. Panigrahy, "Minimum enclosing polytope in high dimensions," *arXiv cs.CG/0407020*, (2004).
[419] Botsinis, Panagiotis, Alanis, Dimitrios, Ng, Soon Xin and Hanzo, Lajos Low-Complexity Soft-Output Quantum-Assisted Multi-User Detection for Direct-Sequence Spreading and Slow Subcarrier-Hopping Aided SDMA-OFDM Systems. *IEEE Access*, PP, (99), doi:10.1109/ACCESS.2014.2322013 (2014).
[420] Botsinis, Panagiotis, Ng, Soon Xin and Hanzo, Lajos Fixed-complexity quantum-assisted multi-user detection for CDMA and SDMA. *IEEE Transactions on Communications*, vol. 62, (no. 3), pp. 990-1000, doi:10.1109/TCOMM.2014.012514.130615 (2014).
[421] G. D. Paparo and M. A. Martin-Delgado, "Google in a quantum network," *Scientific Reports*, vol. 2, (2012).
[422] R. García-Patrón, S. Pirandola, S. Lloyd, and J. H. Shapiro. Reverse coherent information. *Physical Review Letters*, 102(21):210501, (2009).
[423] B. Pelletier, "Informative barycentres in statistics," *Annals of the Institute of Statistical Mathematics*, vol. 57, no. 4, pp. 767–780, (2005).
[424] C. Perez-Delgado, D. Cheung, Models of quantum cellular automata, *Physical Review A* 76, 032320, (2005).
[425] S. Perseguers, M. Lewenstein, A. Acín and J.I. Cirac, Quantum random networks, *Nature Physics*, Advanced Online Publication, DOI:10.1038/NPHYS1665, (2010).
[426] J. R. Petta, A. C. Johnson, J. M. Taylor, E. A. Laird, A. Yacoby, M. D. Lukin, C. M. Marcus, M. P. Hanson, and A. C. Gossard, "Coherent manipulation of coupled electron spins in semiconductor quantum dots," *SCIENCE*, vol. 309, pp. 2180–2184 (2005).
[427] D. Petz, Bregman divergence as relative operator entropy, *Acta Math*. Hungar, 116, 127-131. (2007).
[428] D. Petz, *Quantum information theory and Quantum Statistics*, Springer-Verlag, Heidelberg, Hiv: 6. (2008).
[429] D. Petz and V.E. S Szabó, From quasi-entropy to skew information, *Int. J. Math*. 20, 1421-1430. (2009).
[430] D. Petz, A. Szántó and M. Weiner, Complementarity and the algebraic structure of 4-level quantum systems, *J. Infin. Dim. Anal*., Quantum Probability and Related Topics 12, 99-116. (2009).
[431] D. Petz, Complementarity and the algebraic structure of finite quantum systems, *J. of Physics*: Conference Series 143, 012011. (2009).
[432] D. Petz and J. Pitrik, Markov property of Gaussian states of canonical commutation relation algebras, *J. Math. Phys*. 50, 113517 (2009).
[433] D. Petz, From f-divergence to quantum quasi-entropies and their use, Entropy 12(2010), 304-325. (2010).
[434] D. Petz, Algebraic complementarity in quantum theory, *J. Math. Phys*. 51, 015215 (2010).
[435] D. Petz and C. Sudár, "Geometries of quantum states," *Journal of Mathematical Physics*, vol. 37, no. 6, pp. 2662–2673, (1996).
[436] Physorg Portal, Quantum memory for communication networks of the future, http://www.physorg.com/news/2010-11-quantum-memory-networks-future.html, (2010).
[437] Physorg Portal, Single-photon source may meet the needs of quantum communication systems, http://www.physorg.com/news82281692.html (2006).
[438] Physorg Portal, Researchers convert quantum signals to telecom wavelengths, increase memory times, http://www.physorg.com/news204728305.html (2010).
[439] Physorg Portal, Quantum Communication in Random Networks, http://www.physorg.com/news194080900.html (2010).
[440] J. Pierce. The early days of information theory. *IEEE Transactions on Information Theory*, IT-19(1):3-8, (1973).
[441] M. Planck. Ueber das gesetz der energieverteilung im normalspectrum. *Annalen der Physik*, 4:553-563, (1901).
[442] D. Poulin, J. Tillich, and H. Ollivier, "Quantum serial turbo codes," *IEEE Transactions on Information Theory*, vol. 55, pp. 2776–2798, (2009).
[443] J. Preskill. Lecture notes on *Quantum Information Processing*. http://www.theory.alteh.edu/people/preskill/ph229/#leture. (1998).
[444] J. Preskill. Reliable quantum computers. *Proceedings of the Royal Society A*: Mathematical, Physical and Engineering Sciences, 454(1969):385-410, (1998).
[445] J. Preskill, *Lecture Notes for Physics 229:Quantum Information and Computation*. CreateSpace Independent Publishing Platform, 2015.
[446] M. Radmark, M. Zukowski, and M. Bourennane, Experimental Test of Fidelity Limits in Six-Photon Interferometry and of Rotational Invariance Properties of the Photonic Six-Qubit Entanglement Singlet State, *Phys. Rev. Lett*. 103, 150501, (2009).
[447] V. Rajan. Optimality of the Delaunay triangulation in Rd. *Discrete & Computational Geometry*, 12:189–202, (1994).
[448] J. Renes, G. Smith. Noisy processing and the distillation of private quantum states. *Phys. Rev. Lett*. 98, 020502 (2007).
[449] R. Renka. Algorithm 772: Stripack: Delaunay triangulation and Voronoi diagram on the surface of a sphere. *ACM Transactions on Mathematical Software*, 23(3):416–434, (1997).
[450] S. Richter, R. Werner, Ergodicity of quantum cellular automata. *Journal of Statistical Physics*, 82:963–998. (1996).
[451] M. Ruskai, S. Szarek, and E. Werner, "An Analysis of Completely-Positive Trace Preserving Maps on 2 by 2 Matrices", LANL ArXiV e-print *quant-ph/0101003*, (2001).
[452] K. Sadakane, H. Imai, K. Onishi, M. Inaba, F. Takeuchi, and K. Imai. Voronoi diagrams by divergences with additive weights. In *Symposium on Computational Geometry*, pages 403–404, (1998).
[453] M. Safari and M. Uysal, "Relay-assisted quantum-key distribution over long atmospheric channels," *Journal of Lightwave Technology*, vol. 27, pp. 4508–4515 (2009).
[454] J. Sakurai. *Modern Quantum Mechanics* (2nd Edition). Addison Wesley, (1994).
[455] N. Sangouard, C. Simon, H. de Riedmatten, N. Gisin, Quantum

