Ph.D Thesis:

Quasi-Perfect Codes for the Classical-Quantum Channel

Ph.D Thesis:

Quasi-Perfect Codes for the Classical-Quantum Channel

Author:
Andreu Blasco Coll
andreu.blasco@upc.edu

Advisor:
Javier Rodríguez Fonollosa
javier.fonollosa@upc.edu

Departament de Teoria del Senyal i Comunicacions (TSC)
Carrer Jordi Girona 1-3, Campus Nord, Edifici D5
08034 Barcelona, Spain

Barcelona, May 2023

Acknowledgments

Summary

Quantum computers use the laws of quantum mechanics to do complex operations that classical computers can't solve. Quantum computers and other physical quantum systems require quantum information to be completely isolated from the environment in order to be perfectly functional. Quantum systems that are not completely isolated suffer from decoherence noise and may suffer from errors. Implementing these systems is a huge challenge and development of suboptimal systems with a low error rate seems to be the best way forward to building these systems.

In quantum communications, designing codes that are able to reduce or protect against errors is a necessity. This work focuses on perfect and quasi-perfect quantum codes, which are a family of codes that exists in the classical setting and are optimum in terms of minimizing the error probability for a given number of channel uses. In the first part of the work we generalize the definition of quasi-perfect codes to include both classical codes and quantum codes. We also provide an example of a quantum quasi-perfect code for 2-qubits classical-quantum channels that make use of quantum entanglement and that can be extrapolated to an N-dimensional classical-quantum channel.

The second part of this work focuses on quasi-perfect codes in optical communications, where coherent states are used to convey information through an optical channel, known as the Bosonic channel. The Bosonic channel has infinite dimension, so instead we consider a finite-dimensional approximation of the Bosonic channel with a negligible approximation error for a sufficiently large channel dimension. We show that phase-modulated coherent states constitute a codebook that is quasi-perfect for the approximated channel, and thus are close to optimal for the Bosonic channel.

The last part of the work focuses on stabilizer error correction codes, which are practical codes that use redundancy to protect against errors. Error correction is not specifically used to transmit classical information, but to protect quantum information instead. However,

it is possible that we require to obtain classical information from a quantum state after performing error correction. For these particular cases we may be able to prove that an error correction code is quasi-perfect and thus optimum.

Resum

Els ordinadors quàntics fan servir les lleis de la mecànica quàntica per a realitzar operacions complexes que els ordinadors clàssics no poden resoldre. Els ordinadors quàntics i els altres sistemes quàntics requereixen que la informació quàntica estigui completament aïllada de l'entorn per tal de ser perfectament funcionals. Els sistemes quàntics que no estan completament aïllats són afectats per soroll de decoherència i poden patir errors. Implementar aquests sistemes és un gran repte i l'única manera de construir sistemes quàntics és desenvolupar sistemes subòptims amb una taxa d'error baixa.

En comunicacions quàntiques, dissenyar codis capaços de reduir o protegir contra errors és una necessitat. Aquest treball es centra en codis quàntics perfectes i quasi-perfectes que ja existeixen en sistemes clàssics i que són òptims en termes de minimitzar la probabilitat d'error per un determinat nombre d'usos del canal. A la primera part del treball generalitzem la definició de codis quasi-perfectes per incloure codis clàssics i codis quàntics. També proveïm un exemple de codi quàntic quasi-perfecte per a canals clàssic-quàntics de 2-qubits que fa servir entrellaçat quàntic i que pot extrapolar-se a un canal de dimensió N.

La segona part d'aquest treball es centra en codis quasi-perfectes en comunicacions òptiques, on estats coherents es fan servir per a transmetre informació a través d'un canal òptic, conegut com a canal Bosònic. El canal Bosònic té dimensió infinita, per això considerem en canvi una aproximació del canal Bosònic de dimensió finita, amb un error d'aproximació negligible amb una dimensió de canal suficientment gran. Demostrem que una modulació de fase dels estats coherents constitueix un codi quasi-perfecte pel canal aproximat, i per tant és pràcticament òptim per al canal Bosònic.

L'última part del treball es centra en codis estabilitzadors de correcció d'errors, que són codis pràctics que fan servir redundància per a protegir contra errors. La correcció d'errors no es fa servir específicament per a transmetre informació clàssica, sinó per a protegir la informació quàntica. Tot i això, és possible que requerim obtenir informació clàssica d'un

estat quàntic després de fer servir correcció d'errors. Per a aquests casos, pot ser possible demostrar que un codi de correcció d'errors és quasi-perfecte i per tant òptim.

Resumen

Los ordenadores cuánticos hacen uso de las leyes de la mecánica cuántica para realizar operaciones complejas que los ordenadores clásicos no pueden resolver. Los ordenadores cuánticos y otros sistemas cuánticos requieren que la información cuántica esté completamente aislada del entorno para poder ser perfectamente funcionales. Los sistemas cuánticos que no están completamente aislados son afectados por ruido de decoherencia y pueden sufrir errores. Implementar estos sistemas es un gran reto y la única manera de construir sistemas cuánticos es desarrollar sistemas subóptimos con una tasa de error baja.

En comunicaciones cuánticas, diseñar códigos capaces de reducir o proteger contra errores es una necesidad. Este trabajo se centra en códigos cuánticos perfectos y quasi-perfectos que ya existen en sistemas clásicos y que son óptimos en términos de minimizar la probabilidad de error para un determinado número de usos del canal. En la primera parte del trabajo generalizamos la definición de códigos quasi-perfectos para incluir códigos clásicos y códigos cuánticos. También proveemos un ejemplo de código cuántico quasi-perfecto para canales clásico-cuánticos de 2-qubits que usa entrelazado cuántico y que puede extrapolarse a un canal de dimensión N.

La segunda parte de este trabajo se centra en códigos quasi-perfectos en comunicaciones ópticas, donde se usan estados coherentes para transmitir información a través de un canal óptico, conocido como canal Bosónico. El canal Bosónico tiene dimensión infinita, por eso consideramos en cambio una aproximación del canal Bosónico de dimensión finita, con un error de aproximación negligible con una dimensión del canal suficientemente grande. Demostramos que una modulación de fase de los estados coherentes constituye un código quasi-perfecto para el canal aproximado y, por lo tanto es prácticamente óptimo para el canal Bosónico.

La última parte del trabajo se centra en códigos estabilizadores de corrección de errores, que son códigos prácticos que usan redundancia para proteger contra errores. La corrección

de errores no se usa específicamente para transmitir información clásica, sino para proteger la información cuántica. Aún así, es posible que requiramos obtener información clásica de un estado cuántico después de usar corrección de errores. Para estos casos, puede ser posible demostrar que un código de corrección de errores es quasi-perfecto y, por lo tanto, óptimo.

Contents

Notation

Mathematical notation

$\mathbb{N}$	set of natural numbers
$\mathbb{Z}$	set of integers
$\mathbb{R}$	set of real numbers
$\mathbb{C}$	set of complex numbers
U	unitary operator
X, Y, Z	Pauli matrices
H	Hamdamard matrix
$\mathbb{1}_N$	identity matrix of dimension N
Π	projector matrix
$\mathcal{C}$	code set
$\mathcal{X}, \mathcal{Y}$	alphabets or sets
$\left\|\psi\right\rangle, \left\|\phi\right\rangle$	quantum pure vector states
ρ	quantum density matrix
$\left\|\Phi^+\right\rangle, \left\|\Phi^-\right\rangle, \left\|\Psi^+\right\rangle, \left\|\Psi^-\right\rangle$	Bell states
$N_{A\to B}$	Quantum channel

1

Introduction

1.1 Introduction to quantum information theory and motivation

Quantum information theory combines classical information theory with quantum mechanics. It differs from classical information theory in several aspects. Quantum information theory is indeterministic: it is based on the probabilities of events rather than on their predictions. Unlike in classical systems, a quantum state can be a superposition state; that is, a linear combination of other allowed states.

The simplest unit of quantum information is the qubit (quantum bit) which, can be represented, for example, by the spin of an electron or by the polarization of a photon. More complex systems like a quantum computer are harder to implement; these systems usually are very noisy and suffer from decoherence. Quantum systems can be measured and the measurement outcome becomes a random variable. Let's suppose we want to implement a quantum circuit that prepares the maximally entangled state, which is a quantum state of two qubits which are in the same state, that is, when measured independently they behave like a binary equally distributed random variable but their measurement outcomes are fully correlated. Then when we measure each qubit of the maximally entangled state we may have an outcome of "00" (that is, two classical "0s") with a probability of 50% or an outcome "11" also with 50% probability. Measurement outcomes "01" and "10" are in principle impossible, i.e. their probability is 0. We can simulate the behavior of this circuit using the available (online) IBM Q Experience quantum system simulator. Our simulation consist on performing 1024 measurements of each of the two qubits. Ideally both outcome "00" and "11" should be obtained with probability 0.5 and outcomes "01" and "10" should never happen. The histogram of the simulation shows convergence of the expected results.

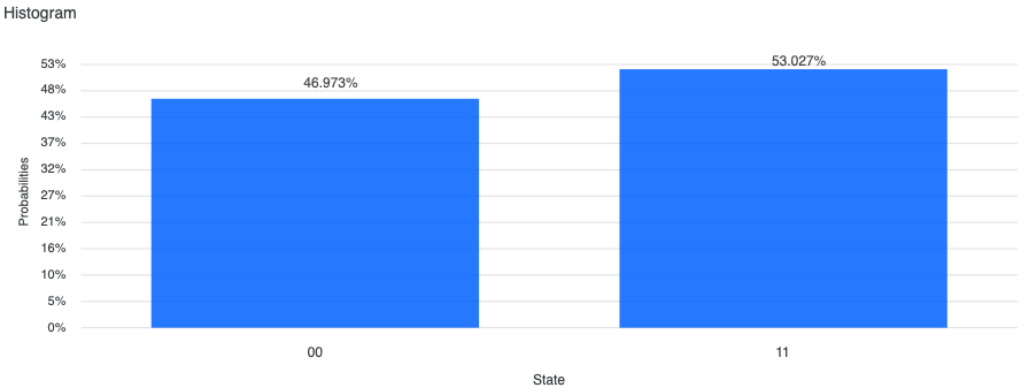

Figure 1.1: Histogram from the simulation of a circuit that generates the maximally entangled state

The same circuit executed on a real quantum computer (also using 1024 iterations) gives a histogram like the one illustrated in Fig.1.2

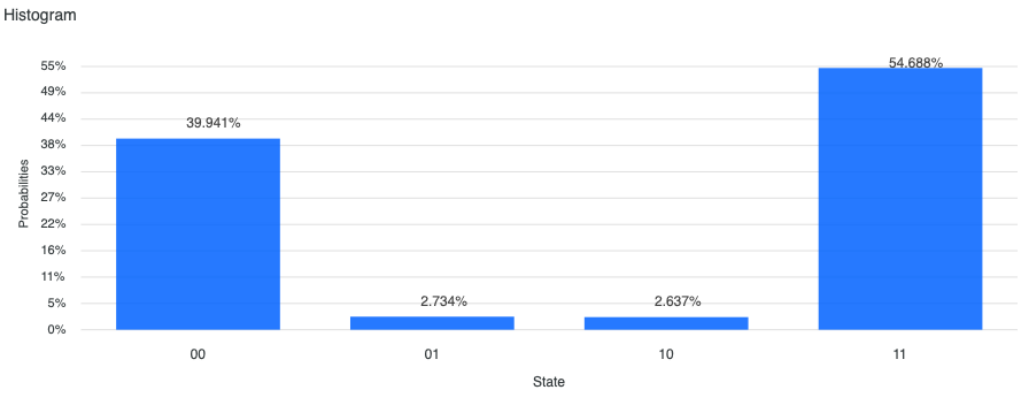

Figure 1.2: Histogram from the implementation on a real quantum computer of a circuit that generates the maximally entangled state

The real implementation differs from the simulation: now outcomes "01" and "10" are also obtained and outcomes "00" and "11" do not seem to be characterized by the same probabilities. This shows that even for a very simple circuit the results when using real quantum computers may be very different from what we expect from the theory of quantum mechanics.

Despite being difficult to implement quantum systems have some benefits over classical ones. They can be unconditionally secure (see for example [12], [13]) due to some particularities of quantum systems (non-cloning theorem). Quantum computers also will be able to solve tasks that classical computers are not able to solve, and in theory be computationally more efficient. Recently Google demonstrated quantum supremacy using a developed 54-qubit processor [14] (that is, they claim that their processor can perform tasks that the classical computer can not perform in practice), so maybe the quantum era is closer than we expect. In any case, it is clear that current quantum systems demand quantum error protecting codes for proper operation.

This work will investigate perfect and quasi-perfect codes in the quantum context. These codes are optimum to minimize the error probability when transmitting information over a classical-quantum channel and thus might be able to contribute to more reliable quantum systems.

1.2 Brief introduction to the history of quantum mechanics

In the 19th century, before the introduction of quantum mechanics, it was believed that classical physics (consisting on Newton's laws of mechanics, Maxwell's electromagnetic theory and Boltzmann's theory of statistical mechanics) were able to explain any physical phenomena. However, as stated in 1901 by William Thomson Kelvin [4], there was some

phenomena that could not be fully explained by the classical theory, namely the failure of the Michelson-Morley experiment and the "ultraviolet catastrophe".

The Michelson-Morley experiment [5] pretended to detect the existence ether, which was believed to be an invisible medium that allowed light waves to travel through vacuum. It was assumed that light waves could not travel through empty space and so there had to be a medium carrying light waves through empty space. However, the experiment provided evidence against the ether theory.

On the other hand, the ultraviolet catastrophe is the classical prediction that a black body would emit an infinite amount of energy at high frequencies, which does not happen in reality. In 1901, Planck considered the hypothesis that radiating energy exists in discrete quantities (in bundles of energy) and used this model to predict how much energy does a black body emits in function of the frequency [6]. Later, Einstein reinforced Planck's theory and showed that it provided an explanation to the photoelectric effect [7]. In 1924, de Broglie stated that every element of matter behaves as both particles and waves [8], and in 1926 Schrödinger formulated a wave equation that describes the evolution of quantum systems [9]. In 1925, Heisenberg introduced an alternative theory called matrix mechanics [10] that was not as popular as the Schrödinger's theory, but later in 1930 Dirac showed that both formalisms were equivalent and unified them [11].

1.3 Quantum postulates

Quantum mechanics are described by the following four postulates:

1. **Postulate 1**: Any isolated physical system has an associated Hilbert space $\mathcal{H}$ of a certain dimension on the field of complex numbers $\mathbb{C}$. This Hilbert space is called the state space. The system is completely defined by a state $|\psi\rangle$ (a unit vector) at any instant. An example is a qubit, which is a two-dimensional vector that is defined by two complex numbers (see Section 2.1). In general, it is a difficult problem to know what is the state space for a specific system, and it would require to delve into the field of quantum electrodynamics. In this work we will always assume that the state space is known.

2. **Postulate 2**: The evolution of a quantum system is described by a unitary operator U acting on the state vector.

3. **Postulate 3**: A quantum measurement is a set of operators $\{\Pi_m\}$, called measurement operators, that act on the state space of the system in order to obtain a classical outcome m. The measurement operation is irreversible: the state after measurement is affected by this process and it is not possible to recover the original state.

4. **Postulate 4**: The state of a composite system (i.e. a system consisting on two or more physical systems) is the tensor product of the state spaces of the smaller systems. For

example, if a system in the state $|\psi\rangle$ is composed by multiple systems in the states $|\psi\rangle_1$,$|\psi\rangle_2$,...,$|\psi\rangle_n$, then the state $|\psi\rangle$ can be decomposed as $|\psi\rangle = |\psi\rangle_1 \otimes |\psi\rangle_2 \otimes \ldots \otimes |\psi\rangle_n$.

The formal definitions and implications of these postulates will be described in Chapter 2.

1.4 Objectives

This section presents the main objectives of this work, which can be summarized as the following:

- Objective 1: Provide a generalization of perfect and quasi-perfect quantum codes defined in the classical context to classical-quantum channels. For this purpose we follow a similar procedure as in the classical case. Perfect and quasi-perfect quantum codes attain the meta-converse bound with equality, and thus they minimize the error probability over a given channel.

- Objective 2: Study simple cases of 2-qubit codes over a classical-quantum channel. The goal is to find perfect and quasi-perfect codes, if they exist, for simplified cases. In Chapter 4, we present some examples of quasi-perfect codes. In particular, the Bell codes for 2-qubits and a number of codewords $M \geq 4$ are quasi-perfect codes even when the quantum state is observed after a quantum erasure channel or a depolarizing channel.

- Objective 3: Find perfect and quasi-perfect codes for more than two qubits, or equivalently for a channel dimension larger than 4. The Bell codes found for 2-qubits can be extrapolated for an arbitrary number of qubits, although there are several ways of building them (see for example [15], [16]). In Chapter 5, we study quasi-perfect codes for the bosonic channel, where the dimension of the channel is infinite. We consider an approximated version of the channel with finite, but arbitrarily large dimension.

- Objective 4: Find quasi-perfect codes that can perform error correction. Perfect and quasi-perfect codes developed in objectives 1, and 2 exhibit a cardinality greater than 2^N where N is the number of qubits. As such, they can't be used directly as quantum error correcting codes. Chapter 6 will focus on quasi-perfect codes in the error correction setting.

2

Quantum theory

This chapter presents the notation and basic quantum concepts that are necessary to understand this work. Textbooks [1], [2], [3] provide a detailed introduction to the area.

2.1 Qubit and the bloch sphere

In the quantum world, the most basic unit of information is the quantum bit or qubit. A general qubit can be represented as the superposition of two quantum states:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{2.1}$$

where α and β are the complex amplitudes of the superposed states $|0\rangle$ and $|1\rangle$, and where:

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2.2}$$

The states $|0\rangle$ and $|1\rangle$ are mathematically represented in a Hilbert space of dimension 2 as the following two column vectors:

$$|0\rangle \triangleq \big[1, 0\big]^T, \tag{2.3}$$

$$|1\rangle \triangleq \big[0, 1\big]^T. \tag{2.4}$$

Similarly, $\langle 0|$ and $\langle 1|$ are defined as the row vectors:

$$\langle 0| \triangleq \big[1, 0\big], \tag{2.5}$$

$$\langle 1| \triangleq \big[0, 1\big]. \tag{2.6}$$

This notation will be used later. A qubit can also be written as:

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)e^{j\psi}\,|1\rangle\,. \tag{2.7}$$

This allows us to represent it visually in a sphere, in function of the angles θ and ψ. This sphere is called Bloch sphere.

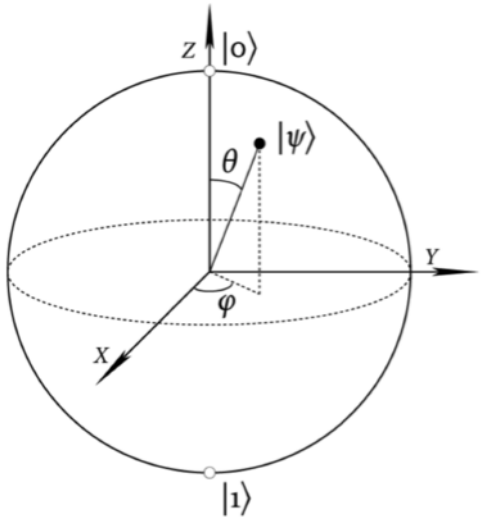

Figure 2.1: Bloch sphere

The $\{|0\rangle, |1\rangle\}$ basis is called the computational basis, but naturally a qubit can be represented in any other basis, for example, another commonly used basis would be the $\{|+\rangle, |-\rangle\}$ basis with:

$$|+\rangle \triangleq \frac{1}{\sqrt{2}}[1,1]^T, \tag{2.8}$$

$$|-\rangle \triangleq \frac{1}{\sqrt{2}}[1,-1]^T. \tag{2.9}$$

There are several ways to physically represent quantum information, including the polarization of a photon, the Fock state of a light wave (see Chapter 5) or the spin of an electron, among others. As an example, consider that the electric field vector of a light wave has the following three components in the x,y and z axis:

$$E(r,t) = \begin{pmatrix} E_x(z,t) \\ E_y(z,t), \\ 0 \end{pmatrix} \tag{2.10}$$

with

$$E_x(z,t) = E_x \cos(kz - \omega t + \alpha_x), \tag{2.11}$$

$$E_y(z,t) = E_y \cos(kz - \omega t + \alpha_y). \tag{2.12}$$

where E_x, E_y are the amplitudes of the electrical field in the x and y axis respectively, α_x, α_y are phases, ω is the angular frequency, r is the position vector, t is the time instant, z is the direction of the wave propagation and k is the wavelength number. When $E_y = 0$ and $E_x(r,t) = E_x \cos kz - \omega t + \alpha_x$, the electric field oscillates on the x axis; in this case the polarization is horizontal. Similarly, when $E_x = 0$ and $E_y(r,t) = E_y \cos kz - \omega t + \alpha_y$ the electric field oscillates on the y axis, and in this case the polarization is vertical.

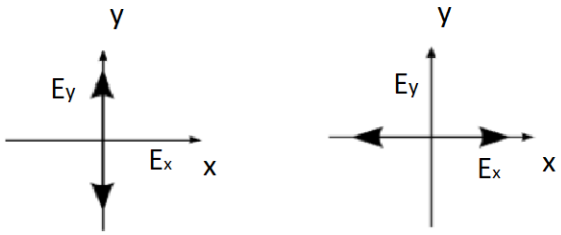

Figure 2.2: Vertical polarization (left), horizontal polarization (right)

A qubit can be represented as the polarization of a photon by assigning $|0\rangle$ to the horizontal polarization, $|0\rangle = |H\rangle$, and $|1\rangle$ to the vertical polarization, $|1\rangle = |V\rangle$.

Also, if $E_y = E_x$, then we have a wave that is a combination of a vertical polarized wave and a horizontal polarized wave. This wave has a 45° polarization and it represents a quantum state $|H\rangle + |V\rangle$ that when normalized, it corresponds to the $|+\rangle$ state. Similarly, if $E_y = -E_x$, then we have $|H\rangle - |V\rangle$ that when normalized, it corresponds to the $|-\rangle$ state. With this, it is possible to create systems that are able to use the $\{|0\rangle, |1\rangle\}$ basis and the $\{|+\rangle, |-\rangle\}$ basis as well.

Figure 2.3: Diagonal polarization, $E_y = E_x$ (left), diagonal polarization, $E_y = -E_x$ (right)

2.2 Quantum evolution

Quantum systems can undergo reversible transformations which are modelled by unitary matrices. This transformations are referred as reversible evolutions or unitary evolutions. Reversibility is a consequence of unitary evolution because unitary operators have an inverse (it is their conjugate transpose). Also, quantum states that go through unitary transformations maintain unit norm. Quantum unitary evolutions can be represented as a quantum circuit, which is a diagram that represents the qubits or quantum states of a quantum system and the unitary operators (also called quantum gates) that are applied to them.

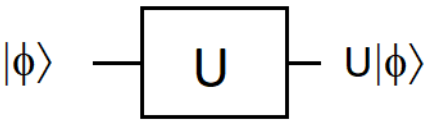

Figure 2.4: Quantum circuit representation of quantum state ϕ undergoing unitary operator U

The most common unitary operators are the Pauli matrices (I, Z, X, Y) and the Hadamard matrix (H):

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{2.13}$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{2.14}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{2.15}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \tag{2.16}$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.17}$$

$$\tag{2.18}$$

In particular, the X operator satisfies $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$ (it changes the amplitude of a qubit) and the Z operator satisfies $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$ (it changes the phase of a qubit). The Y operator is a combination of both operators. The Hadamard gate takes the

$\{|0\rangle, |1\rangle\}$ basis to the $\{|+\rangle, |-\rangle\}$ basis.

2.3 Measurement of qubits

Measurement operations in quantum systems allow us to obtain classical information from a quantum state. In general it is not possible to retrieve the complex amplitudes (α and β) or the phase of a qubit. Instead we can only measure observables, that is, physical parameters of the quantum state. Observables are represented by Hermitian operators (for example the Pauli matrices). The result of the measurement follows the Born rule: the outcome of the measurement is one of the eigenvalues of the operator and the resulting quantum state is the corresponding eigenvector. The probability of having an outcome m when performing a measurement over a qubit ψ is:

$$p_m = \langle\psi| \Pi_m |\psi\rangle, \tag{2.19}$$

where Π_m is the projector onto the eigenspace of the operator used for the measurement corresponding to the eigenvalue λ_m.

For example, if we want to measure the qubit $|\psi\rangle$ defined above in the computational basis we can use the Z operator, which has the following eigen decomposition:

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \Pi_0 - \Pi_1. \tag{2.20}$$

When we make a measurement using Z we obtain one of its eigenvalues, which are 1 and -1. We then associate the eigenvalue '1' to an outcome $m = 0$ and the eigenvalue -1 to an outcome $m = 1$. When we measure a qubit (2.1), we have the following probabilities of obtaining outcome 0 and outcome 1:

$$p_0 = \langle\psi| \Pi_0 |\psi\rangle = \langle\psi| \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} |\psi\rangle = |\alpha|^2, \tag{2.21}$$

$$p_1 = \langle\psi| \Pi_1 |\psi\rangle = \langle\psi| \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} |\psi\rangle = |\beta|^2. \tag{2.22}$$

$$\tag{2.23}$$

We could also use the operator X to make a measurement. In this case, the eigen decomposition is the following:

$$X = |+\rangle\langle +| - |-\rangle\langle -| = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} - \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \Pi_+ - \Pi_-. \tag{2.24}$$

In this case, when we make a measurement on the same qubit we obtain the following

probabilities of outcome 0 and outcome 1:

$$p_0 = \langle\psi| \Pi_+ |\psi\rangle = \frac{1}{2} \langle\psi| \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} |\psi\rangle = \left| \frac{\alpha^2 + \beta^2}{2} \right|, \tag{2.25}$$

$$p_1 = \langle\psi| \Pi_- |\psi\rangle = \frac{1}{2} \langle\psi| \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} |\psi\rangle = \left| \frac{\alpha^2 - \beta^2}{2} \right|. \tag{2.26}$$

$$\tag{2.27}$$

2.4 Composite systems

It is possible to represent systems with multiple qubits in a compact way using the kroenecker product between them. For example, a two qubit system can be represented as the kroenecker product between both qubits:

$$|\psi\rangle = |0\rangle \otimes |0\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{2.28}$$

Naturally the same applies for any other possible states. This is the mathematical model of a two qubit system and models the behavior of them even if they are placed in different locations. States representing more than one qubit are known as composite states. Unitary operators that affect individual qubits that belong to a composite system can also be expressed as a unitary operator that is the kroenecker product of each unitary operator. For example, consider a three-qubit system consisting on three qubits ψ_1, ψ_2 and ψ_3 with each qubit undergoing a unitary transformation U_1, U_2 and U_3. Each qubit's output is $U_1\psi_1$, $U_2\psi_2$ and $U_3\psi_3$, or equivalently, we can represent the output as a unitary operator affecting the whole composite state as follows:

$$(U_1\psi_1 \otimes U_2\psi_2 \otimes U_3\psi_3) = (U_1 \otimes U_2 \otimes U_3)(\psi_1 \otimes \psi_2 \otimes \psi_3), \tag{2.29}$$

where we used the property $(AC)\otimes(BD) = (A\otimes B)(C\otimes D)$ that is satisfied by the kroenecker product operation. This makes it possible to represent quantum systems as a composite input state with unitary operators applied to the composite state. An important unitary operator that is used frequently in quantum systems is the controlled NOT gate (or CNOT gate), which is an operator that takes two input qubits and outputs two qubits. One of the input qubits is a "control" qubit that is not affected by the CNOT operator, and the other one has its amplitude flipped if the control qubit is $|1\rangle$. The CNOT operator can be expressed as:

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{2.30}$$

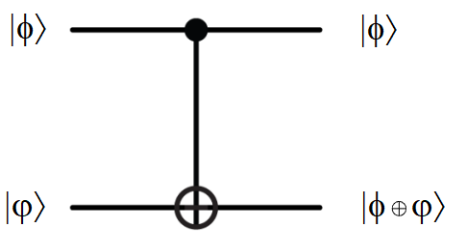

Figure 2.5: Quantum circuit representation of a CNOT gate

A composite quantum state that can not be expressed as the kroenecker product of two states is called an entangled state. For example, the so-called maximally entangled state is defined as:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{2.31}$$

When measured in isolation using the computational basis, each of the qubits delivers a binary random variable. However, the outcome at each of the qubits is always the same, i.e., they are fully correlated, even if measured in different locations. The simplest entangled states are two-qubit states called Bell states, with the one in (2.31) being one of them. There are other three Bell states, which have the form:

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \tag{2.32}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \tag{2.33}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{2.34}$$

$$\tag{2.35}$$

These four states are entangled states that form an orthogonal basis of the four-dimensional Hilbert space, and will be relevant in Section 4.4.1.

2.5 Quantum state matrix representation

The description of quantum systems discussed above is only valid for pure quantum states, that is, states fully represented in a given basis by their complex amplitudes. In general

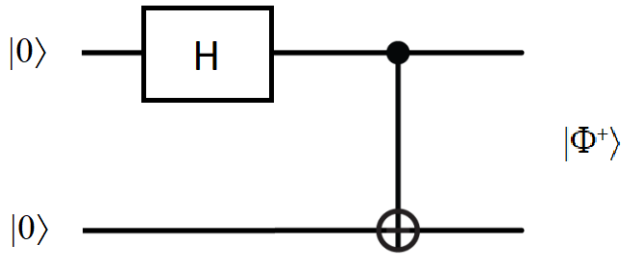

Figure 2.6: Quantum circuit representation of the Bell state $|\Phi^+\rangle$

however, quantum systems might incorporate an additional uncertainty modelled by classical probability theory, that is, they can be characterized by different states each with a certain probability. In this case the quantum state is mixed (not pure) and it must be described using the quantum state matrix representation as:

$$\rho = \sum_{x \in \mathcal{X}} p_x \left|\psi_x\right\rangle \left\langle\psi_x\right| , \tag{2.36}$$

where ρ is called the density operator. Density operators are semidefinite positive and they have unitary trace $\operatorname{Tr} \rho = 1$, since $\sum_{x \in \mathcal{X}} p_x = 1$ and qubits have unitary norm.

2.6 Quantum channels

Let $\mathcal{D}(\mathcal{H})$ represent the space of density operators that act on a Hilbert space $\mathcal{H}$. We denote $\mathcal{N}_{A \to B}$ as a map which takes density operators in $\mathcal{D}(\mathcal{H}_A)$ to density operators in $\mathcal{D}(\mathcal{H}_B)$. A quantum channel is defined as a linear, completely positive and trace-preserving map describing the evolution of a quantum system. A map has these properties if and only if it can be decomposed in the following way:

$$\mathcal{N}_{A \to B}(\rho_A) = \sum_{l=0}^{d-1} V_l \rho_A V_l^\dagger , \tag{2.37}$$

where ρ_A is a density operator belonging to Hilbert space $\mathcal{H}_A$, d is no larger than $\dim(\mathcal{H}_A) \dim(\mathcal{H}_B)$ and V_l are called Kraus operators and belong to the space of square linear operators which take Hilbert space $\mathcal{H}_A$ to Hilbert space $\mathcal{H}_B$. The Kraus operators must satisfy:

$$\sum_{l=0}^{d-1} V_l^\dagger V_l = \mathbb{1}_A. \tag{2.38}$$

The most relevant channel in this work is the classical-quantum channel. The classical quantum channel takes a classical input x and outputs a density operator ρ_x associated to x. It can be modelled as follows:

$$\mathcal{N}_{X\to B}^{CQ}(p_X) = \sum_{x=0}^{d-1} p_X(x)\rho_B^x. \tag{2.39}$$

In general, quantum channels take a quantum state and transform it into another quantum state. An example of a quantum-quantum channel is the Pauli channel, which applies a Pauli operator to the state with a certain probability:

$$\mathcal{N}_{A\to B}^{P} = \sum_{i,j=0}^{1} p(i,j) Z^i X^j \rho X^j Z^i, \tag{2.40}$$

where $p(i,j)$ is the probability of applying Z (for $i=1$) and X (for $j=1$), and X and Z are the Pauli matrices defined before. Note that $X^0 = Z^0 = \mathbb{1}_A$.

The erasure channel is a quantum-quantum channel in which the dimension of the Hilbert space at the output of the channel equals the dimension of the input Hilbert space plus one. Note that this is a generalization of the classical erasure channel. The quantum erasure channel is modelled by the following equation:

$$\mathcal{N}_{A\to B}^{E}(\rho_A) = (1-\epsilon)\mathcal{I}_{A\to B}(\rho_A) + \epsilon|e\rangle\langle e|_B, \tag{2.41}$$

where ϵ is the erasure probability and the Isometric channel $\mathcal{I}_{A\to B}(\rho_A) = I_{A\to B}\rho_A I_{A\to B}^\dagger$ is defined using the Isometry

$$I_{A\to B} = \begin{bmatrix} & \mathbb{1}_A & \\ 0 & \dots & 0 \end{bmatrix}, \tag{2.42}$$

where $\mathbb{1}_A$ is the identity matrix with the same dimensions as the input density operator, i.e. $\dim(\mathcal{H}_A)$. The last channel presented here is the depolarizing channel. The effect of this channel is to leave the input channel state untouched (with probability 1-p) or destroy it completely, and transform it into a uniform distributed classical random variable (with probability p) represented by quantum state π.

$$\mathcal{N}_{A\to B}^{D}(\rho_A) = p\pi + (1-p)\rho_A, \tag{2.43}$$

where $\pi = \frac{1}{\dim(\mathcal{H}_A)}\mathbb{1}_A$.

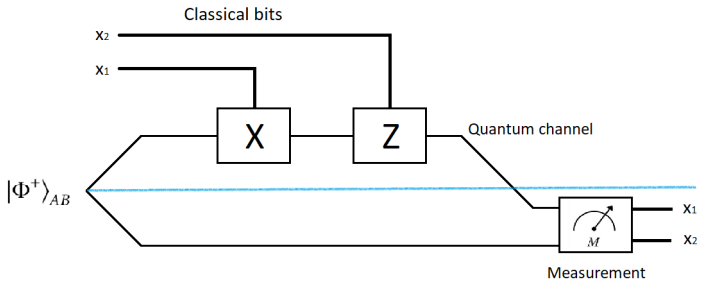

Figure 2.7: Superdense coding protocol implementation

2.7 Quantum protocols

The superdense coding protocol is a quantum protocol used to transmit classical information from Alice (transmitter) to Bob (receiver). The name of the protocol is due to the fact that two classical bits are sent with a single use of the quantum channel (i.e. transmitting only a single qubit), and one entangled pair of qubits. Initially, the protocol has Alice and Bob sharing an ebit, $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)$. Then, it does the following steps:

1. Alice applies a unitary operator (i.e. an I,X, Z or Y operators) to her share of the state, depending on the two classical bits that should be transmitted. For example, if the first bit is a "1", then the X operator is applied, and if the second bit is a "1" the Z operator is applied. Then, the state is transformed into one of the bell states, $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$.

2. Alice transmits her qubit to Bob through the quantum channel.

3. Bob measures the state in the basis $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$. Since this base is orthogonal, he is able to distinguish these four states perfectly. Using the result of the measurement, he can recover the classical bits that were transmitted.

The circuit implementing the superdense coding protocol is represented in 2.7.

