Error Probability Mitigation in Quantum Reading Using Classical Codes

Francisco Revson Fernandes Pereira [1,2,*] and Stefano Mancini [1,2]

1   School of Science and Technology, University of Camerino, I-62032 Camerino, Italy; stefano.mancini@unicam.it
2   INFN, Sezione di Perugia, I-06123 Perugia, Italy
*   Correspondence: revson.ee@gmail.com

Abstract: A general framework describing the statistical discrimination of an ensemble of quantum channels is given by the name quantum reading. Several tools can be applied in quantum reading to reduce the error probability in distinguishing the ensemble of channels. Classical and quantum codes can be envisioned for this goal. The aim of this paper is to present a simple but fruitful protocol for this task using classical error-correcting codes. Three families of codes are considered: Reed–Solomon codes, BCH codes, and Reed–Muller codes. In conjunction with the use of codes, we also analyze the role of the receiver. In particular, heterodyne and Dolinar receivers are taken into consideration. The encoding and measurement schemes are connected by the probing step. As probes, we consider coherent states. In such a simple manner, interesting results are obtained. As we show, there is a threshold below which using codes surpass optimal and sophisticated schemes for any fixed rate and code. BCH codes in conjunction with Dolinar receiver turn out to be the optimal strategy for error mitigation in quantum reading.

Keywords: quantum reading; cyclic codes; Reed–Muller codes; heterodyne receiver; Dolinar receiver

1. Introduction

Quantum state discrimination composes an important part of several quantum computing protocols [1]. Quantum communication relies upon the ability of the receiver to distinguish between a set of information carriers [2,3]. The security of quantum key distribution protocols is based on the impossibility of perfectly distinguishing non-orthogonal states [1]. In both situations, where one needs to show that states are distinguishable or not, the set of quantum states are fixed and an analysis over the minimum achievable error probability is performed. In order to decrease the error probability, the only possible method is optimizing the measurement apparatus. There are paradigms giving more freedom and, therefore, increasing the complexity for analyzing them.

A natural extension of the task of discriminating quantum states is envisioned in quantum channel discrimination [4–13], and, more generally, quantum reading [14]. Quantum reading task is important for modeling and quantifying quantum memories as a useful resource. Information-theoretically bounds, communications protocols, and error probability results can be applied to quantum reading. Quantum reading considers the use of input and output quantum resources to enhance the retrieval of classical information stored in quantum channels. Actually, it considers that one can record bits of information in memory cells by storing a quantum channel picked from a given ensemble. The goal in quantum reading is to optimize the probing strategy as well as the encoding and decoding protocols to reduce the error probability in the discrimination process.

Efficient paths to quantum reading can be foreseen by the use of coding techniques [15–17]. On the first hand, quantum error-correcting codes give interesting candidates to probe the memory cells. The structure of their Hilbert subspace makes them reliable to some dissipator noise due to system-environment interaction [18]. On the other

hand, the encoding process can be implemented using classical error-correcting codes in order to add redundancy and increase error mitigation. Focusing on error probability mitigation as the figure of merit and using short-length classical codes, we consider three families: Reed–Solomon codes, BCH codes, and Reed–Muller codes [19]. These families have a large diversity of parameters, and their values can be easily controllable. Additionally, the existing low-complexity encoding and decoding algorithms make the protocol proposed in this paper realizable with the current technology.

Following the previous reasoning, we consider a quantum reading task where the ensemble is composed of two quantum channels. Each quantum channel is modeled by a pure-lossy bosonic channel with different transmissivities. For the analysis, we will consider the three families of codes mentioned before, two types of receivers, and a probing state. The first receiver is a heterodyne receiver [2]. The use of heterodyne receiver is justifiable due to the phase-insensitivity property of pure-lossy channels. The second one is a Dolinar receiver [2]. This is an adaptive receiver that can achieve the Helstrom bound on distinguishing two quantum states [2]. There is an intrinsic complexity in implementing this receiver, mostly due to the adaptive and fast response characteristics. However, it has been implemented in practice, where its optimality was shown [20]. Lastly, for the probing state, we consider coherent states. Therefore, we aim to show that the improvements and results obtained in the proposed scheme is due to the classical codes and receivers considered.

For any of the three families of classical error-correcting codes considered, we show improvements when compared with optimal strategies using coherent or squeezed states. We compute the average number of photons needed to surpass the optimal strategies for fixed code, rate, and receiver. This value defines a threshold. There are strategies giving a lower threshold. Using the heterodyne receiver, the best strategy is the BCH codes. However, there are some values of rate where Reed–Muller codes have similar performance. Using the Dolinar receiver, BCH and Reed–Solomon codes have almost the same performance. For lower values of rate, the BCH codes perform better than Reed–Solomon. The situation changes when the rate is above 0.45. For any of the codes, the best performances are obtained using the Dolinar receiver. We are able to achieve thresholds in this strategy for an average number of photons below 18. Furthermore, in order to achieve the threshold for a large range of rates, one does not need more than 6 photons per probing state.

This paper establishes an important basis for the use of classical codes in quantum reading. In particular, it has taken the novel path of proposing an explicit use of short-length classical codes and showing how much they impact error mitigation. These results demonstrate the possibility of improving the current technology used on quantum memories by low complexity encoding and decoding schemes. The values of the threshold obtained emphasize this statement. A relevant achievement of this paper is the explicit characterization of error mitigation in terms of different code lengths and code families. One can obviously expect error mitigation by increasing the number of photons used to probe the memory cells, but what can happen when associating classical codes to the scheme is answered quantitatively in this paper.

Due to the novel path taken in this paper by considering classical codes and the error mitigation produced by them, there is not much to be said about the connection with the existing literature. The only related work in the literature is Ref. [17], where the authors proposed polar coding and decoding schemes to achieve the reading capacity. However, the results in Ref. [17] can only be appreciated for large code lengths. One can also find unrelated approaches to quantum reading, such as Ref. [21], where it is shown that entanglement-assisted probing outperforms classical strategies on barcodes data, without any explicit analysis of encoding and decoding schemes.

This paper is organized as follows. In Section 2, we present the main concepts used throughout the paper. A description of the three families of classical codes is given. Additionally, we explain the task of quantum reading and the quantum channel model

considered. Next, in Section 3, we describe the proposed protocol. It is divided into three parts: probing strategy, encoding scheme, and decoding scheme. The performance analysis of the protocol is given in Section 4. Lastly, we draw our conclusions in Section 5.