repeaters based on atomic ensembles and linear optics *arXiv:0906.2699* (2009).

[456] P. K. Sarvepalli, A. Klappenecker, and M. Rotteler, "Asymmetric quantum codes: constructions, bounds and performance," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 465, no. 2105, pp. 1645–1672 (2009).

[457] Schindler et al., "A quantum information processor with trapped ions," *New Journal of Physics*, vol. 15 (2013).

[458] E. Schrödinger. Quantisierung als eigenwertproblem. *Annalen der Physik*, 79:361-376, (1926).

[459] E. Schrödinger. Discussion of probability relations between separated systems. *Proceedings of the Cambridge Philosophical Society*, 31:555-563, (1935).

[460] F. Schmidt-Kaler, S. Gulde, M. Riebe, T. Deuschle, A. Kreuter, G. Lancaster, C. Becher, J. Eschner, H. Hffner, and R. Blatt, "The coherence of qubits based on single Ca+ ions," *Journal of Physics B-Atomic Molecular and Optical Physics*, vol. 36, pp. 623–636, Feb. 14 2003.

[461] B. Schumacher and M. Westmoreland, "Indeterminate-length quantum coding", *Physical Review A* **64**, 2304-2316, (2001).

[462] B. Schumacher and M. Westmoreland. Approximate quantum error correction. *Quantum Information Processing*, 1(1/2):5-12, (2002).

[463] B. Schumacher and M. Westmoreland, "Relative Entropy in quantum information theory" 2000, LANL ArXiV e-print quant-ph/0004045, to appear in *Quantum Computation and Quantum Information: A Millenium Volume* , S. Lomonaco, editor (American Mathematical Society Contemporary Mathematics series), (2000).

[464] B. Schumacher and R. Jozsa, "A new proof of the quantum noiseless coding theorem", *Journal of Modern Optics* **41**, 2343-2349 (1994).

[465] B. Schumacher, P. Hausladen, M. D. Westmoreland and W. K. Wootters "Sending classical bits via quantum bits," *Annals of the New York Academy of Sciences* **755**, 698-705 (1995).