Similarly, the teleportation protocol is used in order to transmit quantum information by transmitting only two classical bits. The name of the protocol is due to the fact that the quantum state that is transmitted is destroyed in the original location and restored at the destination. As it was the case for the superdense coding protocol, Alice and Bob initially share an ebit $|\Phi^+\rangle_{AB}$. The teleportation protocol does the following in order to transmit the qubit $|\psi\rangle_{A'}$ from Alice to Bob:

1. Alice performs a measurement in the basis $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$ on her whole system, consisting on her qubit and her share of the ebit $|\Phi^+\rangle_A$. This makes the whole state collapse to one of four possible states, which are $|\Phi^+\rangle_{A'A} |\psi\rangle_B$, $|\Phi^-\rangle_{A'A} Z |\psi\rangle_B$,

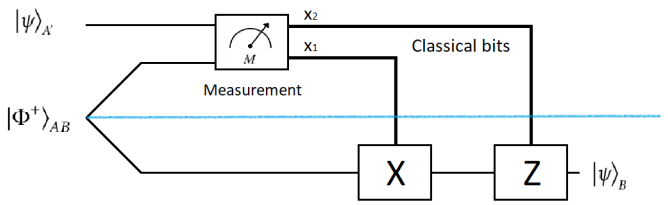

Figure 2.8: Teleportation protocol implementation

$|\Psi^+\rangle_{A'A} X|\psi\rangle_B$, $|\Psi^-\rangle_{A'A} XZ|\psi\rangle_B$. This is because the state of the whole quantum system is $|\psi\rangle_{A'}|\Phi^+\rangle_{AB}$, which can be expressed in the Bell basis as follows:

$$|\psi\rangle_{A'}|\Phi^+\rangle_{AB} = (\alpha|0\rangle_{A'} + \beta|1\rangle_{A'})\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) \tag{2.44}$$

$$= \frac{1}{2}\left(\alpha(|\Phi^+\rangle_{A'A} + |\Phi^-\rangle_{A'A})|0\rangle_B\right) + \left(\beta|\Psi^+\rangle_{A'A} - |\Psi^-\rangle_{A'A})|0\rangle_B\right) + \left(\alpha(|\Psi^+\rangle_{A'A} + |\Psi^-\rangle_{A'A})|1\rangle_B\right) + \left(\beta(|\Phi^+\rangle_{A'A} - |\Phi^-\rangle_{A'A})|1\rangle_B\right) \tag{2.45}$$

$$= \frac{1}{2}\left(|\Phi^+\rangle_{A'A}|\psi\rangle_B + |\Phi^-\rangle_{A'A} Z|\psi\rangle_B + |\Psi^+\rangle_{A'A} X|\psi\rangle_B + |\Psi^-\rangle_{A'A} XZ|\psi\rangle_B\right). \tag{2.46}$$

After the measurement operation the state $|\psi\rangle_{A'}$ is lost, and instead we get $|\psi\rangle_B$ under the effect of a Pauli matrix.

2. Alice sends two classical bits to Bob in order to indicate what was the measurement outcome (i.e. to indicate which of the four states is the state after measurement). Bob uses this information in order to decide what operator should be applied to his share of the ebit in order to recover $|\psi\rangle$. For example, if the result of the measurement is $|\Psi^+\rangle_{A'A} X|\psi\rangle_B$, then he only has to apply an X gate to $X|\psi\rangle_B$ in order to obtain $X(X|\psi\rangle_B) = |\psi\rangle_B$.

The circuit implementing the teleportation protocol is represented in 2.8. Both the superdense coding protocol and the teleportation protocol are examples of applications where entanglement is used, and so classical schemes are not able to replicate these protocols.

3

State of the art

This section presents the state of the art on quasi-perfect codes in the classical setting and on the meta-converse bound in the classical and quantum settings.

3.1 Meta-converse bound

The meta-converse bound in the classical setting was introduced in [28], and it is a bound on the error probability of a Bayesian M-ary hypothesis test. Consider a binary hypothesis test setting, where the objective is to discriminate between two hypothesis, H_0 and H_1 from an observation of a random variable Y that takes values in an alphabet $\mathcal{Y}$. Define $P_0(y)$ as the probability mass function of Y under hypothesis H_0 and $P_1(y)$ as the probability mass function of Y under hypothesis H_1. We define $T(y)$ as the probability of deciding hypothesis H_0 given an observation y. Define $\alpha_\beta(P_0, P_1)$ as the minimum probability of choosing hypothesis H_1 when the true hypothesis is hypothesis H_0 with a constraint on the probability of choosing hypothesis H_0 when hypothesis H_1 is the true hypothesis:

$$\alpha_\beta(P_0, P_1) = \inf_{T:\sum_y T(y)P_1(y)\leq\beta} \left(1 - \sum_y T(y)P_0(y)\right). \tag{3.1}$$

Now, consider the M-ary hypothesis test setting where we want to discriminate between M hypotheses, $H_0, H_1, \ldots, H_{M-1}$. Consider the random variables X and Y taking values in alphabets $\mathcal{X}$ and $\mathcal{Y}$ respectively. In communication systems, a transmitter sends a message m (assigned to hypothesis H_m) over a channel by encoding it to a codeword x, and the receiver will get y with a probability of $P_Y = \sum_{x\in\mathcal{X}} P_X P_{Y|X}$. Since the mapping $m \to x$ is deterministic, x is also assigned to the hypothesis $H_m = H_x$. The receiver will try to guess

the true hypothesis H_x by using, for example, a maximum likelihood receiver (i.e. by deciding H_x such that x maximizes $P_{Y|X}$). The error probability of the system is:

$$P_e = 1 - \frac{1}{M} \sum_y \max_{x \in \mathcal{X}} P_{Y|X}(y|x). \tag{3.2}$$

According to [28] and [46, Theorem 1], the error probability satisfies

$$P_e \geq \inf_{P_X} \sup_{Q_Y} \left\{ \alpha_{\frac{1}{M}} \left(P_X \times P_{Y|X}, P_X \times Q_Y \right) \right\}, \tag{3.3}$$

where $P_X \times P_{Y|X} = \sum_x P_X P_{Y|X}$ and $P_X \times Q_Y = \sum_x P_X Q_Y$. The supremum is over all arbitrary distributions Q_Y, and the infimum is over all input distributions P_X. This lower-bound on the error probability is called the meta-converse bound, and it is a lower bound of the error probability. As it will be shown later, quasi-perfect codes achieve this error probability and so they are optimum.

3.2 Quasi-perfect codes in the classical setting

This section summarizes the results from [29] where quasi-perfect codes in the classical setting are defined.

We consider a binary hypothesis test with hypotheses H_0 and H_1. We define the distributions P_0 and P_1 over the alphabet $\mathcal{Y}$, and $T(y)$ as the probability that the test decides hypothesis H_0 for a given observation y, while the probability of deciding hypothesis H_1 is $1 - T(y)$. We define $\pi_{j|i}$ as the probability of deciding hypothesis j when the true hypothesis is i. In the binary case, we may write:

$$\pi_{0|1}(T) \triangleq \sum_y T(y) P_1(y), \tag{3.4}$$

$$\pi_{1|0}(T) \triangleq \sum_y \left(1 - T(y)\right) P_0(y). \tag{3.5}$$

Also, we define $\alpha_\beta(P_0, P_1) \triangleq \inf_{T:\pi_{0|1} \leq \beta} \pi_{1|0}(T)$. The optimal test T^* that minimizes $\alpha_\beta(P_0, P_1)$ is:

$$T^*(y) \triangleq \mathbb{1}\left[\frac{P_0(y)}{P_1(y)} > \gamma \right] + \theta \mathbb{1}\left[\frac{P_0(y)}{P_1(y)} = \gamma \right], \tag{3.6}$$

where $\mathbb{1}[.]$ is the indicator function and for $\gamma \geq 0$ and $\theta \in [0, 1]$ chosen such that $\beta = \pi_{0|1}(T_N P)$. The proof can be found in [34].

Now, consider the channel coding problem of sending M equiprobable messages $m \in (1, \ldots, M)$ through a classical channel with a transition probability of $P_{Y|X}$, with input $x \in \mathcal{X}$ and output $y \in \mathcal{Y}$. A code $\mathcal{C} = \{x_1, x_2, \ldots, x_M\}$ assigns each message to a channel input x_m. The minimum error probability of the code is given by:

$$P_e(\mathcal{C}) = 1 - \frac{1}{M} \sum_y \max_{x \in \mathcal{C}} P_{Y|X}(y|x). \tag{3.7}$$

We define Q as an arbitrary distribution over the output alphabet $\mathcal{Y}$. For any $y \in \mathcal{Y}$, the input x that maximizes $P_{Y|X}(y|x)$ also maximizes $\frac{P_{Y|X}(y|x)}{Q(y)}$, since $Q(y)$ does not depend on x. With this consideration, we define the sphere of radius τ, $S_x(\tau, Q)$, as the set of outputs y such that given input x have a likelihood of at least $\tau Q(y)$:

$$S_x(\tau, Q) \triangleq \left\{ y \in \mathcal{Y} \;\middle|\; \frac{P_{Y|X}(y|x)}{Q(y)} \geq \tau \right\}. \tag{3.8}$$

Similarly, the interior $S_{i,x}(\tau, Q)$ and the shell $S_{o,x}(\tau, Q)$ of $S_x(\tau, Q)$ are defined as:

$$S_{i,x}(\tau, Q) \triangleq \left\{ y \in \mathcal{Y} \;\middle|\; \frac{P_{Y|X}(y|x)}{Q(y)} > \tau \right\}, \tag{3.9}$$

$$S_{o,x}(\tau, Q) \triangleq \left\{ y \in \mathcal{Y} \;\middle|\; \frac{P_{Y|X}(y|x)}{Q(y)} = \tau \right\}. \tag{3.10}$$

We define the set $\mathcal{Q}$ as the set of distributions Q such that $F_x(\tau, Q)$ does not depend on x, where $F_x(\tau, Q) \triangleq \mathbb{P}\left[Y \in S_x(\tau, Q) : \tau \in [0,1], Y \sim P_{Y|X=x}\right]$:

$$\mathcal{Q} \triangleq \left\{ Q \in \mathcal{P}(\mathcal{Y}) \;\middle|\; F_x(\tau, Q) = F(\tau, Q), \forall x \in \mathcal{X}, \tau \geq 0 \right\}. \tag{3.11}$$

In cases where $\mathcal{Q}$ is not an empty set, we refer to the channel $P_{Y|X}$ as a symmetric channel.

Definition 3.1. *In the classical setting, a code $\mathcal{C}$ is perfect for a channel $P_{Y|X}$ if there exist $\gamma \geq 0$ and $Q \in \mathcal{Q}$ such that the sets $\{S_x(\gamma, Q)\}_{x \in \mathcal{C}}$ are disjoint and*

$$\bigcup_{x \in \mathcal{C}} S_x(\gamma, Q) = \mathcal{Y}. \tag{3.12}$$

Moreover, a code is quasi-perfect if the interior sets $\{S_{i,x}(\gamma, Q)\}_{x \in \mathcal{C}}$ are disjoint and (3.12) is satisfied.

Let $P_{Y|X}$ be a symmetric channel, and let $Q \in \mathcal{Q}$. For $\gamma \geq 0$, the error probability of a code satisfies:

$$P_e(\mathcal{C}) \geq \gamma \left(Q_i(\gamma) - \frac{1}{M} \right) + \sum_{\tau \in \mathcal{L}_Q, \tau \geq \gamma} \tau Q_o(\tau), \tag{3.13}$$

where $Q_i(\gamma) \triangleq \mathbb{P}[\mathcal{Y} \in S_{i,x}(\gamma, Q) : \gamma \in [0,1], \mathcal{Y} \sim Q]$, $Q_o(\gamma) \triangleq \mathbb{P}[\mathcal{Y} \in S_{o,x}(\gamma, Q) : \gamma \in [0,1], \mathcal{Y} \sim Q]$ and $\mathcal{L}_Q$ is defined as

$$\mathcal{L}_Q \triangleq \left\{ \tau \in \mathbb{R} \;\middle|\; \forall x \in \mathcal{X}, \forall y \in \mathcal{Y}, \frac{P_{Y|X}(y|x)}{Q(y)} = \tau \right\}. \tag{3.14}$$

For the proof, see [29].

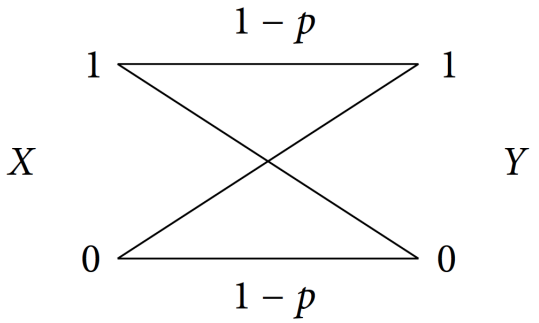

Figure 3.1: Representation of the BSC channel

3.3 Examples of classical quasi-perfect codes

This section presents some examples of quasi-perfect codes for the classical setting. Since it is possible to express classical inputs as quantum states, we will use these examples to compare the classical setting with the quantum setting, and to verify that the definition of quasi-perfect codes in the quantum setting is equivalent to the classical case.

Consider the Binary Symmetric Channel (BSC) defined over a binary input alphabet $\mathcal{X} = \{0, 1\}$ and binary output alphabet $\mathcal{Y} = \{0, 1\}$ with a probability of bit-flip error of p, such that $P(y = 0|x = 0) = (1 - p)$, $P(y = 0|x = 1) = p$, $P(y = 1|x = 0) = p$ and $P(y = 1|x = 1) = (1 - p)$. The graphical representation of the channel is shown in Figure 3.1.

The average error probability for a single use of a channel (no coding) is:

$$P_e = P(x = 0)p + P(x = 1)p = p. \tag{3.15}$$

We may be interested in defining a code to reduce the error probability. Let us consider a code that uses a two-bit input and two codewords. The input alphabet is $\mathcal{X} = \{00, 01, 10, 11\}$, the code is $\mathcal{C} = \{00, 11\}$ and the output alphabet is $\mathcal{Y} = \{00, 01, 10, 11\}$. The channel is described by the following probabilities for $x \in \mathcal{C}$:

$$P(y = 00|x = 00) = (1 - p)^2, \tag{3.16}$$
$$P(y = 01|x = 00) = P(y = 10|x = 00) = (1 - p)p, \tag{3.17}$$
$$P(y = 11|x = 00) = p^2, \tag{3.18}$$
$$P(y = 00|x = 11) = p^2, \tag{3.19}$$
$$P(y = 01|x = 11) = P(y = 10|x = 11) = (1 - p)p, \tag{3.20}$$
$$P(y = 11|x = 11) = (1 - p)^2. \tag{3.21}$$

The decoder will determine that the transmitted codeword is ”00” when receiving ”00”, and when it receives ”11” it is going to determine that the transmitted codeword was ”11”. If the decoder receives ”01” or ”10” it will randomly decide which codeword was sent, for example,

it will decide "00" when codeword "01" is received and "11" when codeword "10" is received. The average error probability of this code is:

$$P_e = P(x=00)(P(y=10|x=00)+P(y=11|x=00)) + P(x=11)(P(y=01|x=11) + P(y=00|x=11)) = P(x=00)((1-p)p+p^2) + P(x=11)((1-p)p+p^2) = p. \tag{3.22}$$

As we see, the error probability has not improved with two channel uses, so it would make sense to use three channel uses instead to protect against errors as we will see later. Even if this example does not make sense in practise, it may be interesting from a theoretical point of view in order to understand what the sets $S_x(\tau, Q)$, $S_i, x(\tau, Q)$ and $S_o, x(\tau, Q)$ represent. Using $Q(y) = 1$ and $\tau = (1-p)p$, we get that $S_i, x(\tau, Q)$ are:

$$S_{i,00}(\tau, Q) = \left\{ y \in \mathcal{Y} \;\middle|\; P_{Y|X}(y|x=00) > (1-p)p \right\} = \{00\}, \tag{3.23}$$

$$S_{i,11}(\tau, Q) = \left\{ y \in \mathcal{Y} \;\middle|\; P_{Y|X}(y|x=11) > (1-p)p \right\} = \{11\}. \tag{3.24}$$

Notice that $\{S_{i,x}(\gamma, Q)\}_{x\in\mathcal{C}}$ are disjoint, which is a requirement for a code to be quasi-perfect. Intuitively, we see that $S_i, x(\tau, Q)$ represents the decoding region that is centred at the input codeword x, and when receiving y we have that the transmitted codeword is x with higher probability than any other codewords for $y \in \{S_{i,x}(\gamma, Q)\}$. Depending on how small τ is, more codewords may be assigned to this decoding region. For example, if we had chosen $p^2 < \tau < (1-p)p$ then we would have $S_{i,00}(\tau, Q) = \{00, 01, 10\}$ and $S_{i,11}(\tau, Q) = \{11, 01, 10\}$. However, in this case we wouldn't prove that the code is quasi-perfect since these sets are not disjoint.

We see that the sets $S_{o,x}(\tau, Q)$ with $\tau = (1-p)p$ are the following:

$$S_{o,00}(\tau, Q) = \left\{ y \in \mathcal{Y} \;\middle|\; P_{Y|X}(y|x=00) = (1-p)p \right\} = \{01, 10\}, \tag{3.25}$$

$$S_{o,11}(\tau, Q) = \left\{ y \in \mathcal{Y} \;\middle|\; P_{Y|X}(y|x=11) = (1-p)p \right\} = \{01, 10\}. \tag{3.26}$$

Intuitively, $S_{o,x}(\tau, Q)$ represents the decoding region between $S_{i,00}(\tau, Q)$ and $S_{i,11}(\tau, Q)$. Finally, we have that $S_x(\tau, Q)$ are:

$$S_{00}(\tau, Q) = \left\{ y \in \mathcal{Y} \;\middle|\; P_{Y|X}(y|x=00) \geq (1-p)p \right\} = \{00, 01, 10\}, \tag{3.27}$$

$$S_{11}(\tau, Q) = \left\{ y \in \mathcal{Y} \;\middle|\; P_{Y|X}(y|x=00) \geq (1-p)p \right\} = \{11, 01, 10\}. \tag{3.28}$$

Since $\bigcup_{x\in\mathcal{C}} S_x(\tau, Q) = \mathcal{Y}$ and $\{S_x(\tau, Q)\}_{x\in\mathcal{C}}$ are not disjoint (but $\{S_{i,x}(\gamma, Q)\}_{x\in\mathcal{C}}$ are), the code is quasi-perfect. This implies that the error probability of the code is optimum for

all 2-bit codes, even though there is no improvement over the 1-bit code. As mentioned, this example is not useful in practise, but it shows that codes that don't improve the error probability with respect to a code of smaller blocklength can actually be quasi-perfect and achieve the optimum error probability for a fixed blocklength.

For a more practical example, consider a code that uses a three-bit input and two codewords. In this case, we have that the input alphabet is $\mathcal{X} = \{000, 001, 010, 011, 100, 101, 110, 111\}$, the code is $\mathcal{C} = \{000, 111\}$ and the output alphabet is $\mathcal{Y} = \{000, 001, 010, 011, 100, 101, 110, 111\}$. The channel is described by the following probabilities for $x \in \mathcal{C}$:

$$P(y = 000|x = 000) = (1-p)^3, \tag{3.29}$$
$$P(y = 001|x = 000) = (y = 010|x = 000) = (y = 100|x = 000) = (1-p)^2 p, \tag{3.30}$$
$$P(y = 011|x = 000) = P(y = 101|x = 000) = P(y = 110|x = 000) = (1-p)p^2, \tag{3.31}$$
$$P(y = 111|x = 000) = p^3, \tag{3.32}$$
$$P(y = 000|x = 111) = p^3, \tag{3.33}$$
$$P(y = 011|x = 111) = P(y = 101|x = 111) = P(y = 110|x = 111)(1-p)^2 p, \tag{3.34}$$
$$P(y = 001|x = 111) = P(y = 010|x = 111) = P(y = 100|x = 111) = (1-p)p^2, \tag{3.35}$$
$$P(y = 111|x = 111) = (1-p)^3. \tag{3.36}$$

The decoder will be able to correct single-bit errors by determining that the transmitted codeword is the one in $\mathcal{C}$ that is closer to the received sequence. So, when receiving "001", "010", "100", the decoder is going to determine that the transmitted codeword is "000", and when receiving "110","101", "011" it is going to determine that the transmitted codeword is "111". So, when a single-bit error occurs, the overall error probability is not affected since we are able to recover the original codeword. With this consideration, the average error probability of the code is:

$$P_e = 1 - (P(x = 000)P(e \geq 2) + P(x = 111)P(e \geq 2) = \tag{3.37}$$
$$P(x = 000)((1-p)p^2 + p^3) + P(x = 111)((1-p)p^2 + p^3) = (1-p)p^2 + p^3) = p^2, \tag{3.38}$$

where $P(e \geq 2)$ is the probability of having two or more errors.

Next we show that this code is perfect. Consider $Q(y) = 1$ and $\tau = (1-p)^2 p - \frac{(1-p)p^2}{2}$. In this case, we have the following:

$$S_{00}(\tau, Q) = \{y \in \mathcal{Y} \mid P_{Y|X}(y|x) \geq (1-p)^2 p - \frac{(1-p)p^2}{2}\} = \{000, 001, 010, 100\}, \tag{3.39}$$
$$S_{11}(\tau, Q) = \{y \in \mathcal{Y} \mid P_{Y|X}(y|x) \geq (1-p)^2 p - \frac{(1-p)p^2}{2}\} = \{111, 011, 101, 110\}. \tag{3.40}$$

And for the other regions we have:

$$S_{i,00}(\tau, Q) = \{y \in \mathcal{Y} \mid P_{Y|X}(y|x) > (1-p)^2 p - \frac{(1-p)p^2}{2}\} = \{000, 001, 010, 100\}, \quad (3.41)$$

$$S_{i,11}(\tau, Q) = \{y \in \mathcal{Y} \mid P_{Y|X}(y|x) > (1-p)^2 p - \frac{(1-p)p^2}{2}\} = \{111, 011, 101, 110\}, \quad (3.42)$$

$$S_{o,00}(\tau, Q) = \{y \in \mathcal{Y} \mid P_{Y|X}(y|x) = (1-p)^2 p - \frac{(1-p)p^2}{2}\} = \{\}, \quad (3.43)$$

$$S_{o,11}(\tau, Q) = \{y \in \mathcal{Y} \mid P_{Y|X}(y|x) = (1-p)^2 p - \frac{(1-p)p^2}{2}\} = \{\}. \quad (3.44)$$

In this example, $S_{o,00}(\tau, Q)$ and $S_{o,11}(\tau, Q)$ are empty sets. We can see that the sets $\{S_i, x\}$ for $x \in \mathcal{C}$ are disjoint and $\bigcup_{x \in \mathcal{C}} S_{i,x}(\tau, Q) = \mathcal{Y}$, which implies that the code is perfect.

3.4 Meta-converse bound in the quantum setting

The quantum meta-converse bound was derived in [30] and is a lower bound on the error probability of a quantum code ($P_e(C)$) with cardinality M, as in the classical setting. This section summarizes its derivation.

Consider a binary hypothesis tests that discriminates between two quantum density operators W_0 and W_1 acting on a Hilbert space $\mathcal{H}$. A measurement for each density operator is defined in the form of two positive operator-valued measures Π_0 and Π_1 (POVM), such that $\Pi_0 + \Pi_1 = \mathbb{1}$, where $\mathbb{1}$ is the identity matrix. These measurement operators applied to W_0 (and W_1) have outcome 0 (or 1) with probability $\mathrm{Tr}(W_0\Pi_0)$ (or $\mathrm{Tr}(W_1\Pi_1)$).

We define $\epsilon_{1|0}$ as the probability of deciding hypothesis 1 (or equivalently W_1) when the true one is hypothesis 0 (probability of false alarm) and $\epsilon_{0|1}$ as the probability of deciding hypothesis 0 (or equivalently W_0) when hypothesis 1 is the true hypothesis (probability of miss-detection). Considering this, we have the following:

$$\epsilon_{1|0} = 1 - \mathrm{Tr}(W_0\Pi_0), \quad (3.45)$$

$$\epsilon_{0|1} = \mathrm{Tr}(W_1\Pi_0). \quad (3.46)$$

We define

$$\alpha_\beta(W_0||W_1) \triangleq \inf_{\Pi_0 : \epsilon_{0|1} \leqslant \beta} (\epsilon_{1|0}) \quad (3.47)$$

as the minimum probability of false alarm over all possible tests Π_0 having a maximum probability of miss-detection of β. The quantum Neyman-Pearson lemma [33] states that a test T_{op} is an optimum test for this binary hypothesis test problem if and only if it lies on

the positive and null eigenspaces of the matrix $W_0 - tW_1$ where $t \geqslant 0$. Specifically, we define:

$$P_t^+ \triangleq \{W_0 - tW_1 > 0\}, \tag{3.48}$$
$$P_t^- \triangleq \{W_0 - tW_1 < 0\}, \tag{3.49}$$
$$P_t^0 \triangleq \{W_0 - tW_1 = 0\}, \tag{3.50}$$
$$\tag{3.51}$$

where $\{A > 0\} \triangleq \sum_{i:\lambda_i>0} E_i$, $\{\lambda_i\}$ are the eigenvalues resulting from the spectral decomposition of A ($A = \sum_i \lambda_i E_i$) and $\{E_i\}$ are the orthogonal projections onto the corresponding eigenspaces. Then the optimum test minimizing (3.47) satisfies:

$$T_{op} = P_t^+ + p_t^0, \tag{3.52}$$

where $0 \leq p_t^0 \leq P_t^0$.

Consider now the case of multiple hypothesis testing, that is, we have to discriminate among M quantum states $\{W_1,W_2,...,W_M\}$, each with an associated probability of occurring $\{p_1,p_2,...,p_M\}$. In this case we need to define a POVM set $\mathcal{P} = \{\Pi_1, \Pi_2, ..., \Pi_M\}$ such that $\sum_m \Pi_m = \mathbb{1}$ in order to make a measurement over the observed quantum state and decide which is the true hypothesis. The average error probability of the test is:

$$\epsilon(\mathcal{P}) \triangleq 1 - \sum_{m=1}^{M} p_m \operatorname{Tr}(W_m \Pi_m), \tag{3.53}$$

and the minimum average error probability is obtained by optimizing over all possible test $\mathcal{P}$:

$$\epsilon \triangleq \min_{\mathcal{P}} \epsilon(\mathcal{P}). \tag{3.54}$$

We design the test $\mathcal{P}$ in order to minimize the average error probability. The optimum test does not have a closed form, but it is known that it has to satisfy the Holevo-Yuen-Kennedy-Lax conditions:

Lemma 3.1 (Holevo-Yuen-Kennedy-Lax conditions). *A decoder $\mathcal{P}^\star = \{\Pi_1^\star, \ldots, \Pi_M^\star\}$ minimizes (3.54) if and only if, for each $m = 1, \ldots, M$,*

$$\big(\Lambda(\mathcal{P}^\star) - p_m W_m\big)\Pi_m^\star \;=\; \Pi_m^\star\big(\Lambda(\mathcal{P}^\star) - p_m W_m\big) \;=\; 0, \tag{3.55}$$
$$\Lambda(\mathcal{P}^\star) - p_m W_m \;\geq\; 0, \tag{3.56}$$

where

$$\Lambda(\mathcal{P}^\star) \triangleq \sum_{m=1}^{M} p_m W_m \Pi_m^\star = \sum_{m=1}^{M} p_m \Pi_m^\star W_m \tag{3.57}$$

is required to be self-adjoint.

Proof: The theorem follows from [31, Th. 4.1, Eq. (4.8)] or [32, Th. I] after simplifying the optimality conditions. ■

The multiple hypothesis problem can be simplified by transforming it into a binary hypothesis problem. We define the following matrices:

$$\mathcal{T} \triangleq diag(p_1 W_1, ..., p_M W_M), \tag{3.58}$$

$$\mathcal{D}(\mu_0) \triangleq \frac{1}{M} diag(\mu_0, ..., \mu_0). \tag{3.59}$$

The $\mathcal{T}$ matrix is a block diagonal matrix containing all the possible quantum states associated to a hypothesis weighted by their corresponding classical probabilities, and the $\mathcal{D}(\mu_0)$ matrix is also a block diagonal matrix built using an arbitrary density operator μ_0.

If we use a test $\mathcal{P} = \{\Pi_1, \Pi_2, ..., \Pi_M\}$ to discriminate quantum states W_1, W_2,..., W_M we can define a binary hypothesis test to discriminate $\mathcal{T}$ and $\mathcal{D}(\mu_0)$ which will have the following false alarm and miss-detection probabilities:

$$\epsilon_{1|0}(\mathcal{P}) = 1 - \sum_{m=1}^{M} p_m Tr(W_m \Pi_m) = \epsilon(\mathcal{P}), \tag{3.60}$$

$$\epsilon_{0|1}(\mathcal{P}) = \frac{1}{M} \sum_{m=1}^{M} Tr(\mu_0 \Pi_m) = \frac{1}{M}. \tag{3.61}$$

Considering this and the definition of $\alpha_\beta(W_0||W_1)$ above, it is possible to get a lower bound on the average error probability:

$$\epsilon(\mathcal{P}) \geq \max_{\mu_0} \alpha_{\frac{1}{M}}(\mathcal{T}||\mathcal{D}(\mu_0)). \tag{3.62}$$

It is possible to show that an optimum test satisfying Lemma 3.1 achieves this bound with respect to some specific μ_0. Take $\mu_0 = \mu_0^* = \frac{1}{c_0^*}\Lambda(\mathcal{P}^*)$ with c_0^* being a normalization constant and $t = Mc_0^*$. If we take $\mathcal{P}^* = \{\Pi_1^*, \Pi_2^*, ..., \Pi_M^*\}$ then:

$$T - tD(\mu_0) = diag(p_1 W_1 - \Lambda(\mathcal{P}^*), p_2 W_2 - \Lambda(\mathcal{P}^*), ..., p_M W_M - \Lambda(\mathcal{P}^*)). \tag{3.63}$$

According to the quantum Neyman-Pearson theorem the optimum test $\mathcal{T}_{op}$ that minimizes the average error probability corresponds to the non-negative eigenspace of the matrix $\mathcal{T} - t\mathcal{D}(\mu_0)$. If we define $\mathcal{T}_{op} = diag(\mathcal{T}_{op_1}, \mathcal{T}_{op_2}, ..., \mathcal{T}_{op_M})$ then $\mathcal{T}_{op_m}$ must be on the non-negative eigenspace of $p_m W_m - \Lambda(\mathcal{P}^*)$. Also, in order to satisfy the Holevo-Yuen-Kennedy-Lax conditions it should also be on the non-positive eigenspace of $\mathcal{T} - t\mathcal{D}(\mu_0)$, so it has to be on the null eigenspace. In this case we have:

$$\epsilon_{1|0}(\mathcal{T}_{op}) = \epsilon(\mathcal{P}^*), \tag{3.64}$$

$$\epsilon_{0|1}(\mathcal{T}_{op}) = \frac{1}{M}. \tag{3.65}$$

Which means that for the test satisfying the Holevo-Yuen-Kennedy-Lax conditions and using $\mu_0 = \mu_0^*$ we have:

$$\epsilon = \alpha_{\frac{1}{M}}(\mathcal{T}||\mathcal{D}(\mu_0)). \tag{3.66}$$

This means that the test $\mathcal{P} = \mathcal{P}^*$ attains the minimum probability of error. As we will see later, quantum quasi-perfect codes achieve this bound and thus are optimum.

4

Quantum perfect and quasi-perfect codes

This chapter presents the main results of this thesis, which can be found in [21] and [22]. It is organized as follows: Section 4.1 presents the problem of transmitting classical information over a classical-quantum channel, Section 4.2 introduces a definition of symmetric channels, Section 4.3 defines quasi-perfect codes for classical-quantum channels and Section 4.4 shows examples of quantum quasi-perfect codes.

4.1 Classical-quantum channels

We consider the channel coding problem of transmitting M equiprobable messages over a one-shot classical-quantum channel $x \to W_x$, with $x \in \mathcal{X}$ and $W_x \in \mathcal{D}(\mathcal{H})$. While the results from Section 3.4 were derived for discrimination among non-equiprobable alternatives, in the remainder of this work we consider the channel coding problem with equiprobable messages for clarity of exposition. A channel code is defined as a mapping from the message set $\{1, \ldots, M\}$ into a set of M codewords $\mathcal{C} = \{x_1, \ldots, x_M\}$. For a source message m, the decoder receives the associated density operator W_{x_m} and must decide on the transmitted message.

With some abuse of notation, for a fixed code, sometimes we shall write $W_m \triangleq W_{x_m}$. The minimum error probability for a code $\mathcal{C}$ is then given by

$$\mathsf{P}_{\mathrm{e}}(\mathcal{C}) \triangleq \min_{\{\Pi_1,\ldots,\Pi_M\}} \left\{ 1 - \frac{1}{M} \sum_{m=1}^{M} \operatorname{Tr}\big(W_m \Pi_m\big) \right\}. \tag{4.1}$$

This problem corresponds precisely to the M-ary quantum hypothesis testing problem described in Section 3.4. In contrast to the classical setting, in which (4.1) is minimized by the maximum likelihood decoder, the minimizer of (4.1) corresponds to any POVM satisfying

the optimality conditions from Lemma 3.1.

A direct application of (3.62) provides an alternative expression for $\mathsf{P}_{\mathrm{e}}(\mathcal{C})$. Let P denote a (classical) distribution over the input alphabet $\mathcal{X}$ and define

$$PW \triangleq \sum\nolimits_{x\in\mathcal{X}} P(x)\Big(|x\rangle\langle x| \otimes W_x\Big), \tag{4.2}$$

$$P \otimes \mu \triangleq \Big(\sum\nolimits_{x\in\mathcal{X}} P(x)\,|x\rangle\langle x|\Big) \otimes \mu. \tag{4.3}$$

We denote by $P_{\mathcal{C}}$ the input distribution induced by the codebook $\mathcal{C}$, hence $P_{\mathcal{C}}W = \frac{1}{M}\sum_{x\in\mathcal{C}}\big(|x\rangle\langle x|\otimes W_x\big)$ and $P_{\mathcal{C}} \otimes \mu = \big(\frac{1}{M}\sum_{x\in\mathcal{C}}|x\rangle\langle x|\big) \otimes \mu$. Using (3.62) we obtain the following result.

Theorem 4.1 (Classical-quantum meta-converse bound)**.** *Let $\mathcal{C}$ be any codebook of cardinality M for a channel $x \to W_x$, with $x \in \mathcal{X}$ and $W_x \in \mathcal{D}(\mathcal{H})$. Then,*

$$\mathsf{P}_e(\mathcal{C}) = \sup_{\mu}\Big\{\alpha_{\frac{1}{M}}\big(P_{\mathcal{C}}W \,\|\, P_{\mathcal{C}} \otimes \mu\big)\Big\} \tag{4.4}$$

$$\geq \inf_{P}\sup_{\mu}\Big\{\alpha_{\frac{1}{M}}\big(PW \,\|\, P \otimes \mu\big)\Big\}. \tag{4.5}$$

where the maximization is over auxiliary states $\mu \in \mathcal{D}(\mathcal{H})$, and the minimization is over (classical) input distributions P.