2. Preliminaries

This section introduces the main concepts of classical codes and quantum reading needed for this paper. We begin with a brief overview of cyclic codes and then specialize in Reed–Solomon and BCH codes. Subsequently, we show a construction method for Reed–Muller codes that is similar to Reed–Solomon codes. Lastly, the quantum reading task is introduced. The general concept is given, followed by a detailed description of the channel model adopted.

2.1. Classical Codes

2.1.1. Cyclic Codes

A linear code C over $\mathbb{F}_q$ with parameters $[n, k, d]_q$ is called cyclic if for any codeword $(c_0, c_1, \ldots, c_{n-1}) \in C$ implies $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. Defining a map from $\mathbb{F}_q^n$ to $\mathbb{F}_q[x]/(x^n - 1)$, which takes $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ to $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_q[x]/(x^n - 1)$, we can see that a linear code C is cyclic if and only if it corresponds to an ideal of the ring $\mathbb{F}_q[x]/(x^n - 1)$. Since any ideal in $\mathbb{F}_q[x]/(x^n - 1)$ is principal, then any cyclic code C is generated by a polynomial $g(x)$, which divides $(x^n - 1)$. These polynomials are called generator polynomials.

A way to characterize the parameters of a cyclic code is by means of the generator polynomial and its defining set. Roughly speaking, the defining set characterizes the common zeros of all polynomials $c(x) \in C$. More precisely, let n and q be relative prime, so $q^e \equiv 1 \mod n$, for some integer e. Fix an element β of order n in an extension $\mathbb{F}_{q^e}$ of $\mathbb{F}_q$. We have that the defining set of C, which is denoted by $Z(C)$, is $Z(C) = \{i \in \mathbb{Z}_n : c(\beta^i) = 0 \text{ for all } c(x) \in C\}$. The family of Reed–Solomon (RS) codes is a particular case of cyclic codes, where the generator polynomial has some additional properties.

Definition 1. *Let α be a primitive element of $\mathbb{F}_q$. Let $b \geq 0$, $n = q - 1$, and $1 \leq k \leq n$. A cyclic code $RS_k(n, b)$ of length n over $\mathbb{F}_q$ is a* Reed–Solomon (RS) code *if the generator polynomial is given by*

$$g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \cdots \cdots (x - \alpha^{b+n-k-1}).$$

Since the minimal distance of any cyclic code is bounded from below by the maximum number of consecutive elements in $Z(C)$ and the Singleton bound says that the minimal distance of a $[n, k]$ code is not greater than $n - k + 1$, we see that RS codes have minimal distance equal to $n - k + 1$. Thus, for fixed length and dimension, they have maximal possible minimal distance and, therefore, they are named maximal distance separable (MDS) codes.

Even though the previous definition of RS codes describes them properly, there is a more practical way to construct RS codes. Choose an enumeration $\mathcal{P} = (P_1, \ldots, P_n)$ of n mutually distinct points in $\mathbb{F}_q$. Let $\mathbb{F}_q[X]$ be the set of all polynomials in the variable X with coefficients in $\mathbb{F}_q$. The RS code is given by

$$RS_k(n, b) = \{ev_{\mathcal{P}}(f) : f \in \mathbb{F}_q[X], \deg(f) < k\}, \tag{1}$$

where *ev* is the evaluation map defined by

$$ev_{\mathcal{P}} : \mathbb{F}_q[X] \quad \rightarrow \quad \mathbb{F}_q^n, \tag{2}$$
$$f(X) \quad \mapsto \quad (f(P_1), \ldots, f(P_n)). \tag{3}$$

For the decoding scheme, we apply the Berlekamp–Massey algorithm [22] (Section 5.4.2). Since we are using small RS codes, meaning that the length of the RS codes is significantly shorter than LDPC or Turbo codes, the Berlekamp–Massey algorithmic fulfills our needs.

Before presenting BCH codes, we need to introduce the concept of minimal polynomials. Let $\beta \in \mathbb{F}_{q^e}$. The minimal polynomial over $\mathbb{F}_q$ of β is the monic polynomial with smallest degree, $M(x)$, and coefficients in $\mathbb{F}_q$ such that $M(\beta) = 0$. If $\beta = \alpha^i$ for some primitive nth root of unity $\alpha \in \mathbb{F}_{q^e}$, we denote the minimal polynomial of β by $M^{(i)}(x)$.

Definition 2. *Let $\mathbb{F}_q$ be a finite field, n and q be relative prime, and α be a primitive nth root of unity. A cyclic code $BCH(\delta, b)$ of length n over $\mathbb{F}_q$ is a Bose–Chaudhuri–Hocquenghem (BCH) code of design distance δ if the generator polynomial is given by*

$$g(x) = lcm\{M^{(b)}(x), M^{(b+1)}(x), \ldots, M^{(b+\delta-2)}(x)\}, \tag{4}$$

for some integer $b \geq 0$. If $n = q^e - 1$ then the BCH code is called primitive and if $b = 1$ it is called narrow-sense.

The dimension of a BCH code is equal to $k = n - \deg(g(x))$, similarly to the Reed–Solomon code case. The minimal distance can also be computed using the defining set of $BCH(\delta, b)$. However, there is no general formula for BCH codes. We would need to introduce the concept of q-ary cyclotomic coset modulo n and analyze each code in order to obtain the respective dimension. Therefore, it is beyond the scope of this paper. The performance analysis of the code is based on error probability and rate.

The encoding algorithm used for BCH codes is implemented via matrix multiplication, which has complexity $O(n^2)$. For the decoding algorithm, the Berlekamp–Massey algorithm is also used.

2.1.2. Reed–Muller Codes

The construction of Reed–Muller codes is similar to the one presented for Reed–Solomon codes using evaluation map. The difference relies on the set of polynomials considered. Take a vector space $\mathbb{F}_q^m$, where m is an integer. Choose an enumeration $\mathcal{P} = (P_1, \ldots, P_n)$ of n mutually distinct points in $\mathbb{F}_q^m$. The evaluation map is defined as

$$ev_{\mathcal{P}} \colon \mathbb{F}_q[X_1, \ldots, X_m] \quad \rightarrow \quad \mathbb{F}_q^n, \tag{5}$$
$$f(X_1, \ldots, X_m) \quad \mapsto \quad (f(P_1), \ldots, f(P_n)), \tag{6}$$

where $\mathbb{F}_q[X_1, \ldots, X_m]$ is the set of all polynomials in the variables $X_1, \ldots, X_m$ with coefficients in $\mathbb{F}_q$. We can define Reed–Muller codes by means of evaluating polynomials.