[466] B. Schumacher , "Quantum coding", *Physical Review A* **51**, 2738-2747 (1995).

[467] B. Schumacher, "Sending entanglement through noisy quantum channels", *Physical Review A* **54**, 2614-2628 (1996).

[468] B. Schumacher and M. A. Nielsen, "Quantum data processing and error correction", *Physical Review A* **54**, 2629-2629 (1996).

[469] B. Schumacher and M. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A*, vol. 56, no. 1, pp. 131–138, (1997).

[470] B. Schumacher and M. Westmoreland, "Quantum privacy and quantum coherence", *Physical Review Letters* **80**, 5695-5697 (1998).

[471] B. Schumacher, H. Barnum and M. A. Nielsen) "Information transmission through a noisy quantum channel", *Physical Review A* **57**, 4153-4175 (1998).

[472] B. Schumacher, C. M. Caves, M. A. Nielsen, and H. Barnum, "Information theoretic approach to quantum error correction and reversible measurement", *Proceedings of the Royal Society of London A* **454**, 277-304 (1998).

[473] B. Schumacher and M. Westmoreland, "Optimal Signal Ensembles", LANL ArXiV e-print *quant-ph/9912122,* (1999).

[474] B. Schumacher and M. Westmoreland, "Characterizations of classical and quantum communication processes", *Chaos, Solitons and Fractals* **10**, 1719-1736 (1999).

[475] R. Seidel. Convex hull computations. In J. E. Goodman and J. O'Rourke, editors, *Handbook of Discrete and Computational Geometry*, 2nd ed., chapter 22. Chapman & Hall/CRC, (2004).

[476] T. Shang, X.-J. Zhao, and J.-W. Liu, "Quantum network coding based on controlled teleportation," *IEEE Communications Letters*, vol. 18, pp. 865–868 (2014).

[477] C. Shannon, „A mathematical theory of communication", Bell System Tech. J. 27, 379 - 423, 623 - 656 (1948).

[478] C. Shannon, "The zero-error capacity of a noisy channel," *IEEE Trans. Information Theory*, pp. 8–19, (1956).

[479] J. H. Shapiro, "Normal-mode approach to wave propagation in the turbulent atmosphere," *Appl. Opt.*, vol. 13, pp. 2614–2619 (1974).

[480] J. H. Shapiro, "Near-field turbulence effects on quantum-key distribution," *Phys. Rev. A*, vol. 67, p. 022309 (2003).

[481] Jeffrey H. Shapiro, Secure Communication using Gaussian-State Quantum Illumination, , *arXiv:0903.3150* (2009).

[482] M. Sharir. Algorithmic motion planning. In J. E. Goodman and J. O'Rourke, editors, *Handbook of Discrete and Computational Geometry*, 2nd edn., chapter 47. Chapman & Hall/CRC, (2004).

[483] M. Sharir. Almost tight upper bounds for lower envelopes in higher dimensions. *Discrete and Computational Geometry*, 12(1):327–346, (1994).

[484] J. Shewchuck. Delaunay refinement algorithms for triangular mesh generation. *Comput. Geom. Theory Appl*., 22:21–74, (2002).

[485] P. Shirley, M. Ashikhmin, M. Gleicher, S. Marschner, E. Reinhard, K. Sung, W. Thompson, and P. Willemsen. *Fundamentals of Computer Graphics*, 2nd edn. A.K. Peters, (2005).

[486] M. Shirokov, „The Holevo capacity of finite dimensional channels and the additivity problem", *Commun. Math. Phys*. 262, 137 - 159 (2006).

[487] P. Shor, "The quantum channel capacity and coherent information." lecture notes, MSRI Workshop on Quantum Computation, Available online at http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/. (2002).

[488] P. Shor. Additivity of the classical capacity of entanglement-breaking quantum channels. *Journal of Mathematical Physics*, 43(9):4334-4340, arXiv:quant-ph/0201149, (2002).

[489] P. Shor. Quantum Information, Statistics, Probability (Dedicated to A. S. Holevo on the occasion of his 60th Birthday): The classical capacity achievable by a quantum channel assisted by limited entanglement. Rinton Press, Inc., *arXiv:quant-ph/0402129*, (2004).

[490] P. W. Shor. Equivalence of additivity questions in quantum information theory. *Communications in Mathematical Physics*, 246(3):453-472, arXiv:quant-ph/0305035. (2004).