Proof: The identity (4.4) is a direct application of ((3.62)). The relaxation (4.5) follows by minimizing (4.4) over all input distributions, not necessarily induced by a codebook. ■

The right-hand-side of (4.4) coincides with the finite block-length converse bound by Matthews and Wehner [42, Eq. (45)], particularized for a classical-quantum channel with an input state induced by the codebook $\mathcal{C}$. The lower bound (4.5) corresponds to [42, Eq. (46)] specialized to the classical-quantum setting (see also [43, Sec. 4.6] for a direct derivation for classical quantum channels). The classical analogous of (4.5) is usually referred to as meta-converse bound, since several converse bounds in the literature can be derived from it. As it is the case in the classical-quantum setting, in the following we shall refer to this result as *meta-converse*.

Theorem 4.1 implies that the quantum generalization of the meta-converse bound proposed by Matthews and Wehner in [42, Eq. (45)] is tight for a fixed codebook $\mathcal{C}$. By fixing μ to be the state induced at the system output, the lower bound (4.5) recovers the converse bound [41, Th. 1], which is a rederivation of previous results in [44] (see [44, Remarks 10 and 15]). This bound is not tight in general since (i) the minimizing P does not need to coincide with the input state induced by the best codebook, and (ii) the choice of μ_0 in [41, Th. 1] does not maximize the resulting bound in general.

4.2 Symmetric channels

Definition 4.1. *We define a symmetric classical-quantum channel as a classical-quantum channel $x \to W_x$, with $x \in \mathcal{X}$ and $W_x \in \mathcal{D}(\mathcal{H})$ satisfying*

$$W_x = U_x \bar{W} U_x^\dagger, \tag{4.6}$$

for all $x \in \mathcal{X}$, where $\bar{W} \in \mathcal{D}(\mathcal{H})$ does not depend on x and U_x is a unitary linear operator that acts on $\mathcal{H}$ and is parametrized by x.

The definition of symmetric channels is the same as the definition of covariant channels, which can be found in the literature (see, e.g., [17] or [18, Sec. 9.7]). We define G as a compact group, $\mathcal{H}_A$ as the input Hilbert space and $\mathcal{H}_B$ as the output Hilbert space of a quantum channel $\mathcal{N} : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_B)$. The covariant channel is defined as the channel $\mathcal{N}_{A\to B}$ that satisfies $\mathcal{N}_{A\to B}(V_g \rho V_g^\dagger) = U_g \mathcal{N}_{A\to B}(\rho) U_g^\dagger$ for every input state $\rho \in \mathcal{D}(\mathcal{H}_A)$, where $g \to V_g$, $g \to U_g$, $g \in G$ are projective representations of G in the input and output Hilbert spaces of the channel respectively. For a classical-quantum channel $\mathcal{N}_{X\to B}$ with $\mathcal{N}_{X\to B} : x \to W_x$, $x \in \mathcal{X}$, $W_x \in \mathcal{D}(\mathcal{H}_B)$, we can define the orthogonal basis $|x\rangle\langle x|$. Then, for V_x such that $|x\rangle\langle x| = V_x|0\rangle\langle 0|V_x^\dagger$, it follows that $W_x = U_x \mathcal{N}_{X\to B}(|0\rangle\langle 0|) U_x^\dagger = U_x W_0 U_x^\dagger$. This means that any covariant quantum channel with classical (orthogonal) inputs also satisfies (4.6). This definition of symmetry is similar to the one considered in [19, 20] with the additional assumption $U_x = U^x$, $U^{|\mathcal{X}|} = \mathbb{1}$, for some unitary U. However, we do not impose any particular structure on the unitary representations U_x.

4.3 Quasi-perfect codes

For any operator $\mu \in \mathcal{D}(\mathcal{H})$, and parameter $t \in \mathbb{R}$ we define

$$\mathcal{E}_x(t, \mu) \triangleq \big\{ W_x - t\mu \geq 0 \big\}, \tag{4.7}$$

For a symmetric channel $x \to W_x = U_x \bar{W} U_x^\dagger$, $x \in \mathcal{X}$, we consider the set of auxiliary operators $\mu \in \mathcal{D}(\mathcal{H})$ such that they commute with the unitary transformations U_x, $x \in \mathcal{X}$. More precisely, for a symmetric channel $x \to W_x$, we define

$$\mathcal{U}_W \triangleq \big\{ \mu \in \mathcal{D}(\mathcal{H}) \mid U_x \mu = \mu U_x \big\}. \tag{4.8}$$

Then, for any symmetric channel $x \to W_x$, $x \in \mathcal{X}$, $W_x \in \mathcal{D}(\mathcal{H})$, and $\mu \in \mathcal{U}_W$, it follows that

$$\begin{aligned} \mathcal{E}_x(t, \mu) &= \big\{ U_x \bar{W} U_x^\dagger - t\mu \geq 0 \big\} && (4.9) \\ &= U_x \big\{ \bar{W} - t U_x^\dagger \mu U_x \geq 0 \big\} U_x^\dagger && (4.10) \\ &= U_x \bar{\mathcal{E}}(t, \mu) U_x^\dagger, && (4.11) \end{aligned}$$

where in the last step we used the fact that $\mu U_x = U_x \mu$ and defined $\bar{\mathcal{E}}(t, \mu) \triangleq \big\{ \bar{W} - t\mu \geq 0 \big\}$, which does not depend on $x \in \mathcal{X}$.

Similarly to (4.7), we define

$$\mathcal{E}_x^{\circ}(t,\mu) \triangleq \big\{W_x - t\mu = 0\big\}, \tag{4.12}$$
$$\mathcal{E}_x^{\bullet}(t,\mu) \triangleq \big\{W_x - t\mu > 0\big\}, \tag{4.13}$$

and

$$F_x^{\bullet}(t,\mu) \triangleq \mathrm{Tr}\big(W_x \mathcal{E}_x^{\bullet}(t,\mu)\big), \tag{4.14}$$
$$G_x^{\bullet}(t,\mu) \triangleq \mathrm{Tr}\big(\mu\, \mathcal{E}_x^{\bullet}(t,\mu)\big), \tag{4.15}$$

where, $F_{\bullet}(\cdot) \triangleq F_x^{\bullet}(\cdot)$, $G_{\bullet}(\cdot) \triangleq G_x^{\bullet}(\cdot)$, independent of $x \in \mathcal{X}$ for symmetric channels.

Definition 4.2. *A code $\mathcal{C}$ is perfect for a classical-quantum channel $x \to W_x$, if there exist a scalar t and a state $\mu \in \mathcal{D}(\mathcal{H})$ such that the projectors $\big\{\mathcal{E}_x(t,\mu)\big\}_{x\in\mathcal{C}}$ are orthogonal to each other and $\sum_{x\in\mathcal{C}} \mathcal{E}_x(t,\mu) = \mathbb{1}$. More generally, a code is quasi-perfect if there exist t and $\mu \in \mathcal{D}(\mathcal{H})$ such that the projectors $\big\{\mathcal{E}_x^{\bullet}(t,\mu)\big\}_{x\in\mathcal{C}}$ are orthogonal to each other, and for $I_{\bullet} \triangleq \sum_{x\in\mathcal{C}} \mathcal{E}_x^{\bullet}(t,\mu)$, $I_{\circ} \triangleq \mathbb{1} - I_{\bullet}$, it holds that $\sum_{x\in\mathcal{C}} \mathcal{E}_x^{\circ}(t,\mu) = cI_{\circ}$ where $c \in \mathbb{R}$, $c > 0$ is a normalizing constant that depends on the code $\mathcal{C}$.*

Example 1 (Classical 2-bit Binary Symmetric Channel): We consider the classical Binary Symmetric Channel from Section 3.3 in order to draw comparisons between classical and quantum quasi-perfect codes. We denote the BSC channel by $\mathcal{N}_{A\to B}(|\phi_x\rangle\langle\phi_x|)$, where $|\phi_x\rangle$ is a quantum state representing a classical state. We denote the probability of a bit-flip error as δ, and use the assumption that $(1-\delta) > \delta$. Let's consider the case of using two uses of the channel to transmit two possible quantum states, $|00\rangle\langle 00|$ and $|11\rangle\langle 11|$, corresponding to the input codewords (in bits) $'00'$ and $'11'$ respectively. The quantum channel states are then $W_{00} = \mathcal{N}_{A\to B}(|00\rangle\langle 00|)$ and $W_{11} = \mathcal{N}_{A\to B}(|11\rangle\langle 11|)$, or equivalently:

$$W_{00} = \begin{pmatrix} (1-\delta)^2 & 0 & 0 & 0 \\ 0 & \delta(1-\delta) & 0 & 0 \\ 0 & 0 & (1-\delta)\delta & 0 \\ 0 & 0 & 0 & \delta^2 \end{pmatrix}, \tag{4.16}$$

$$W_{11} = \begin{pmatrix} \delta^2 & 0 & 0 & 0 \\ 0 & (1-\delta)\delta & 0 & 0 \\ 0 & 0 & \delta(1-\delta) & 0 \\ 0 & 0 & 0 & (1-\delta)^2 \end{pmatrix}. \tag{4.17}$$

Let's take $\mu = \frac{1}{4}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$ and $t = 4\delta(1-\delta)$. Then we have that:

$$\mathcal{E}_{00} = \{W_{00} - t\mu \geq 0\} = \left\{ \begin{pmatrix} (1-\delta)^2 - \delta(1-\delta) & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta^2 - \delta(1-\delta) \end{pmatrix} \geq 0 \right\} = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&0\end{pmatrix}, \tag{4.18}$$

$$\mathcal{E}_{11} = \{W_{11} - t\mu \geq 0\} = \left\{ \begin{pmatrix} \delta^2 - \delta(1-\delta) & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & (1-\delta)^2 - \delta(1-\delta) \end{pmatrix} \geq 0 \right\} = \begin{pmatrix}0&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}. \tag{4.19}$$

Notice that this coincides with the classical regions $S_{00}(\tau, Q)$ and $S_{11}(\tau, Q)$ from Section 3.3. The classical interior and shell regions of S_x also coincide with $\mathcal{E}_x^\bullet$ and $\mathcal{E}_x^\circ, x \in \{00, 11\}$ respectively. We have that:

$$\mathcal{E}_{00}^\bullet = \{W_{00} - t\mu > 0\} = \begin{pmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}, \tag{4.20}$$

$$\mathcal{E}_{11}^\bullet = \{W_{11} - t\mu > 0\} = \begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&1\end{pmatrix}, \tag{4.21}$$

$$\mathcal{E}_{00}^\circ = \{W_{00} - t\mu = 0\} = \begin{pmatrix}0&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&0\end{pmatrix}, \tag{4.22}$$

$$\mathcal{E}_{11}^\circ = \{W_{11} - t\mu = 0\} = \begin{pmatrix}0&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&0\end{pmatrix}. \tag{4.23}$$

With this, we can check the orthogonality condition that the code must satisfy in order to be quasi-perfect:

$$\mathcal{E}_{00}^\bullet \mathcal{E}_{11}^\bullet = \begin{pmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&1\end{pmatrix} = 0. \tag{4.24}$$

We also see that the second condition is satisfied as well:

$$\mathcal{E}_{00}^{\circ} + \mathcal{E}_{11}^{\circ} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = cI_{\circ}, \tag{4.25}$$

where $I_{\circ} = \mathbb{1} - I_{\bullet} = \mathbb{1} - \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$. Notice that neither $\mathcal{E}_{00}, \mathcal{E}_{11}$ are orthogonal to each other, nor $\mathcal{E}_{00} + \mathcal{E}_{11}$ is the identity matrix, which means that the code is quasi-perfect but not perfect as in the classical case. We see that the example provided here and the one in Section 3.3 are completely equivalent.

Example 2 (Classical 3-bit Binary Symmetric Channel): Consider the 3-bit codebook from Section 3.3 used to transmit classical information through the classical BSC channel, consisting on the codewords $\{|000\rangle\langle 000|, |000\rangle\langle 111|\}$. The quantum states at the output of the channel are:

$$W_{000} = \begin{pmatrix} (1-\delta)^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & (1-\delta)^2\delta & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & (1-\delta)^2\delta & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & (1-\delta)\delta^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & (1-\delta)^2\delta & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & (1-\delta)\delta^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & (1-\delta)\delta^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \delta^3 \end{pmatrix}, \tag{4.26}$$

$$W_{111} = \begin{pmatrix} \delta^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & (1-\delta)\delta^2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & (1-\delta)\delta^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & (1-\delta)^2\delta & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & (1-\delta)\delta^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & (1-\delta)^2\delta & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & (1-\delta)^2\delta & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & (1-\delta)^3 \end{pmatrix}. \tag{4.27}$$

We use $t = 8\delta(1-\delta)^2$ and $\mu = \frac{1}{8}I_8$, where I_8 is the identity matrix of dimension 8. Then

$\mathcal{E}_{000}$ is:

$$\mathcal{E}_{000} = \{W_{000} - t\mu \geq 0\}$$
$$= \left\{ \begin{pmatrix} (1-\delta)^3 - \delta(1-\delta)^2 & 0\,0 & 0 & 0 & 0 & 0 & 0 \\ 0\,0 & 0\,0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0\,0 & 0 & 0 & 0 & 0 & 0 \\ 0\,0 & 0\,0 & (1-\delta)\delta^2 - \delta(1-\delta)^2 & 0 & 0 & 0 & 0 \\ 0 & 0\,0 & 0 & 0 & 0 & 0 & 0 \\ 0\,0 & 0\,0 & 0 & (1-\delta)\delta^2 - \delta(1-\delta)^2 & 0 & 0 & 0 \\ 0 & 0\,0 & 0 & 0 & (1-\delta)\delta^2 - \delta(1-\delta)^2 & 0 & 0 \\ 0 & 0\,0 & 0 & 0 & 0 & 0 & \delta^3 - \delta(1-\delta)^2 \end{pmatrix} \geq 0 \right\}$$
$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{4.28}$$

Similarly, $\mathcal{E}_{111}$ is:

$$\mathcal{E}_{111} = \{W_{111} - t\mu \geq 0\} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{4.29}$$

Notice that $\mathcal{E}_{000}$ and $\mathcal{E}_{111}$ coincide with the regions $S_{000}(\tau, Q)$ and $S_{111}(\tau, Q)$ from the 3-bit classical example for the BSC channel of Section 3.3. Also, we can see that the code is perfect, since $\mathcal{E}_{000}$ and $\mathcal{E}_{111}$ are orthogonal to each other and $\mathcal{E}_{000} + \mathcal{E}_{111} = \mathbb{1}$.

Example 3 (Pure State Channel): We consider the channel $x \to W_x = |\varphi_x\rangle\langle\varphi_x|$, with classical input x and a quantum pure-state output $|\varphi_x\rangle\langle\varphi_x|$ on a n-dimensional Hilbert space $\mathcal{H}$. Any pure-state W_x can be constructed via unitary transformations from an arbitrary pure-state $\bar{W} = |\psi\rangle\langle\psi|$, which means that the pure-state channel is symmetric according to definition 4.1. If there are no further restrictions on the output of the system (that is, it can be an arbitrary pure state $W_x = U_x \bar{W} U_x^\dagger$), then the auxiliary state μ which commutes with all unitary linear operator U_x, $x \in \mathcal{X}$, is the normalized identity matrix (or equivalently the maximally mixed state), $\mu = \frac{1}{n}\mathbb{1}$. According to Definition 4.2, a code $\mathcal{C}$ with $M = n$ orthogonal pure states is perfect for this channel with parameters $t = n$ and $\mu = \frac{1}{n}\mathbb{1}$, since the projectors $\mathcal{E}_x\big(n, \frac{1}{n}\mathbb{1}\big) = \big\{|\varphi_x\rangle\langle\varphi_x| - \mathbb{1} \geq 0\big\} = |\varphi_x\rangle\langle\varphi_x|$ are orthogonal for $x \in \mathcal{C}$, and they form a basis for $\mathcal{H}$. Note that this particular case can be reduced to a classical problem, since the channel outputs commute with each other. Similarly, a code with $M \geq n$ is quasi-perfect for this channel with parameters $t = n$ and $\mu = \frac{1}{n}\mathbb{1}$ provided that $\sum_{x\in\mathcal{C}} |\varphi_x\rangle\langle\varphi_x| = c\mathbb{1}$ with

$c = \frac{M}{n}$. A family of codes fulfilling this properties will be studied in detail in Section 4.4.1. For these quasi-perfect codes, the interiors $\mathcal{E}_x^\bullet\big(n, \frac{1}{n}\mathbb{1}\big) = \big\{|\varphi_x\rangle\langle\varphi_x| - \mathbb{1} > 0\big\} = 0$, hence they are orthogonal to each other, and the channel outputs don't commute with each other. For $M < n$, the codes for this channel and the auxiliary state $\mu = \frac{1}{n}\mathbb{1}$ are neither perfect nor quasi-perfect.

The next result provides an alternative expression for the error probability of perfect and quasi-perfect codes.

Theorem 4.2 (Error probability of quasi-perfect codes). *Let the channel $x \to W_x$, $x \in \mathcal{X}$, $W_x \in \mathcal{D}(\mathcal{H})$, and $\mu \in \mathcal{U}_W$ be symmetric, and let $\mathcal{C}$ be perfect or quasi-perfect with parameters t and μ. Then,*

$$P_e(\mathcal{C}) = 1 - F_\bullet(t, \mu) + t\big(G_\bullet(t, \mu) - |\mathcal{C}|^{-1}\big), \tag{4.30}$$

where $|\mathcal{C}|$ denotes the cardinality of the codebook $\mathcal{C}$.

Proof: Let $\mathcal{C} = \{x_1, \ldots, x_M\}$ be an arbitrary code for the (symmetric) channel $x \to W_x$. To avoid ambiguities, we shall denote by $\bar{t}$ the smallest value of t such that the projectors $\big\{\mathcal{E}_x^\bullet(t, \mu)\big\}_{x\in\mathcal{C}}$ are orthogonal to each other for a certain code $\mathcal{C}$. We shall refer to $\bar{t}$ as the *packing radius* of the code $\mathcal{C}$ with respect to state μ.

We define the orthogonal basis $\{\bar{E}(i)\}$ associated to the eigenspace of $\big\{\bar{W} - \bar{t}\mu \geq 0\big\}$ such that

$$\bar{\mathcal{E}}^\bullet(\bar{t}, \mu) = \sum_{i\in\mathcal{I}^\bullet} \bar{E}(i), \tag{4.31}$$

$$\mathcal{E}_x^\bullet(\bar{t}, \mu) = U_x\bar{\mathcal{E}}^\bullet(\bar{t}, \mu)U_x^\dagger = \sum_{i\in\mathcal{I}^\bullet} U_x\bar{E}(i)U_x^\dagger = \sum_{i\in\mathcal{I}^\bullet} E_x(i), \tag{4.32}$$

where we let $E_x(i) \triangleq U_x\bar{E}(i)U_x^\dagger$. Here, $\mathcal{I}^\bullet$ denotes the set of basis indexes associated to the strictly positive eigenvalues. Note that the projectors $E_x(i)$ are orthogonal to $E_{x'}(i)$ for $x \neq x'$, $i \in \mathcal{I}^\bullet$ since the projectors $\{\mathcal{E}_x^\bullet(\bar{t}, \mu)\}$ for $x \in \mathcal{C}$ are orthogonal to each other. Similarly, we also write

$$\bar{\mathcal{E}}^\circ(\bar{t}, \mu) = \sum_{i\in\mathcal{I}^\circ} \bar{E}(i), \tag{4.33}$$

$$\mathcal{E}_x^\circ(\bar{t}, \mu) = U_x\bar{\mathcal{E}}^\circ(\bar{t}, \mu)U_x^\dagger = \sum_{i\in\mathcal{I}^\circ} U_x\bar{E}(i)U_x^\dagger = \sum_{i\in\mathcal{I}^\circ} E_x(i). \tag{4.34}$$

where $\mathcal{I}^\circ$ denotes the set of basis indexes associated to the zero eigenvalues. In this later case however, there is no orthogonality condition between the projectors $E_x(i)$ for $i \in \mathcal{I}^\circ$ for different codewords $x \in \mathcal{C}$. Now define $d_\bullet \triangleq M|\mathcal{I}^\bullet|$ and $d_\circ \triangleq n - d_\bullet$, where $n = \dim(\mathcal{H})$. The code specific constant associated with a quasi-perfect code $\mathcal{C}$ is $c \triangleq \frac{M|\mathcal{I}^\circ|}{d_\circ}$.

We consider the decoder $\mathcal{T} = \{\Pi_1, \ldots, \Pi_M\}$ with projectors

$$\Pi_m = \mathcal{E}^{\bullet}_{x_m}(\bar{t},\mu) + \frac{1}{c}\mathcal{E}^{\circ}_{x_m}(\bar{t},\mu) \tag{4.35}$$

$$= U_{x_m}\bar{\mathcal{E}}^{\bullet}(\bar{t},\mu)U^{\dagger}_{x_m} + \frac{1}{c}U_{x_m}\bar{\mathcal{E}}^{\circ}(\bar{t},\mu)U^{\dagger}_{x_m} \tag{4.36}$$

$$= U_{x_m}\bar{\Pi}U^{\dagger}_{x_m}, \quad m = 1,\dots,M, \tag{4.37}$$

where

$$\bar{\Pi} = \bar{\mathcal{E}}^{\bullet}(\bar{t},\mu) + \frac{1}{c}\bar{\mathcal{E}}^{\circ}(\bar{t},\mu). \tag{4.38}$$

Note that this definition implies

$$\sum_{m=1}^{M}\Pi_m = I_{\bullet} + I_{\circ} = \mathbb{1}, \tag{4.39}$$

as required.

We next show that this decoder satisfies the Holevo-Yuen-Kennedy-Lax conditions from Lemma 3.1 and therefore it minimizes the probability of error. To this end, we write

$$\Lambda(\mathcal{T}) = \frac{1}{M}\sum_{\ell=1}^{M} W_\ell\Pi_\ell \tag{4.40}$$

$$= \frac{1}{M}\sum_{\ell=1}^{M} U_l\bar{W}\bar{\Pi}U_l^{\dagger} \tag{4.41}$$

$$= \frac{1}{M}\sum_{\ell=1}^{M} U_l\bar{W}\bar{\mathcal{E}}^{\bullet}(\bar{t},\mu)U_l^{\dagger} + \frac{1}{Mc}\sum_{\ell=1}^{M} U_l\bar{W}\bar{\mathcal{E}}^{\circ}(\bar{t},\mu)U_l^{\dagger}. \tag{4.42}$$

Then, it follows that

$$\left(\Lambda(\mathcal{T}) - \frac{1}{M}W_m\right)\Pi_m = \left(\frac{1}{M}\sum_{\ell\neq m}^{M} W_\ell\Pi_\ell\right)\Pi_m + \frac{1}{M}W_m\Pi_m(\Pi_m - I) \tag{4.43}$$

$$= \left(\frac{1}{M}\sum_{\ell\neq m}^{M} W_\ell\Pi_\ell\right)\Pi_m + \frac{1}{Mc}\left(\frac{1}{c}-1\right)W_m\mathcal{E}^{\circ}_m(\bar{t},\mu) \tag{4.44}$$

$$= \left(\frac{1}{M}\sum_{\ell\neq m}^{M} W_\ell\Pi_\ell\right)\Pi_m + \frac{1}{Mc}\left(\frac{1}{c}-1\right)\bar{t}\mu\mathcal{E}^{\circ}_m(\bar{t},\mu). \tag{4.45}$$

We consider the first term in (4.45) only. This term can be decomposed as

$$\left(\frac{1}{M}\sum_{\ell\neq m}^{M} W_\ell \Pi_\ell\right)\Pi_m = \frac{1}{M}\left(\sum_{\ell\neq m}^{M} W_\ell \mathcal{E}_\ell^\bullet(\bar{t},\mu) + \frac{1}{c}\sum_{\ell\neq m}^{M} W_\ell \mathcal{E}_\ell^\circ(\bar{t},\mu)\right)\left(\mathcal{E}_m^\bullet(\bar{t},\mu) + \frac{1}{c}\mathcal{E}_m^\circ(\bar{t},\mu)\right) \tag{4.46}$$

$$= \frac{1}{M}\left(\sum_{\ell\neq m}^{M} W_\ell \mathcal{E}_\ell^\bullet(\bar{t},\mu) + \frac{1}{c}\bar{t}\mu\sum_{\ell\neq m}^{M} \mathcal{E}_\ell^\circ(\bar{t},\mu)\right)\left(\mathcal{E}_m^\bullet(\bar{t},\mu) + \frac{1}{c}\mathcal{E}_m^\circ(\bar{t},\mu)\right) \tag{4.47}$$

$$= \frac{1}{M}\left(\sum_{\ell\neq m}^{M} W_\ell \mathcal{E}_\ell^\bullet(\bar{t},\mu) + \bar{t}\mu I_\circ - \frac{1}{c}\bar{t}\mu\mathcal{E}_m^\circ(\bar{t},\mu)\right)\frac{1}{c}\mathcal{E}_m^\circ(\bar{t},\mu) \tag{4.48}$$

$$= \frac{1}{Mc}\left(\sum_{\ell\neq m}^{M} W_\ell \mathcal{E}_\ell^\bullet(\bar{t},\mu)\mathcal{E}_m^\circ(\bar{t},\mu) + \left(1-\frac{1}{c}\right)\bar{t}\mu\mathcal{E}_m^\circ(\bar{t},\mu)\right) \tag{4.49}$$

$$= \frac{1}{Mc}\left(\sum_{\ell\neq m}^{M} W_\ell \mathcal{E}_\ell^\bullet(\bar{t},\mu) I_\circ \mathcal{E}_m^\circ(\bar{t},\mu) + \left(1-\frac{1}{c}\right)\bar{t}\mu\mathcal{E}_m^\circ(\bar{t},\mu)\right) \tag{4.50}$$

$$= \frac{1}{Mc}\left(1-\frac{1}{c}\right)\bar{t}\mu\mathcal{E}_m^\circ(\bar{t},\mu). \tag{4.51}$$

Here, the first equality follows by noting that $W_\ell\mathcal{E}_\ell^\circ(\bar{t},\mu) = \bar{t}\mu\mathcal{E}_\ell^\circ(\bar{t},\mu)$ since $\mathcal{E}_\ell^\circ(\bar{t},\mu)$ is the projector associated to the nullspace of $W_\ell - \bar{t}\mu$. Combining (4.51) with (4.45) we prove that $\left(\Lambda(\mathcal{T}) - \frac{1}{M}W_m\right)\Pi_m = 0$. Following analogous steps we show that $\Pi_m\left(\Lambda(\mathcal{T}) - \frac{1}{M}W_m\right) = 0$ and hence the decoder satisfies the optimality condition (3.55).

On the other hand,

$$\Lambda(\mathcal{T}) - \frac{1}{M}W_m = \frac{1}{M}\left(\sum_{\ell\neq m}^{M} W_\ell \mathcal{E}_\ell^\bullet(\bar{t},\mu) + \frac{1}{c}\bar{t}\mu\sum_{\ell\neq m}^{M} \mathcal{E}_\ell^\circ(\bar{t},\mu)\right) + \frac{1}{M}W_m(\Pi_m - I). \tag{4.52}$$

Considering only the second term, we obtain

$$\frac{1}{M}W_m(\Pi_m - I) = \frac{1}{M}W_m\mathcal{E}_m^\bullet(\bar{t},\mu) + \frac{1}{M}W_m\frac{1}{c}\mathcal{E}_m^\circ(\bar{t},\mu) - \frac{1}{M}W_m \tag{4.53}$$

$$= \frac{1}{M}\bar{t}\mu\frac{1}{c}\mathcal{E}_m^\circ(\bar{t},\mu) - \frac{1}{M}W_m I_\circ - \frac{1}{M}W_m\sum_{\ell\neq m}\mathcal{E}_\ell^\bullet(\bar{t},\mu), \tag{4.54}$$

where in (4.54) we used that $W_m = W_m I_\bullet + W_m I_\circ$ and that $\sum_\ell \mathcal{E}_\ell^\bullet(\bar{t},\mu) = I_\bullet$. Continuing from (4.52):

$$\frac{1}{M}\left(\sum_{\ell\neq m}^{M} W_\ell \mathcal{E}_\ell^\bullet(\bar{t},\mu) + \frac{1}{c}\bar{t}\mu\sum_{\ell=1}^{M} \mathcal{E}_\ell^\circ(\bar{t},\mu)\right) - \frac{1}{M}W_m I_\circ - \frac{1}{M}W_m\sum_{\ell\neq m}\mathcal{E}_\ell^\bullet(\bar{t},\mu) \tag{4.55}$$

$$= \frac{1}{M}\sum_{\ell\neq m}^{M} W_\ell \mathcal{E}_\ell^\bullet(\bar{t},\mu) - \frac{1}{M}W_m\sum_{\ell\neq m}\mathcal{E}_\ell^\bullet(\bar{t},\mu) + \frac{1}{M}\bar{t}\mu I_\circ - \frac{1}{M}W_m I_\circ. \tag{4.56}$$

The eigenvectors of $W_m - \bar{t}\mu$ corresponding to positive eigenvalues belong to the subspace spanned by $I_\bullet$. This means that $I_\circ(\frac{1}{M}W_m - \frac{1}{M}\bar{t}\mu) \leq 0$, and so $\frac{1}{M}\bar{t}\mu I_\circ - \frac{1}{M}W_m I_\circ \geq 0$. On the other hand we have that:

$$\frac{1}{M}\sum_{\ell\neq m}^{M} W_\ell \mathcal{E}_\ell^\bullet(\bar{t},\mu) - \frac{1}{M}W_m \sum_{\ell\neq m} \mathcal{E}_\ell^\bullet(\bar{t},\mu) = \frac{1}{M}\sum_{\ell\neq m}^{M}(W_\ell - W_m)\mathcal{E}_\ell^\bullet(\bar{t},\mu) \tag{4.57}$$

$$> \frac{1}{M}\sum_{\ell\neq m}^{M}(\bar{t}\mu - W_m)\mathcal{E}_\ell^\bullet(\bar{t},\mu) \tag{4.58}$$

$$> \frac{1}{M}\sum_{\ell\neq m}^{M}(\bar{t}\mu - \bar{t}\mu)\mathcal{E}_\ell^\bullet(\bar{t},\mu) = 0. \tag{4.59}$$

where in (4.58) we used $W_\ell \mathcal{E}_\ell^\bullet(\bar{t},\mu) > \bar{t}\mu\mathcal{E}_\ell^\bullet(\bar{t},\mu)$, and (4.59) follows since $W_m\mathcal{E}_{\ell\neq m}^\bullet(\bar{t},\mu) < \bar{t}\mu\mathcal{E}_{\ell\neq m}^\bullet(\bar{t},\mu)$ which holds since $\mathcal{E}_{\ell\neq m}^\bullet(\bar{t},\mu)$ and $\mathcal{E}_m^\bullet(\bar{t},\mu)$ being orthogonal implies that $\mathcal{E}_{\ell\neq m}^\bullet(\bar{t},\mu)$ must belong to the negative eigenspace of $W_m - \bar{t}\mu$. We conclude that $\Lambda(\mathcal{T}) - \frac{1}{M}W_m \geq 0$.