Definition 3. *Let $\mathbb{F}_q$ be a finite field, and r, m be integers such that $0 \leq r < m(q-1)$. Let $n = q^m$ and $\mathcal{P} = (P_1, \ldots, P_n)$ be an enumeration of all elements in $\mathbb{F}_q^m$. A block code $RM(r, m)$ of length n over $\mathbb{F}_q$ is a Reed–Muller code of order or degree r in m variables if it is given by the set*

$$RM(r, m) = \{ev_{\mathcal{P}}(f) \colon f \in \mathbb{F}_q[X_1, \ldots, X_m], deg(f) \leq r\}. \tag{7}$$

It is possible to show that the dimension of a $RM(r, m)$ over $\mathbb{F}_q$ is equal to the size of the set [19] (Proposition 5.4.7)

$$E_q(r, m) = \{\mathbf{e} \in \mathbb{N}_0^m \colon \quad 0 \leq e_i \leq q - 1 \text{ for all } i$$
$$\text{and } e_1 + \cdots + e_m \leq e\}. \tag{8}$$

The encoding algorithm used to construct the Reed–Muller codes is via generator matrix. We use the standard majority logic vote method due to Irving S. Reed [23] in order to decode the received string.

2.2. Quantum Memory Cell and Quantum Reading

We now provide a description of quantum memory cells and quantum reading suitable for this paper. A quantum memory cell is defined as the set $\Phi = \{\mathcal{W}^x, p_x\}_{x \in \mathcal{X}}$ of quantum channels. For a fixed x, quantum input and output Hilbert spaces $\mathcal{H}_{B'}$ and $\mathcal{H}_B$, respectively, we have

$$\mathcal{W}^x \colon \mathcal{D}(\mathcal{H}_{B'}) \quad \to \mathcal{D}(\mathcal{H}_B) \tag{9}$$
$$\rho \quad \mapsto \mathcal{W}^x(\rho), \tag{10}$$

where $\mathcal{D}(\mathcal{H}_{B'}), \mathcal{D}(\mathcal{H}_B)$ are the sets of input and output density states of the quantum channel $\mathcal{W}^x$, and $p_x = P_X\{X = x\}$ is the probability distribution law of X. We call $x \in \mathcal{X}$ the quantum memory cell index. We consider $\mathcal{X}$ binary and the distribution of the random variable X describing the label of the quantum channels to be Bernoulli with probability $p = 1/2$.

The quantum reading protocol consists in probing a memory cell in order to discriminate between its possible index values, i.e., between quantum channels. Additionally, and more important to this paper, it is assumed that the encoder can use classical codes during the writing process on the quantum channels arising from the quantum memory cell in order to reduce the error probability. Let **c** be a codeword of a classical code. Then, the encoder is able to choose the quantum memory cell index and, therefore, which channel is to be placed, according to **c**. Since the encoder chooses the quantum memory cell index, we can assume, without loss of generality, that a source code is performed on the information bits to produce evenly distributed indexes. A schematic of the quantum reading protocol is given in Figure 1.
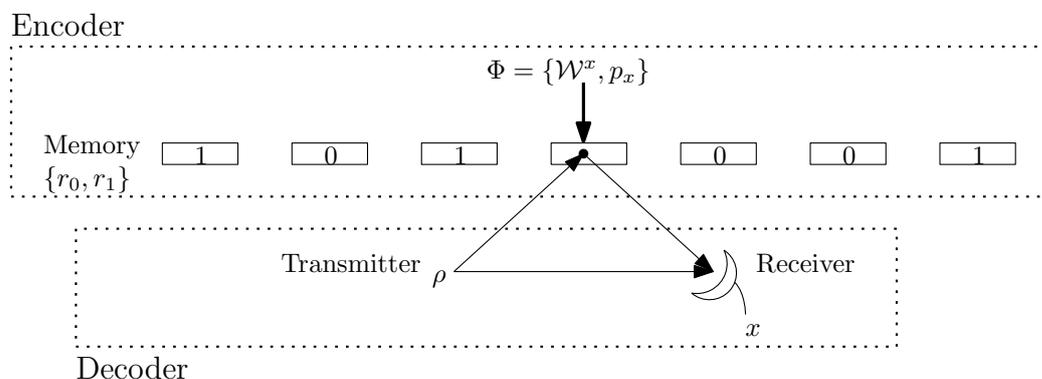

Figure 1. Quantum reading protocol.

For the quantum channel model, we use bosonic pure-lossy channels. They are a reasonable basic continuous variables model for optical memories. Thus, the binary channel ensemble is given by $\Phi = \{\mathcal{W}^x, p_x\}_{x=0,1}$, where $p_0 = p_1 = 1/2$, and $\mathcal{W}^x$ represents a pure-lossy channel with transmissivity $0 \le \kappa_x \le 1$. The action of each $\mathcal{W}^x$ channel in the Heisenberg picture is described by the map

$$\hat{a}_B \to \sqrt{\kappa_x}\hat{a}_B - \sqrt{1-\kappa_x}\hat{a}_E, \tag{11}$$

where $\hat{a}_B$ is the annihilation operator of the probe mode and $\hat{a}_E$ is that of an environmental vacuum mode. We are considering that the two parameters κ_0 and κ_1 assume values in the interval $[0, 1]$, since it is considered that the optical memories are read by reflection.