[491] P. Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52(4):R2493-R2496, (1995).

[492] P. Shor. Fault-tolerant quantum computation. Annual *IEEE Symposium on Foundations of Computer Science*, page 56, (1996).

[493] P. Shor and J. Smolin, Quantum Error-Correcting Codes Need Not Completely Reveal the Error Syndrome, *arXiv:quant-ph/9604006v2*, (1996).

[494] P. Shor. Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAMJ. Comp*.,26(5):1484-1509, (1997).

[495] G. Smith, D. Leung. Typical entanglement in stabilizer states. quant-ph/0510232. *Phys. Rev. A* 74, 062314 (2006).

[496] G. Smith, J. Smolin. Degenerate quantum codes for Pauli channels. *Phys. Rev. Lett*. 98, 030501 (2007).

[497] G. Smith, J. Yard, Quantum Communication with Zero-capacity Channels. *Science* 321, 1812-1815 (2008).

[498] G. Smith, J. Smolin. Additive extensions of a quantum channel. *IEEE Information Theory Workshop Proceedings* (2008).

[499] G. Smith, J. Renes, J. Smolin. Structured codes improve the Bennett-Brassard-84 quantum key rate. *Phys. Rev. Lett*. 100, 170502 (2008).

[500] G. Smith, J. Smolin, A. Winter. The quantum capacity with symmetric side channels. *IEEE Trans. Info. Theory* 54, 9, 4208-4217 (2008).

[501] G. Smith. The private classical capacity with a symmetric side channel and its application to quantum cryptography. *Phys. Rev. A* 78, 022306 (2008).

[502] G. Smith, John Smolin. Can non-private channels transmit quantum information? *Phys. Rev. Lett*. 102, 010501 (2009).

[503] G. Smith and J. A. Smolin, "Extensive Nonadditivity of Privacy," *Physical Review Letters*, vol. 103, no. 12, p. 120503, Sep. *arXiv:0904.4050*. (2009).

[504] G. Smith: Quantum Channel Capacities, *Information Theory Workshop* (ITW), 2010 IEEE, Aug. 30 2010-Sept. 3 2010. page(s): 1 - 5 arXiv:1007.2855, (2010).

[505] G. Smith, J. A. Smolin and J. Yard, Gaussian bosonic synergy: quantum communication via realistic channels of zero quantum capacity, *arXiv:1102.4580v1*, (2011).

[506] J. Smolin, G. Smith, S. Wehner. A simple family of nonadditive quantum codes. *Phys. Rev. Lett*. 99, 130505 (2007).

[507] A. Steane, Error correcting codes in quantum theory. *Physical Review Letters*, 77(5):793-797, (1996).

[508] M. Steiner, P. Neumann, J. Beck, F. Jelezko, and J. Wrachtrup, Universal enhancement of the optical readout fidelity of single electron spins at nitrogen-vacancy centers in diamond, *Phys. Rev. B* 81, 035205, (2010).

[509] A. M. Stephens, Z.W. Evans, S.J. Devitt, A.D. Greentree, A.G. Fowler, W.J. Munro, J.L. O'Brien, K. Nemoto and L.C.L. Hollenberg, A Deterministic optical quantum computer using photonic modules, *Physical Review A*. 78, 032318, (2008).

[510] W. F. Stinespring. Positive functions on C*-algebras. *Proceedings of the American Mathematical Society*, 6:211-216, (1955).

[511] Hiroki Takesue, Toshihiko Sasaki, Kiyoshi Tamaki, and Masato Koashi, Experimental quantum key distribution without monitoring signal disturbance, *Nature Photonics* 9, 827-831 (2015).

[512] W. Thomson (1st Baron Kelvin). Nineteenth-century clouds over the dynamical theory of heat and light. *The London, Edinburgh and Dublin*