As the decoder $\mathcal{T} = \{\Pi_1, \ldots, \Pi_M\}$ satisfies the optimality conditions from Lemma 3.1, it minimizes (4.1). Then, combining (3.57), (4.1), and (4.14) we obtain that the error probability of this code can be rewritten as

$$\mathsf{P}_{\mathrm{e}}(\mathcal{C}) = 1 - \mathrm{Tr}\big(\Lambda(\mathcal{T}^\star)\big) = 1 - \mathrm{Tr}\left(\frac{1}{M}\sum_{m=1}^{M} W_m\mathcal{E}_m^\bullet(\bar{t},\mu) + \frac{1}{Mc}\sum_{m=1}^{M} W_m\mathcal{E}_m^\circ(\bar{t},\mu)\right) \tag{4.60}$$

$$= 1 - \frac{1}{M}\sum_{m=1}^{M} F_{x_m}^\bullet(\bar{t},\mu) - \frac{1}{Mc}\,\mathrm{Tr}\left(\sum_{m=1}^{M}\bar{t}\mu\mathcal{E}_m^\circ(\bar{t},\mu)\right) \tag{4.61}$$

$$= 1 - \frac{1}{M}\sum_{m=1}^{M} F_{x_m}^\bullet(\bar{t},\mu) - \frac{\bar{t}}{M}\,\mathrm{Tr}\big(\mu I_\circ\big). \tag{4.62}$$

Now, noting that $\mu = \mu(I_\circ + I_\bullet)$ we obtain

$$\mathrm{Tr}\big(\mu I_\circ\big) = 1 - \mathrm{Tr}\left(\mu\sum_{m=1}^{M}\mathcal{E}_m^\bullet(\bar{t},\mu)\right) = 1 - \sum_{m=1}^{M} G_{x_m}^\bullet(\bar{t},\mu), \tag{4.63}$$

where the second equality follows from (4.15). Then, substituting (4.63) in (4.62), and using the fact that $F_\bullet(\bar{t},\mu) = F_x^\bullet(\bar{t},\mu)$ and $G_\bullet(\bar{t},\mu) = G_x^\bullet(\bar{t},\mu)$ for symmetric channels, and $M = |\mathcal{C}|$, we obtain

$$\mathsf{P}_{\mathrm{e}}(\mathcal{C}) = 1 - F_\bullet(\bar{t},\mu) + \bar{t}(G_\bullet(\bar{t},\mu) - |\mathcal{C}|^{-1}). \tag{4.64}$$

■

Theorem 4.3 (Quasi-perfect codes attain the meta-converse)**.** *Let the channel $x \to W_x$ be symmetric and let $\mathcal{C}$ be perfect or quasi-perfect with parameters t and $\mu \in \mathcal{U}_W$. Then, for $M = |\mathcal{C}|$,*

$$P_e(\mathcal{C}) = \inf_{P}\sup_{\mu'} \alpha_{\frac{1}{M}}\big(PW \,\|\, P\otimes\mu'\big). \tag{4.65}$$

Proof: The proof is provided in Appendix 4.C. ■

Remark 4.1. *A special channel to consider is the erasure channel, that takes a quantum state on Hilbert space $\mathcal{H}_A$ and outputs a quantum state on Hilbert space $\mathcal{H}_B$, where systems A and B have dimensions d_A and d_B respectively. The erasure channel is defined by:*

$$\mathcal{N}^E_{A\to B}(\rho_x) = (1-\epsilon)\mathcal{I}_{A\to B}(\rho_x) + \epsilon|e\rangle\langle e|_B, \tag{4.66}$$

where ρ_x is the input quantum state and the Isometric channel $\mathcal{I}_{A\to B}(\rho_M) = I_{A\to B}\rho_M I^\dagger_{A\to B}$ is defined using the isometry

$$I_{A\to B} = \begin{bmatrix} & \mathbb{1}_M & \\ 0 & \dots & 0 \end{bmatrix} \tag{4.67}$$

as unique Kraus operator and where $\{|0\rangle,\dots,|M-1\rangle,|e\rangle\}$ form an orthonormal basis on $\mathcal{H}_B$. In this case we express the output state $W_x = \mathcal{N}^E_{A\to B}(\rho_x)$ as $W_x = W_x I_{A\to B} I^\dagger_{A\to B} + W_x|e\rangle\langle e|_B = W_x I_{A\to B} I^\dagger_{A\to B} + \epsilon|e\rangle\langle e|_B$. The eigenspace of $\{W_x - \bar{t}\mu = 0\}$ consist of the eigenspace of $\{\mathcal{I}_{A\to B}(\rho_M) - \bar{t}\mu = 0\}$ plus the eigenvector $|e\rangle\langle e|_B$. Equivalently, we can express $\mathcal{E}^\circ_x(\bar{t},\mu)$ as $\mathcal{E}^\circ_x(\bar{t},\mu) = \sum_{i\in\mathcal{I}^\circ} E_x(i) = \mathcal{E}'^\circ_x(\bar{t},\mu) + |e\rangle\langle e|_B$, where $\mathcal{E}'^\circ_x(\bar{t},\mu)$ is the eigenspace of $\{\mathcal{I}_{A\to B}(\rho_M) - \bar{t}\mu = 0\}$ and $|e\rangle\langle e|_B$ does not depend on x (i.e. all codewords share the same eigenvector $|e\rangle\langle e|_B$). The input state has no effect on the term $\epsilon|e\rangle\langle e|_B$, so for this case we introduce the following generalized definition of quasi-perfect codes which can accommodate the different input and output dimensions of the erasure channel:

Definition 4.3. *A code $\mathcal{C}$ is generalized quasi-perfect if there exists t and $\mu \in \mathcal{D}(\mathcal{H})$ such that the projectors $\{\mathcal{E}^\bullet_x(t,\mu)\}_{x\in\mathcal{C}}$ are orthogonal to each other, fulfilling $\sum_{x\in\mathcal{C}} \mathcal{E}^\bullet_x(t,\mu) = I_\bullet$. Moreover we also require that $\sum_{x\in\mathcal{C}} \mathcal{E}'^\circ_x(\bar{t},\mu) = C_{\mathcal{C}} I_{\circ A}$, where $I_{\circ A} = I_{A\to B} I^\dagger_{A\to B} - I_\bullet$, $\mathcal{E}'^\circ_x(\bar{t},\mu) = \mathcal{E}^\circ_x(\bar{t},\mu) - |e\rangle\langle e|_B$ and $C_{\mathcal{C}} \in \mathbb{R}$, $C_{\mathcal{C}} > 0$ is a normalizing constant that depends on the code $\mathcal{C}$.*

The following lemma shows that generalized quasi-perfect codes are optimum among all codes of the same blocklength and cardinality:

Theorem 4.4 (Generalized quasi-perfect codes attain the meta-converse bound)**.** *Let the channel $x \to W_x$ be symmetric and let $\mathcal{C}$ be generalized quasi-perfect with parameters t and $\mu \in \mathcal{U}_W$. Then, for $M = |\mathcal{C}|$,*

$$P_e(\mathcal{C}) = \inf_P \sup_{\mu'} \alpha_{\frac{1}{M}}\big(PW \,\|\, P\otimes\mu'\big). \tag{4.68}$$

Proof. We define the POVM as follows:

$$\bar{\Pi} = \bar{\mathcal{E}}^\bullet(\bar{t},\mu) + \frac{1}{C_{\mathcal{C}}}\bar{\mathcal{E}}'^\circ(\bar{t},\mu) + \frac{1}{M}|e\rangle\langle e|_B, \tag{4.69}$$

where $\bar{\mathcal{E}}'^{\circ}(\bar{t},\mu) = \bar{\mathcal{E}}^{\circ}(\bar{t},\mu) - |e\rangle\langle e|_B$. Following similar steps as in the proof of Theorem 4.2, it is possible to show that the optimality conditions from Lemma 3.1 are satisfied. We have:

$$\begin{aligned}\Lambda(\mathcal{T}) &= \frac{1}{M}\sum_{\ell=1}^{M} U_l \bar{W} \bar{\mathcal{E}}^{\bullet} U_l^{\dagger} + \frac{1}{MC_{\mathcal{C}}}\sum_{\ell=1}^{M} U_l \bar{W} \bar{\mathcal{E}}'^{\circ}(\bar{t},\mu) U_l^{\dagger} \\ &\quad + \frac{1}{M} W|e\rangle\langle e|_B = \Lambda(\mathcal{T})' + \frac{1}{M} W|e\rangle\langle e|_B, \end{aligned} \tag{4.70}$$

and so:

$$\begin{aligned}&\left(\Lambda(\mathcal{T}) - \frac{1}{M} W_m\right)\Pi_m \\ &= \left(\Lambda(\mathcal{T})' - \frac{1}{M} W_m I_{A\to B} I_{A\to B}^{\dagger}\right)\Pi_m \\ &\qquad + \left(\frac{1}{M} W|e\rangle\langle e|_B - \frac{1}{M} W|e\rangle\langle e|_B\right)\Pi_m = 0, \end{aligned} \tag{4.71}$$

where we used that $\left(\Lambda(\mathcal{T})' - \frac{1}{M} W_m I_{A\to B} I_{A\to B}^{\dagger}\right)\Pi_m = 0$ as shown in the proof of Theorem 4.2. Similarly $\Pi_m\left(\Lambda(\mathcal{T}) - \frac{1}{M} W_m\right) = 0$, showing that (3.55) holds. Also, $\Lambda(\mathcal{T}) - \frac{1}{M} W_m$ is semidefinite positive because $\Lambda(\mathcal{T}) - \frac{1}{M} W_m$
$= \Lambda(\mathcal{T})' - \frac{1}{M} W_m I_{A\to B} I_{A\to B}^{\dagger} + \frac{1}{M} W|e\rangle\langle e|_B - \frac{1}{M} W|e\rangle\langle e|_B = \Lambda(\mathcal{T})' - \frac{1}{M} W_m I_{A\to B} I_{A\to B}^{\dagger}$. We conclude that the conditions from Lemma 3.1 are also satisfied in this case. The rest of the proof follows the same steps as in Theorem 4.2 and Theorem 4.3. □

4.4 Examples of quantum quasi-perfect codes

4.4.1 Pure 2-qubit classical-quantum channel (Bell codes)

We consider an arbitrary 2-qubit pure-state classical-quantum channel given by

$$x \to W_x = |\varphi_x\rangle\langle\varphi_x|. \tag{4.72}$$

We define the codebook $\mathcal{C} = \{x_1, \ldots, x_M\}$, with even cardinality $M = 2K \geq 4$, such that the output of the channel of the m-th codeword is $W_m = |\varphi_{x_m}\rangle\langle\varphi_{x_m}|$ with

$$|\varphi_{x_m}\rangle = \begin{cases} \frac{1}{\sqrt{2}}\left(|00\rangle + e^{j\phi_k}|11\rangle\right), & m = 1 + 2k, \\ \frac{1}{\sqrt{2}}\left(|01\rangle + e^{j\phi_k}|10\rangle\right), & m = 2 + 2k, \end{cases} \tag{4.73}$$

where $\phi_k = 2\pi k/K$, for $k = 0 \ldots K-1$.

This code is a generalization of the Bell states that we refer to as Bell code. The channel output for codeword x_m is thus given by the pure state $W_{x_m} = W_m$ which is defined as $W_m = |\varphi_{x_m}\rangle\langle\varphi_{x_m}|$. For example, if $M = 4$, we have that $K = 2$ and $\varphi_0 = 0$, $\varphi_1 = \pi$,

obtaining the following:

$$|\varphi_{x_1}\rangle \equiv \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big), \tag{4.74}$$

$$|\varphi_{x_2}\rangle \equiv \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big), \tag{4.75}$$

$$|\varphi_{x_3}\rangle \equiv \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big), \tag{4.76}$$

$$|\varphi_{x_4}\rangle \equiv \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big), \tag{4.77}$$

which are the Bell states. Similarly, for $M = 8$, we have $K = 4$, $\varphi_0 = 0$, $\varphi_1 = \frac{\pi}{2}$, $\varphi_2 = \pi$, $\varphi_3 = \frac{3\pi}{2}$ and:

$$|\varphi_{x_1}\rangle \equiv \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big), \tag{4.78}$$

$$|\varphi_{x_2}\rangle \equiv \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big), \tag{4.79}$$

$$|\varphi_{x_3}\rangle \equiv \frac{1}{\sqrt{2}}\big(|00\rangle + j\,|11\rangle\big), \tag{4.80}$$

$$|\varphi_{x_4}\rangle \equiv \frac{1}{\sqrt{2}}\big(|01\rangle + j\,|10\rangle\big), \tag{4.81}$$

$$|\varphi_{x_5}\rangle \equiv \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big), \tag{4.82}$$

$$|\varphi_{x_6}\rangle \equiv \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big), \tag{4.83}$$

$$|\varphi_{x_7}\rangle \equiv \frac{1}{\sqrt{2}}\big(|00\rangle - j\,|11\rangle\big), \tag{4.84}$$

$$|\varphi_{x_8}\rangle \equiv \frac{1}{\sqrt{2}}\big(|01\rangle - j\,|10\rangle\big), \tag{4.85}$$

which are phase-modulated states that are built from the Bell states. As we show next, this codebook constitutes a quasi-perfect code.

Proposition 4.1. *The 2-qubit classical-quantum channel $W_x = |\varphi_x\rangle\langle\varphi_x|$ is symmetric and the Bell code $\mathcal{C}$ is quasi-perfect for this channel. Moreover,*

$$P_e(\mathcal{C}) = \alpha_{\frac{1}{M}}\big(W_x \,\|\, \mu_0\big) = 1 - \frac{4}{M}. \tag{4.86}$$

Proof: We have that $\sum_{x\in\mathcal{C}} |\varphi_x\rangle\langle\varphi_x| = \frac{M}{4}\mathbb{1}_4$, which means that the code is quasi-perfect as mentioned in Example 3 in Section 4.3. From Example 3, we have $t = n = 4$, $\mu = \frac{1}{4}\mathbb{1}$ and $\mathcal{E}_x^{\bullet}\big(n, \frac{1}{n}\mathbb{1}\big) = 0$, which means that $F_{\bullet}(\cdot) = G_{\bullet}(\cdot) = 0$. Using (4.64), we obtain that $\mathsf{P}_{\mathrm{e}}(\mathcal{C}) = 1 - t\frac{1}{M} = 1 - \frac{4}{M}$. ∎

4.4.2 Example: pure 2-qubit classical-quantum channel followed by a quantum erasure channel

Consider a classical-quantum channel followed by the quantum erasure channel:

$$\mathcal{N}_{A\to B}(\rho_A) = (1-\epsilon)\mathcal{I}_{A\to B}(\rho_A) + \epsilon|e\rangle\langle e|_B,$$

where the Isometric channel $\mathcal{I}_{A\to B}(\rho_A) = I_{A\to B}\rho_A I_{A\to B}^\dagger$ is defined using the isometry $I_{A\to B}$ from (4.67), particularized for $d_A = 4$, $d_B = 5$. The channel is then defined by $W_x = \mathcal{N}_{A\to B}(|\varphi_x\rangle\langle\varphi_x|_A)$.

For $M = 2K > 3$, we use the Bell codebook $\mathcal{C} = \{x_1, \ldots, x_M\}$ of Section 4.4.1. The channel output for codeword x_m is thus given by the state $W_{x_m} = W_m$ which is defined as $W_m = \mathcal{N}_{A\to B}\big(|\varphi_{x_m}\rangle\langle\varphi_{x_m}|_A\big)$.

Proposition 4.2. *The 2-quit classical-quantum erasure channel is symmetric and the Bell code $\mathcal{C}$ is generalized quasi-perfect for this channel. Moreover,*

$$P_e(\mathcal{C}) = \alpha_{\frac{1}{M}}\big(W_x \,\|\, \mu_0\big) = 1 - \frac{4-3\epsilon}{M}. \tag{4.87}$$

Proof: The proof is provided in Appendix 4.A. ∎

4.4.3 Example: pure 2-qubit classical-quantum channel followed by a quantum depolarizing channel

Consider a classical-quantum channel followed by the depolarizing channel:

$$\mathcal{N}_{A\to B}(\rho_A) = p\frac{1}{4}\mathbb{1}_4 + (1-p)\rho_A.$$

Consider the Bell codes defined in the previous cases. The channel output for codeword x_m is thus given by the state $W_{x_m} = W_m$ which is defined as $W_m = \mathcal{N}_{A\to B}\big(|\varphi_{x_m}\rangle\langle\varphi_{x_m}|_A\big)$.

Proposition 4.3. *The 2-qubit classical-quantum depolarizing channel is symmetric and the Bell code $\mathcal{C}$ is quasi-perfect for this channel. Moreover,*

$$P_e(\mathcal{C}) = \alpha_{\frac{1}{M}}\big(W_x \,\|\, \mu_0\big) = 1 - \frac{1}{M}(4-3p). \tag{4.88}$$

Proof: The proof is provided in the Appendix 4.B. ∎

4.4.4 Extension to N-qubit classical-quantum channels

This section shows that the Bell codes for the 2-qubit classical-quantum channel can be extended to an N-qubit classical-quantum channel.

Consider an arbitrary N-qubit classical-quantum channel with pure outputs given by

$$|\varphi\rangle = \sum_{l=0}^{2^N-1} \alpha_l |l\rangle \tag{4.89}$$

$$= \sum_{l=0}^{2^N-1} \alpha_l |l_{N-1}\dots l_0\rangle \tag{4.90}$$

$$= \alpha_0 |0\dots 00\rangle + \alpha_1 |0\dots 01\rangle + \dots + \alpha_{2^N-1} |1\dots 11\rangle \tag{4.91}$$

for $\sum_{l=0}^{2^N-1} |\alpha_l|^2 = 1$ and where $l_{N-1}\dots l_0$ are the digits of the binary representation of l. The channel is then defined by the mapping $x \to W_x = |\varphi_x\rangle\langle\varphi_x|$. For $M = 2^{N-1}K \geq 2^N$, the N-qubit Bell codebook of cardinality M is given by $\mathcal{C} = \{x_1, \dots, x_M\}$ with the following channel outputs:

$$|\varphi_{x_m}\rangle = \begin{cases} \frac{1}{\sqrt{2}}\left(|00\rangle + e^{j\phi_k}|11\rangle\right) \otimes |l_{N-3}\dots l_0\rangle, \\ \qquad m = 1 + 2k + 2Kl, \\ \\ \frac{1}{\sqrt{2}}\left(|01\rangle + e^{j\phi_k}|10\rangle\right) \otimes |l_{N-3}\dots l_0\rangle, \\ \qquad m = 2 + 2k + 2Kl, \end{cases} \tag{4.92}$$

where $\phi_k = 2\pi k/K$, $k = 0, \dots, K-1$, and where $l = 0, \dots, 2^{N-2} - 1$.

The channel output for codeword x_m is thus given by the pure state $W_m = |\varphi_{x_m}\rangle\langle\varphi_{x_m}|$.

Proposition 4.4. *Let $\mu_0 = \frac{1}{2^N}\mathbb{1}_{2^N}$. The N-qubit classical-quantum channel is symmetric and the N-qubit Bell code $\mathcal{C}$ is quasi-perfect for this channel. Moreover,*

$$P_e(\mathcal{C}) = \alpha_{\frac{1}{M}}\left(W_x \,\|\, \mu_0\right) = 1 - \frac{2^N}{M}. \tag{4.93}$$

Proof: The proof is the same to that of Proposition 4.1 and it is omitted here. ■

Appendix

4.A Proof of Proposition 4.2

Let ρ_B be the average density matrix as observed by the decoder. For $M > 3$ it follows that

$$\rho_B = \frac{1}{M}\sum_{m=1}^{M} W_m = \frac{1}{M}\sum_{m=1}^{M} \mathcal{N}_{A\to B}\left(|\varphi_{x_m}\rangle\langle\varphi_{x_m}|_A\right) = \begin{bmatrix} & & 0 \\ (1-\epsilon)\frac{1}{4}\mathbb{1}_4 & & \vdots \\ & & 0 \\ 0 & \dots & 0 \quad \epsilon \end{bmatrix}. \tag{4.94}$$

Define decoder $\mathcal{P} = \{\Pi_1, \dots, \Pi_M\}$ as

$$\Pi_m = \frac{1}{M}\rho_B^{-\frac{1}{2}} W_m \rho_B^{-\frac{1}{2}} = \frac{1}{M}\begin{bmatrix} & & 0 \\ 4\,|\varphi_{x_m}\rangle\langle\varphi_{x_m}| & & \vdots \\ & & 0 \\ 0 & \dots & 0 \quad 1 \end{bmatrix}. \tag{4.95}$$

It is possible to check that $\Pi_m \geq 0$ and that $\sum_{m=1}^{M}\Pi_m = \mathbb{1}_5$. Moreover,

$$\Lambda(\mathcal{P}) \triangleq \frac{1}{M}\sum_{m=1}^{M} W_m\Pi_m = \frac{1}{M}\begin{bmatrix} & & 0 \\ (1-\epsilon)\mathbb{1}_4 & & \vdots \\ & & 0 \\ 0 & \dots & 0 \quad \epsilon \end{bmatrix}. \tag{4.96}$$

Conditions (3.55) and (3.56) from Lemma 3.1 are satisfied by this decoder as we show next. First we can see that

$$\Lambda(\mathcal{P})\Pi_m^\star = \frac{1}{M} W_m \Pi_m^\star, \tag{4.97}$$

which implies (3.55). Equation (3.56) in Lemma 3.1 is satisfied since, for arbitrary unit norm vector $|\psi'\rangle \triangleq \begin{bmatrix} |\psi\rangle \\ \pi \end{bmatrix}$, where $|\pi| \leq 1$, $\langle\psi|\psi\rangle = 1 - |\pi|^2$,

$$\frac{\langle\psi'|\,\Lambda(\mathcal{P})\,|\psi'\rangle}{\frac{1}{M}\,\langle\psi'|\,W_m\,|\psi'\rangle} = \frac{\frac{1}{M}\left[(1-\epsilon)\,\langle\psi|\psi\rangle + \epsilon|\pi|^2\right]}{\frac{1}{M}\left[(1-\epsilon)|\,\langle\psi|\varphi_{x_m}\rangle\,|^2 + \epsilon|\pi|^2\right]} \geq 1, \tag{4.98}$$

where the inequality is implied by the Cauchy-Schwarz inequality since $|\,\langle\psi|\varphi_{x_m}\rangle\,|^2 \leq \langle\psi|\psi\rangle\,\langle\varphi_{x_m}|\varphi_{x_m}\rangle = \langle\psi|\psi\rangle$. As (4.98) implies $\langle\psi|\,(\Lambda(\mathcal{P}) - \frac{1}{M}W_m)\,|\psi\rangle \geq 0$ for an arbitrary $|\psi\rangle$, then (3.56) follows.We conclude that $\mathcal{P} = \{\Pi_1, \ldots, \Pi_M\}$ minimizes the error probability for $\mathcal{C}$.

Let

$$\mu_0 = \frac{1}{4-3\epsilon}\begin{bmatrix} & & 0 \\ & (1-\epsilon)\mathbb{1}_4 & \vdots \\ & & 0 \\ 0 & \ldots\ 0 & \epsilon \end{bmatrix}. \tag{4.99}$$

We prove that

$$\mathcal{E}_x(t,\mu_0) = \begin{cases} \mathbb{1}_5, & t < 0, \\ |v_1'\rangle\,\langle v_1'| + |v_2'\rangle\,\langle v_2'|\,, & 0 \leq t \leq t_0, \\ 0, & t > t_0, \end{cases} \tag{4.100}$$

where $|v_1'\rangle = \begin{bmatrix} |\varphi_x\rangle \\ 0 \end{bmatrix}$, $|v_2'\rangle = \left[0,0,0,0,1\right]^T$ and $t_0 \geq 0$. For $t < 0$ the identity is trivial since both $W_x \geq 0$ and $\mu_0 \geq 0$. For the $t \geq 0$ region, we consider:

$$W_x - t\mu_0 = \begin{bmatrix} (1-\epsilon)\,|\varphi_x\rangle\,\langle\varphi_x| & 0 \\ 0 & \epsilon \end{bmatrix} - \frac{t}{4-3\epsilon}\begin{bmatrix} (1-\epsilon)\mathbb{1}_4 & 0 \\ 0 & \epsilon \end{bmatrix} \tag{4.101}$$

$$= \begin{bmatrix} (1-\epsilon)(|\varphi_x\rangle\,\langle\varphi_x| - \frac{t}{4-3\epsilon}\mathbb{1}_4) & 0 \\ 0 & \epsilon(1-\frac{t}{4-3\epsilon}) \end{bmatrix}. \tag{4.102}$$

For $t > 4-3\epsilon$ the matrix $W_x - t\mu_0$ has no positive eigenvalues. For $0 \leq t \leq 4-3\epsilon$ it has two positive eigenvalues whose eigenvectors are $|v_1'\rangle = |\varphi_x\rangle$ and $|v_2'\rangle = \left[0,0,0,0,1\right]^T$, obtaining (4.100).

Taking $t = 4-3\epsilon$ we see that $\frac{1}{M}W_m - \Lambda(\mathcal{P}) = \frac{1}{M}W_m - \frac{t}{M}\mu_0$ is negative semidefinite. Hence, $\mathcal{E}_{x_m}(t,\mu_0) \triangleq \left\{W_m - t\mu_0 \geq 0\right\} = \left\{W_m - t\mu_0 = 0\right\} = \mathcal{E}^{\circ}_{x_m}(t,\mu_0)$ is the null eigenspace of $\frac{1}{M}W_m - \Lambda(\mathcal{P})$. This also implies that $\mathcal{E}^{\bullet}_{x_m}(t,\mu_0) = 0$, hence $\left\{\mathcal{E}^{\bullet}_x(t,\mu)\right\}_{x\in\mathcal{C}}$ are orthogonal to each other. For this choice of t and μ_0, we also have that

$$\mathcal{E}_{x_m}(t,\mu_0) = \begin{bmatrix} |\varphi_x\rangle\,\langle\varphi_x| & 0 \\ 0 & 1 \end{bmatrix}. \tag{4.103}$$

We conclude that $\sum_{x\in\mathcal{C}} \mathcal{E}_x(t,\mu) = \begin{bmatrix} \frac{M}{4}\mathbb{1}_4 & 0 \\ 0 & M \end{bmatrix}$, which means that $\mathcal{E}_x'^{\circ}(\bar{t},\mu) = \frac{M}{4} I_{\circ A}$, where $\mathcal{E}_x'^{\circ}(\bar{t},\mu)$ and $I_{\circ A}$ were defined in Definition 4.3. This proves that the code is generalized quasi-perfect. The error probability using the optimal decoder $\mathcal{P}$ is:

$$\mathsf{P}_{\mathrm{e}}(\mathcal{C}) = 1 - \frac{1}{M}\sum_{m=1}^{M} \mathrm{Tr}\big(W_m \Pi_m\big) \tag{4.104}$$

$$= 1 - \mathrm{Tr}\big(\Lambda(\mathcal{P})\big) \tag{4.105}$$

$$= 1 - \frac{4-3\epsilon}{M}, \tag{4.106}$$

where in the last step we used (4.96).

4.B Proof of Proposition 4.3

Define decoder $\mathcal{P} = \{\Pi_1, \ldots, \Pi_M\}$ as

$$\Pi_m = \frac{4}{M} |\varphi_{x_m}\rangle \langle\varphi_{x_m}| . \tag{4.107}$$

This set of projectors satisfy $\Pi_i \geq 0$ and $\sum_{i=1}^{M} \Pi_i = \mathbb{1}_4$. For this decoder, we have

$$\Lambda(\mathcal{T}) \triangleq \frac{1}{M}\sum_{i=1}^{M} W_i \Pi_i \tag{4.108}$$

$$= \frac{4}{M^2}\sum_{i=1}^{M} W_i |\varphi_{x_i}\rangle \langle\varphi_{x_i}| \tag{4.109}$$

$$= \frac{1}{4M}(4-3p)\mathbb{1}_4. \tag{4.110}$$

It follows that

$$\Lambda(\mathcal{T})\Pi_i = \frac{1}{M} W_i \Pi_i, \tag{4.111}$$

which implies (3.55). Equation (3.56) is satisfied since, for arbitrary unit norm vector $|\psi\rangle$,

$$\frac{\langle\psi|\Lambda(\mathcal{T})|\psi\rangle}{\frac{1}{M}\langle\psi|W_i|\psi\rangle} = \frac{\frac{1}{4M}(4-3p)}{\frac{1}{4M}(p+4(1-p)|\langle\psi|\varphi_{x_i}\rangle|^2)} \tag{4.112}$$

$$\geq \frac{4-3p}{p+4(1-p)} = 1. \tag{4.113}$$

So $\mathcal{T} = \{\Pi_1, \ldots, \Pi_M\}$ minimizes the error probability for the Bell code $\mathcal{C}$.

We can also see that the channel is symmetric, because $W_x = U_x W_y U_x$
$= U_x(p\frac{1}{4}\mathbb{1}_4 + (1-p)\rho_y)U_x = U_x p\frac{1}{4}\mathbb{1}_4 U_x + (1-p)U_x|\alpha_y\rangle\langle\alpha_y|U_x = p\frac{1}{4}\mathbb{1}_4 + (1-p)|\alpha_x\rangle\langle\alpha_x|$,

with U_x being a unitary matrix such that $U_x \left|\alpha_y\right\rangle \left\langle\alpha_y\right| U_x = \left|\alpha_x\right\rangle \left\langle\alpha_x\right|$.
Next, we prove that the Bell code is quasi-perfect for the depolarizing channel. Recall that

$$\mathcal{E}_x(t,\mu_0) = \big\{W_x - t\mu_0 \geq 0\big\}. \tag{4.114}$$

Let $\mu_0 = \frac{1}{4}\mathbb{1}$. We obtain the eigenvector associated to the largest eigenvalue of $W_x - t\mu_0$. To this end, we consider an arbitrary unit-norm vector $\left|v\right\rangle$. The largest eigenvalue of $W_x - t\mu_0$ is given by

$$\begin{aligned}
&\max_v \left\langle v\right| \left(W_x - t\mu_0\right) \left|v\right\rangle && (4.115)\\
&\quad = \max_v \left\{\frac{p}{4} + (1-p)\left|\left\langle v|\varphi_x\right\rangle\right|^2 - \frac{t}{4}\right\} && (4.116)\\
&\quad = 1 - \frac{3}{4}p - \frac{t}{4}. && (4.117)
\end{aligned}$$

The vector $\left|v\right\rangle$ maximizing (4.116) is $\left|v\right\rangle = \left|\varphi_x\right\rangle$. We can observe that $t = t_0$ corresponds to the case for which the maximum eigenvalue of $\left|\alpha_m\right\rangle \left\langle\alpha_m\right| - t\mu_0$ is equal to zero, which is obtained with $t_0 = 4-3p$. For $0 \leq t \leq 4-3p$, (4.117) is the only non-negative eigenvalue with associated eigenvector $\left|v\right\rangle = \left|\varphi_x\right\rangle$. Therefore, for this interval, we obtain $\mathcal{E}_x(t,\mu_0) = \left|\varphi_x\right\rangle \left\langle\varphi_x\right|$.

Take $t = 4-3p$, then $\frac{1}{M}W_m - \Lambda(\mathcal{T})$ is negative semidefinite and $\mathcal{E}^{\bullet}_{x_m}(t,\mu_0) = 0$. As a result, $\big\{\mathcal{E}^{\bullet}_{x_m}(t,\mu_0)\big\}_{x\in\mathcal{C}}$ are orthogonal to each other. Similarly, for this choice of t and μ_0, it follows that $\sum_{x\in\mathcal{C}} \mathcal{E}^{\circ}_x(t,\mu) = \frac{M}{4}\mathbb{1}_4$ and so the code is quasi-perfect. Using the optimal decoder $\mathcal{T}$, we obtain that the probability of error is

$$\begin{aligned}
\mathsf{P}_{\mathrm{e}}(\mathcal{C}) &= 1 - \frac{1}{M}\sum_{i=1}^{M} \mathrm{Tr}\big(W_i\Pi_i\big) && (4.118)\\
&= 1 - \mathrm{Tr}\big(\Lambda(\mathcal{T})\big) && (4.119)\\
&= 1 - \frac{4-3p}{M}, && (4.120)
\end{aligned}$$

where in the last step we used (4.110).

4.C Proof of Theorem 4.3

We need to introduce a couple of lemmas in order to prove Theorem 4.3.

Lemma 4.1. *For any binary hypothesis test discriminating between the quantum states ρ_0 and ρ_1, it follows that*

$$\begin{aligned}
&\alpha_\beta(\rho_0\|\rho_1)\\
&\quad = \sup_{t\geq 0}\Big\{\mathrm{Tr}\big(\rho_0\big\{\rho_0 - t\rho_1 \leq 0\big\}\big) + t\big(\mathrm{Tr}\big(\rho_1\big\{\rho_0 - t\rho_1 > 0\big\}\big) - \beta\big)\Big\} && (4.121)\\
&\quad \geq \mathrm{Tr}\big(\rho_0\big\{\rho_0 - t'\rho_1 \leq 0\big\}\big) - t'\beta, && (4.122)
\end{aligned}$$

for any $t' \geq 0$.

Proof:

For any operator $A \geq 0$ and $0 \leq T \leq \mathbb{1}$, it holds that $\mathrm{Tr}\big(A\{A > 0\}\big) \geq \mathrm{Tr}\big(AT\big)$ [45, Eq. 8]. For $A = \rho_0 - t'\rho_1$ and $T = T_{\mathrm{op}}$ defined in (3.52), this inequality becomes

$$\mathrm{Tr}\big((\rho_0 - t'\rho_1)P_{t'}^{+}\big) \geq \mathrm{Tr}\big((\rho_0 - t'\rho_1)T_{\mathrm{op}}\big), \tag{4.123}$$

where we defined $P_{t'}^{+} \triangleq \{\rho_0 - t'\rho_1 > 0\}$. Indeed, (4.123) holds with equality for the value $t' = t$ appearing in (3.52), as $\mathrm{Tr}\big((\rho_0 - t\rho_1)\theta_t^0\big) = 0$ for any $0 \leq \theta_t^0 \leq \big\{\rho_0 - t\rho_1 = 0\big\}$, since θ_t^0 is in the null-space of $\rho_0 - t\rho_1$.

After some algebra, (4.123) yields

$$-\mathrm{Tr}\big(\rho_0 T_{\mathrm{op}}\big) \geq -\mathrm{Tr}\big(\rho_0 P_{t'}^{+}\big) + t'\,\mathrm{Tr}\big(\rho_1(P_{t'}^{+} - T_{\mathrm{op}})\big). \tag{4.124}$$

Summing one to both sides of (4.124) and noting that $\alpha_\beta(\rho_0\|\rho_1) = 1 - \mathrm{Tr}\big(\rho_0 T_{\mathrm{op}}\big)$ and $\beta = \mathrm{Tr}\big(\rho_1 T_{\mathrm{op}}\big)$, we obtain

$$\begin{aligned}&\alpha_\beta(\rho_0\|\rho_1)\\ &\geq \mathrm{Tr}\big(\rho_0\{\rho_0 - t'\rho_1 \leq 0\}\big) + t'\,\mathrm{Tr}\big(\rho_1 P_{t'}^{+}\big) - t'\beta.\end{aligned} \tag{4.125}$$

As (4.123) holds with equality for the value $t' = t$ appearing in (3.52), so it does (4.125) after optimization over the parameter $t' \geq 0$. Then, (4.121) follows. To obtain the lower bound (4.122), we fix $t' \geq 0$ and use that $\mathrm{Tr}\big(\rho_1\big\{\rho_0 - t'\rho_1 > 0\big\}\big) \geq 0$. ∎

Lemma 4.2. *Let $\rho_0 = PW$ and $\rho_1 = P \otimes \mu$ be defined in (4.2) and (4.3), respectively. Then, the optimal trade-off (3.47) for a hypothesis test between ρ_0 and ρ_1 satisfies*

$$\begin{aligned}&\alpha_\beta\big(PW \,\|\, P \otimes \mu\big)\\ &\quad= \inf_{\substack{\{\beta'_x\}:\\ \beta = \sum_x P(x)\beta'_x}} \sum_{x\in\mathcal{X}} P(x)\alpha_{\beta'_x}\big(W_x \,\|\, \mu\big).\end{aligned} \tag{4.126}$$

Proof: We consider Lemma 4.1 with $\rho_0 \leftarrow PW$ and $\rho_1 \leftarrow P \otimes \mu$. Then, using the block-diagonal structure of PW and $P \otimes \mu$, the identity (4.121) yields

$$\begin{aligned}&\alpha_\beta\big(PW \,\|\, P \otimes \mu\big)\\ &= \sup_{t\geq 0}\Bigg\{\sum_{x\in\mathcal{X}} P(x)\,\mathrm{Tr}\big(W_x\{W_x - t\mu \leq 0\}\big)\\ &\qquad + t\Bigg(\sum_{x\in\mathcal{X}} P(x)\,\mathrm{Tr}\big(\mu\{W_x - t\mu > 0\}\big) - \beta\Bigg)\Bigg\}\end{aligned} \tag{4.127}$$

$$\begin{aligned}&= \sup_{t\geq 0}\Bigg\{\sum_{x\in\mathcal{X}} P(x)\Bigg(\mathrm{Tr}\big(W_x\{W_x - t\mu \leq 0\}\big)\\ &\qquad + t\Big(\mathrm{Tr}\big(\mu\{W_x - t\mu > 0\}\big) - \beta'_x\Big)\Bigg)\Bigg\}\end{aligned} \tag{4.128}$$

for any $\{\beta'_x\}$, $x \in \mathcal{X}$, such that $\sum_x P(x)\beta'_x = \beta$.

We relax the optimization (4.128) by allowing t to be different for each x. Then, we obtain the following upper bound on $\alpha_\beta\big(PW \,\|\, P \otimes \mu\big)$,

$$\begin{aligned}
&\alpha_\beta\big(PW \,\|\, P \otimes \mu\big) \\
&\leq \sum_{x\in\mathcal{X}} P(x) \sup_{t_x \geq 0} \Big\{ \mathrm{Tr}\big(W_x\big\{W_x - t_x\mu \leq 0\big\}\big) \\
&\qquad + t_x\Big(\mathrm{Tr}\big(\mu\big\{W_x - t_x\mu > 0\big\}\big) - \beta'_x\Big)\Big\} \qquad (4.129)\\
&= \sum_{x\in\mathcal{X}} P(x)\alpha_{\beta'_x}\big(W_x \,\|\, \mu\big), \qquad (4.130)
\end{aligned}$$

where in the last step we applied the identity (4.121) from Lemma 4.1 with $\rho_0 \leftarrow W_x$ and $\rho_1 \leftarrow \mu$. The bound (4.129)-(4.130) holds for any $\{\beta'_x\}$, $x \in \mathcal{X}$, such that $\sum_x P(x)\beta'_x = \beta$. Then, to prove (4.126) we only need to show that there exist $\{\beta'_x\}$ satisfying $\sum_x P(x)\beta'_x = \beta$ and such that (4.129) holds with equality.