Optimal Error Probability

In Ref. [15], the error probability under the optimization of the probe state and the measurement apparatus used in the receiver is analyzed. The optimization considers that the decoder can probe the memory cells as many times as necessary, and Helstrom's measurements are at its disposal. Using coherent states, they show that the optimal error probability is

$$P_c = \frac{1 - \sqrt{1 - \exp[-\overline{n}(\sqrt{\kappa_0} - \sqrt{\kappa_1})]}}{2},\tag{12}$$

where $\overline{n}$ is the average number of photons. On the other hand, they also consider non-classical probes described via Einstein–Podolsky–Rosen transmitter. It is composed of s pairs of signals and references, entangled via two-mode squeezing. The squeezing parameter ξ of the two-mode squeezing state and the parameter s are connected by the expression $\xi = \operatorname{arcsinh}\sqrt{\frac{\overline{n}}{s}}$. Optimizing the error probability in terms of the parameter s, the following expression of the error probability is obtained

$$P_s = \frac{\exp(-\mu\overline{n})}{2},\tag{13}$$

where

$$\mu = \frac{\kappa_0 + \kappa_1 + 2}{2} - 2\sqrt{\kappa_0\kappa_1} - \sqrt{(1 - \kappa_0)(1 - \kappa_1)}.\tag{14}$$

In the following section, we are going to analyze the error probability derived from the use of classical codes and compare it with the previous optimal error probabilities.

3. Proposed Protocol

This section is divided in two. Initially, we present the probing strategy applied to the memory cells. Afterward, the encoding and decoding protocols implemented to incorporate and retrieve information from the memory cells are shown. In particular, the heterodyne and Dolinar receivers used to measure the output probe state are described.

3.1. Probing Strategy

Choosing the probing state is an important step in any metrological system. However, our focus is on the improvement of using classical codes. Therefore, we have opted to apply single-mode coherent states in the probing step. Their implementation is not so complex as compared with squeezed states, and one can also use standard optical devices to manipulate the phase and amplitude of the coherent state.

We are going to describe a single-mode coherent state via the basis of Fock states and the Wigner function. The first characterization will help us to compute the probability distribution obtained in the photodetector. The second characterization is important when we consider the action of the displacement operator and the description of the probability distribution in a heterodyne detection.

Let $\{|n\rangle\}$, $n = 0, 1, 2, \ldots$, be the basis of Fock states. A single-mode coherent state $|\alpha\rangle$ can be written as

$$|\alpha\rangle = e^{\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle.\tag{15}$$

Its Wigner function reads

$$W_\alpha(\mathbf{r}) = \frac{2}{\pi} e^{-(\mathbf{r}-\overline{\mathbf{r}})^T(\mathbf{r}-\overline{\mathbf{r}})},\tag{16}$$

where

$$\overline{\mathbf{r}} = \begin{pmatrix} \sqrt{2}\mathrm{Re}\{\alpha\} \\ \sqrt{2}\mathrm{Im}\{\alpha\} \end{pmatrix}.\tag{17}$$

Since the Wigner function gives a quasiprobability description of a quantum state, we see that a coherent state is Gaussian.

3.2. Encoding and Decoding Protocols

The encoding process consists in storing the information to be read in the future. Suppose we have an information vector **i** to be stored. Due to imperfect storing or reading of the information vector, the noise inherently prohibits us from reading the information perfectly. We need to add redundancies in order to overcome this issue and, in our case, use classical codes. Therefore, we first produce a codeword over $\mathbb{F}_2$ written in the memory cell labels. Suppose the information vector is a K bits string, the encoder uses **i** to derive the codeword $\mathbf{c} = (c_1, \ldots, c_N)$ of length N. If the classical code is constructed over $\mathbb{F}_{2^s}$, with $s > 1$ an integer, then it is needed to choose a basis of $\mathbb{F}_{2^s}$ over $\mathbb{F}_2$ and represent each coordinate c_j, $1 \leq j \leq N$, in that basis. This basis expansion process will be implemented when we use Reed–Solomon codes. After producing the codeword **c** over $\mathbb{F}_2$, we can move to the second step, which consists of associating each coordinate of **c** to the corresponding quantum memory cell index.

Observe that we are assuming that the quantum memory cell is composed of two quantum channels. However, the same method can be extended to quantum memory cells with cardinality p^s, where p is a prime number and $s \geq 1$ is an integer.

The decoding protocol consists of two parts. The first one is measuring the probing state in order to estimate the quantum memory cell. After probing the set of N memory cells, a noisy string or vector is obtained. Below we present in detail the measurement apparatus used through the paper, the heterodyne and Dolinar receiver. After producing the noisy vector, a decoding algorithm computes the best candidate of codeword for the classical code in consideration. The decoding algorithms used for the codes used in this paper have been discussed in Section 2.

3.2.1. Heterodyne Receiver with Maximum Likelihood Estimator

Suppose we plan to recover the information stored in the memory cells, then we probe each memory cell with a coherent state. The output state contains the information stored in the memory cell. The lossy channel will give $|\kappa_x \alpha\rangle$, for $x = 0, 1$, once applied to the coherent state $|\alpha\rangle$. So, we need to retrieve the information about x. For this goal, the heterodyne and Dolinar receiver are used. The heterodyne receiver is presented in this subsection, and Dolinar receiver in the following.

Heterodyne receivers are used when one wishes to retrieve the information stored in the parameter α of the coherent state [2]. See Figure 2. The POVM describing this receiver is

$$\Pi_\beta = \frac{1}{\pi} |\beta\rangle\langle\beta|. \tag{18}$$

Thus, the probability distribution obtained after probing the memory cell in the j-th position and using a heterodyne receiver is given by

$$p_Y(\beta) = \frac{1}{\pi} \langle\beta| \mathcal{W}^{c_j}(|\alpha\rangle\langle\alpha|) |\beta\rangle, \tag{19}$$

where $\beta \in \mathbb{C}$ and Y is the random variable describing the output probability distribution. After this step, we need to divide the complex plane in order to estimate if c_j is equal to zero or one. This is implemented via the maximum likelihood estimator. The partition of the complex plane and the decision rules are described by

$$\hat{c}_j = \begin{cases} 1, & \text{if } \Lambda(\beta) \geq \eta, \\ 0, & \text{if } \Lambda(\beta) < \eta, \end{cases} \tag{20}$$