Philosophical Magazine and Journal of Science, 2(6):1, (1901).
[513] T. Toffoli, & N. Margolus, Invertible cellular automata: A review. *Physica D*: Nonlinear Phenomena, 45:229–253. (1990).
[514] G. Toth, & C. Lent, Quantum computing with quantum-dot cellular automata. *Physical Review A*, 63:052315. (2001).
[515] P. V. Trinh, N. T. Dang, and A. T. Pham, "All-optical relaying fso systems using edfa combined with optical hard-limiter over atmospheric turbulence channels," *Journal of Lightwave Technology*, vol. 33, pp. 4132–4144 (2015).
[516] K. Tsujino, D. Fukuda, G. Fujii, S. Inoue, M. Fujiwara, M. Takeoka, and M. Sasaki, "Quantum receiver beyond the standard quantum limit of coherent optical communication," *Phys. Rev. Lett*., vol. 106, p. 250503 (2011).
[517] A. M. Tyryshkin, J. J. L. Morton, S. C. Benjamin, A. Ardavan, G. A. D. Briggs, J. W. Ager, and S. A. Lyon, "Coherence of spin qubits in silicon," *Journal of Physics-Condensed Matter*, vol. 18, pp. S783–S794, (2006).
[518] W. G. Unruh, Maintaining coherence in quantum computers. *Physical Review A*, 51(2):992-997, (1995).
[519] L. Vandersypen, M. Steffen, G. Breyta, C. Yannoni, M. Sherwood, and I. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature*, vol. 414, pp. 883–887 (2001).
[520] R. Van Meter, T. Ladd, W.J. Munro, and K. Nemoto, Communication Links for Distributed Quantum Computation, *IEEE Transactions on Computers*, 56(12), 1643-1653 (2008).
[521] R. Van Meter, T. D. Ladd, W. J. Munro, and K. Nemoto, System Design for a Long-Line Quantum Repeater, *IEEE/ACM Transactions on Networking* 17, 1002 (2009).
[522] R. Van Meter, T. Satoh, T. D. Ladd, W. J. Munro, K. Nemoto, Path Selection for Quantum Repeater Networks, Networking *Science*, Vol. 3, Issue 1-4, pp 82-95 (2013).
[523] R. Van Meter, *Quantum Networking*, John Wiley and Sons Ltd, ISBN 1118648927, 9781118648926 (2014).
[524] V.Vedral, "The Role of Relative Entropy in Quantum Information Theory". *Rev. Mod. Phys*, 10.1103/RevModPhys.74.197. (2000).
[525] V.Vedral and M. B. Plenio, "Basics of quantum computation". *Prog. Quant. Electron*., 22, 1–39. (1998).
[526] K. Vollbrecht, & J. Cirac, Quantum simulators, continuous-time automata, and translationally invariant systems. *Phys. Rev. Lett*., 100:010501, (2008).
[527] G. Voronoi. Nouvelles applications des parametres continusa la theorie des formes quadratiques. Premier M'emoire: Sur quelques propri'et'es des formes quadratiques positives parfaites. *J. Reine Angew. Math*., 133:97–178, (1907).
[528] G. Voronoi. Nouvelles applications des parametres continusa la theorie des formes quadratiques. *Deuxi'eme M'emoire: Recherches sur les parall'ello'edres primitifs. J. Reine Angew. Math*., 134:198–287, (1908).
[529] L. Wang and R. Renner. One-shot classical-quantum capacity and hypothesis testing. *arXiv:1007.5456*, (2010).
[530] J. Watrous, *Lecture Notes in Quantum Computation*, University of Calgary, (2006).
[531] J. Watrous, On one-dimensional quantum cellular automata. In: *Proceedings of the 36th Annual Symposium on Foundations of Computer Science*, pp 528–537. (1995).
[532] R. Wein, J. van den Berg, and D. Halperin. The visibility-Voronoi complex and its applications. *Comput. Geom. Theory Appl*., 36:66–87, (2007).
[533] E. Welzl. Constructing the visibility graph for n line segments in O(n2) time. *Inform. Process. Lett*., 20:167–171, (1985).
[534] E. Welzl. Partition trees for triangle counting and other range searching problems. In Proc. 4th Annu. *ACM Sympos. Comput. Geom*., pages 23–33, (1988).
[535] E. Welzl. Smallest enclosing disks (balls and ellipsoids). In H. Maurer, editor, *New Results and New Trends in Computer Science*, number 555 in *Lecture Notes in Computer Science*, pages 359–370, (1991).
[536] M. Wilde, H. Krovi, and T. A. Brun. Coherent communication with continuous quantum variables. *Physical Review A*, 75(6):060303(R), (2007).
[537] M. Wilde and Min-Hsiu Hsieh. Public and private resource trade-offs for a quantum channel. *arXiv:1005.3818*. (2010).
[538] M. Wilde, *From Classical to Quantum Shannon Theory*, arxiv.org/abs/1106.1445, (2011).
[539] M. Wilde and M.-H. Hsieh, "The quantum dynamic capacity formula of a quantum channel," *Quantum Information Processing*, vol. 11, pp. 1431–1463 (2012).