The value of t maximizing (4.128) induces the Neyman-Pearson test (3.52), which due to the block-diagonal structure of the problem, can be decomposed into the sub-tests

$$T'_x = \big\{W_x - t\mu > 0\big\} + \theta^0_x. \qquad (4.131)$$

Each of these subtests induces a type-I error probability α'_x and a type-II error probability β'_x, that, according to the Neyman-Pearson lemma, satisfy $\sum_x P(x)\alpha'_x = \alpha_\beta\big(PW \,\|\, P \otimes \mu\big)$ and $\sum_x P(x)\beta'_x = \beta$. For this choice of $\{\beta'_x\}$, the optimization in (4.129) yields $t_x = t$ (as the t parameter in the Neyman-Pearson subtests is unique), and therefore (4.129) holds with equality. The result thus follows. ∎

Now we can prove Theorem 4.3. From Theorem 4.1, we have that the right-hand side of (4.65) is a lower bound to the error probability of any code. Then, to prove (4.65) we only need to show that the error probability of a quasi-perfect code $\mathcal{C}$ coincides with this lower bound. Using (4.121) in Lemma 4.1, with $t' = t$, we have that for symmetric channels:

$$\begin{aligned}
\alpha_{\beta_x}\big(W_x \,\|\, \mu\big) &\geq 1 - F^\bullet_x(t,\mu) + t\big(G^\bullet_x(t,\mu) - \beta_x\big) \qquad (4.132)\\
&= 1 - F_\bullet(t,\mu) + t\big(G_\bullet(t,\mu) - \beta_x\big). \qquad (4.133)
\end{aligned}$$

Then, using Lemma 4.2, we have the following:

$$\begin{aligned}
\inf_P \sup_{\mu'} \alpha_{\frac{1}{M}}\big(PW \,\|\, P \otimes \mu'\big) &\geq \inf_{\substack{\{P(x),\beta_x\}:\\ \sum_x P(x)\beta_x = \frac{1}{M}}} \sum_{x\in\mathcal{X}} P(x)\alpha_{\beta_x}\big(W_x \,\|\, \mu\big) \qquad (4.134)\\
&\geq \inf_{\substack{\{P(x),\beta_x\}:\\ \sum_x P(x)\beta_x = \frac{1}{M}}} \Big(1 - F_\bullet(t,\mu) + t\Big(G_\bullet(t,\mu) - \textstyle\sum_x P(x)\beta_x\Big)\Big) \qquad (4.135)\\
&= 1 - F_\bullet(t,\mu) + t\left(G_\bullet(t,\mu) - \frac{1}{M}\right), \qquad (4.136)
\end{aligned}$$

which coincides with the error probability of quasi-perfect codes. This implies that $Pe(\mathcal{C}) \geq \inf_P \sup_{\mu'} \alpha_{\frac{1}{M}}\left(PW \,\|\, P \otimes \mu'\right) \geq Pe(\mathcal{C})$, proving the equality.

5

Quasi-perfect codes for coherent states

This chapter presents the main results of [22]. We study quasi-perfect codes for the transmission of coherent states. The information is conveyed by a laser pulse and transmitted through an optical channel. We will show that phase-modulated codes are quasi-perfect for an approximation of the channel.

5.1 Introduction to optical communications and coherent states

In optical communications systems the information is transmitted in the form of light, generated by a laser or a LED. Optical communications have the advantage of having a high bandwidth due to the fact that the carrier central frequency is very high (of the order of Terahertz). The general classical-quantum channel is composed by a classical channel, where the information is conveyed through an electrical signal that is converted to an optical quantum signal and transmitted through a quantum channel. The optical signal is then received by an optical detector and converted back to electrical. The signal generated by the laser is a quasi-monochromatic light pulse, that is, a light pulse that has an electric field with the following expression:

$$\bar{E}(r,t) = E(r,t)e^{-j\omega t+\phi}, \tag{5.1}$$

where $E(r,t)$ is in $\sqrt{photons}/(s \cdot m^2)$ units and is a term that depends on the mode and temporal mode, i.e. $E(r,t) = \psi(r)s(t)$. The light source (laser) generates photons as a random Poisson process with a mean number of photons equal to:

$$N = \int_0^T \int_A |\bar{E}(r,t)|^2 dr dt, \tag{5.2}$$

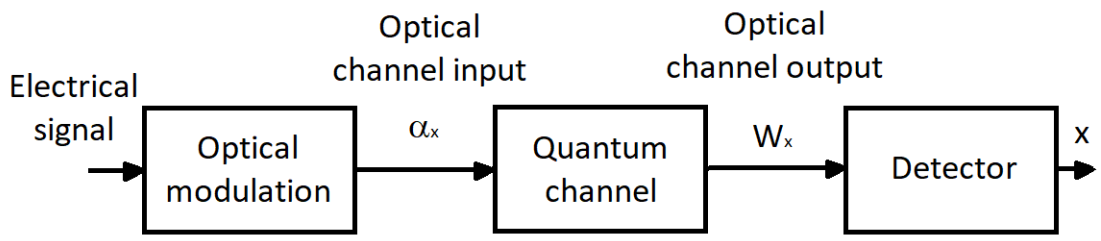

Figure 5.1: Optical channel model

where A is the aperture area of the light pulse and T is the pulse duration. Ideally, the optical receiver detects the photons, and collects information about the arriving number of photons (clicks) and their arrival time. The number of photons is a Poisson process with:

$$p_k = \frac{e^{-N} N^k}{k!}, \tag{5.3}$$

where p_k is the probability of having k photon arrivals and N is the mean number of photons. It is possible to represent the state of the electromagnetic field produced by the laser as a coherent state, defined as:

$$|\alpha\rangle \equiv e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle\,, \tag{5.4}$$

where α is a complex amplitude, $|\alpha|^2$ is the average number of photons of the state $|\alpha\rangle$ and $|n\rangle$ is the photon number state, also known as Fock state. Coherent states were introduced in the quantum optics field by Glauber (see [23]). In general, it is not possible to produce a state with a predetermined number of photons n, and so it is not possible to use a photon number modulation-based system to transmit classical information. Instead, it is common to use a phase-modulation of the coherent state $|\alpha\rangle$ by associating different hypothesis to different values of the phase of α. An overview of some types of modulations and optical receivers is presented next.

There are different types of modulations that can be used to transmit classical information in this setting. The simplest one is the On-Off keying modulation. In this case, the transmitter will either send a pulse over a period of time T or send nothing, and the receiver will decide hypothesis H_0 if it receives nothing or H_1 if it receives the pulse.

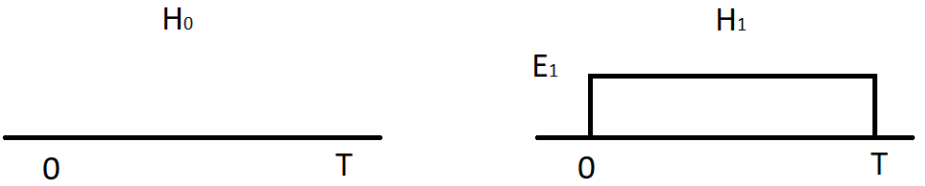

Figure 5.2: On-Off keying modulation

In this case, if nothing is transmitted (hypothesis 0) the number of photons that the receiver detects are 0. This means that there will be no error in this case, since the receiver will always decide H_0. On the other hand, if a pulse is transmitted then the receiver will decide H_1 if it receives at least a photon, and will decide H_0 if no photon is received. So, when the true hypothesis is H_1, the probability of error is the probability of having 0 arriving photons, and it can be obtained using (5.3). The overall error probability assuming a uniform input distribution is:

$$P_e = P(H_0) \cdot 0 + P(H_1)e^{-N} = \frac{1}{2}e^{-N}. \tag{5.5}$$

A more elaborated strategy is to use an offset in order to have hypothesis 0 being $|\beta\rangle$ instead of $|0\rangle$, and $|\alpha+\beta\rangle$ instead of $|\alpha\rangle$ (this is called a displacement operation). This strategy utilizing displacement was proposed by Kennedy [24] and can be implemented by using a beamsplitter. The error probability obtained is

$$P_e = \frac{1}{2}(1 - e^{-(|\beta^2|)}) + \frac{1}{2}e^{-(|\alpha+\beta|)^2}, \tag{5.6}$$

This expression can be optimized over β and it gives a better error probability than the one in (5.5). Other types of modulation are phase modulations, such as the BPSK modulation or Q-ary PSK modulations. Implementing a BPSK modulation can be done by using a Kennedy receiver with a displacement α of the input state, such that hypothesis $|-\alpha\rangle$ and hypothesis $|\alpha\rangle$ become $|0\rangle$ and $|2\alpha\rangle$. In this case, the probability of error is:

$$P_e = \frac{1}{2}e^{-4N}. \tag{5.7}$$

Another strategy to implement a BPSK modulation receiver was defined by Dolinar in [25] and explored in later works [26], [27]. The Dolinar receiver uses a feedback pulse in order to optimize the error probability. The input pulse has a constant amplitude of E or $-E$ depending on which one is the true hypothesis. This pulse is divided into several segments $s(t)$ with the same amplitude as the original pulse, and each one is fed to the detector at

different times. The receiver will use one of two possible pulses $u_+(t)$ and $u_-(t)$ as feedback (see Figure 5.3).

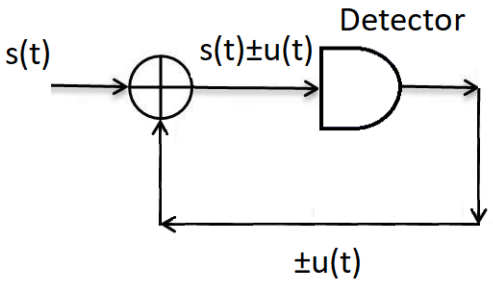

Figure 5.3: Dolinar receiver

The feedback signals can be expressed as:

$$u_+(t) = \frac{-E}{\sqrt{1 - e^{-4Nt/T}}}, \tag{5.8}$$

$$u_-(t) = \frac{E}{\sqrt{1 - e^{-4Nt/T}}}. \tag{5.9}$$

They are pulses that initially have a high amplitude and then they tend to E or $-E$ as time passes.

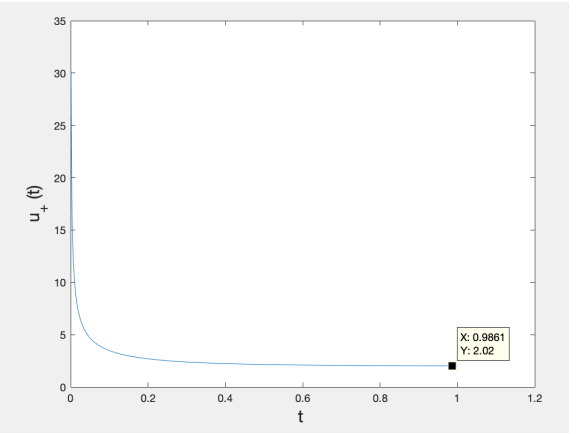

Figure 5.4: Plot of u_+ in function of time, with $E = 2$

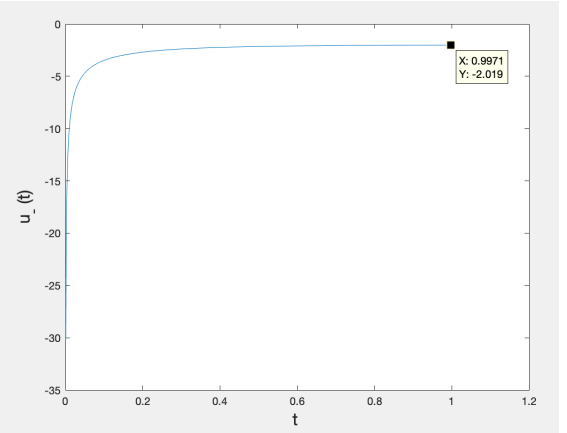

Figure 5.5: Plot of u_- in function of time, with $-E = -2$

Initially, the detector is going to assume that the receiving signal corresponds to one of the hypothesis (i.e. it assumes either that $s(t)$ has a positive amplitude or a negative amplitude). Then, it will choose to use u_+ as feedback if the assumption was that the signal had negative amplitude (or in other words, the detector assumes hypothesis H_0) or u_- if the assumption was that the signal had positive amplitude (the detector assumes hypothesis H_1). The feedback is added to the next input segment $s(t)$, as shown in Figure 5.3. Since for lower values of time $u_+(t)$ and $u_-(t)$ have very high amplitudes compared to the amplitude of $s(t)$, the sum $y(t) = s(t) + u_\pm(t)$ is positive if $u_+(t)$ is used as feedback, or negative if $u_-(t)$ is used. In other words, the sign of $s(t) + u_\pm(t)$ is determined by the feedback pulse $u_\pm(t)$ (notice that the feedback signal always has a higher amplitude than the $s(t)$ signal, in terms of absolute value). The detector is going to use the same feedback signal until it detects a click, which is a photon arrival. Once this happens, the detector is going to assume

that the true hypothesis is H_0 if the pulse $u_-(t)$ was used as feedback. Similarly, the detector is going to assume that the true hypothesis is H_1 if $u_+(t)$ was used as feedback. Next, it will change the feedback signal from $u_-(t)$ to $u_+(t)$ or from $u_+(t)$ to $u_-(t)$ and repeat the process until another click is detected. This process is iterated for all the pulse duration T. When all the signal segments have entered the detector, it will determine that the true hypothesis corresponds to the last assumption it made. Notice that as t tends to T, $u_+(t)$ and $u_-(t)$ tend to E and $-E$ respectively. If the true hypothesis is H_0, then $s(t)$ has an amplitude of $-E$ and so the amplitude of $s(t) + u_+(t)$ tends to zero as t tends to T, which means that it is going to be less probable to get clicks.

This iterative process use all the arriving photons in contrast to the Kennedy receiver, and is able to achieve an optimum probability of error, which is

$$P_e = \frac{1}{2}\left[1 - \sqrt{1 - e^{-4N}}\right]. \tag{5.10}$$

This is proven in [25]. For the case of having multiple hypothesis, it is necessary to use a Q-ary PSK modulation. An implementation of a QPSK receiver was proposed by Bondurant and it uses a similar concept to the Kennedy receiver. The detector receives one out of Q possible hypothesis corresponding to Q quantum states with different phases (for example, for $Q = 4$, it would be $|\alpha\rangle$, $|-\alpha\rangle$, $|j\alpha\rangle$ and $|-j\alpha\rangle$). Then, the receiver input signal is displaced in order to "null" one of the possible states (for $Q = 4$, the constellation is moved to $|0\rangle$, $|2\alpha\rangle$, $|j\alpha + \alpha\rangle$ and $|-j\alpha + \alpha\rangle$ by using a displacement of α, so that the state $|-\alpha\rangle$ becomes $|0\rangle$). Next, the receiver waits for clicks. If photons are detected, then the receiver will consider that the hypothesis corresponding to the state that has been nulled is not the true hypothesis because no photons should have been detected, and in this case it will repeat the same process by nulling another hypothesis. If no photons are detected, then it determines that the true hypothesis is the one that corresponds to the state that has been displaced to $|0\rangle$.

In the next section, we will analyse codes using Q-ary PSK modulations to show that they are quasi-perfect for an approximated bosonic channel. We will use an optimum POVM for measurement and not consider the difficulties in implementing these receivers. Our line of work will be focused on the optimality of the actual codes rather than the design of the detectors.

5.2 Quasi-perfect codes for the bosonic classical-quantum channel

In this section, we explore quasi-perfect codes for the transmission of coherent states. Recall that coherent states are represented by:

$$|\alpha\rangle \equiv e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \tag{5.11}$$

Notice that the dimension of $|\alpha\rangle$ is infinite. We instead want to consider a finite dimensional quantum receiver that implements collective measurements by using a POVM defined in a

Hilbert space of dimension N, $\mathcal{H}_N$, i.e., restricting the dimension of the Fock states $|n\rangle$ to N, $n \in \{0, \ldots, N-1\}$.

We define the Nth order approximation $|\alpha\rangle_N \in \mathcal{H}_N$ of a coherent state $|\alpha\rangle$ as:

$$|\alpha\rangle_N \equiv \frac{1}{\sqrt{C_N}} \sum_{n=0}^{N-1} \frac{\alpha^n}{\sqrt{n!}} |n\rangle , \tag{5.12}$$

$$C_N = \sum_{n=0}^{N-1} \frac{|\alpha|^{2n}}{n!}. \tag{5.13}$$

To determine how close the approximation is with respect to the original state we make use of the concept of Pure-State Fidelity, which is calculated as a function of the order of approximation N,

$$\begin{aligned} F(N) &= |\langle\alpha|\alpha\rangle_N|^2 = \frac{C_N}{e^{|\alpha|^2}} \\ &= \frac{1}{1 + C_N^{-1} \sum_{n=N}^{\infty} \frac{|\alpha|^{2n}}{n!}} = \frac{1}{1+\epsilon_N}, \end{aligned} \tag{5.14}$$

for $\epsilon_N = C_N^{-1} \sum_{n=N}^{\infty} \frac{|\alpha|^{2n}}{n!}$. Note that $\lim_{N\to\infty} \epsilon_N = 0$ which means that if N is sufficiently large, the Fidelity between the original and the approximated state tends to one. The Fidelity and the Trace Distance $|| \, |\alpha\rangle\langle\alpha| - |\alpha\rangle\langle\alpha|_N \, ||_1$ for pure states are related as follows:

$$\begin{aligned} &\frac{1}{2} || \, |\alpha\rangle\langle\alpha| - |\alpha\rangle\langle\alpha|_N \, ||_1 = \sqrt{1 - F(N)} \\ &\quad = \sqrt{\frac{\epsilon_N}{1+\epsilon_N}} \approx \sqrt{\epsilon_N}. \end{aligned} \tag{5.15}$$

Since $\lim_{N\to\infty} \epsilon_N = 0$ for sufficiently large N, if a measurement using an arbitrary operator Π on the approximated state $|\alpha\rangle_N$ succeeds with high probability, it also does succeed with high probability if applied to the original state $|\alpha\rangle$ since:

$$\begin{aligned} &\frac{1}{2} || \, |\alpha\rangle\langle\alpha| - |\alpha\rangle\langle\alpha|_N \, ||_1 \\ &= \max_{0 \le \Delta \le I} \{ \mathrm{Tr}\{\Delta(|\alpha\rangle\langle\alpha| - |\alpha\rangle\langle\alpha|_N)\} \} \\ &\ge |\langle\alpha| \Pi |\alpha\rangle - \langle\alpha|_N \Pi |\alpha\rangle_N|. \end{aligned} \tag{5.16}$$

We are interested in the channel coding problem of transmitting M equiprobable messages through a classical-quantum channel. Messages are represented by the classical random variable x, over a one-shot approximated coherent quantum channel $x \to |\alpha_x\rangle\langle\alpha_x|_N$, with $\alpha_x \equiv a e^{i\theta_x}$, $\theta_x \in [0, 2\pi)$. A channel code is defined as a mapping from the message set $\{1, \ldots, M\}$ into a set of M codewords $\mathcal{C} = \{x_1, \ldots, x_M\}$. The decoder operates in a finite dimensional Hilbert space of dimension N, $\mathcal{H}_N$. For a source message m, the decoder decides which was the transmitted message. Define $\mathcal{C} = \{x_1, \ldots, x_M\}$, with $\alpha_{x_m} \equiv a\delta_{x_m} \equiv a e^{i\theta_{x_m}}$, $\theta_{x_m} = \frac{2\pi(m-1)}{M}$ for a code with cardinality M, and for each message $m = 1, ..., M$, i.e. as in

a classical PSK modulation. Note that this implies that $a = |\alpha_{x_m}|$.

The analysis that is presented here will consider the particular case of having the same message cardinality M as the dimension of the POVM's Hilbert space N, in other words, we consider $N = M$.

Define ρ_M as the density matrix observed by the M-dimensional decoder. For $N = M \geq 2$ it follows that

$$\begin{aligned}\rho_M &= \frac{1}{M}\sum_{m=1}^{M} |\alpha_{x_m}\rangle \langle \alpha_{x_m}|_M \\ &= \frac{1}{C_M}\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & a^2 & 0 & \dots & 0 \\ 0 & 0 & \frac{a^4}{2} & \dots & 0 \\ \vdots & & & \vdots & \\ 0 & 0 & 0 & \dots & \frac{a^{2(M-1)}}{(M-1)!} \end{bmatrix},\end{aligned} \tag{5.17}$$

where

$$|\alpha_{x_m}\rangle_M \equiv \frac{1}{\sqrt{C_M}}\sum_{n=0}^{M-1}\frac{\alpha_{x_m}^n}{\sqrt{n!}}|n\rangle\,. \tag{5.18}$$

We define the state density matrix when the message x_m is transmitted as W_m, i.e, $W_m \equiv |\alpha_{x_m}\rangle \langle \alpha_{x_m}|_M$. Also, let $\alpha_m \equiv \alpha_{x_m}$ and $\delta_m \equiv \delta_{x_m}$ to simplify the notation. We consider the decoder $\mathcal{P} = \{\Pi_1, \dots, \Pi_M\}$ where

$$\begin{aligned}\Pi_m =& \frac{1}{M}\rho_M^{-\frac{1}{2}} W_m \rho_M^{-\frac{1}{2}} \\ =& \frac{1}{M}\begin{bmatrix} 1 & \delta_m^* & \delta_m^{*2} & \dots & \delta_m^{*M-1} \\ \delta_m & 1 & \delta_m^* & \dots & \delta_m^{*M-2} \\ \delta_m^2 & \delta_m & 1 & \dots & \delta_m^{*M-3} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ \delta_m^{M-1} & \delta_m^{M-2} & \delta_m^{M-3} & \dots & 1 \end{bmatrix}.\end{aligned} \tag{5.19}$$

One can check that $\Pi_m \geq 0$ and that $\sum_{m=1}^{M}\Pi_m = \mathbb{1}_M$. Moreover,

$$\begin{aligned}\Lambda(\mathcal{P}) &\triangleq \frac{1}{M}\sum_{m=1}^{M} W_m \Pi_m \\ &= \frac{1}{M}\frac{B_M}{C_M}\begin{bmatrix} 1 & 0 & 0 & ... & 0 \\ 0 & a & 0 & ... & 0 \\ 0 & 0 & \frac{a^2}{\sqrt{2}} & ... & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & ... & \frac{a^{M-1}}{\sqrt{(M-1)!}} \end{bmatrix},\end{aligned} \tag{5.20}$$

with $C_M = \sum_{n=0}^{M-1} \frac{a^{2n}}{n!}$, and $B_M = \sum_{n=0}^{M-1} \frac{a^n}{\sqrt{n!}}$. Then one can check that

$$\Lambda(\mathcal{P})\Pi_m = \frac{1}{M} W_m \Pi_m. \tag{5.21}$$

Also, for any unit vector $|v\rangle$,

$$\begin{aligned} \frac{\langle v| \Lambda(\mathcal{P}) |v\rangle}{\frac{1}{M} \langle v| W_m |v\rangle} &= \frac{\langle v| \Lambda(\mathcal{P})^{\frac{1}{2}} \Lambda(\mathcal{P})^{\frac{1}{2}} |v\rangle}{\frac{1}{M} |\langle v|\alpha_m\rangle|^2} \\ = \frac{M \langle u|u\rangle}{|\langle u| \Lambda(\mathcal{P})^{\frac{1}{2}} |\alpha_m\rangle|^2} &\geq \frac{M}{\langle \alpha_m| \Lambda(\mathcal{P})^{-1} |\alpha_m\rangle} = 1, \end{aligned} \tag{5.22}$$

which proves that $\Lambda(\mathcal{P}) - \frac{1}{M} W_m \geq 0$.

We check the symmetry of the one-shot coherent channel $x \to |\alpha_x\rangle \langle\alpha_x|_M$, with $|\alpha_x| = a$. In our channel we have $\alpha_y = \alpha_x e^{i(\theta_y - \theta_x)}$, i.e. $|\alpha_y\rangle = \Theta |\alpha_x\rangle$, where Θ is a diagonal matrix which elements incorporate the corresponding phase shifts. Note that $\Theta^H \Theta = I$. Since (4.6) holds, we conclude that the channel is symmetric.

We prove that $\mathcal{C}$ is quasi-perfect for $\mu = \mu_0$ and $t = t_0$, with t_0 and μ_0 defined below. Recall that a code is quasi-perfect with respect to μ_0 and t_0 if it satisfies that $\{\mathcal{E}_x^\bullet(t_0, \mu_0)\}$ for $x \in \mathcal{C}$ are orthogonal to each other and also that $\sum_{x \in \mathcal{C}} \mathcal{E}_x^\circ(t, \mu) = C_{\mathcal{C}} I_\circ$. From the optimality condition of the decoder (5.22) we can see that $\Lambda(\mathcal{P}) - \frac{1}{M} W_x \geq 0$, which implies that $\mathcal{E}_x(t_0, \mu_0) \triangleq \{W_x - t_0 \mu_0 \geq 0\} = \{W_x - t_0 \mu_0 = 0\} = \mathcal{E}_x^\circ(t_0, \mu_0)$ is the null eigenspace of $\frac{1}{M} W_x - \Lambda(\mathcal{P})$. This also implies that $\mathcal{E}_x^\bullet(t, \mu_0) = 0$, hence $\{\mathcal{E}_x^\bullet(t_0, \mu)\}$ for $x \in \mathcal{C}$ are orthogonal to each other. Also, $d_\circ = n = M$ because $d_\bullet = 0$, which implies that $C_{\mathcal{C}} = 1$.

Recall that

$$\mathcal{E}_x(t, \mu_0) = \{|\alpha_x\rangle \langle\alpha_x|_M - t\mu_0 \geq 0\}. \tag{5.23}$$

Let $\mu_0 = \frac{M C_M}{(B_M)^2} \Lambda(\mathcal{P})$, we prove that

$$\mathcal{E}_x(t_0, \mu_0) = |v_{x,t_0}\rangle \langle v_{x,t_0}|_M . \tag{5.24}$$

We obtain the eigenvector associated to the largest eigenvalue of $|\alpha_x\rangle \langle\alpha_x| - t\mu_0$. To this end, we consider an arbitrary unit-norm vector $|v\rangle$. The largest eigenvalue of $|\alpha_m\rangle \langle\alpha_m| - t\mu_0$ is given by

$$\begin{aligned} &\max_{|v\rangle : \langle v|v\rangle = 1} \langle v| \left(|\alpha_x\rangle \langle\alpha_x| - t\mu_0\right) |v\rangle = \\ &\max_{|v\rangle : \langle v|v\rangle = 1} \left\{ \langle v|\alpha_x\rangle \langle\alpha_x|v\rangle - t \langle v| \mu_0 |v\rangle \right\}. \end{aligned} \tag{5.25}$$

We can observe that $t = t_0$ corresponds to the case for which the maximum eigenvalue of $|\alpha_m\rangle \langle\alpha_m| - t\mu_0$ is equal to zero, which implies

$$|\alpha_x\rangle \langle\alpha_x|v\rangle = t_0 \mu_0 |v\rangle . \tag{5.26}$$

Note that (5.26) implies

$$|v_{x,t_0}\rangle = \frac{1}{\sqrt{M}} \begin{bmatrix} 1 \\ \delta_x \\ \delta_x^2 \\ \vdots \\ \delta_x^{M-1} \end{bmatrix}. \tag{5.27}$$

Multiplying by $\langle \alpha_x | \, \mu_0^{-1}$ at both sides of (5.26) we obtain

$$\langle \alpha_x | \, \mu_0^{-1} \, |\alpha_x\rangle \, \langle \alpha_x | v\rangle = \frac{(B_M)^2}{C_M} \, \langle \alpha_x | v\rangle = t_0 \, \langle \alpha_x | v\rangle \,, \tag{5.28}$$

from which we obtain $t_0 = \frac{(B_M)^2}{C_M}$.

Now, we can see that using (5.27),

$$\sum_{x\in\mathcal{C}} \mathcal{E}_x(t_0,\mu) = \sum_{x\in\mathcal{C}} |v_{x,t_0}\rangle \, \langle v_{x,t_0}| \tag{5.29}$$

$$= \frac{1}{M} \sum_{m=1}^{M} \begin{bmatrix} 1 & \delta_m^* & \delta_m^{*2} & \dots & \delta_m^{*M-1} \\ \delta_m & 1 & \delta_m^* & \dots & \delta_m^{*M-2} \\ \delta_m^2 & \delta_m & 1 & \dots & \delta_m^{*M-3} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ \delta_m^{M-1} & \delta_m^{M-2} & \delta_m^{M-3} & \dots & 1 \end{bmatrix} = \mathbb{1}_M. \tag{5.30}$$

So, we conclude that the code is quasi-perfect.

We can also easily find the error probability of this code, which is the minimum error probability among all possible codes of cardinality M for this channel. Using the optimal decoder $\mathcal{P}$, we obtain that the probability of error is

$$\mathsf{P}_{\mathrm{e}}(\mathcal{C}) = 1 - \frac{1}{M} \sum_{m=1}^{M} \mathrm{Tr}\big(W_i \Pi_i\big) \tag{5.31}$$

$$= 1 - \frac{1}{M} \frac{B_M^2}{C_M}. \tag{5.32}$$

Notice that the code is quasi-perfect only for the truncated bosonic channel. However, due to (5.16), for sufficiently large N the error probability in (5.32) is close to the optimal error probability for the original bosonic channel.

5.3 Quasi-perfect codes for the bosonic channel incorporating a depolarizing channel

Consider the Nth-order approximation of the bosonic classical-quantum channel of (5.13) observed after a quantum depolarizing channel, defined as:

$$\mathcal{N}^D_{A\to B}(\rho_M) = p\frac{1}{M}\mathbb{1}_M + (1-p)\rho_M. \tag{5.33}$$

The combined classical-quantum channel is thus $W_x = \mathcal{N}^D_{A\to B}\big(|\alpha_x\rangle\langle\alpha_x|_A\big)$. Using the codebook $\mathcal{C}$ defined in (5.18), the channel output is given by $W_m = \mathcal{N}^D_{A\to B}\big(|\alpha_{x_m}\rangle\langle\alpha_{x_m}|_A\big)$, $m = 1, \ldots, M$.

Proposition 5.1. *For $N = M$, the bosonic classical-quantum channel incorporating a depolarizing channel is symmetric and the code $\mathcal{C}$ is quasi-perfect for this channel.*

Moreover,

$$P_e(\mathcal{C}) = \alpha_{\frac{1}{M}}\big(W_x \,\|\, \mu_0\big) = 1 - \frac{(1-p)B_M^2}{MC_M} - \frac{p}{M}, \tag{5.34}$$

which is obtained using decoder $\mathcal{P} = \{\Pi_1, \ldots, \Pi_M\}$ with

$$\Pi_m = \frac{1}{M}|\pi_m\rangle\langle\pi_m|, \tag{5.35}$$

$$\pi_m = \big[1, e^{j\theta_m}, e^{2j\theta_m}, e^{3j\theta_m}, ..., e^{(M-1)j\theta_m}\big]^T. \tag{5.36}$$

Proof. The proof is provided in Appendix 5.A. □

5.4 Generalized quasi-perfect codes for the bosonic channel incorporating an erasure channel

Consider the Nth-order approximation of the bosonic classical-quantum channel (5.13) observed after a quantum erasure channel, defined as

$$\mathcal{N}^E_{A\to B}(\rho_M) = (1-\epsilon)\mathcal{I}_{A\to B}(\rho_M) + \epsilon|e\rangle\langle e|_B.$$

where the Isometric channel $\mathcal{I}_{A\to B}(\rho_M) = I_{A\to B}\rho_M I^\dagger_{A\to B}$ is defined using the isometry

$$I_{A\to B} = \begin{bmatrix} & \mathbb{1}_M & \\ 0 & \ldots & 0 \end{bmatrix} \tag{5.37}$$

as unique Kraus operator and where $\{|0\rangle, \ldots, |M-1\rangle, |e\rangle\}$ form an orthonormal basis in $\mathcal{H}_B$, where the dimension of $\mathcal{H}_\mathcal{B}$ is d_B. The combined classical-quantum channel is then $W_x = \mathcal{N}^E_{A\to B}\big(|\alpha_x\rangle\langle\alpha_x|_A\big)$. Using the codebook $\mathcal{C}$ defined in (5.18), the channel output is given by $W_m = \mathcal{N}^E_{A\to B}\big(|\alpha_{x_m}\rangle\langle\alpha_{x_m}|_A\big)$, $m = 1, \ldots, M$.

Proposition 5.2. *For $M = d_B$, the truncated bosonic channel incorporating an erasure channel is symmetric and the code $\mathcal{C}$ is generalized quasi-perfect for this channel. Moreover,*

$$P_e(\mathcal{C}) = \alpha_{\frac{1}{M}}\big(W_x \,\|\, \mu_0\big) = 1 - \frac{(1-\epsilon)B_M^2}{MC_M} - \frac{\epsilon}{M}, \tag{5.38}$$

which is obtained using decoder $\mathcal{P} = \{\Pi_1, \ldots, \Pi_M\}$ *with*

$$\Pi_m = \frac{1}{M} \begin{bmatrix} 1 & \delta_m^* & \delta_m^{*2} & \ldots & \delta_m^{*M-1} & 0 \\ \delta_m & 1 & \delta_m^* & \ldots & \delta_m^{*M-2} & 0 \\ \delta_m^2 & \delta_m & 1 & \ldots & \delta_m^{*M-3} & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ \delta_m^{M-1} & \delta_m^{M-2} & \delta_m^{M-3} & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{bmatrix}. \tag{5.39}$$

Proof: The proof is provided in the Appendix 5.B ■

Appendix

5.A Proof of Proposition 5.1

The density matrix ρ_M observed by the decoder in this case is:

$$\begin{aligned}\rho_M &= \frac{1}{M}\sum_{m=1}^{M}(1-p)\left|\alpha_{x_m}\right\rangle\left\langle\alpha_{x_m}\right|_M + p\frac{1}{M}\mathbb{1} \\ &= \begin{bmatrix} (1-p)\frac{1}{C_M}+\frac{1}{M}p & 0 & 0 & \dots & 0 \\ 0 & (1-p)\frac{a^2}{C_M}+\frac{1}{M}p & 0 & \dots & 0 \\ 0 & 0 & (1-p)\frac{a^4}{2C_M}+\frac{1}{M}p & \dots & 0 \\ \vdots & & & \vdots & \\ 0 & 0 & 0 & \dots & (1-p)\frac{a^{2(M-1)}}{C_M(M-1)!}+\frac{1}{M}p \end{bmatrix}.\end{aligned} \tag{5.40}$$

It is easy to see that the channel is still symmetric since $W_x = U_x W_y U_x = U_x(p\frac{1}{M}\mathbb{1}_M + (1-p)\rho_y)U_x = U_x p\frac{1}{M}\mathbb{1}_M U_x + (1-p)U_x\left|\alpha_y\right\rangle\left\langle\alpha_y\right|U_x = p\frac{1}{M}\mathbb{1}_M + (1-p)\left|\alpha_x\right\rangle\left\langle\alpha_x\right|$, with U_x being a unitary matrix such that $U_x\left|\alpha_y\right\rangle\left\langle\alpha_y\right|U_x = \left|\alpha_x\right\rangle\left\langle\alpha_x\right|$, as in the case without the depolarizing channel.