where

$$\Lambda(\beta) = \frac{p_{Y|X}(\beta|1)}{p_{Y|X}(\beta|0)} \qquad (21)$$

and

$$\eta = \frac{p_0}{p_1}, \qquad (22)$$

with p_0 as the probability of 0 in a codeword **c** and $p_1 = 1 - p_0$. From the Wigner function of the coherent state, we see that the distribution of $p_{Y|X}(\beta|x)$, $x = 0, 1$, is Gaussian. Therefore, the partition of the plane can be made from the parameter of the coherent state and the reflexivities of the memory cells.
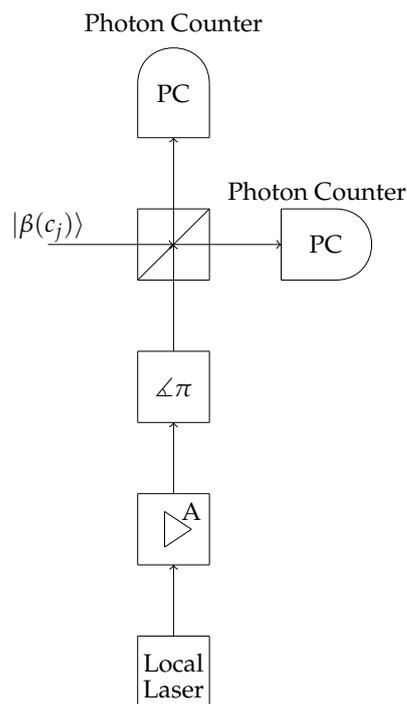

Figure 2. Heterodyne receiver schematic.

3.2.2. Dolinar Receiver

Dolinar receiver takes a different road than the heterodyne receiver [2]. It is an adaptive receiver. Suppose there are two coherent states, $|\alpha\rangle$ and $|\gamma\rangle$, we want to distinguish. Initially, the Dolinar receiver makes a guess of the true state and subtracts it from the state to be determined. This leads to the state $|\psi - \phi\rangle$, where ψ is the state to be determined and ϕ is the guess. Next, the resulting state is measured in a photodetector. For the computational simulation, we use

$$Q_1 = \sum_{n=1}^{\infty} (1 - \eta)^n |n\rangle\langle n|, \qquad (23)$$

where $1 - \eta$ is the detection efficiency, Q_1 is the click operator and $Q_0 = \mathbb{I} - Q_1$ is the no-click operator. If there is a click, then the guess is changed and the process is repeated with the same state to be determined. Otherwise, the receiver declares that the true state is the one it has guessed. An illustrative schematic is shown in Figure 3.

For numerical and analytical analysis of the above process, we need to clarify the feedback process shown. First of all, we are considering that the feedback is fast. Consider that the feedback runs l times and the incoming state is $|\alpha\rangle$. Then, in each round, the receiver has $\left|\frac{\alpha}{\sqrt{l}}\right\rangle$ as the input state. This is the state that the receiver has to guess. Observe that increasing too much the number of rounds, l, in the receiver will make it more susceptible to errors. In particular, we will use $l = 2$ in the following.
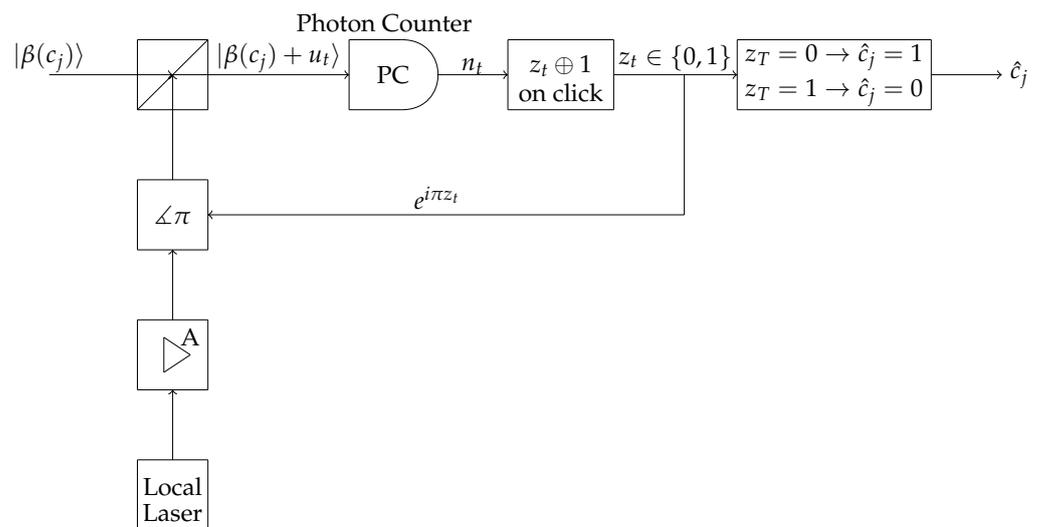
Figure 3. Dolinar receiver schematic.

The second point is about the subtracted state $|\phi\rangle$. To optimize the error probability, $|\phi\rangle$ needs to be of time-varying amplitude as shown in [2]. For simplicity, we are assuming that $|\phi\rangle$ can be instantaneously changed into one of the two possible states. Even though not optimal, this strategy gives significant improvements when compared with the heterodyne receiver. See the following section.

4. Analysis of Error Probability Using Classical Codes

Consider memory cells $\{\mathcal{W}^0, \mathcal{W}^1\}$, where $p_0 = p_1 = 1/2$, with reflexivities κ_0 and κ_2, respectively. Suppose a string of memory cells is encoded via a classical code $\mathcal{C}$. The information stored in the string is retrieved by probing them via a coherent state. From the result obtained, we analyze the error probability between the actual information **i** encoded by $\mathcal{C}$ and the estimated information $\hat{\mathbf{i}}$ after decoding the noisy string after the probing step.