[540] M. Wilde, M.-H. Hsieh, and Z. Babar, "Entanglement-assisted quantum turbo codes," *IEEE Transactions on Information Theory*, vol. 60, pp. 1203–1222 (2014).
[541] P. Williams, H. Clearwater, *Ultimate Zero and One Computing at the Quantum Frontier*. New York, USA : COPERNICUS Springer-Verlag New York (2000).
[542] A. Winter. The capacity of the quantum multiple access channel. *IEEE Transactions on Information Theory*, 47:3059-3065, (2001).
[543] A. Winter and Serge Massar. Compression of quantum-measurement operations. *Physical Review A*, 64(1):012311, (2001).
[544] A. J. Winter. "Extrinsic" and "intrinsic" data in quantum measurements: asymptotic convex decomposition of positive operator valued measures. *Communications in Mathematical Physics*, 244(1):157-185, (2004).
[545] A. Winter, „The maximum output p-norm of quantum channels is not multiplicative for any $p > 2$", *ArXiv:0707.0402*, (2007).
[546] A. Winter. Coding theorem and strong converse for quantum channels. *IEEE Transactions on Information Theory*, 45(7):2481-2485, (1999).
[547] A. Winter. *Coding Theorems of Quantum Information Theory*. PhD thesis, Universitat Bielefeld, arXiv:quant-ph/9907077, (1999).
[548] M. Wolf and J. Eisert, Classical information capacity of a class of quantum channels. *New Journal of Physics*, 7(93), (2005).
[549] M. M. Wolf, D. P-Garcia, G. Giedke, Quantum Capacities of Bosonic Channels, arXiv:*quant-ph/0606132v1*, (2006).
[550] M. Wolf and David Pérez-García. Quantum capacities of channels with small environment. *Physical Review A*, 75(1):012303, (2007).
[551] W. Wootters and W. H. Zurek, A single quantum cannot be cloned. *Nature*, 299:802–803, doi:10.1038/299802a0. (1982).
[552] M. Worboys and M. Duckham. GIS, a Computing Perspective, 2nd edn. Chapman & Hall/CRC, (2004).
[553] L. Jian-Wu, C. Zi, S. Jin-Jing, and G. Ying, "Quantum secret sharing with quantum graph states," *Acta Physica Sinica*, vol. 65, (2016).
[554] WorldWideScience.org, Sample records for quantum computer development from WorldWideScience.org, http://worldwidescience.org/ (2011).
[555] J. Yard. *Simultaneous classical-quantum capacities of quantum multiple access channels*. PhD thesis, Stanford University, Stanford, CA,arXiv:quant-ph/0506050.(2005).
[556] J. Yard, I. Devetak, and P. Hayden. *Capacity theorems for quantum multiple access channels*. In Proceedings of the International Symposium on Information Theory, pages 884-888, Adelaide, Australia, (2005).
[557] J. Yard, P. Hayden, and I. Devetak. Quantum broadcast channels, *arXiv:quant-ph/0603098*., (2006).
[558] J. Yard, P. Hayden, and I. Devetak. Capacity theorems for quantum multiple-access channels: Classical-quantum and quantum-quantum capacity regions. *IEEE Transactions on Information Theory*, 54(7):3091-3113, (2008).
[559] B. Yen and J. Shapiro. Multiple-access bosonic communications. *Physical Review A*, 72(6):062312, (2005).
[560] R. Yeung. *A First Course in Information Theory. Information Technology: Transmission, Processing, and Storage*. Springer (Kluwer Academic/Plenum Publishers), New York, New York, USA, (2002).
[561] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, (2017).
[562] S. Yoshizawa and K. Tanabe, "Dual differential geometry associated with Kullback-Leibler information on the Gaussian distributions and its 2-parameter deformations," *SUT Journal of Mathematics*, vol. 35, no. 1, pp. 113–137, (1999).
[563] Z-S. Yuan, Y. Chen, B. Zhao, S. Chen, J. Schmiedmayer, J. Pan, Experimental demonstration of a BDCZ quantum repeater node, *Nature* 454, 1098-1101, doi:10.1038/nature07241; (2008).
[564] A. Zeilinger, "Experiment and the foundations of quantum physics," *Rev. Mod. Phys.*, vol. 71, pp. S288–S297 (1999).
[565] Xiao-Song Ma, Thomas Herbst, Thomas Scheidl, Daqing Wang, Sebastian Kropatschek, William Naylor, Bernhard Wittmann, Alexandra Mech, Johannes Kofler, Elena Anisimova, Vadim Makarov, Thomas Jennewein, Rupert Ursin and Anton Zeilinger, Quantum teleportation over 143 kilometres using active feed-forward, *Nature* 489, 269-273 (2012).
[566] W. Zhang, S. Hranilovic, and C. Shi, "Soft-switching hybrid fso/rf links using short-length raptor codes: design and implementation," *IEEE*