To prove that the code is quasi-perfect, $\{\mathcal{E}_x^\bullet(t,\mu)\}$ must be orthogonal to each other and $\sum_{x\in\mathcal{C}}\mathcal{E}_x(t,\mu) = c\mathbb{1}$. Let's take $t = t_0 = Mc_0$, where $c_0 = \mathrm{Tr}(\Lambda(\mathcal{P}))$, and $\mu = \mu_0 = \frac{1}{c_0}\Lambda(\mathcal{P}) = \frac{1}{c_0}\frac{1}{M}\sum_{m=1}^{M}W_m\Pi_m$. In this case we have:

$$\mathcal{E}_x^\bullet(t,\mu) = \{W_x - t\mu > 0\} = \{(1-p)\left|\alpha_x\right\rangle\left\langle\alpha_x\right| + \frac{p}{M}I - M\Lambda(\mathcal{P}) > 0\} \tag{5.41}$$

$$= \{(1-p)\left|\alpha_x\right\rangle\left\langle\alpha_x\right| + \frac{p}{M}I - M((1-p)\Lambda(\mathcal{P})_{\mathrm{wpol}} + \frac{p}{M^2}I) > 0\} \tag{5.42}$$

$$= \{(1-p)\left|\alpha_x\right\rangle\left\langle\alpha_x\right| - M(1-p)\Lambda(\mathcal{P})_{\mathrm{wpol}} > 0\}, \tag{5.43}$$

where $\Lambda(\mathcal{P})_{\text{wpol}}$ is the $\Lambda(\mathcal{P})$ that we defined in (5.20). Notice that (5.43) is equivalent to:

$$\mathcal{E}_x^{\bullet}(t,\mu) = \{\frac{1}{M}\left|\alpha_x\right\rangle\left\langle\alpha_x\right| - \Lambda(\mathcal{P})_{\text{wpol}} > 0\}, \tag{5.44}$$

and from (5.22) we know that $\Lambda(\mathcal{P})_{\text{wpol}} - \frac{1}{M}\left|\alpha_x\right\rangle\left\langle\alpha_x\right| \geq 0$. This means that $\mathcal{E}_x^{\bullet}(t,\mu) = 0$ and so $\{\mathcal{E}_x^{\bullet}(t,\mu)\}$ are orthogonal.

To obtain $\mathcal{E}_x(t,\mu)$, we obtain the eigenvector corresponding to the largest eigenvalue of $W_x - t\mu$, similar to (5.25):

$$\begin{aligned}&\max_{|v\rangle:\langle v|v\rangle=1}\left\{\langle v|\left(W_x - t\mu_0\right)|v\rangle\right\} = \\ &\max_{|v\rangle:\langle v|v\rangle=1}\left\{(1-p)\left\langle v|\alpha_x\right\rangle\left\langle\alpha_x|v\right\rangle - (1-p)M\left\langle v\right|\Lambda(\mathcal{P})_{\text{wpol}}\left|v\right\rangle\right\}.\end{aligned} \tag{5.45}$$

where we used $\mu = \mu_0$ and $t = t_0$. In this case the maximum eigenvalue is 0, so we can write the following:

$$\left\langle v|\alpha_x\right\rangle\left\langle\alpha_x|v\right\rangle = M\left\langle v\right|\Lambda(\mathcal{P})_{\text{wpol}}\left|v\right\rangle \tag{5.46}$$

Now, using $|v\rangle = \frac{1}{\sqrt{M}}\begin{bmatrix}1 & \delta_x & \delta_x^2 & \dots & \delta_x^{M-1}\end{bmatrix}^T$ as in (5.27), we can see that (5.46) is satisfied since

$$\left\langle v|\alpha_x\right\rangle\left\langle\alpha_x|v\right\rangle = \frac{1}{M}\frac{B_M^2}{C_M}, \tag{5.47}$$

$$M\left\langle v\right|\Lambda(\mathcal{P})_{\text{wpol}}\left|v\right\rangle = \frac{1}{M}\frac{B_M^2}{C_M}. \tag{5.48}$$

This means that $\mathcal{E}_x(t,\mu) = \left|v_x\right\rangle\left\langle v_x\right|$ and so $\sum_{x\in\mathcal{C}}\mathcal{E}_x(t_0,\mu) = \mathbb{1}$, proving that the second condition also holds. We conclude that the code is quasi-perfect. The probability of error is obtained by using $P_e(\mathcal{C}) = 1 - \text{Tr}(\Lambda(\mathcal{P})) = 1 - \frac{(1-p)B_M^2}{MC_M} - \frac{p}{M}$.

5.B Proof of Proposition 5.2

For this case, we have that

$$\begin{aligned}\rho_M &= \frac{1}{M}\sum_{m=1}^{M} W_m \\ &= \frac{1}{C_M}\begin{bmatrix}(1-\epsilon) & 0 & 0 & \dots & 0 & 0\\ 0 & (1-\epsilon)a^2 & 0 & \dots & 0 & 0\\ 0 & 0 & (1-\epsilon)\frac{a^4}{2} & \dots & 0 & 0\\ \vdots & & & \vdots & & \\ 0 & 0 & 0 & \dots & (1-\epsilon)\frac{a^{2(M-1)}}{(M-1)!} & 0\\ 0 & 0 & 0 & \dots & 0 & \epsilon\end{bmatrix},\end{aligned} \tag{5.49}$$

and

$$\begin{aligned}\Lambda(\mathcal{P}) &\triangleq \frac{1}{M}\sum_{m=1}^{M} W_m \Pi_m \\ &=(1-\epsilon)\frac{1}{M}\frac{B_M}{C_M}\begin{bmatrix} 1 & 0 & 0 & ... & 0 & 0 \\ 0 & a & 0 & ... & 0 & 0 \\ 0 & 0 & \frac{a^2}{\sqrt{2}} & ... & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & 0 & ... & \frac{a^{M-1}}{\sqrt{(M-1)!}} & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & \epsilon \end{bmatrix}. \end{aligned} \tag{5.50}$$

Now, using $t = (1-\epsilon)\frac{B_M^2}{C_M} + \epsilon$ and $\mu = \mu_0 = \frac{1}{c_0}\Lambda(\mathcal{P})$ (with c_0 being a normalizing constant) we have that the matrix $W_x - t\mu$ has two positive eigenvalues whose eigenvectors are $|v_1\rangle = \frac{1}{\sqrt{M}}\begin{bmatrix}1 & \delta_x & \delta_x^2 & \dots & \delta_x^{M-1}\end{bmatrix}^T$ (the same as in (5.27)) and $|v_2\rangle = \begin{bmatrix}0,0,0,0,1\end{bmatrix}^T$. This means that:

$$\sum_{x\in\mathcal{C}} \mathcal{E}_{x_m}(t,\mu) = \begin{bmatrix} \mathbb{1} & 0 \\ 0 & M \end{bmatrix}. \tag{5.51}$$

Also, $\mathcal{E}^{\bullet}_{x_m}(t,\mu) = 0$ for all $x \in \mathcal{C}$, and so $\{\mathcal{E}^{\bullet}_{x_m}(t,\mu)\}$ are orthogonal to each other. Since both conditions are satisfied, we conclude that the code is quasi-perfect. As in the previous cases, the probability of error is $P_e(\mathcal{C}) = 1 - Tr(\Lambda(\mathcal{P})) = 1 - \frac{(1-\epsilon)B_M^2}{MC_M} - \frac{\epsilon}{M}$.

6

Quasi-perfect codes in error correction

This chapter focuses on the quantum error correction setting. Gottesman's works [37], [38], [39] and Calderbank's, Rains's and Shor's works [35], [36] provide an introduction to this field.

6.1 Quantum error correction

As we know, quantum channels may introduce errors to a quantum state. In previous chapters, we introduced optimal codes to discriminate quantum states in classical-quantum channels. However, we may be interested instead in protecting quantum states against quantum errors. To do so, it is necessary to add ancilla qubits to the state, so the detector can use extra information in order to determine if an error has occurred and to correct it. An important particularity of error correction in the quantum setting is that the quantum state should be preserved when determining whether an error has occurred or not. This means that directly measuring the quantum state using an optimal POVM is not a good strategy for error correction, because then the state will collapse to one of the eigenvectors of the measurement operators, and the original state would be lost. Instead the error correction process should focus on determining if a particular set of error have occurred without obtaining any information of the original quantum state (the one unaffected by errors). In general, errors are modelled as amplitude errors (that is, one or more qubits affected by an X matrix), phase errors (that is, one or more qubits affected by a Z matrix) or both. We refer to these type of errors as Pauli errors, since they are modelled as unitary Pauli matrices.

A quantum error correction code $\mathcal{C}$ is used to encode a k-qubit quantum state into a n-qubit quantum state, with $n > k$, in order to protect it from channel errors. The code generates up to 2^k different codewords that constitute the coding space. To correct two errors

e_x and e_y from a set of correctable errors E, we need to be able to distinguish the state corresponding to the codeword ψ_i affected by the error e_x from the state corresponding to the codeword ψ_j affected by error e_y, with $i \neq j$ and e_x, e_y being unitary matrices. To guarantee that we are able to distinguish both these states perfectly, they should be orthonormal:

$$\langle\psi_i| e_x^\dagger e_y |\psi_j\rangle = 0. \tag{6.1}$$

Only if this condition is satisfied for all the codewords and any $e_x \in E$, $e_y \in E$, then an adequate measurement makes it possible to correct any error of the set E. The other condition that needs to be satisfied to properly correct errors is that the measurement must not change the state when no error occurs. In other words, we should not get information about the codespace because in this case we would be distorting the input quantum state. We get information of error $e = e_x^\dagger e_y$ by measuring $\langle\psi| e_x^\dagger e_y |\psi\rangle$ for all possible errors e_x, e_y. The result of this measurement should be independent on the codeword, that is:

$$\langle\psi_i| e_x^\dagger e_y |\psi_i\rangle = \langle\psi_j| e_x^\dagger e_y |\psi_j\rangle \tag{6.2}$$

for all $|\psi_i\rangle, |\psi_j\rangle \in \mathcal{C}$. Combining both conditions, we obtain that

$$\langle\psi_i| e_x^\dagger e_y |\psi_j\rangle = c_e \delta_{ij}, \tag{6.3}$$

where δ is the Dirac function and c_e is a constant that only depends on the error vectors e_x, e_y. If this condition holds, then the decoder may perform a measurement in order to obtain knowledge about the (possible) errors that may have occurred, that is, in order to obtain the syndrome. Then, depending on the syndrome obtained the decoder applies a Pauli operator to recover the original state.

6.2 Stabilizer codes

A stabilizer correction quantum code is an error correction code that consists on a commutative group S called *stabilizer* and a coding space $\mathcal{T}$ that is determined by the stabilizer. The code encodes a k-qubit state belonging to $\mathcal{T}$ (a codeword) into a n-qubit state. The coding space $\mathcal{T}$ has a dimension of 2^k and is build as follows:

$$\mathcal{T} = \{|\psi\rangle \;\; | \;\; S_x |\psi\rangle = |\psi\rangle \;\; \forall S_x \in \mathcal{S}\}, \tag{6.4}$$

with $S_x \in \mathcal{S}$, $x \in \{1, 2, \ldots |S|\}$. We denote the set of correctable errors $E = \{e_1, e_2, ..., e_n\}$ as the set of Pauli errors that can be corrected by the decoder. Then for all $e_x \in E$, $x \in \{1, \ldots, |E|\}$ there is at least one stabilizer element S_x that anti-commutes with e_x, that is, $S_x e_x = -e_x S_x$.

The decoder may use a POVM to make a measurement to detect possible errors without affecting the codeword. To do that, consider the projectors $\Pi_x = \frac{I_n + S_x}{2}$ and $\bar{\Pi}_x = \frac{I_n - S_x}{2}$, where Π_x and $\bar{\Pi}_x$ are built using the stabilizer component S_x and where I_n is the identity

matrix of dimension n. A measurement of the quantum state $|\psi\rangle\langle\psi|$ using the projector Π_x will have a probability of outcome '1' being the following:

$$\begin{aligned}\mathrm{Tr}\left(\frac{I_n+S_x}{2}|\psi\rangle\langle\psi|\right) &= \mathrm{Tr}\left(\left(\frac{I_n}{2}|\psi\rangle+\frac{S_x}{2}|\psi\rangle\right)\langle\psi|\right)\\ &= \mathrm{Tr}\left(\left(\frac{|\psi\rangle}{2}+\frac{|\psi\rangle}{2}\right)\langle\psi|\right) = \mathrm{Tr}(|\psi\rangle\langle\psi|) = 1. \end{aligned} \tag{6.5}$$

If the quantum state was affected by an error e_x that anti-commutes with S_x and the state became $e_x|\psi\rangle\langle\psi|e_x^\dagger$ then the probability of obtaining outcome '1' using the projector Π_x would be:

$$\begin{aligned}\mathrm{Tr}\left(\frac{I_n+S_x}{2}e_x|\psi\rangle\langle\psi|e_x^\dagger\right) &= \mathrm{Tr}\left(\left(\frac{I_n}{2}e_x|\psi\rangle+\frac{S_x}{2}e_x|\psi\rangle\right)\langle\psi|e_x^\dagger\right)\\ &= \mathrm{Tr}\left(\left(e_x\frac{|\psi\rangle}{2}-e_x\frac{|\psi\rangle}{2}\right)\langle\psi|e_x^\dagger\right) = 0. \end{aligned} \tag{6.6}$$

So the projector will give an outcome of '1' when there is no error e_x. Similarly, for the projector $\bar{\Pi}_x$:

$$\mathrm{Tr}\left(\frac{I_n-S_x}{2}|\psi\rangle\langle\psi|\right) = \mathrm{Tr}\left(\left(\frac{I_n}{2}|\psi\rangle-\frac{S_x}{2}|\psi\rangle\right)\langle\psi|\right) = \mathrm{Tr}\left(\left(\frac{|\psi\rangle}{2}-\frac{|\psi\rangle}{2}\right)\langle\psi|\right) = 0 \tag{6.7}$$

$$\begin{aligned}\mathrm{Tr}\left(\frac{I_n-S_x}{2}e_x|\psi\rangle\langle\psi|e_x^\dagger\right) &= \mathrm{Tr}\left(\left(\frac{I_n}{2}e_x|\psi\rangle-\frac{S_x}{2}e_x|\psi\rangle\right)\langle\psi|e_x^\dagger\right)\\ &= \mathrm{Tr}\left(\left(e_x\frac{|\psi\rangle}{2}+e_x\frac{|\psi\rangle}{2}\right)\langle\psi|e_x^\dagger\right) = 1. \end{aligned} \tag{6.8}$$

So, using the POVM $\{\Pi_x, \bar{\Pi}_x\}$ to perform a measurement will allow us to detect error e_x with certainty. Notice that $\Pi_x + \bar{\Pi}_x = I_n$ because of the way the projectors are build and $\Pi_x \geq 0$, $\bar{\Pi}_x \geq 0$, confirming that this POVM is valid. To detect and correct multiple errors, we need to make use of all the stabilizer elements and build the projectors $\Pi_1, \Pi_2, \ldots, \Pi_{|\mathcal{S}|}, \bar{\Pi}_1, \bar{\Pi}_2, \ldots, \bar{\Pi}_{|\mathcal{S}|}$. Then, the POVM that the error correction decoder uses is build using all the combinations of Π_x and $\bar{\Pi}_x$, that is,
$\{\Pi_1\Pi_2\ldots\Pi_{|\mathcal{S}|}, \Pi_1\Pi_2\ldots\bar{\Pi}_{|\mathcal{S}|}, \ldots, \bar{\Pi}_1\bar{\Pi}_2\ldots\bar{\Pi}_{|\mathcal{S}|}\}$. The syndrome is obtained directly from the outcome of the measurement. Then, the decoder will use a look-up table in order to determine the operator that needs to be applied to the quantum state to do the error correction procedure.

Example A trivial example of a stabilizer code is the Shor 9-qubit code that encodes a single qubit into a 9-qubit codeword as follows:

$$|0_L\rangle \triangleq (|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle), \tag{6.9}$$

$$|1_L\rangle \triangleq (|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle). \tag{6.10}$$

This code was defined by Shor in [40] and is the equivalent to the repetition code in the classical case. The code has a stabilizer S defined as follows:

$$S_1 = Z \otimes Z \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I, \tag{6.11}$$
$$S_2 = Z \otimes I \otimes Z \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I, \tag{6.12}$$
$$S_3 = I \otimes I \otimes I \otimes Z \otimes Z \otimes I \otimes I \otimes I \otimes I, \tag{6.13}$$
$$S_4 = I \otimes I \otimes I \otimes Z \otimes I \otimes Z \otimes I \otimes I \otimes I, \tag{6.14}$$
$$S_5 = I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes Z \otimes Z \otimes I, \tag{6.15}$$
$$S_6 = Z \otimes Z \otimes I \otimes I \otimes I \otimes I \otimes Z \otimes I \otimes Z, \tag{6.16}$$
$$S_7 = X \otimes X \otimes X \otimes X \otimes X \otimes X \otimes I \otimes I \otimes I, \tag{6.17}$$
$$S_8 = I \otimes I \otimes I \otimes X \otimes X \otimes X \otimes X \otimes X \otimes X. \tag{6.18}$$

Now, an amplitude error (X error) to the first qubit ($e_1 = X \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I$) will anti-commute with S_1 and S_2, an amplitude error to the second qubit will anti-commute with S_1, an amplitude error to the third qubit will anti-commute with S_2, etc. Similarly, different (single) phase errors will anti-commute with at least one of the stabilizers S_6, S_7, S_8. Using these properties, the decoder can differentiate between single qubit amplitude and/or phase errors and correct them.

Other simple examples include the 7-qubit Steane code [47] and the 5-qubit code given in Section 6.3.

6.3 Performance of error correction quasi-perfect codes

This section shows how to study the performance of a quantum error correction system consisting on a codebook and a set of stabilizers by using the properties of quasi-perfect codes. In contrast to previous chapters, error correction does not involve making a measurement of a quantum state. However, we may want to protect a qubit (or multiple qubits) using error protection and later measure it to obtain some classical information from it. For example, we may want to implement the superdense coding protocol to transmit classical information between Alice and Bob. As we've seen in Section 2.7, Alice needs to send her share of the entangled state through the quantum channel. If the quantum channel is noisy, then errors to the qubit will be more likely to happen, and (classical) communication will not be possible. In this case, we may need to implement an error correction code in order to protect the qubit against errors, while maintaining the entanglement properties which would not be possible if we measured the state. We may also need to protect Bob's qubit from decoherence by implementing error correction.

We can show that a particular error correction code is optimum by proving that it is quasi-perfect. As we will see later, even if the code is quasi-perfect the error correction procedure may degrade the error probability. As an example, we will consider the 5-qubit

error correction code which is the simplest code that can be used to correct Pauli errors to a single qubit. For the channel model, we consider two channels: the depolarizing channel, which is a simple and trivial case, and the Pauli channel, which is a more interesting but also a more complicated channel to study.

Consider the 5-qubit stabilizer code $\mathcal{C} = \{|0_L\rangle, |1_L\rangle\}$ with

$$\begin{aligned}|0_L\rangle = \frac{1}{4}[\ &|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle + |01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle \\ &- |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle - |10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle\ ],\end{aligned} \tag{6.19}$$

$$\begin{aligned}|1_L\rangle = \frac{1}{4}[\ &|11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle + |10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle \\ &- |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle - |01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle\ ].\end{aligned} \tag{6.20}$$

and with the following stabilizers:

$$S_1 = X \otimes Z \otimes Z \otimes X \otimes I, \tag{6.21}$$
$$S_2 = I \otimes X \otimes Z \otimes Z \otimes X, \tag{6.22}$$
$$S_3 = X \otimes I \otimes X \otimes Z \otimes Z, \tag{6.23}$$
$$S_4 = Z \otimes X \otimes I \otimes X \otimes Z. \tag{6.24}$$

Consider the 5-qubit classical-quantum channel $\boldsymbol{x} \to W_x = |\varphi_x\rangle\langle\varphi_x|$ observed after a quantum depolarizing channel, defined as

$$W_x^D = \mathcal{N}_{A\to B}^D(|\varphi_x\rangle\langle\varphi_x|) = (1-p)|\varphi_x\rangle\langle\varphi_x| + \frac{p}{32}\mathbb{1}_{32}, \tag{6.25}$$

with $|\varphi_0\rangle = |0_L\rangle$ and $|\varphi_1\rangle = |1_L\rangle$.

First, we show that the code is quasi-perfect for the depolarizing channel. To do that, consider $t = p$ and $\mu = \frac{I}{32}$. Then, we have:

$$\mathcal{E}_0^\bullet = \{(1-p)\,|0_L\rangle\,\langle 0_L| + \frac{p}{32}I - t\mu > 0\} = \{(1-p)\,|0_L\rangle\,\langle 0_L| + \frac{p}{32}I - \frac{p}{32}I > 0\} \tag{6.26}$$
$$= \{(1-p)\,|0_L\rangle\,\langle 0_L| > 0\} = |0_L\rangle\,\langle 0_L|\,, \tag{6.27}$$
$$\mathcal{E}_1^\bullet = \{(1-p)\,|1_L\rangle\,\langle 1_L| + \frac{p}{32}I - t\mu > 0\} = \{(1-p)\,|1_L\rangle\,\langle 1_L| + \frac{p}{32}I - \frac{p}{32}I > 0\} \tag{6.28}$$
$$= \{(1-p)\,|1_L\rangle\,\langle 1_L| > 0\} = |1_L\rangle\,\langle 1_L|\,. \tag{6.29}$$

Since $|0_L\rangle$ and $|1_L\rangle$ are orthogonal codewords, we have that $\mathcal{E}_0^\bullet$ and $\mathcal{E}_1^\bullet$ are orthogonal. Also, we have that

$$\mathcal{E}_0 = \{(1-p)\,|0_L\rangle\,\langle 0_L| \geq 0\} = I, \tag{6.30}$$
$$\mathcal{E}_1 = \{(1-p)\,|1_L\rangle\,\langle 1_L| \geq 0\} = I. \tag{6.31}$$

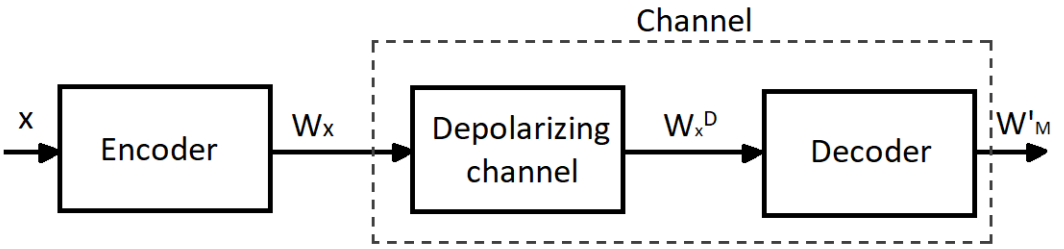

Figure 6.1: Source and channel model

So we have that $\sum_{x\in\mathcal{C}} \mathcal{E}_x = \mathcal{E}_0 + \mathcal{E}_1 = 2I$. Also, the channel is symmetric since $W_x = U_x W_x U_x^\dagger = (1-p)U_x |\bar{\alpha}\rangle \langle\bar{\alpha}| U_x^\dagger + U_x \frac{p}{32} I U_x^\dagger = (1-p)U_x |\bar{\alpha}\rangle \langle\bar{\alpha}| U_x^\dagger + \frac{p}{32} I$ because $U_x U_x^\dagger = I$, where $\bar{\alpha}$ does not depend on x . We conclude that the code is quasi-perfect and achieves the optimum error probability.

Next we want to check that the error correction does not degrade the probability of error. We should take into consideration that the error correction procedure may affect the probability of error. If we wanted to obtain classical information from the quantum state (for example, we would like to know whether codeword $|0\rangle_L$ or $|1\rangle_L$ is transmitted) ideally we would use the optimum POVM in order to make a measurement of the state. Since the code is quasi-perfect, we know that the error probability is optimum in this case. The error probability that we get when measuring the quantum state after performing error correction may be higher than the one we get by using the optimum POVM to measure the state directly. That is the case when we consider the Pauli channel as the channel model, as we will see later.

In order to check the optimality of the error correction procedure, we consider that the decoder is part of the channel (see Figure 6.1). We compute the optimum error probability at the output of the depolarizing channel since we know that the code is quasi-perfect in this case. Then, we compute the probability of error obtained by using the error correction decoder and compare it to the optimum.

Since the code is quasi-perfect and the channel is symmetric, we can compute the optimum error probability as:

$$P_e(\mathcal{C}) = 1 - F_\bullet(t,\mu) + t\left(G_\bullet(t,\mu) - \frac{1}{M}\right). \tag{6.32}$$

To obtain the first term we can use the symmetry property and use any of the codewords for

the calculation:

$$F_\bullet(t,\mu) = \mathrm{Tr}(W_0\mathcal{E}_0^\bullet(t,\mu)) = (1-p)\,\mathrm{Tr}(|0_L\rangle\langle 0_L|) + \frac{p}{32}\,\mathrm{Tr}(|0_L\rangle\langle 0_L|) = (1-p) + \frac{p}{32}. \tag{6.33}$$

Similarly, the second term is obtained as follows:

$$t\left(G_\bullet(t,\mu) - \frac{1}{M}\right) = p\left(\mathrm{Tr}(\mu\mathcal{E}_0^\bullet) - \frac{1}{2}\right) = p\left(\frac{1}{32} - \frac{1}{2}\right). \tag{6.34}$$

The optimum error probability is:

$$P_e(\mathcal{C}) = 1 - (1-p) - \frac{p}{32} + \frac{p}{32} - \frac{p}{2} = \frac{p}{2}. \tag{6.35}$$

We obtain the same error probability when we try to discriminate the states after the error correction procedure, because with probability $(1-p)$ the detector is going to correctly assume that the state wasn't affected by any errors, and with probability p is going to randomly decide that a single-qubit Pauli error occurred and try to correct it by applying the same Pauli matrix to the state. Thus, the average error probability after error correction is also $\frac{p}{2}$, which means that implementing error correction for a depolarizing channel does not worsen the error probability. That is not necessarily the case for other channels, as we will see next.

We would like to analyse a more complex case; in particular, we study the optimality of the code when we transmit the quantum information through a quantum Pauli channel. Since error correction is aimed at correcting Pauli errors, it makes more sense to consider the Pauli channel in order to model the errors. Similar to the previous section, we first show that the code itself is quasi-perfect for the Pauli channel, and then we compare the optimum error probability to the one that we obtain using the error correction procedure.

Consider the 5-qubit stabilizer code $\mathcal{C} = \{|0_L\rangle, |1_L\rangle\}$ defined by equations (6.19), (6.20), with the following stabilizers:

$$S_1 = X \otimes Z \otimes Z \otimes X \otimes I, \tag{6.36}$$
$$S_2 = I \otimes X \otimes Z \otimes Z \otimes X, \tag{6.37}$$
$$S_3 = X \otimes I \otimes X \otimes Z \otimes Z, \tag{6.38}$$
$$S_4 = Z \otimes X \otimes I \otimes X \otimes Z. \tag{6.39}$$

Consider the 5-qubit classical-quantum channel $x \to W_x = |\varphi_x\rangle\langle\varphi_x|$ observed after a quantum Pauli channel, defined as

$$W_x^P = \mathcal{N}_{A\to B}^P(|\varphi_x\rangle\langle\varphi_x|) = \sum_{k,l} p_{x_{k,l}} X(k)Z(l)|\varphi_x\rangle\langle\varphi_x|(X(k)Z(l))^\dagger, \tag{6.40}$$

where $|\varphi_0\rangle = |0_L\rangle$, $|\varphi_1\rangle = |1_L\rangle$ and $p_{x_{k,l}}$ is the probability of having a certain type of errors X, Z or Y in each qubit. The matrices $X(k)$, $Z(l)$ are 32×32 matrices that consist on a Kroenecker product of identity matrices I with X and Z matrices respectively, and k and l are indexes that specify k_1, k_2, k_3, k_4 and k_5, and l_1, l_2, l_3, l_4 and l_5 with $X(k) = X^{k_1} \otimes X^{k_2} \otimes X^{k_3} \otimes X^{k_4} \otimes X^{k_5}$ and $Z(l) = Z^{l_1} \otimes Z^{l_2} \otimes Z^{l_3} \otimes Z^{l_4} \otimes Z^{l_5}$. The sum is over all values of k and l, or equivalently over all combinations of k_1, k_2, k_3, k_4, k_5, l_1, l_2, l_3, l_4 and l_5. Notice that the probability of getting an error Y on a qubit is the probability of getting both an error X and Z because $Y(k)|\varphi_x\rangle\langle\varphi_x|Y(k)^\dagger = X(k)Z(k)|\varphi_x\rangle\langle\varphi_x|(Z(k)X(k))^\dagger$. We will assume that the probabilities of getting X and Z errors on a qubit are independent for all qubits. With this assumption, we define the probability p_{ixjz}, with $i \in \{0,1,2,3,4,5\}$, $j \in \{0,1,2,3,4,5\}$, $i = k_1 + k_2 + k_3 + k_4 + k_5$ and $j = l_1 + l_2 + l_3 + l_4 + l_5$ as the probability of W_x having an i number of X errors and j number of Z errors. In particular, we define the following:

$$p_{ixjz} = p_x^i (1-p_x)^{5-i} p_z^j (1-p_z)^{5-j}, \tag{6.41}$$

where p_x and p_z are the probabilities of having a single-qubit X or Z error respectively. Then, the Pauli channel in (6.40) can be expressed as:

$$W_x^P = \mathcal{N}_{A\to B}^P(|\varphi_x\rangle\langle\varphi_x|) = \sum_{k,l} p_{ixjz} X(k)Z(l)|\varphi_x\rangle\langle\varphi_x|(X(k)Z(l))^\dagger. \tag{6.42}$$

Our objective is to prove that the channel is symmetric and that the code is quasi-perfect for the Pauli channel.

To prove symmetry, we need to show that W_x can be expressed as $W_x = U_x \bar{W} U_x^\dagger$ for $x \in \mathcal{X}$ where $\bar{W}$ does not depend on x. In order to do that, we need to define what is the set of W_x. In general it is not trivial to prove symmetry of the code over all possible 5-qubit states (notice that in this case the channel states are mixed states in contrast to previous examples where the states where pure). We decided to restrict the input alphabet $\mathcal{X}$ to all states that are a Pauli transformation (an application of an X, Z or Y matrix to one or multiple qubits) of $|0\rangle_L$ defined in (6.19). The state $|1\rangle_L$ in (6.20) can be obtained as

$$U_1 = (X \otimes X \otimes X \otimes X \otimes X), \tag{6.43}$$

$$|1\rangle_L = U_1 |0\rangle_L , \tag{6.44}$$

so it satisfies this assumption. In this case we can define $W_0 = \bar{W} = \mathcal{N}_{A\to B}^P(|0\rangle_L \langle 0|_L)$ and $W_x = \mathcal{N}_{A\to B}^P(|\varphi_x\rangle\langle\varphi_x|) = N_{A\to B}^P(U_x |0\rangle_L \langle 0|_L U_x)$, where U_x is a Pauli transformation unitary matrix. We can then write the following:

$$W_0 = \sum_{k,l} p_{ixjz} X(k)Z(l) |0\rangle_L \langle 0|_L (X(k)Z(l))^\dagger, \tag{6.45}$$

$$W_x = \sum_{k,l} p_{ixjz} X(k)Z(l)U_x |0\rangle_L \langle 0|_L U_x (X(k)Z(l))^\dagger. \tag{6.46}$$

To prove symmetry, we need to show that $W_x = U_x \bar{W} U_x$. To do that, notice that U_x commutes or anti-commutes with any other matrix that is also a Kroenecker product of Pauli matrices:

$$X(i)Z(j) = \pm Z(j)X(i). \tag{6.47}$$

Thus, we have:

$$\begin{aligned} U_x \bar{W} U_x &= U_x \left(\sum_{k,l} p_{ixjz} X(k)Z(l) \left|0\right\rangle_L \left\langle 0\right|_L (X(k)Z(l))^\dagger \right) U_x \\ &= \sum_{k,l} p_{ixjz} X(k)Z(l) U_x \left|0\right\rangle_L \left\langle 0\right|_L U_x (X(k)Z(l))^\dagger = W_x. \end{aligned} \tag{6.48}$$

Proving $W_x = U_x \bar{W} U_x$. We conclude that the channel is symmetric.

To prove that the code is quasi-perfect, we need to show that $\mathcal{E}_0^\bullet(t,\mu)$ and $\mathcal{E}_1^\bullet(t,\mu)$ defined as:

$$\mathcal{E}_0^\bullet(t,\mu) = \{W_0 - t\mu > 0\} = \left\{ \sum_{k,l} p_{ixjz} X(k)Z(l) \left|0\right\rangle_L \left\langle 0\right|_L (X(k)Z(l))^\dagger - t\mu > 0 \right\}, \tag{6.49}$$

$$\mathcal{E}_1^\bullet(t,\mu) = \{W_1 - t\mu > 0\} = \left\{ \sum_{k,l} p_{ixjz} X(k)Z(l) \left|1\right\rangle_L \left\langle 1\right|_L (X(k)Z(l))^\dagger - t\mu > 0 \right\}. \tag{6.50}$$

are orthogonal, and that $\mathcal{E}_0(t,\mu) + \mathcal{E}_1(t,\mu) = cI$, where $c \in \mathbb{R}$, $c > 0$ and:

$$\mathcal{E}_0(t,\mu) = \{W_0 - t\mu \geq 0\}, \tag{6.51}$$

$$\mathcal{E}_1(t,\mu) = \{W_1 - t\mu \geq 0\}. \tag{6.52}$$

The proof is provided in Appendix 6.A. The error probability of the code obtained by using the optimum POVM to directly measure the quantum state is given in (6.92). We can also check that the error correction procedure degrades the error probability, as shown in (6.147).

This section shows how it is possible to prove that an error correction code is quasi-perfect and thus optimum for discriminating between states, even though the analysis is particular for each case. We also show that the error correction procedure may introduce a degradation to the error probability when discriminating between two or more quantum states, since error correction focuses on recovering the original quantum state rather than on optimizing the code and the associated POVM in order to distinguish states in a classical-quantum channel.

In general, it is not trivial to show that a particular code is quasi-perfect, and even in the 5-qubit example that has been presented here it has been necessary to make a strong assumption to show that the code satisfies the symmetry condition. However, this shows that the theory presented in the previous sections can be used in practical schemes and may be worth exploring its application to error correction and not only to state discrimination.