A sample plot is shown in Figure 4. For a fixed rate $R = \frac{K}{N}$, where N and K are the length and dimension of the classical code, respectively, we compute the error probability for several values of the average number of photons. The receiver is also fixed. For the particular case of Figure 4, we used a heterodyne receiver. The analysis described in detail for the heterodyne and Dolinar receivers below focuses on the crosspoint or threshold where using the classical code gives improvement compared to the optimal receiver using coherent or squeezed states. As an example, the value of the threshold using RS code with rate $R = 25/255$ and Dolinar receiver is equal to 3.2, as one can see in Figure 4. Notice that the threshold depends on the slope of the error probability curve for each code and receiver. Therefore, it depends on the family of the code, the parameters of the code, and the receiver used. See below the error mitigation behavior analyzed under the perspective of the threshold for three families of classical codes, with several rates, and two types of receivers.
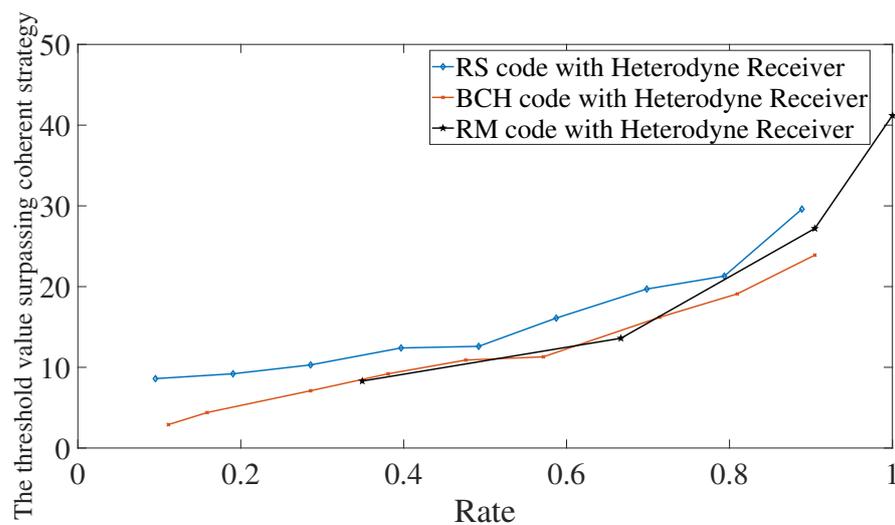
4.1. Heterodyne Receiver

For fixed values of transmissivities, κ_0 and κ_1, the analysis given in this paper consider the behavior of error mitigation for different codes. Because of analytical difficulties in deriving a closed formula for the error probability using classical codes, we adopted numerical simulations as the means of comparison between our case of study and the literature.

The first characterization is presented in Figure 5. The behaviors of the three codes are similar. First of all, as the rate increases, it also increases the value of the threshold. Increasing the rate means that we have less redundancy and, therefore, the code has the error-correction capability decreased, which imposes the need for probing with higher energy in order to surpass the optimal strategies. Secondly, the threshold values go up

to 45 photons. This means that we can keep in the quantum regime for surpassing the optimal strategies when using classical codes.
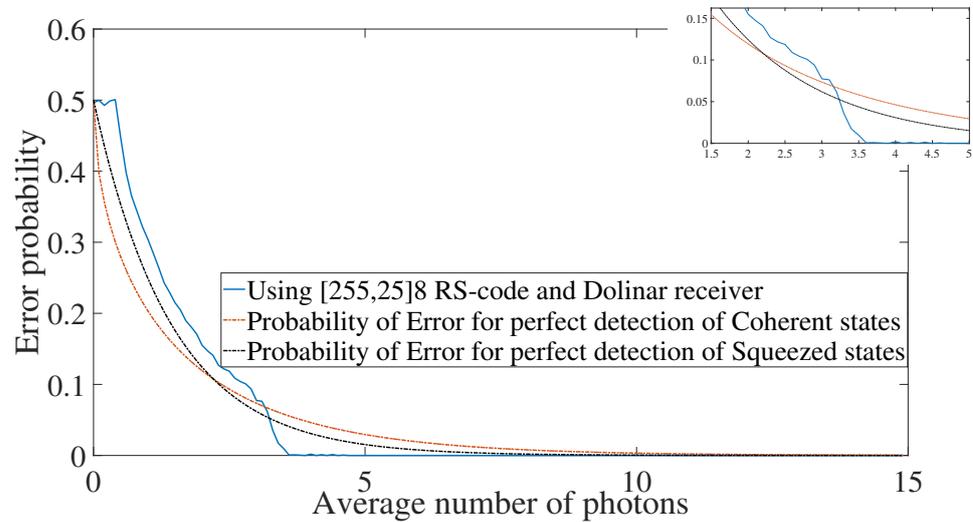
Figure 4. Error probability decay using $[255, 25]_8$ Reed–Solomon code and Dolinar receiver for $\kappa_0 = 0.1$ and $\kappa_1 = 0.95$.


Figure 5. Error mitigation using Reed–Solomon, BCH, or Reed–Muller codes. All codes are considered in conjunction with a heterodyne receiver. The memory cells have transmissivities equal to $\kappa_0 = 0.1$ and $\kappa_1 = 0.95$.

Comparing between codes, BCH codes and Reed–Muller codes have similar performances. However, it is important to remember that there are some limitations in using Reed–Muller codes since the choice of parameters does not have much freedom compared with BCH and Reed–Solomon codes. For Reed–Solomon codes, we see that they request probing with more energy, but such an increase of energy is less than 5 photons. Therefore, in practical applications, one would choose the code that has an encoder and decoder at the disposal with the lowest complexities.

Next, the behavior of the error mitigation is investigated for different values of transmissivities and using Reed–Muller codes. The first aspect one can see is that the performance highly depends on the difference between the transmissivities κ_0 and κ_1. For transmissivities where κ_0 and κ_1 are closer, the output probe states have position and momentum which are closer. Therefore, the heterodyne receiver in conjunction with maximum likelihood estimator has a higher probability of estimating the value encoded in the