Journal on Selected Areas in Communications, vol. 27, pp. 1698–1708 (2009).

[567] Zhang Y, Djordjevic IB, Gao X., On the quantum-channel capacity for orbital angular momentum-based free-space optical communications, *Opt Lett*. *37*(15):3267-9 (2012).

[568] Q. Zhang, W. Saad, M. Bennis, and M. Debbah, "Quantum Game Theory for Beam Alignment in Millimeter Wave Device-to-Device Communications," in *Proc. of the IEEE Global Communications Conference (GLOBECOM)*, Washington, DC, USA, December 2016.

[569] W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, and G.-C. Guo, "Quantum Secure Direct Communication with Quantum Memory," *Physical Review Letters*, vol. 118, (2017).

APPENDIX

A. Partial Trace

If we have a density matrix which describes only a subset of a larger quantum space, then we talk about the reduced density matrix. The larger quantum system can be expressed as the tensor product of the reduced density matrices of the subsystems, if there is no correlation (entanglement) between the subsystems. On the other hand, if we have two subsystems with reduced density matrices ρ_A and ρ_B, then from the overall density matrix denoted by ρ_{AB} the subsystems can be expressed as $\rho_A{=}Tr_B\left(\rho_{AB}\right)$ and $\rho_B{=}Tr_A\left(\rho_{AB}\right)$, where Tr_B and Tr_A refers to the partial trace operators. So, this partial trace operator can be used to generate one of the subsystems from the joint state $\rho_{AB}{=}\left|\psi_A\right\rangle\left\langle\psi_A\right|\otimes\left|\psi_B\right\rangle\left\langle\psi_B\right|$, then

$$\begin{aligned}\rho_A{=}Tr_B\left(\rho_{AB}\right){=}&Tr_B\left(\left|\psi_A\right\rangle\left\langle\psi_A\right|\otimes\left|\psi_B\right\rangle\left\langle\psi_B\right|\right)\\ {=}&\left|\psi_A\right\rangle\left\langle\psi_A\right|Tr\left(\left|\psi_B\right\rangle\left\langle\psi_B\right|\right){=}\left|\psi_A\right\rangle\left\langle\psi_A\right|\left\langle\psi_B\mid\psi_B\right\rangle.\end{aligned} \tag{A.1}$$

Since the inner product is trivially $\left\langle\psi_B\mid\psi_B\right\rangle=1$, therefore

$$Tr_B\left(\rho_{AB}\right){=}\left\langle\psi_B\mid\psi_B\right\rangle\left|\psi_A\right\rangle\left\langle\psi_A\right|{=}\left|\psi_A\right\rangle\left\langle\psi_A\right|{=}\rho_A. \tag{A.2}$$

In the calculation, we used the fact that $Tr\left(\left|\psi_1\right\rangle\left\langle\psi_2\right|\right){=}\left\langle\psi_2\mid\psi_1\right\rangle$. In general, if we have to systems $A{=}\left|i\right\rangle\left\langle k\right|$ and $B{=}\left|j\right\rangle\left\langle l\right|$, then the partial trace can be calculated as

$$Tr_B\left(A{\otimes}B\right){=}ATr\left(B\right), \tag{A.3}$$

since

$$\begin{aligned}Tr_2\left(\left|i\right\rangle\left\langle k\right|\otimes\left|j\right\rangle\left\langle l\right|\right){=}&\left|i\right\rangle\left\langle k\right|\otimes Tr\left(\left|j\right\rangle\left\langle l\right|\right)\\ {=}&\left|i\right\rangle\left\langle k\right|\otimes\left\langle l\mid j\right\rangle\\ {=}&\left\langle l\mid j\right\rangle\left|i\right\rangle\left\langle k\right|,\end{aligned} \tag{A.4}$$

where $\left|i\right\rangle\left\langle k\right|\otimes\left|j\right\rangle\left\langle l\right|=\left|i\right\rangle\left|j\right\rangle\left(\left|k\right\rangle\left|l\right\rangle\right)^T$.