Appendix

6.A Analysis of the 5-qubit stabilizer code

With some abuse of notation we will write $\mathcal{E}_x = \mathcal{E}_x(t,\mu)$ and $\mathcal{E}_x^\bullet = \mathcal{E}_x^\bullet(t,\mu)$. Let's take $\mu = \frac{I}{32}$ and $t = t_0$. The value of t_0 that proves that the code is quasi-perfect depends on the eigenvalues of the matrix W_0 (the matrix W_1 has also the same eigenvalues). Define the following values:

$$\begin{aligned}\lambda_1 &= p_{0x2z} + p_{p0x3z} + 3p_{2x1z} + 7p_{2x2z} + 7p_{2x3z} + 3p_{2x4z} + p_{4x0z} + 2p_{p4x1} + 2p_{4x2z} \\ &\quad + 2p_{4x3z} + 2p_{4x4z} + p_{4x5z}, \qquad (6.53)\\ \lambda_2 &= p_{0x2z} + p_{0x3z} + p_{2x0z} + 4p_{2x1z} + 5p_{2x2z} + 5p_{2x3z} + 4p_{2x4z} + p_{2x5z} + p_{4x1z} \\ &\quad + 4p_{4x2z} + 4p_{4x3z} + p_{4x4z}, \qquad (6.54)\\ \lambda_3 &= p_{0x1z} + p_{0x4z} + p_{2x0z} + 2p_{2x1z} + 7p_{2x2z} + 7p_{2x3z} + 2p_{2x4z} + p_{2x5z} + 2p_{4x1z} \\ &\quad + 3p_{4x2z} + 3p_{4x3z} + 2p_{4x4z}, \qquad (6.55)\\ \lambda_4 &= p_{0x0z} + p_{0x5z} + 5p_{2x1z} + 5p_{2x2z} + 5p_{2x3z} + 5p_{2x4z} + 5p_{4x2z} + 5p_{4x3z}, \qquad (6.56)\\ \lambda_5 &= 5p_{1x2z} + 5p_{1x3z} + 5p_{3x1z} + 5p_{3x2z} + 5p_{3x3z} + 5p_{3x4z} + p_{5x0z} + p_{5x5z}, \qquad (6.57)\\ \lambda_6 &= p_{1x1z} + 4p_{1x2z} + 4p_{1x3z} + p_{1x4z} + p_{3x0z} + 4p_{3x1z} + 5p_{3x2z} + 5p_{3x3z} + 4p_{3x4z} \\ &\quad + p_{3x5z} + p_{5x2z} + p_{5x3z}, \qquad (6.58)\\ \lambda_7 &= 2p_{1x1z} + 3p_{1x2z} + 3p_{1x3z} + 2p_{1x4z} + p_{3x0z} + 2p_{3x1z} + 7p_{3x2z} + 7p_{3x3z} + 2p_{3x4z} \\ &\quad + p_{3x5z} + p_{5x1z} + p_{5x4z}, \qquad (6.59)\\ \lambda_8 &= p_{1x0z} + 2p_{1x1z} + 2p_{1x2z} + 2p_{1x3z} + 2p_{1x4z} + p_{1x5z} + 3p_{3x1z} + 7p_{3x2z} + 7p_{3x3z} \\ &\quad + 3p_{3x4z} + p_{5x2z} + p_{5x3z}. \qquad (6.60)\end{aligned}$$

The eigenvalues of the W_0 matrix are λ_5 and λ_4 with multiplicity 1 and λ_1,λ_2,λ_3, λ_6, λ_7 and λ_8 with multiplicity 5. Consider $\lambda_{i_1} \geq \lambda_{i_2} \geq \lambda_{i_3} \geq \lambda_{i_4} \geq \lambda_{i_5} \geq \lambda_{i_6} \geq \lambda_{i_7} \geq \lambda_{i_8}$, $\lambda_{i_j} \in \{\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6, \lambda_7, \lambda_8\}$, $j \in \{1,2,3,4,5,6,7,8\}$. Then, we choose $t_0 = 32\left(\frac{\lambda_{4_i} + \lambda_{5_i}}{2}\right)$ in

order to take half of the eigenvalues of the original matrix W_0 when calculating $\{W_0 - t_0 \frac{I}{32} \geq 0\}$. Then, we obtain that $\mathcal{E}_0^\bullet = \mathcal{E}_0$ and $\mathcal{E}_1^\bullet = \mathcal{E}_1$ with:

$$\mathcal{E}_0^\bullet = \frac{1}{16} \begin{pmatrix}
11 & 0 & 0 & -3 & 0 & -1 & -3 & 0 & 0 & -1 & -1 & 0 & -3 & 0 & 0 & 1 & 0 & -3 & -1 & 0 & -1 & 0 & 0 & 1 & -3 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 5 & -3 & 0 & 1 & 0 & 0 & -3 & 1 & 0 & 0 & -1 & 0 & 3 & 1 & 0 & -3 & 0 & 0 & 1 & 0 & -1 & -1 & 0 & 0 & -3 & -1 & 0 & 1 & 0 & 0 & -1 \\
0 & -3 & 5 & 0 & -3 & 0 & 0 & 1 & 1 & 0 & 0 & -1 & 0 & -1 & -3 & 0 & 1 & 0 & 0 & -3 & 0 & -1 & -1 & 0 & 0 & 1 & 3 & 0 & 1 & 0 & 0 & -1 \\
-3 & 0 & 0 & 11 & 0 & -3 & -1 & 0 & 0 & 1 & 1 & 0 & -1 & 0 & 0 & 3 & 0 & -1 & -3 & 0 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 3 & 0 & -1 & -1 & 0 \\
0 & 1 & -3 & 0 & 5 & 0 & 0 & -3 & -3 & 0 & 0 & -1 & 0 & -1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 3 & -1 & 0 & 0 & 1 & -1 & 0 & -3 & 0 & 0 & -1 \\
-1 & 0 & 0 & -3 & 0 & 11 & -3 & 0 & 0 & 3 & -1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & -1 & 0 & 3 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & -3 & 1 & 0 \\
-3 & 0 & 0 & -1 & 0 & -3 & 11 & 0 & 0 & 1 & -3 & 0 & -1 & 0 & 0 & -1 & 0 & -1 & 1 & 0 & 1 & 0 & 0 & 3 & -1 & 0 & 0 & -1 & 0 & -1 & 3 & 0 \\
0 & -3 & 1 & 0 & -3 & 0 & 0 & 5 & 1 & 0 & 0 & 3 & 0 & -1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & -1 & 3 & 0 & 0 & 1 & -1 & 0 & 1 & 0 & 0 & 3 \\
0 & 1 & 1 & 0 & -3 & 0 & 0 & 1 & 5 & 0 & 0 & 3 & 0 & -1 & -3 & 0 & -3 & 0 & 0 & 1 & 0 & -1 & -1 & 0 & 0 & -3 & -1 & 0 & 1 & 0 & 0 & -1 \\
-1 & 0 & 0 & 1 & 0 & 3 & 1 & 0 & 0 & 11 & 3 & 0 & 1 & 0 & 0 & -3 & 0 & -3 & -1 & 0 & -1 & 0 & 0 & 1 & -3 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
-1 & 0 & 0 & 1 & 0 & -1 & -3 & 0 & 0 & 3 & 11 & 0 & -3 & 0 & 0 & 1 & 0 & 1 & 3 & 0 & -1 & 0 & 0 & 1 & 1 & 0 & 0 & -3 & 0 & 1 & 1 & 0 \\
0 & -1 & -1 & 0 & -1 & 0 & 0 & 3 & 3 & 0 & 0 & 5 & 0 & -3 & -1 & 0 & -1 & 0 & 0 & 3 & 0 & 1 & 1 & 0 & 0 & -1 & -3 & 0 & -1 & 0 & 0 & 1 \\
-3 & 0 & 0 & -1 & 0 & 1 & -1 & 0 & 0 & 1 & -3 & 0 & 11 & 0 & 0 & 3 & 0 & -1 & 1 & 0 & -3 & 0 & 0 & -1 & -1 & 0 & 0 & -1 & 0 & 3 & -1 & 0 \\
0 & 3 & -1 & 0 & -1 & 0 & 0 & -1 & -1 & 0 & 0 & -3 & 0 & 5 & 3 & 0 & -1 & 0 & 0 & -1 & 0 & -3 & 1 & 0 & 0 & -1 & 1 & 0 & 3 & 0 & 0 & 1 \\
0 & 1 & -3 & 0 & 1 & 0 & 0 & 1 & -3 & 0 & 0 & -1 & 0 & 3 & 5 & 0 & 1 & 0 & 0 & 1 & 0 & -1 & 3 & 0 & 0 & 1 & -1 & 0 & 1 & 0 & 0 & 3 \\
1 & 0 & 0 & 3 & 0 & 1 & -1 & 0 & 0 & -3 & 1 & 0 & 3 & 0 & 0 & 11 & 0 & -1 & 1 & 0 & 1 & 0 & 0 & 3 & -1 & 0 & 0 & -1 & 0 & -1 & 3 & 0 \\
0 & -3 & 1 & 0 & 1 & 0 & 0 & 1 & -3 & 0 & 0 & -1 & 0 & -1 & 1 & 0 & 5 & 0 & 0 & -3 & 0 & -1 & 3 & 0 & 0 & 1 & -1 & 0 & -3 & 0 & 0 & -1 \\
-3 & 0 & 0 & -1 & 0 & 1 & -1 & 0 & 0 & -3 & 1 & 0 & -1 & 0 & 0 & -1 & 0 & 11 & -3 & 0 & 1 & 0 & 0 & 3 & -1 & 0 & 0 & -1 & 0 & 3 & -1 & 0 \\
-1 & 0 & 0 & -3 & 0 & -1 & 1 & 0 & 0 & -3 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & -3 & 11 & 0 & 3 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & -3 & 0 \\
0 & 1 & -3 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 3 & 0 & -1 & 1 & 0 & -3 & 0 & 0 & 5 & 0 & 3 & -1 & 0 & 0 & 1 & -1 & 0 & 1 & 0 & 0 & 3 \\
-1 & 0 & 0 & 1 & 0 & 3 & 1 & 0 & 0 & -1 & -1 & 0 & -3 & 0 & 0 & 1 & 0 & 1 & 3 & 0 & 11 & 0 & 0 & -3 & -3 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & -1 & -1 & 0 & 3 & 0 & 0 & -1 & -1 & 0 & 0 & 1 & 0 & -3 & -1 & 0 & -1 & 0 & 0 & 3 & 0 & 5 & -3 & 0 & 0 & 3 & 1 & 0 & -1 & 0 & 0 & 1 \\
0 & -1 & -1 & 0 & -1 & 0 & 0 & 3 & -1 & 0 & 0 & 1 & 0 & 1 & 3 & 0 & 3 & 0 & 0 & -1 & 0 & -3 & 5 & 0 & 0 & -1 & -3 & 0 & -1 & 0 & 0 & 1 \\
1 & 0 & 0 & -1 & 0 & 1 & 3 & 0 & 0 & 1 & 1 & 0 & -1 & 0 & 0 & 3 & 0 & 3 & 1 & 0 & -3 & 0 & 0 & 11 & -1 & 0 & 0 & 3 & 0 & -1 & -1 & 0 \\
-3 & 0 & 0 & -1 & 0 & 1 & -1 & 0 & 0 & -3 & 1 & 0 & -1 & 0 & 0 & -1 & 0 & -1 & 1 & 0 & -3 & 0 & 0 & -1 & 11 & 0 & 0 & 3 & 0 & -1 & 3 & 0 \\
0 & -3 & 1 & 0 & 1 & 0 & 0 & 1 & -3 & 0 & 0 & -1 & 0 & -1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 3 & -1 & 0 & 0 & -1 & 0 & 0 & 3 & 0 & 0 & 3 \\
0 & -1 & 3 & 0 & -1 & 0 & 0 & -1 & -1 & 0 & 0 & -3 & 0 & 1 & -1 & 0 & -1 & 0 & 0 & -1 & 0 & 1 & -3 & 0 & 0 & 3 & 5 & 0 & 3 & 0 & 0 & 1 \\
1 & 0 & 0 & 3 & 0 & 1 & -1 & 0 & 0 & 1 & -3 & 0 & -1 & 0 & 0 & -1 & 0 & -1 & 1 & 0 & 1 & 0 & 0 & 3 & 3 & 0 & 0 & 11 & 0 & 3 & -1 & 0 \\
0 & 1 & 1 & 0 & -3 & 0 & 0 & 1 & 1 & 0 & 0 & -1 & 0 & 3 & 1 & 0 & -3 & 0 & 0 & 1 & 0 & -1 & -1 & 0 & 0 & 1 & 3 & 0 & 5 & 0 & 0 & 3 \\
1 & 0 & 0 & -1 & 0 & -3 & -1 & 0 & 0 & 1 & -3 & 0 & -1 & 0 & 0 & 3 & 1 & 0 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 3 & 0 & 0 & 11 & 3 & 0 \\
1 & 0 & 0 & -1 & 0 & 1 & 3 & 0 & 0 & 1 & 1 & 0 & -1 & 0 & 0 & 3 & 0 & -1 & -3 & 0 & 1 & 0 & 0 & -1 & 3 & 0 & 0 & -1 & 0 & 3 & 11 & 0 \\
0 & -1 & -1 & 0 & -1 & 0 & 0 & 3 & -1 & 0 & 0 & 1 & 0 & 1 & 3 & 0 & -1 & 0 & 0 & 3 & 0 & 1 & 1 & 0 & 0 & 3 & 1 & 0 & 3 & 0 & 0 & 5
\end{pmatrix}, \tag{6.61}$$

$$\mathcal{E}_1^\bullet = \frac{1}{16} \begin{pmatrix}
5 & 0 & 0 & 3 & 0 & 1 & 3 & 0 & 0 & 1 & 1 & 0 & 3 & 0 & 0 & -1 & 0 & 3 & 1 & 0 & 1 & 0 & 0 & -1 & 3 & 0 & 0 & -1 & 0 & -1 & -1 & 0 \\
0 & 11 & 3 & 0 & -1 & 0 & 0 & 3 & -1 & 0 & 0 & 1 & 0 & -3 & -1 & 0 & 3 & 0 & 0 & -1 & 0 & 1 & 1 & 0 & 0 & 3 & 1 & 0 & -1 & 0 & 0 & 1 \\
0 & 3 & 11 & 0 & 3 & 0 & 0 & -1 & -1 & 0 & 0 & 1 & 0 & 1 & 3 & 0 & -1 & 0 & 0 & 3 & 0 & 1 & 1 & 0 & 0 & -1 & -3 & 0 & -1 & 0 & 0 & 1 \\
3 & 0 & 0 & 5 & 0 & 3 & 1 & 0 & 0 & -1 & -1 & 0 & 1 & 0 & 0 & -3 & 0 & 1 & 3 & 0 & -1 & 0 & 0 & 1 & 1 & 0 & 0 & -3 & 0 & 1 & 1 & 0 \\
0 & -1 & 3 & 0 & 11 & 0 & 0 & 3 & 3 & 0 & 0 & 1 & 0 & 1 & -1 & 0 & -1 & 0 & 0 & -1 & 0 & -3 & 1 & 0 & 0 & -1 & 1 & 0 & 3 & 0 & 0 & 1 \\
1 & 0 & 0 & 3 & 0 & 5 & 3 & 0 & 0 & -3 & 1 & 0 & -1 & 0 & 0 & -1 & 0 & -1 & 1 & 0 & -3 & 0 & 0 & -1 & -1 & 0 & 0 & -1 & 0 & 3 & -1 & 0 \\
3 & 0 & 0 & 1 & 0 & 3 & 5 & 0 & 0 & -1 & 3 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & -1 & 0 & -1 & 0 & 0 & -3 & 1 & 0 & 0 & 1 & 0 & 1 & -3 & 0 \\
0 & 3 & -1 & 0 & 3 & 0 & 0 & 11 & -1 & 0 & 0 & -3 & 0 & 1 & -1 & 0 & -1 & 0 & 0 & -1 & 0 & 1 & -3 & 0 & 0 & -1 & 1 & 0 & -1 & 0 & 0 & -3 \\
0 & -1 & -1 & 0 & 3 & 0 & 0 & -1 & 11 & 0 & 0 & -3 & 0 & 1 & 3 & 0 & 3 & 0 & 0 & -1 & 0 & 1 & 1 & 0 & 0 & 3 & 1 & 0 & -1 & 0 & 0 & 1 \\
1 & 0 & 0 & -1 & 0 & -3 & -1 & 0 & 0 & 5 & -3 & 0 & -1 & 0 & 0 & 3 & 0 & 3 & 1 & 0 & 1 & 0 & 0 & -1 & 3 & 0 & 0 & -1 & 0 & -1 & -1 & 0 \\
1 & 0 & 0 & -1 & 0 & 1 & 3 & 0 & 0 & -3 & 5 & 0 & 3 & 0 & 0 & -1 & 0 & -1 & -3 & 0 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 3 & 0 & -1 & -1 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & -3 & -3 & 0 & 0 & 11 & 0 & 3 & 1 & 0 & 1 & 0 & 0 & -3 & 0 & -1 & -1 & 0 & 0 & 1 & 3 & 0 & 1 & 0 & 0 & -1 \\
3 & 0 & 0 & 1 & 0 & -1 & 1 & 0 & 0 & -1 & 3 & 0 & 5 & 0 & 0 & -3 & 0 & 1 & -1 & 0 & 3 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & -3 & 1 & 0 \\
0 & -3 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 3 & 0 & 11 & -3 & 0 & 1 & 0 & 0 & 1 & 0 & 3 & -1 & 0 & 0 & 1 & -1 & 0 & -3 & 0 & 0 & -1 \\
0 & -1 & 3 & 0 & -1 & 0 & 0 & -1 & 3 & 0 & 0 & 1 & 0 & -3 & 11 & 0 & -1 & 0 & 0 & -1 & 0 & 1 & -3 & 0 & 0 & -1 & 1 & 0 & -1 & 0 & 0 & -3 \\
-1 & 0 & 0 & -3 & 0 & -1 & 1 & 0 & 0 & 3 & -1 & 0 & -3 & 0 & 0 & 5 & 0 & 1 & -1 & 0 & -1 & 0 & 0 & -3 & 1 & 0 & 0 & 1 & 0 & 1 & -3 & 0 \\
0 & 3 & -1 & 0 & -1 & 0 & 0 & -1 & 3 & 0 & 0 & 1 & 0 & 1 & -1 & 0 & 11 & 0 & 0 & 3 & 0 & 1 & -3 & 0 & 0 & -1 & 1 & 0 & 3 & 0 & 0 & 1 \\
3 & 0 & 0 & 1 & 0 & -1 & 1 & 0 & 0 & 3 & -1 & 0 & 1 & 0 & 0 & 1 & 0 & 5 & 3 & 0 & -1 & 0 & 0 & -3 & 1 & 0 & 0 & 1 & 0 & -3 & 1 & 0 \\
1 & 0 & 0 & 3 & 0 & 1 & -1 & 0 & 0 & -3 & 1 & 0 & 3 & 0 & 0 & 11 & 0 & -1 & 1 & 0 & 1 & 0 & 0 & 3 & -1 & 0 & 0 & -1 & 0 & -1 & 3 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & -3 & -3 & 0 & 0 & 11 & 0 & 3 & 1 & 0 & 1 & 0 & 0 & -3 & 0 & -1 & -1 & 0 & 0 & 1 & 3 & 0 & 1 & 0 & 0 & -1 \\
3 & 0 & 0 & 1 & 0 & -1 & 1 & 0 & 0 & -1 & 3 & 0 & 5 & 0 & 0 & -3 & 0 & 1 & -1 & 0 & 3 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & -3 & 1 & 0 \\
0 & -3 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 3 & 0 & 11 & -3 & 0 & 1 & 0 & 0 & 1 & 0 & 3 & -1 & 0 & 0 & 1 & -1 & 0 & -3 & 0 & 0 & -1 \\
0 & -1 & 3 & 0 & -1 & 0 & 0 & -1 & 3 & 0 & 0 & 1 & 0 & -3 & 11 & 0 & -1 & 0 & 0 & -1 & 0 & 1 & -3 & 0 & 0 & -1 & 1 & 0 & -1 & 0 & 0 & -3 \\
-1 & 0 & 0 & -3 & 0 & -1 & 1 & 0 & 0 & 3 & -1 & 0 & -3 & 0 & 0 & 5 & 0 & 1 & -1 & 0 & -1 & 0 & 0 & -3 & 1 & 0 & 0 & 1 & 0 & 1 & -3 & 0 \\
0 & 3 & -1 & 0 & -1 & 0 & 0 & -1 & 3 & 0 & 0 & 1 & 0 & 1 & -1 & 0 & 11 & 0 & 0 & 3 & 0 & 1 & -3 & 0 & 0 & -1 & 1 & 0 & 3 & 0 & 0 & 1 \\
3 & 0 & 0 & 1 & 0 & -1 & 1 & 0 & 0 & 3 & -1 & 0 & 1 & 0 & 0 & 1 & 0 & 5 & 3 & 0 & -1 & 0 & 0 & -3 & 1 & 0 & 0 & 1 & 0 & -3 & 1 & 0 \\
1 & 0 & 0 & 3 & 0 & 1 & -1 & 0 & 0 & -3 & 1 & 0 & 3 & 0 & 0 & 11 & 0 & -1 & 1 & 0 & 1 & 0 & 0 & 3 & -1 & 0 & 0 & -1 & 0 & -1 & 3 & 0 \\
0 & 1 & 1 & 0 & -3 & 0 & 0 & 1 & 1 & 0 & 0 & -1 & 0 & 3 & 1 & 0 & -3 & 0 & 0 & 1 & 0 & -1 & -1 & 0 & 0 & 1 & 3 & 0 & 5 & 0 & 0 & 3 \\
1 & 0 & 0 & -1 & 0 & -3 & -1 & 0 & 0 & 1 & -3 & 0 & -1 & 0 & 0 & 3 & 1 & 0 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 3 & 0 & 0 & 11 & 3 & 0 \\
1 & 0 & 0 & -1 & 0 & 1 & 3 & 0 & 0 & 1 & 1 & 0 & -1 & 0 & 0 & 3 & 0 & -1 & -3 & 0 & 1 & 0 & 0 & -1 & 3 & 0 & 0 & -1 & 0 & 3 & 11 & 0 \\
0 & -1 & -1 & 0 & -1 & 0 & 0 & 3 & -1 & 0 & 0 & 1 & 0 & 1 & 3 & 0 & -1 & 0 & 0 & 3 & 0 & 1 & 1 & 0 & 0 & 3 & 1 & 0 & 3 & 0 & 0 & 5
\end{pmatrix}. \tag{6.62}$$

And using (6.61) and (6.62) we check that $\mathcal{E}_0 + \mathcal{E}_1 = I$ and $\mathcal{E}_0^\bullet$, $\mathcal{E}_1^\bullet$ are orthogonal, proving that the 5-qubit code is also quasi-perfect for the Pauli channel. The optimum error probability of the code can be obtained by using $P_e(\mathcal{C}) = 1 - F_\bullet(t,\mu) + t\left(G_\bullet(t,\mu) - \frac{1}{M}\right)$, where $\frac{1}{M} = \frac{1}{2}$, $G_\bullet(t,\mu) = \mathrm{Tr}(\mu\mathcal{E}_0^\bullet) = \frac{1}{2}$ and $F_\bullet(t,\mu) = \mathrm{Tr}(W_0\mathcal{E}_0^\bullet(t,\mu))$.

Define:

$$A_0 = \frac{p_{0x0z} + 5p_{0x1z} + 10p_{0x2z} + 10p_{0x3z} + 3p_{0x4z} + p_{0x5z}}{16}, \tag{6.63}$$

$$A_1 = \frac{5p_{1x0z} + 25p_{1x1z} + 50p_{1x2z} + 50p_{1x3z} + 25p_{1x4z} + 5p_{1x5z}}{16}, \tag{6.64}$$

$$A_2 = \frac{10p_{2x0z} + 50p_{2x1z} + 100p_{2x2z} + 100p_{2x3z} + 50p_{2x4z} + 10p_{2x5z}}{16}, \tag{6.65}$$

$$A_3 = \frac{10p_{3x0z} + 50p_{3x1z} + 100p_{3x2z} + 100p_{3x3z} + 50p_{3x4z} + 10p_{3x5z}}{16}, \tag{6.66}$$

$$A_4 = \frac{5p_{4x0z} + 25p_{4x1z} + 50p_{4x2z} + 50p_{4x3z} + 25p_{4x4z} + 5p_{4x5z}}{16}, \tag{6.67}$$

$$A_5 = \frac{p_{5x0z} + 5p_{5x1z} + 10p_{5x2z} + 10p_{5x3z} + 3p_{5x4z} + p_{5x5z}}{16}, \tag{6.68}$$

$$B_0 = \frac{p_{0x0z} + p_{0x1z} - 2p_{0x2z} - 2p_{0x3z} + p_{0x4z} + p_{0x5z}}{16}, \tag{6.69}$$

$$B_1 = \frac{3p_{1x0z} + 3p_{1x1z} - 6p_{1x2z} - 6p_{1x3z} + 3p_{1x4z} + 3p_{1x5z}}{16}, \tag{6.70}$$

$$B_2 = \frac{2p_{2x0z} + 2p_{2x1z} - 4p_{2x2z} - 4p_{2x3z} + 2p_{2x4z} + 2p_{2x5z}}{16}, \tag{6.71}$$

$$B_3 = \frac{2p_{3x0z} + 2p_{3x1z} - 4p_{3x2z} - 4p_{3x3z} + 2p_{3x4z} + 2p_{3x5z}}{16}, \tag{6.72}$$

$$B_4 = \frac{3p_{4x0z} + 3p_{4x1z} - 6p_{4x2z} - 6p_{4x3z} + 3p_{4x4z} + 3p_{4x5z}}{16}, \tag{6.73}$$

$$B_5 = \frac{p_{5x0z} + p_{5x1z} - 2p_{5x2z} - 2p_{5x3z} + p_{5x4z} + p_{5x5z}}{16}, \tag{6.74}$$

$$C_0 = \frac{p_{0x0z} - 3p_{0x1z} + 2p_{0x2z} + 2p_{0x3z} - 3p_{0x4z} + p_{0x5z}}{16}, \tag{6.75}$$

$$C_1 = \frac{p_{1x0z} + p_{1x1z} - 2p_{1x2z} - 2p_{1x3z} + p_{1x4z} + p_{1x5z}}{16}, \tag{6.76}$$

$$C_2 = \frac{2p_{2x0z} - 6p_{2x1z} + 4p_{2x2z} + 4p_{2x3z} - 6p_{2x4z} + 2p_{2x5z}}{16}, \tag{6.77}$$

$$C_3 = \frac{2p_{3x0z} - 6p_{3x1z} + 4p_{3x2z} + 4p_{3x3z} - 6p_{3x4z} + 2p_{3x5z}}{16}, \tag{6.78}$$

$$C_4 = \frac{p_{4x0z} + p_{4x1z} - 2p_{4x2z} - 2p_{4x3z} + p_{4x4z} + p_{4x5z}}{16}, \tag{6.79}$$

$$C_5 = \frac{p_{5x0z} - 3p_{5x1z} + 2p_{5x2z} + 2p_{5x3z} - 3p_{5x4z} + p_{5x5z}}{16}, \tag{6.80}$$

$$D_1 = \frac{p_{1x0z} - 3p_{1x1z} + 2p_{1x2z} + 2p_{1x3z} - 3p_{1x4z} + p_{1x5z}}{16}, \tag{6.81}$$

$$D_4 = \frac{p_{4x0z} - 3p_{4x1z} + 2p_{4x2z} + 2p_{4x3z} - 3p_{4x4z} + p_{4x5z}}{16}, \tag{6.82}$$

$$x_1 = A_0 + A_2 + A_4, \tag{6.83}$$

$$x_2 = B_0 + B_2 - B_4, \tag{6.84}$$

$$x_3 = B_0 - B_2 + C_4, \tag{6.85}$$

$$x_4 = C_0 - C_2 + D_4, \tag{6.86}$$

$$x_5 = A_1 + A_3 + A_5, \tag{6.87}$$

$$x_6 = B_1 - B_3 - B_5, \tag{6.88}$$

$$x_7 = C_1 - B_3 + B_5, \tag{6.89}$$

$$x_8 = D_1 - C_3 + C_5. \tag{6.90}$$

The matrix W_0 can be expressed as:

$$W_0 = \begin{pmatrix}
x_1 & 0 & 0 & -x_2 & 0 & x_3 & -x_2 & 0 & 0 & x_3 & x_3 & 0 & -x_2 & 0 & 0 & -x_4 & 0 & -x_2 & x_3 & 0 & x_3 & 0 & 0 & -x_4 & -x_2 & 0 & 0 & -x_4 & 0 & -x_4 & -x_4 & 0 \\
0 & x_5 & -x_6 & 0 & x_7 & 0 & 0 & -x_6 & x_7 & 0 & 0 & -x_7 & 0 & x_6 & x_8 & 0 & -x_6 & 0 & 0 & x_7 & 0 & -x_7 & -x_8 & 0 & 0 & -x_6 & -x_8 & 0 & x_8 & 0 & 0 & -x_8 \\
0 & -x_6 & x_5 & 0 & -x_6 & 0 & 0 & x_7 & x_7 & 0 & 0 & -x_7 & 0 & -x_8 & -x_6 & 0 & x_7 & 0 & 0 & -x_6 & 0 & -x_8 & -x_7 & 0 & 0 & x_8 & x_6 & 0 & x_8 & 0 & 0 & -x_8 \\
-x_2 & 0 & 0 & x_1 & 0 & -x_2 & x_3 & 0 & 0 & -x_3 & -x_3 & 0 & x_4 & 0 & 0 & x_2 & 0 & x_3 & -x_2 & 0 & -x_4 & 0 & 0 & x_3 & x_4 & 0 & 0 & x_2 & 0 & x_4 & x_4 & 0 \\
0 & x_7 & -x_6 & 0 & x_5 & 0 & 0 & -x_6 & -x_6 & 0 & 0 & -x_8 & 0 & -x_7 & x_7 & 0 & x_7 & 0 & 0 & x_8 & 0 & x_6 & -x_7 & 0 & 0 & x_8 & -x_8 & 0 & -x_6 & 0 & 0 & -x_8 \\
x_3 & 0 & 0 & -x_2 & 0 & x_1 & -x_2 & 0 & 0 & x_2 & x_4 & 0 & -x_3 & 0 & 0 & -x_3 & 0 & -x_3 & x_4 & 0 & x_2 & 0 & 0 & -x_3 & -x_4 & 0 & 0 & -x_4 & 0 & -x_2 & -x_4 & 0 \\
-x_2 & 0 & 0 & x_3 & 0 & -x_2 & x_1 & 0 & 0 & -x_4 & -x_2 & 0 & x_3 & 0 & 0 & x_3 & 0 & x_4 & -x_3 & 0 & -x_3 & 0 & 0 & x_2 & x_4 & 0 & 0 & x_4 & 0 & x_4 & x_2 & 0 \\
0 & -x_6 & x_7 & 0 & -x_6 & 0 & 0 & x_5 & x_8 & 0 & 0 & x_6 & 0 & -x_7 & x_7 & 0 & x_8 & 0 & 0 & x_7 & 0 & -x_7 & x_6 & 0 & 0 & x_8 & -x_8 & 0 & x_8 & 0 & 0 & x_6 \\
0 & x_7 & x_7 & 0 & -x_6 & 0 & 0 & x_8 & x_5 & 0 & 0 & x_6 & 0 & -x_7 & -x_6 & 0 & -x_6 & 0 & 0 & x_8 & 0 & -x_8 & -x_8 & 0 & 0 & -x_6 & -x_7 & 0 & x_7 & 0 & 0 & -x_8 \\
x_3 & 0 & 0 & -x_3 & 0 & x_2 & -x_4 & 0 & 0 & x_1 & x_2 & 0 & -x_3 & 0 & 0 & x_2 & 0 & -x_2 & x_4 & 0 & x_4 & 0 & 0 & -x_4 & -x_2 & 0 & 0 & -x_3 & 0 & -x_3 & -x_4 & 0 \\
x_3 & 0 & 0 & -x_3 & 0 & x_4 & -x_2 & 0 & 0 & x_2 & x_1 & 0 & -x_2 & 0 & 0 & -x_3 & 0 & -x_4 & x_2 & 0 & x_4 & 0 & 0 & -x_4 & -x_3 & 0 & 0 & -x_2 & 0 & -x_4 & -x_3 & 0 \\
0 & -x_7 & -x_7 & 0 & -x_8 & 0 & 0 & x_6 & x_6 & 0 & 0 & x_5 & 0 & -x_6 & -x_7 & 0 & -x_8 & 0 & 0 & x_6 & 0 & x_8 & x_8 & 0 & 0 & -x_7 & -x_6 & 0 & -x_8 & 0 & 0 & x_7 \\
-x_2 & 0 & 0 & x_4 & 0 & -x_3 & x_3 & 0 & 0 & -x_3 & -x_2 & 0 & x_1 & 0 & 0 & x_2 & 0 & x_4 & -x_4 & 0 & -x_2 & 0 & 0 & x_4 & x_3 & 0 & 0 & x_4 & 0 & x_2 & x_3 & 0 \\
0 & x_6 & -x_8 & 0 & -x_7 & 0 & 0 & -x_7 & -x_7 & 0 & 0 & -x_6 & 0 & x_5 & x_6 & 0 & -x_8 & 0 & 0 & -x_8 & 0 & -x_6 & x_8 & 0 & 0 & -x_7 & x_8 & 0 & x_6 & 0 & 0 & x_7 \\
0 & x_8 & -x_6 & 0 & x_7 & 0 & 0 & x_7 & -x_6 & 0 & 0 & -x_7 & 0 & x_6 & x_5 & 0 & x_8 & 0 & 0 & x_8 & 0 & -x_8 & x_6 & 0 & 0 & x_8 & -x_7 & 0 & x_7 & 0 & 0 & x_6 \\
-x_4 & 0 & 0 & x_2 & 0 & -x_3 & x_3 & 0 & 0 & -x_2 & -x_3 & 0 & x_2 & 0 & 0 & x_1 & 0 & x_4 & -x_4 & 0 & -x_4 & 0 & 0 & x_2 & x_4 & 0 & 0 & x_3 & 0 & x_3 & x_2 & 0 \\
0 & -x_6 & x_7 & 0 & x_7 & 0 & 0 & x_8 & -x_6 & 0 & 0 & -x_8 & 0 & -x_8 & x_8 & 0 & x_5 & 0 & 0 & -x_6 & 0 & -x_7 & x_6 & 0 & 0 & x_7 & -x_7 & 0 & -x_6 & 0 & 0 & -x_8 \\
-x_2 & 0 & 0 & x_3 & 0 & -x_3 & x_4 & 0 & 0 & -x_2 & -x_4 & 0 & x_4 & 0 & 0 & x_4 & 0 & x_1 & -x_2 & 0 & -x_3 & 0 & 0 & x_2 & x_3 & 0 & 0 & x_3 & 0 & x_2 & x_4 & 0 \\
x_3 & 0 & 0 & -x_2 & 0 & x_4 & -x_3 & 0 & 0 & x_4 & x_2 & 0 & -x_4 & 0 & 0 & -x_4 & 0 & -x_2 & x_1 & 0 & x_2 & 0 & 0 & -x_3 & -x_3 & 0 & 0 & -x_4 & 0 & -x_4 & -x_2 & 0 \\
0 & x_7 & -x_6 & 0 & x_8 & 0 & 0 & x_7 & x_8 & 0 & 0 & x_6 & 0 & -x_8 & x_8 & 0 & -x_6 & 0 & 0 & x_5 & 0 & x_6 & -x_7 & 0 & 0 & x_7 & -x_7 & 0 & x_8 & 0 & 0 & x_6 \\
x_3 & 0 & 0 & -x_4 & 0 & x_2 & -x_3 & 0 & 0 & x_4 & x_4 & 0 & -x_2 & 0 & 0 & -x_4 & 0 & -x_3 & x_2 & 0 & x_1 & 0 & 0 & -x_2 & -x_2 & 0 & 0 & -x_4 & 0 & -x_3 & -x_3 & 0 \\
0 & -x_7 & -x_8 & 0 & x_6 & 0 & 0 & -x_7 & -x_8 & 0 & 0 & x_8 & 0 & -x_6 & -x_8 & 0 & -x_7 & 0 & 0 & x_6 & 0 & x_5 & -x_6 & 0 & 0 & x_6 & x_8 & 0 & -x_7 & 0 & 0 & x_7 \\
0 & -x_8 & -x_7 & 0 & -x_7 & 0 & 0 & x_6 & -x_8 & 0 & 0 & x_8 & 0 & x_8 & x_6 & 0 & x_6 & 0 & 0 & -x_7 & 0 & -x_6 & x_5 & 0 & 0 & -x_8 & -x_6 & 0 & -x_7 & 0 & 0 & x_7 \\
-x_4 & 0 & 0 & x_3 & 0 & -x_3 & x_2 & 0 & 0 & -x_4 & -x_4 & 0 & x_4 & 0 & 0 & x_2 & 0 & x_2 & -x_3 & 0 & -x_2 & 0 & 0 & x_1 & x_4 & 0 & 0 & x_2 & 0 & x_3 & x_3 & 0 \\
-x_2 & 0 & 0 & x_4 & 0 & -x_4 & x_4 & 0 & 0 & -x_2 & -x_3 & 0 & x_3 & 0 & 0 & x_4 & 0 & x_3 & -x_3 & 0 & -x_2 & 0 & 0 & x_4 & x_1 & 0 & 0 & x_2 & 0 & x_3 & x_2 & 0 \\
0 & -x_6 & x_8 & 0 & x_8 & 0 & 0 & -x_8 & -x_6 & 0 & 0 & -x_7 & 0 & -x_7 & x_8 & 0 & x_7 & 0 & 0 & x_7 & 0 & x_6 & -x_8 & 0 & 0 & x_5 & x_6 & 0 & x_7 & 0 & 0 & x_6 \\
0 & -x_8 & x_6 & 0 & -x_8 & 0 & 0 & -x_8 & -x_7 & 0 & 0 & -x_6 & 0 & x_8 & -x_7 & 0 & -x_7 & 0 & 0 & -x_7 & 0 & x_8 & -x_6 & 0 & 0 & x_6 & x_5 & 0 & x_6 & 0 & 0 & x_7 \\
-x_4 & 0 & 0 & x_2 & 0 & -x_4 & x_4 & 0 & 0 & -x_3 & -x_2 & 0 & x_4 & 0 & 0 & x_3 & 0 & x_3 & -x_3 & 0 & -x_4 & 0 & 0 & x_2 & x_2 & 0 & 0 & x_1 & 0 & x_2 & x_3 & 0 \\
0 & x_8 & x_8 & 0 & -x_6 & 0 & 0 & x_8 & x_7 & 0 & 0 & -x_8 & 0 & x_6 & x_7 & 0 & -x_6 & 0 & 0 & x_8 & 0 & -x_7 & -x_7 & 0 & 0 & x_7 & x_6 & 0 & x_5 & 0 & 0 & x_6 \\
-x_4 & 0 & 0 & x_4 & 0 & -x_2 & x_4 & 0 & 0 & -x_3 & -x_4 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_2 & -x_4 & 0 & -x_3 & 0 & 0 & x_3 & x_3 & 0 & 0 & x_2 & 0 & x_1 & x_2 & 0 \\
-x_4 & 0 & 0 & x_4 & 0 & -x_4 & x_2 & 0 & 0 & -x_4 & -x_3 & 0 & x_3 & 0 & 0 & x_2 & 0 & x_4 & -x_2 & 0 & -x_3 & 0 & 0 & x_3 & x_2 & 0 & 0 & x_3 & 0 & x_2 & x_1 & 0 \\
0 & -x_8 & -x_8 & 0 & -x_8 & 0 & 0 & x_6 & -x_8 & 0 & 0 & x_7 & 0 & x_7 & x_6 & 0 & -x_8 & 0 & 0 & x_6 & 0 & x_7 & x_7 & 0 & 0 & x_6 & x_7 & 0 & x_6 & 0 & 0 & x_5
\end{pmatrix}. \tag{6.91}$$

We then obtain that:

$$P_e(\mathcal{C}) = 1 - \mathrm{Tr}(W_0 \mathcal{E}_0^{\bullet}(t,\mu)) = 1 - (11x_1 + 15x_2 - 5x_3 - 5x_4 + 5x_5 + 15x_6 + 5x_7 + 5x_8)\,. \tag{6.92}$$

With that, we have proved that the optimum error probability for this channel using two input codewords and with the assumption that we've used to prove symmetry has the expression in (6.92) and is satisfied by the codebook in (6.19), (6.20).