memory cell erroneously. This will imply in a receiver output string with more errors. For a code with the same rate to surpass the optimal receiver, it needs more probing energy so that error probability decreases. This is the reason why one needs more energy for $\kappa_0 = 0.3$ and $\kappa_1 = 0.75$, and why the slope of the curve is higher than the case with $\kappa_0 = 0.1$ and $\kappa_1 = 0.95$. See Figure 6. For Reed–Solomon and BCH codes, we have the same behavior.
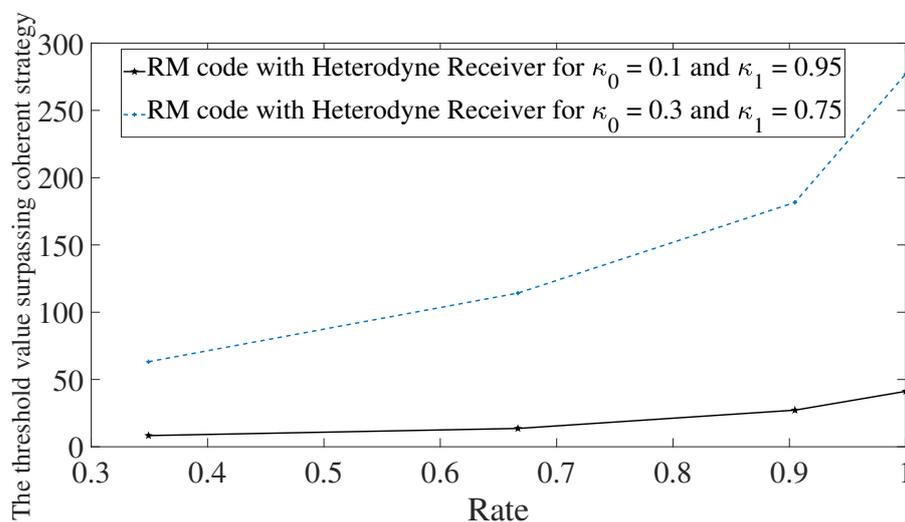
Figure 6. Comparison of performance using Reed–Muller codes for memory cells with different transmissivities. Solid line refers to memory cells with trasmittivities given by $\kappa_0 = 0.1$ and $\kappa_1 = 0.95$. Dotted line refers to memory cells with transmittivities $\kappa_0 = 0.3$ and $\kappa_1 = 0.75$.
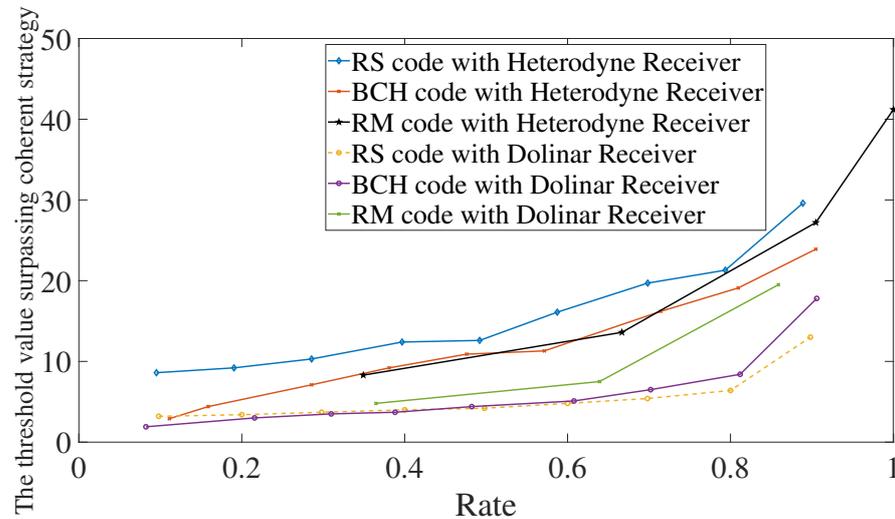
4.2. Dolinar Receiver

The Dolinar receiver is a powerful receiver that can be used for achieving the Helstrom bound on the error probability of distinguishing quantum states. As mentioned before, it also comes with an inherited complexity due to its adaptive character. Nonetheless, it can be implemented in practice [20]. For the analysis shown below, we need to impose some defects on the Dolinar receiver, otherwise the results obtained would be unrealistic. The structure and procedure for implementing the Dolinar receiver is the one explained in Section 3. The defect imposed for the results below is over the efficiency of the photodetector, which we consider to be equal to 0.9. This value is close to the one obtained with the current technology for some photodetectors. One additional defect that could be added is dark counting. However, to consider an experiment with dark counting would need additional parameters, such as the rate of measurement over the memory cells. The complexity in dealing with these details could fade the importance of the codes used and mislead the analysis.

Let the reflexivities be $\kappa_0 = 0.1$ and $\kappa_1 = 0.95$. It is shown in Figure 7 the performance using Reed–Solomon, BCH, or Reed–Muller codes in conjunction with a heterodyne or Dolinar receiver. Reed–Solomon and BCH codes in conjunction with Dolinar receiver give the best performance between them all. For low rates, BCH codes with heterodyne or Dolinar receivers give similar results. In particular, for rates below 0.1, the threshold value of using BCH codes with the heterodyne receiver is 3.2 and with Dolinar receiver is 1.9. However, the difference between heterodyne and Dolinar receiver accentuates for a higher rate. The performance using the Dolinar receiver is shown in detail in Figure 8.

The performance of using Reed–Solomon or BCH codes in conjunction with Dolinar receiver is quite similar. For some rate $R \in [0.4, 0.5]$, Reed–Solomon codes show better error mitigation than BCH codes. However, for practical reasons, BCH codes may be the best choice. The reason is that Reed–Solomon codes are constructed in an extended field $\mathbb{F}_{2^s}$, for some integer s, of $\mathbb{F}_2$. This imposes the need to constantly decompose the coordinates of the codewords on a basis of $\mathbb{F}_{2^s}$ over $\mathbb{F}_2$. Such decomposition is implemented in the encoding

and when writing the received string to feed the decoder. It is a not-so-demanding process, but may be substantial for choosing in favor of BCH codes.

Figure 7. Comparison between heterodyne receiver and Dolinar receiver when using Reed–Solomon, BCH, and Reed–Muller codes. We are considering that the photodetector used in the Dolinar receiver has efficiency equal to 0.9 and memory cells have transmissivities $\kappa_0 = 0.1$ and $\kappa_1 = 0.95$.
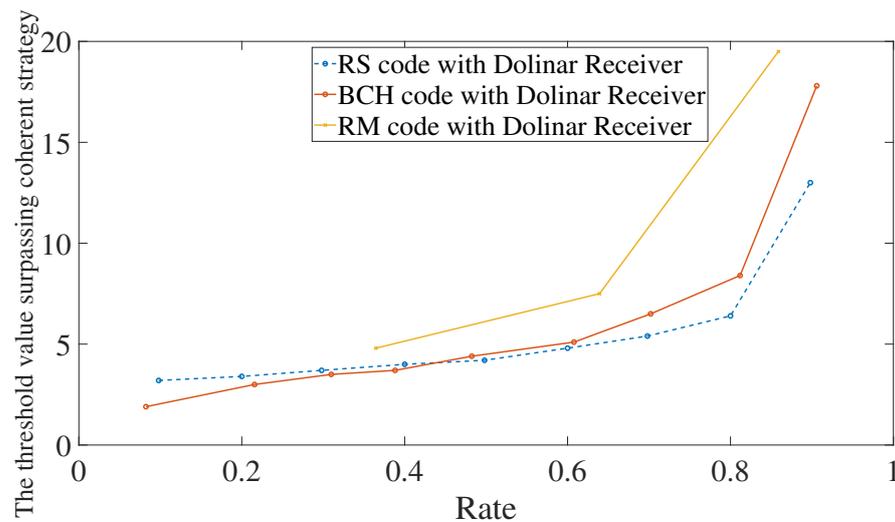
Figure 8. Error mitigation using Reed–Solomon, BCH, or Reed–Muller codes in conjunction with Dolinar receiver. We are considering that the photodetector used in the Dolinar receiver has efficiency equal to 0.9 and memory cells have transmissivities $\kappa_0 = 0.1$ and $\kappa_1 = 0.95$.