In this expression we have used the fact that $\left(AB^T\right)\otimes\left(CD^T\right)=\left(A{\otimes}C\right)\left(B^T{\otimes}D^T\right)=\left(A{\otimes}C\right)\left(B{\otimes}D\right)^T$.

B. Quantum Entanglement

A quantum system ρ_{AB} is separable if it can be written as a tensor product of the two subsystems $\rho_{AB}{=}\rho_A{\otimes}\rho_B$. Beside product states $\rho_A{\otimes}\rho_B$ which represent a composite system consisting of several independent states merged by means of tensor product $\otimes$ similarly to classical composite systems, quantum mechanics offers a unique new phenomenon called *entanglement*. For example the so called *Bell states* (or EPR states, named after Einstein, Podolsky and Rosen) are entangled ones:

$$\begin{aligned}\left|\beta_{00}\right\rangle{=}&\tfrac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right),\\ \left|\beta_{01}\right\rangle{=}&\tfrac{1}{\sqrt{2}}\left(\left|01\right\rangle+\left|10\right\rangle\right),\\ \left|\beta_{10}\right\rangle{=}&\tfrac{1}{\sqrt{2}}\left(\left|00\right\rangle-\left|11\right\rangle\right),\\ \left|\beta_{11}\right\rangle{=}&\tfrac{1}{\sqrt{2}}\left(\left|01\right\rangle-\left|10\right\rangle\right).\end{aligned} \tag{A.5}$$

C. Fidelity

Theoretically, quantum states have to preserve their original superposition during the whole transmission, without the disturbance of their actual properties. Practically, quantum channels are entangled with the environment which results in mixed states at the output. Mixed states are classical probability weighted sum of pure states where these probabilities appear due to the interaction with the environment (i.e., noise). Therefore, we introduce a new quantity, which is able to describe the quality of the transmission of the superposed states through the quantum channel. The quantity which measures this distance is called the *fidelity*. The fidelity for two pure quantum states is defined as

$$F\left(\left|\varphi\right\rangle,\left|\psi\right\rangle\right)=\left|\left\langle\varphi\right|\left.\psi\right\rangle\right|^2. \tag{A.6}$$

The fidelity of quantum states can describe the relation of Alice pure channel input state $\left|\psi\right\rangle$ and the received mixed quantum system $\sigma{=}\sum_{i=0}^{n-1}p_i\rho_i{=}\sum_{i=0}^{n-1}p_i\left|\psi_i\right\rangle\left\langle\psi_i\right|$ at the channel output as

$$F\left(\left|\psi\right\rangle,\sigma\right)=\left\langle\psi\right|\sigma\left|\psi\right\rangle=\sum_{i=0}^{n-1}p_i\left|\left\langle\psi\right|\left.\psi_i\right\rangle\right|^2. \tag{A.7}$$

Fidelity can also be defined for *mixed* states σ and ρ

$$F\left(\rho,\sigma\right)=\left[Tr\left(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right)\right]^2=\sum_i p_i\left[Tr\left(\sqrt{\sqrt{\sigma_i}\rho_i\sqrt{\sigma_i}}\right)\right]^2. \tag{A.8}$$

Next we list the major properties of fidelity

$$0{\le}F\left(\sigma,\rho\right){\le}1, \tag{A.9}$$

$$F\left(\sigma,\rho\right){=}F\left(\rho,\sigma\right), \tag{A.10}$$

$$F\left(\rho_1{\otimes}\rho_2,\sigma_1{\otimes}\sigma_2\right){=}F\left(\rho_1,\sigma_1\right)F\left(\rho_2,\sigma_2\right), \tag{A.11}$$

$$F\left(U\rho U^\dagger,U\sigma U^\dagger\right){=}F\left(\rho,\sigma\right), \tag{A.12}$$

$$F\left(\rho,a\sigma_1{+}(1{-}a)\sigma_2\right){\ge}aF\left(\rho,\sigma_1\right){+}(1{-}a)F\left(\rho,\sigma_2\right),\ a{\in}\left[0,1\right]. \tag{A.13}$$