Since the code is quasi-perfect, we know that using an optimal POVM to measure the state at the output of the Pauli channel would achieve the optimum error probability. However, we should consider that the error correction procedure of the decoder may include a degradation of the error probability, as mentioned in the analysis for the depolarizing channel case.

In order to obtain the error probability after the error correction procedure, we consider that the decoder is part of the channel as we did for the depolarizing channel (see Figure 6.2). The degradation of the error probability introduced by using error correction is the difference between the error probability with error correction and (6.92).

We define the following projectors:

$$P_1 = \frac{I + S1}{2}, \quad \bar{P}_1 = \frac{I - S1}{2}, \tag{6.93}$$

$$P_2 = \frac{I + S2}{2}, \quad \bar{P}_2 = \frac{I - S2}{2}, \tag{6.94}$$

$$P_3 = \frac{I + S3}{2}, \quad \bar{P}_3 = \frac{I - S3}{2}, \tag{6.95}$$

$$P_4 = \frac{I + S4}{2}, \quad \bar{P}_4 = \frac{I - S4}{2}. \tag{6.96}$$

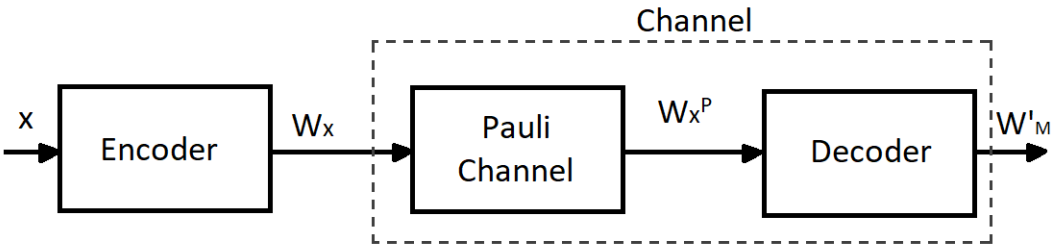

Figure 6.2: Source and channel model

We define the POVM $\mathcal{T} = \{P_1P_2P_3P_4, \bar{P}_1P_2P_3P_4, P_1\bar{P}_2P_3P_4, ..., \bar{P}_1\bar{P}_2\bar{P}_3\bar{P}_4\}$ in order to determine if an error has occurred and to obtain the syndrome. The decoder uses a look-up table in order to obtain the syndrome from the outcome of the measurement, as shown in Table 6.1.

$P_1P_2P_3P_4$	0000	$I \otimes I \otimes I \otimes I \otimes I$
$P_1P_2P_3\bar{P}_4$	0001	$X \otimes I \otimes I \otimes I \otimes I$
$P_1P_2\bar{P}_3P_4$	0010	$I \otimes I \otimes Z \otimes I \otimes I$
$P_1P_2\bar{P}_3\bar{P}_4$	0011	$I \otimes I \otimes I \otimes I \otimes X$
$P_1\bar{P}_2P_3P_4$	0100	$I \otimes I \otimes I \otimes I \otimes Z$
$P_1\bar{P}_2P_3\bar{P}_4$	0101	$I \otimes Z \otimes I \otimes I \otimes I$
$P_1\bar{P}_2\bar{P}_3P_4$	0110	$I \otimes I \otimes I \otimes X \otimes I$
$P_1\bar{P}_2\bar{P}_3\bar{P}_4$	0111	$I \otimes I \otimes I \otimes I \otimes Y$
$\bar{P}_1P_2P_3P_4$	1000	$I \otimes X \otimes I \otimes I \otimes I$
$\bar{P}_1P_2P_3\bar{P}_4$	1001	$I \otimes I \otimes I \otimes Z \otimes I$
$\bar{P}_1P_2\bar{P}_3P_4$	1010	$Z \otimes I \otimes I \otimes I \otimes I$
$\bar{P}_1P_2\bar{P}_3\bar{P}_4$	1011	$Y \otimes I \otimes I \otimes I \otimes I$
$\bar{P}_1\bar{P}_2P_3P_4$	1100	$I \otimes I \otimes X \otimes I \otimes I$
$\bar{P}_1\bar{P}_2P_3\bar{P}_4$	1101	$I \otimes Y \otimes I \otimes I \otimes I$
$\bar{P}_1\bar{P}_2\bar{P}_3P_4$	1110	$I \otimes I \otimes Y \otimes I \otimes I$
$\bar{P}_1\bar{P}_2\bar{P}_3\bar{P}_4$	1111	$I \otimes I \otimes I \otimes Y \otimes I$

Table 6.1: Look-up table that the detector uses for error correction. Left: POVM elements. Center: Corresponding syndrome. Right: Error correction operator that the decoder applies

Let's define a POVM $\mathcal{P} = \{\Pi_0, \Pi_1\}$ consisting of the following projectors in order to measure the state after error correction:

$$\Pi_0 = 16\,\mathrm{diag}(|0_L\rangle\langle 0_L|), \tag{6.97}$$

$$\Pi_1 = 16\,\mathrm{diag}(|1_L\rangle\langle 1_L|). \tag{6.98}$$

Where $\Pi_0 + \Pi_1 = I$ is satisfied because of the orthogonality between Π_0 and Π_1. Notice that $\mathrm{Tr}(\Pi_0 |0_L\rangle \langle 0_L|) = 1$, $\mathrm{Tr}(\Pi_0 |1_L\rangle \langle 1_L|) = 0$, $\mathrm{Tr}(\Pi_1 |0_L\rangle \langle 0_L|) = 0$ and $\mathrm{Tr}(\Pi_1 |1_L\rangle \langle 1_L|) = 1$. It is possible to check that the Yuen-Kennedy-Lax conditions are satisfied by this POVM:

$$(\Lambda(\mathcal{P}) - \frac{1}{M}W_0)\Pi_0 = \frac{1}{M}(W_0\Pi_0 + W_1\Pi_1\Pi_0 - W_0\Pi_0) = 0, \tag{6.99}$$

$$(\Lambda(\mathcal{P}) - \frac{1}{M}W_1)\Pi_1 = \frac{1}{M}(W_0\Pi_0\Pi_1 + W_1\Pi_1 - W_1\Pi_1) = 0, \tag{6.100}$$

$$\Lambda(\mathcal{P}) - \frac{1}{M}W_0 = \frac{1}{M}(W_0\Pi_0 + W_1\Pi_1) - \frac{1}{M}W_0 = \frac{1}{M}(W_1\Pi_1 - W_0\Pi_1), \tag{6.101}$$

$$\Lambda(\mathcal{P}) - \frac{1}{M}W_1 = \frac{1}{M}(W_0\Pi_0 + W_1\Pi_1) - \frac{1}{M}W_1 = \frac{1}{M}(W_0\Pi_0 - W_1\Pi_0), \tag{6.102}$$

where in the two last equations we used that $W_0\Pi_0 - W_0 = -W_0\Pi_1$ and $W_1\Pi_1 - W_1 = -W_1\Pi_0$. The error probability is the following:

$$P_{e,ec} = \frac{\mathrm{Tr}(W_{0,ec}\Pi_1) + \mathrm{Tr}(W_{1,ec}\Pi_0)}{2} = \mathrm{Tr}(W_{0,ec}\Pi_1), \tag{6.103}$$

where $W_{0,ec}$, $W_{1,ec}$ are states that represent the effect of error correction applied to W_0 and W_1 respectively. To formally define $W_{0,ec}$ and $W_{1,ec}$, we should first consider the effect of the error correction detector to the quantum state in a practical scheme. The state W_x, $x \in \{0, 1\}$ would be measured using the POVM $\mathcal{T}$ in order to obtain the syndrome. This measurement operation would make the state collapse to a state $W_{x_{M_k}}$, $k \in \{0, 1, ..., 15\}$,

with:

$$W_{x_{M_0}} = \frac{P_1P_2P_3P_4W_xP_1P_2P_3P_4}{\mathrm{Tr}(P_1P_2P_3P_4W_x)}, \tag{6.104}$$

$$W_{x_{M_1}} = \frac{P_1P_2P_3\bar{P}_4W_xP_1P_2P_3\bar{P}_4}{\mathrm{Tr}(P_1P_2P_3\bar{P}_4W_x)}, \tag{6.105}$$

$$W_{x_{M_2}} = \frac{P_1P_2\bar{P}_3P_4W_xP_1P_2\bar{P}_3P_4}{\mathrm{Tr}(P_1P_2\bar{P}_3P_4W_x)}, \tag{6.106}$$

$$W_{x_{M_3}} = \frac{P_1P_2\bar{P}_3\bar{P}_4W_xP_1P_2\bar{P}_3\bar{P}_4}{\mathrm{Tr}(P_1P_2\bar{P}_3\bar{P}_4W_x)}, \tag{6.107}$$

$$W_{x_{M_4}} = \frac{P_1\bar{P}_2P_3P_4W_xP_1\bar{P}_2P_3P_4}{\mathrm{Tr}(P_1\bar{P}_2P_3P_4W_x)}, \tag{6.108}$$

$$W_{x_{M_5}} = \frac{P_1\bar{P}_2P_3\bar{P}_4W_xP_1\bar{P}_2P_3\bar{P}_4}{\mathrm{Tr}(P_1\bar{P}_2P_3\bar{P}_4W_x)}, \tag{6.109}$$

$$W_{x_{M_6}} = \frac{P_1\bar{P}_2\bar{P}_3P_4W_xP_1\bar{P}_2\bar{P}_3P_4}{\mathrm{Tr}(P_1\bar{P}_2\bar{P}_3P_4W_x)}, \tag{6.110}$$

$$W_{x_{M_7}} = \frac{P_1\bar{P}_2\bar{P}_3\bar{P}_4W_xP_1\bar{P}_2\bar{P}_3\bar{P}_4}{\mathrm{Tr}(P_1\bar{P}_2\bar{P}_3\bar{P}_4W_x)}, \tag{6.111}$$

$$W_{x_{M_8}} = \frac{\bar{P}_1P_2P_3P_4W_x\bar{P}_1P_2P_3P_4}{\mathrm{Tr}(\bar{P}_1P_2P_3P_4W_x)}, \tag{6.112}$$

$$W_{x_{M_9}} = \frac{\bar{P}_1P_2P_3\bar{P}_4W_x\bar{P}_1P_2P_3\bar{P}_4}{\mathrm{Tr}(\bar{P}_1P_2P_3\bar{P}_4W_x)}, \tag{6.113}$$

$$W_{x_{M_{10}}} = \frac{\bar{P}_1P_2\bar{P}_3P_4W_x\bar{P}_1P_2\bar{P}_3P_4}{\mathrm{Tr}(\bar{P}_1P_2\bar{P}_3P_4W_x)}, \tag{6.114}$$

$$W_{x_{M_{11}}} = \frac{\bar{P}_1P_2\bar{P}_3\bar{P}_4W_x\bar{P}_1P_2\bar{P}_3\bar{P}_4}{\mathrm{Tr}(\bar{P}_1P_2\bar{P}_3\bar{P}_4W_x)}, \tag{6.115}$$

$$W_{x_{M_{12}}} = \frac{\bar{P}_1\bar{P}_2P_3P_4W_x\bar{P}_1\bar{P}_2P_3P_4}{\mathrm{Tr}(\bar{P}_1\bar{P}_2P_3P_4W_x)}, \tag{6.116}$$

$$W_{x_{M_{13}}} = \frac{\bar{P}_1\bar{P}_2P_3\bar{P}_4W_x\bar{P}_1\bar{P}_2P_3\bar{P}_4}{\mathrm{Tr}(\bar{P}_1\bar{P}_2P_3\bar{P}_4W_x)}, \tag{6.117}$$

$$W_{x_{M_{14}}} = \frac{\bar{P}_1\bar{P}_2\bar{P}_3P_4W_x\bar{P}_1\bar{P}_2\bar{P}_3P_4}{\mathrm{Tr}(\bar{P}_1\bar{P}_2\bar{P}_3P_4W_x)}, \tag{6.118}$$

$$W_{x_{M_{15}}} = \frac{\bar{P}_1\bar{P}_2\bar{P}_3\bar{P}_4W_x\bar{P}_1\bar{P}_2\bar{P}_3\bar{P}_4}{\mathrm{Tr}(\bar{P}_1\bar{P}_2\bar{P}_3\bar{P}_4W_x)}. \tag{6.119}$$

The outcome of the measurement is a 4-bit number that indicates the Pauli operator that must be applied to $W_{x_{M_k}}$ according to Table 6.1. For example, if the outcome of the measurement is '0110', then the detector will apply an X operator to the fourth qubit. After this error

correction stage, the states $W_{x_{M_k}}$ become $W'_{x_{M_k}}$ as follows:

$$W'_{x_{M_0}} = W_{x_{M_0}}, \tag{6.120}$$
$$W'_{x_{M_1}} = X_1 W_{x_{M_1}} X_1, \tag{6.121}$$
$$W'_{x_{M_2}} = Z_3 W_{x_{M_2}} Z_3, \tag{6.122}$$
$$W'_{x_{M_3}} = X_5 W_{x_{M_3}} X_5, \tag{6.123}$$
$$W'_{x_{M_4}} = Z_5 W_{x_{M_4}} Z_5, \tag{6.124}$$
$$W'_{x_{M_5}} = Z_2 W_{x_{M_5}} Z_2, \tag{6.125}$$
$$W'_{x_{M_6}} = X_4 W_{x_{M_6}} X_4, \tag{6.126}$$
$$W'_{x_{M_7}} = Y_5 W_{x_{M_6}} Y_5, \tag{6.127}$$
$$W'_{x_{M_8}} = X_2 W_{x_{M_8}} X_2, \tag{6.128}$$
$$W'_{x_{M_9}} = Z_4 W_{x_{M_9}} Z_4, \tag{6.129}$$
$$W'_{x_{M_{10}}} = Z_1 W_{x_{M_{10}}} Z_1, \tag{6.130}$$
$$W'_{x_{M_{11}}} = Y_1 W_{x_{M_{11}}} Y_1, \tag{6.131}$$
$$W'_{x_{M_{12}}} = X_3 W_{x_{M_{12}}} X_3, \tag{6.132}$$
$$W'_{x_{M_{13}}} = Y_2 W_{x_{M_{13}}} Y_2, \tag{6.133}$$
$$W'_{x_{M_{14}}} = Y_3 W_{x_{M_{14}}} Y_3, \tag{6.134}$$
$$W'_{x_{M_{15}}} = Y_4 W_{x_{M_{15}}} Y_4, \tag{6.135}$$

where

$$X_1 = X \otimes I \otimes I \otimes I \otimes I, \quad Z_1 = Z \otimes I \otimes I \otimes I \otimes I, \quad Y_1 = Y \otimes I \otimes I \otimes I \otimes I, \tag{6.136}$$
$$X_2 = I \otimes X \otimes I \otimes I \otimes I, \quad Z_2 = I \otimes Z \otimes I \otimes I \otimes I, \quad Y_2 = I \otimes Y \otimes I \otimes I \otimes I, \tag{6.137}$$
$$X_3 = I \otimes I \otimes X \otimes I \otimes I, \quad Z_3 = I \otimes I \otimes Z \otimes I \otimes I, \quad Y_3 = I \otimes I \otimes Y \otimes I \otimes I, \tag{6.138}$$
$$X_4 = I \otimes I \otimes I \otimes X \otimes I, \quad Z_4 = I \otimes I \otimes I \otimes Z \otimes I, \quad Y_4 = I \otimes I \otimes I \otimes Y \otimes I, \tag{6.139}$$
$$X_5 = I \otimes I \otimes I \otimes I \otimes X, \quad Z_5 = I \otimes I \otimes I \otimes I \otimes Z, \quad Y_5 = I \otimes I \otimes I \otimes I \otimes Y. \tag{6.140}$$

We define $W_{0,ec}$ and $W_{1,ec}$ as the sum of all the possible states $W'_{x_{M_k}}$ resulting from the error measurement operation, weighted by their probability:

$$W_{0,ec} = \sum_{k=0}^{15} p_k W'_{0_{M_k}}, \tag{6.141}$$
$$W_{1,ec} = \sum_{k=0}^{15} p_k W'_{1_{M_k}}, \tag{6.142}$$

where $p_k = \mathrm{Tr}(P_k W_x P_k)$, $P_k \in \mathcal{T}$. The $W_{x,ec}$ states are essentially the expected state at the output of the error correction detector. Then, the probability of error can be obtained by

using (6.103). For each $P_k \in \mathcal{T}$, we have:

$$\begin{aligned}&\mathrm{Tr}(P_1P_2P_3P_4W_0P_1P_2P_3P_4\Pi_1)\\&= 5p_{1x2z} + 5p_{1x3z} + 5p_{3x1z} + 5p_{3x2z} + 5p_{3x3z} + 5p_{3x4z} + 5p_{5x0z} + 5p_{5x5z},\end{aligned} \tag{6.143}$$

$$\begin{aligned}&\mathrm{Tr}(P_1P_2P_3\bar{P}_4W_0P_1P_2P_3\bar{P}_4\Pi_1) = \mathrm{Tr}(P_1P_2\bar{P}_3\bar{P}_4W_0P_1P_2\bar{P}_3\bar{P}_4\Pi_1) = \mathrm{Tr}(P_1\bar{P}_2\bar{P}_3P_4W_0P_1\bar{P}_2\bar{P}_3P_4\Pi_1)\\&= \mathrm{Tr}(\bar{P}_1P_2P_3P_4W_0\bar{P}_1P_2P_3P_4\Pi_1) = \mathrm{Tr}(\bar{P}_1\bar{P}_2P_3P_4W_0\bar{P}_1\bar{P}_2P_3P_4\Pi_1)\\&= p_{0x2z} + p_{0x3z} + 3p_{2x1z} + 7p_{2x2z} + 7p_{2x3z} + 3p_{2x4z} + p_{4x0z}\\&\qquad + 2p_{4x1z} + 2p_{4x2z} + 2p_{4x3z} + 2p_{4x4z} + p_{4x5z},\end{aligned} \tag{6.144}$$

$$\begin{aligned}&\mathrm{Tr}(P_1P_2\bar{P}_3P_4W_0P_1P_2\bar{P}_3P_4\Pi_1) = \mathrm{Tr}(P_1\bar{P}_2P_3P_4W_0P_1\bar{P}_2P_3P_4\Pi_1) = \mathrm{Tr}(P_1\bar{P}_2P_3\bar{P}_4W_0P_1\bar{P}_2P_3\bar{P}_4\Pi_1)\\&= \mathrm{Tr}(\bar{P}_1P_2P_3\bar{P}_4W_0\bar{P}_1P_2P_3\bar{P}_4\Pi_1) = \mathrm{Tr}(\bar{P}_1P_2\bar{P}_3P_4W_0\bar{P}_1P_2\bar{P}_3P_4\Pi_1)\\&= 2p_{1x1z} + 3p_{1x2z} + 3p_{1x3z} + 2p_{1x4z} + p_{3x0z} + 2p_{3x1z} + 7p_{3x2z}\\&\qquad + 7p_{3x3z} + 2p_{3x4z} + p_{3x5z} + p_{5x1z} + p_{5x4z},\end{aligned} \tag{6.145}$$

$$\begin{aligned}&\mathrm{Tr}(P_1\bar{P}_2\bar{P}_3\bar{P}_4W_0P_1\bar{P}_2\bar{P}_3\bar{P}_4\Pi_1) = \mathrm{Tr}(\bar{P}_1P_2\bar{P}_3\bar{P}_4W_0\bar{P}_1P_2\bar{P}_3\bar{P}_4\Pi_1) = \mathrm{Tr}(\bar{P}_1\bar{P}_2P_3\bar{P}_4W_0\bar{P}_1\bar{P}_2P_3\bar{P}_4\Pi_1)\\&= \mathrm{Tr}(\bar{P}_1\bar{P}_2\bar{P}_3P_4W_0\bar{P}_1\bar{P}_2\bar{P}_3P_4\Pi_1) = \mathrm{Tr}(\bar{P}_1\bar{P}_2\bar{P}_3\bar{P}_4W_0\bar{P}_1\bar{P}_2\bar{P}_3\bar{P}_4\Pi_1)\\&= p_{0x2z} + p_{0x3z} + p_{2x0z} + 4p_{2x1z} + 5p_{2x2z} + 5p_{2x3z} + 4p_{2x4z}\\&\qquad + p_{2x5z} + p_{4x1z} + 4p_{4x2z} + 4p_{4x3z} + p_{4x4z}.\end{aligned} \tag{6.146}$$

And the total error probability is:

$$\begin{aligned}P_{e,ec}(\mathcal{C}) = {}& 10p_{0x2z} + 10p_{0x3z} + 10p_{1x1z} + 20p_{1x2z} + 20p_{1x3z} + 10p_{1x4z} + 5p_{2x0z} + 35p_{2x1z}\\&+ 60p_{2x2z} + 60p_{2x3z} + 35p_{2x4z} + 5p_{2x5z} + 5p_{3x0z} + 15p_{3x1z} + 40p_{3x2z} + 40p_{3x3}\\&+ 15p_{3x4z} + 5p_{3x5z} + 5p_{4x0z} + 15p_{4x1z} + 30p_{4x2z} + 30p_{4x3z} + 15p_{4x4z} + 5p_{4x5z}\\&+ p_{5x0z} + 5p_{5x1z} + 5p_{5x4z} + p_{5x5z}.\end{aligned} \tag{6.147}$$

The error probability that is obtained using error correction is larger than the optimum one (i.e. the error probability obtained by directly using a POVM to measure the quantum state). For example, using $p_x = 0.04$ and $p_z = 0.03$, we obtain that $P_{e,ec}(\mathcal{C}) \approx 0.0242$ and $P_e(C) \approx 0.0193$. The degradation of the error probability due to the use of error correction can be calculated as $P_{e,ec}(\mathcal{C}) - P_e(\mathcal{C})$.

7

Conclusions

In this work we introduced a new family of codes for transmitting information through a classical-quantum channels that optimize the error probability under a symmetry condition. These codes are called quasi-perfect codes and are the equivalent of the quasi-perfect codes for classical channels.

In Chapter 4, we introduced the definition of quasi-perfect codes and generalized quasi-perfect codes for the classical-quantum channel. This definition is similar to the one in the classical case, and it's also valid for classical channels. We proved that the quasi-perfect codes attain the meta-converse bound with equality under a symmetry condition, and so they optimize the probability of error of a classical-quantum channel for a fixed cardinality of the code and dimension of the codewords. In that chapter we also showed some particular examples of quasi-perfect codes that satisfy the symmetry condition. The most interesting ones are the Bell codes, which are a generalization of the Bell states for 2-qubit channels. These codes are quasi-perfect for a code cardinality M larger than the channel dimension N. In general, practical codes are the opposite in the sense that they use a smaller cardinality of the code in order to reduce the probability of error.

In Chapter 5 we studied the optical channel, where the information is transmitted using coherent states, through the bosonic channel. This channel has infinite dimension, so we considered its truncated approximation of dimension N. We showed that the phase-modulated coherent states constitute a quasi-perfect code for this truncated channel, as long as the number of codewords M is the same as the dimension of the truncated channel N. A phase-modulated codebook of finite cardinality M used for the infinite-dimensional bosonic channel is not quasi-perfect, but for sufficiently large N the bosonic channel can be approximated to the truncated channel with a negligible error. This makes this code nearly optimal even for

the bosonic channel, providing an example of a practical code that uses $M < N$ which is close to optimal.

In Chapter 6, we focused on stabilizer error correction codes, which are practical codes that use $M < N$. Error correction codes are in general used to preserve quantum information and not to transmit classical information, however there may be situations where we want to measure a state after undergoing error correction. In these cases it may be interesting to show that an error correction code is optimum for a state discrimination problem. We showed that the 5-qubit stabilizer code is an example of a quasi-perfect code for the 5-qubit Pauli channel. The analysis to prove that is very case-specific, which means that it is not possible to make any claim about other stabilizer codes being quasi-perfect without making a particular analysis for each case. We also proved that the error correction procedure makes the probability of error increase when we want to distinguish codewords using an optimal POVM.

Bibliography

[1] M. M. Wilde. *From Classical to Quantum Shannon Theory*. Cambridge University Press: 2011.

[2] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. 10th Anniversary Edition. Cambridge University Press: Cambridge, 2010. ISBN 9781107002173.

[3] G. Cariolaro. *Quantum Communications*. Springer: 2015. ISBN 9783319155999.

[4] W. T. Kelvin. Nineteenth-century clouds over the dynamical theory of heat and light. *The London, Edinburgh and Dublin Philosophical Magazine and Journal of Science*, 1901, **2**(7), pp. 1–40.

[5] A. A. Michelson and E. W. Morley. On the Relative Motion of the Earth and the Luminiferous Ether. *American Journal of Science*, 1887, **34**(203), pp. 333–345.

[6] M. Planck. Über das gesetz der energieverteilung im normalspektrum. *Ann. Phys.*, 1901, **309**(3), pp. 553–563.

[7] A. Einstein. Über einen die erzeugung und verwandlung des lichtes betreffenden heuristischen gesichtspunkt. *Ann. Phys.*, 1905, **322**(6) pp. 132–148.

[8] L. de Broglie. *Recherches sur la théorie des Quanta*. Migration - université en cours d'affectation, 1924.

[9] E. Schrödinger. Quantisierung als eigenwertproblem. *Ann. Phys.*, 1926, **384**(4), pp. 361–376.

[10] W. Heisenberg. Über quantentheoretische umdeutung kinematischer und mechanischer beziehungen. *Z. Physik*, 1925, **33**, pp. 879–893.

[11] P. A. M. Dirac. *The Principles of Quantum Mechanics*. Oxford University Press: UK, 1930.

[12] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus and M. Peev. The Security of Practical Quantum Key Distribution. *Rev. Mod. Phys.*, 2009, **81**(3), pp. 1301–1350.

[13] H. Lo and H. F. Chau. Unconditional Security Of Quantum Key Distribution Over Arbitrarily Long Distances. *Science*, 1998, **283**, pp. 2050–2056.

[14] F. Arute, K. Arya, D. Bacon et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 2019, **574**, pp. 505–510.

[15] M. Acín , D. Bruss, M. Lewenstein and A. Sanpera. Classification of Mixed Three-Qubit States. *Phys. Rev. Lett.*, 2001 **87**(4).

[16] W. Dür, G. Vidal and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys.Rev. A*, 2000, **62**.

[17] A. S. Holevo. A note on covariant dynamical semigroups. *Rep. Math. Phys.*, 1993, **32**(2), pp. 211–216.

[18] M. Hayashi. *Quantum Information Theory: Mathematical Foundation*. Second edition. Springer: 2017.

[19] H. Cheng, M. Hsieh and M. Tomamichel. Sphere-Packing Bound for Symmetric Classical-Quantum Channels. *IEEE Int. Symp. Inf. Theory*, 2017.

[20] H. Cheng, M. Hsieh and M. Tomamichel. Quantum Sphere-Packing Bounds with Polynomial Prefactors. *IEEE Trans. Inf. Theory*, 2019, **65**(5), pp. 2872–2898.

[21] A. B. Coll, G. Vazquez-Vilar and J. R. Fonollosa. Generalized Perfect Codes for Symmetric Classical-Quantum Channels. *IEEE Trans. Inf. Theory*, 2022, **68**(9), pp. 5923–5936.

[22] A. B. Coll, and J. R. Fonollosa. Perfect and Quasi-Perfect Codes for the Bosonic Classical-Quantum Channel. *IEEE Trans. Quantum Eng.*, 2023, **4**.

[23] R. J. Glauber. Coherent and Incoherent States of the Radiation Field. *Phys. Rev.*, 1963, **131**(5), pp. 2766–2788.

[24] R. S. Kennedy. A Near-Optimum Receiver for the Binary Coherent State Quantum Channel. *MIT Res. Lab. Electron. Quart. Progr. Rep.*, 1973, **108**, pp. 219–225.

[25] S. J. Dolinar. An Optimum Receiver for the Binary Coherent State Quantum Channel. *MIT Res. Lab. Electron. Quart. Progr. Rep.*, 1973, **111**, pp. 115–120.

[26] R. L. Cook, P. J. Martin and J. M. Geremia. Optical coherent state discrimination using a closed-loop quantum measurement. *Nature*, 2007, **446**, pp. 774–777.

[27] I. Katz, Y. Kochman and J. M. Geremia. On the Optimality of Dolinar's Receiver. *IEEE Information Theory Workshop*, 2020.

[28] Y. Polyanskiy, H. V. Poor and S. Verdú. Channel coding rate in the finite blocklength regime. *IEEE Trans. Inf. Theory*, 2010, **56**(5), pp. 2307–2359.

[29] G. Vazquez-Vilar, A. G. Fàbregas and S. Verdú. The Error Probability of Generalized Perfect Codes via the Meta-Converse. *IEEE Trans. Inf. Theory*, 2019, **65**(9), pp. 5705–5717.

[30] G. Vazquez-Vilar. Multiple quantum hypothesis testing expressions and classical-quantum channel converse bounds. *IEEE Int. Symp. Inf. Theory*, Barcelona, 2016.

[31] A. S. Holevo. Statistical decision theory for quantum systems. *J. Multivar. Anal.*, 1973, **3**(4), pp. 337–394.

[32] H. Yuen, R. Kennedy and M. Lax. Optimum testing of multiple hypotheses in quantum detection theory. *IEEE Trans. Inf. Theory*, 1975, **21**(2), pp. 125–134.

[33] A. Jenčová. Quantum hypothesis testing and sufficient subalgebras. in *Lett. Math. Phys.*, 2010, **93**(1), pp. 15–27.

[34] J. Neyman and E. S. Pearson. On the problem of the most efficient tests of statistical hypotheses. *Phil. Trans. R. Soc. Lond. A*, 1933, **231**, pp. 289–337.

[35] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane. Quantum Error Correction and Orthogonal Geometry. *Phys. Rev. Lett.*, 1997, **78**(3).

[36] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane. Quantum errors correction via codes over GF (4). *IEEE Trans. Inf. Theory*, 1998, **44**(4), pp. 1369–1387.

[37] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A*, 1996, **54**(3), pp. 1862–1868.

[38] D. Gottesman. *Stabilizer codes and quantum error correction.* California Institute of Technology, Pasadena, 1997.

[39] D. Gottesman. An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation. *Proc. Sympos. Appl. Math.*, 2009.

[40] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 1995, **52**(4), pp. 493–496.

[41] W. Ligong and R. Renato. One-shot classical-quantum capacity and hypothesis testing. *Phys. Rev. Lett.*, 2012, **108**(20).

[42] W. Matthews and S. Wehner. Finite blocklength converse bounds for quantum channels. *IEEE Trans. Inf. Theory*, 2014, **60**(11), pp. 7317–7329.

[43] M. Hayashi. *Quantum Information: An Introduction*. Springer: Berlin, 2006 ISBN 9783540302667

[44] M. Hayashi and H. Nagaoka. General formulas for capacity of classical-quantum channels. *IEEE Trans. Inf. Theory*, 2003, **49**(7), pp. 1753–1768.

[45] H. Nagaoka and M. Hayashi. An information-spectrum approach to classical and quantum hypothesis testing for simple hypotheses. *IEEE Trans. Inf. Theory*, 2007, **53**(2), pp. 534–549.

[46] G. Vazquez-Vilar, A. T. Campo, A. G. Fàbregas and A. Martinez. Bayesian M-Ary Hypothesis Testing: The Meta-Converse and Verdú-Han Bounds Are Tight. *IEEE Trans. Inf. Theory*, 2016, **62**(5), pp. 2324–2333.

[47] A. Steane. Multiple Particle Interference and Quantum Error Correction. *arXiv preprint arXiv:quant-ph/9601029v3*, 1996.