There is a last point to consider. The accomplishments presented using Dolinar receiver could be due to the receiver and, therefore, no code is needed. However, this is not true. Since the efficiency of the photodetector is below one, we have that the error probability without code but using Dolinar receiver is bounded from below. In particular, for the efficiency of 0.9 considered in our simulation and for any value of the average number of photons, the error probability is always above 0.12%. So, to improve further the error mitigation, one needs to amend additional tools, such as classical codes.

5. Final Remarks

We have shown that classical error-correcting codes can be used as a tool to reduce error probability in quantum reading. They have been applied in a short length range. Even so, error mitigation is accomplished. Above all, they can exhibit improvements when compared with optimal strategies using coherent or two-mode squeezed states once a

threshold is crossed. All of these for two types of receivers, heterodyne receiver or Dolinar receiver. We also studied the situation when the channel transmissivities are closer. It was shown that the error mitigation deteriorates but one can still surpass the optimal strategies probing with a state with higher energy. The same conclusion is obtained for the Dolinar receiver. As an overall conclusion of the analysis presented, BCH codes are the optimal code choice for error mitigation in the quantum reading task among the families of codes considered.

Several aspects could be further investigated in future works. Firstly, how the error probability mitigation behaves using codes with larger lengths and different rates. Some examples of possible choices of codes are LDPC and Turbo codes. It is expected that using codes with larger lengths and lower rates reduces the error probability. However, we do not know how this reduction will behave in this or in different scenarios. Secondly, analytical upper and lower bounds need to be obtained for a broader understanding of the current results. Lastly, it is expected that classical codes performance depends on the weight distribution of the code. This result may help to derive the error bounds mentioned before.

References

1. Hirvensalo, M. *Quantum Computing*; Springer: Berlin/Heidelberg, Germany, 2003.
2. Cariolaro, G. *Quantum Communications*; Springer-Verlag GmbH: Berlin/Heidelberg, Germany, 2015.
3. Mancini, S.; Winter, A. *A Quantum Leap in Information Theory*; WSPC: Singapore, 2020.
4. Childs, A.M.; Preskill, J.; Renes, J. Quantum information and precision measurement. *J. Mod. Opt.* **2000**, *47*, 155–176. [CrossRef]
5. Acín, A. Statistical distinguishability between unitary operations. *Phys. Rev. Lett.* **2001**, *87*, 17. [CrossRef] [PubMed]
6. Gilchrist, A.; Langford, N.K.; Nielsen, M.A. Distance measures to compare real and ideal quantum processes. *Phys. Rev. A* **2005**, *71*, 6. [CrossRef]
7. Sacchi, M.F. Optimal discrimination of quantum operations. *Phys. Rev. A* **2005**, *71*, 6. [CrossRef]
8. Sacchi, M.F. Entanglement can enhance the distinguishability of entanglement-breaking channels. *Phys. Rev. A* **2005**, *72*, 1. [CrossRef]
9. Wang, G.; Ying, M. Unambiguous discrimination among quantum operations. *Phys. Rev. A* **2006**, *73*, 4. [CrossRef]
10. Duan, R.; Feng, Y.; Ying, M. Perfect distinguishability of quantum operations. *Phys. Rev. Lett.* **2009**, *103*, 21. [CrossRef] [PubMed]
11. Hayashi, M. Discrimination of two channels by adaptive methods and its application to quantum system. *IEEE Trans. Inf. Theory* **2009**, *55*, 3807–3820. [CrossRef]
12. Harrow, A.W.; Hassidim, A.; Leung, D.W.; Watrous, J. Adaptive versus nonadaptive strategies for quantum channel discrimination. *Phys. Rev. A* **2010**, *81*, 3. [CrossRef]
13. Rexiti, M.; Mancini, S. Discriminating qubit amplitude damping channels. *J. Phys. A Math. Theor.* **2021**, *54*, 165303. [CrossRef]
14. Pirandola, S. Quantum reading of a classical digital memory. *Phys. Rev. Lett.* **2011**, *106*, 9. [CrossRef] [PubMed]
15. Pirandola, S.; Lupo, C.; Giovannetti, V.; Mancini, S.; Braunstein, S.L. Quantum reading capacity. *New J. Phys.* **2011**, *13*, 113012. [CrossRef]
16. Das, S.; Wilde, M.M. Quantum rebound capacity. *Phys. Rev. A* **2019**, *100*, 3. [CrossRef]
17. Pereira, F.R.F.; Mancini, S. Polar codes for quantum reading. *arXiv* **2020**, arXiv:2012.07198.
18. Pereira, F.R.; Mancini, S. Stabilizer codes for open quantum systems. *arXiv* **2021**, arXiv:2107.11914.
19. Pellikaan, R.; Wu, X.-W.; Bulygin, S.; Jurrius, R. *Codes, Cryptology and Curves with Computer Algebra*; Cambridge University Press: Cambridge, UK, 2017.

20. Cook, R.L.; Martin, P.J.; Geremia, J.M. Optical coherent state discrimination using a closed-loop quantum measurement. *Nature* **2007**, *446*, 774–777. [CrossRef] [PubMed]
21. Banchi, L.; Zhuang, Q.; Pirandola, S. Quantum-enhanced barcode decoding and pattern recognition. *Phys. Rev. Appl.* **2020**, *14*, 6. [CrossRef]
22. Huffman, W.C.; Pless, V. *Fundamentals of Error-Correcting Codes*; Cambridge University Press: Cambridge, UK, 2003.
23. Reed, I. A class of multiple-error-correcting codes and the decoding scheme. *Trans. IRE Prof. Group Inf. Theory* **1954**, *4*, 38–49. [CrossRef]