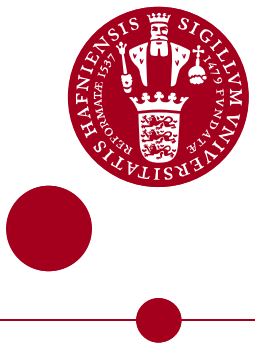
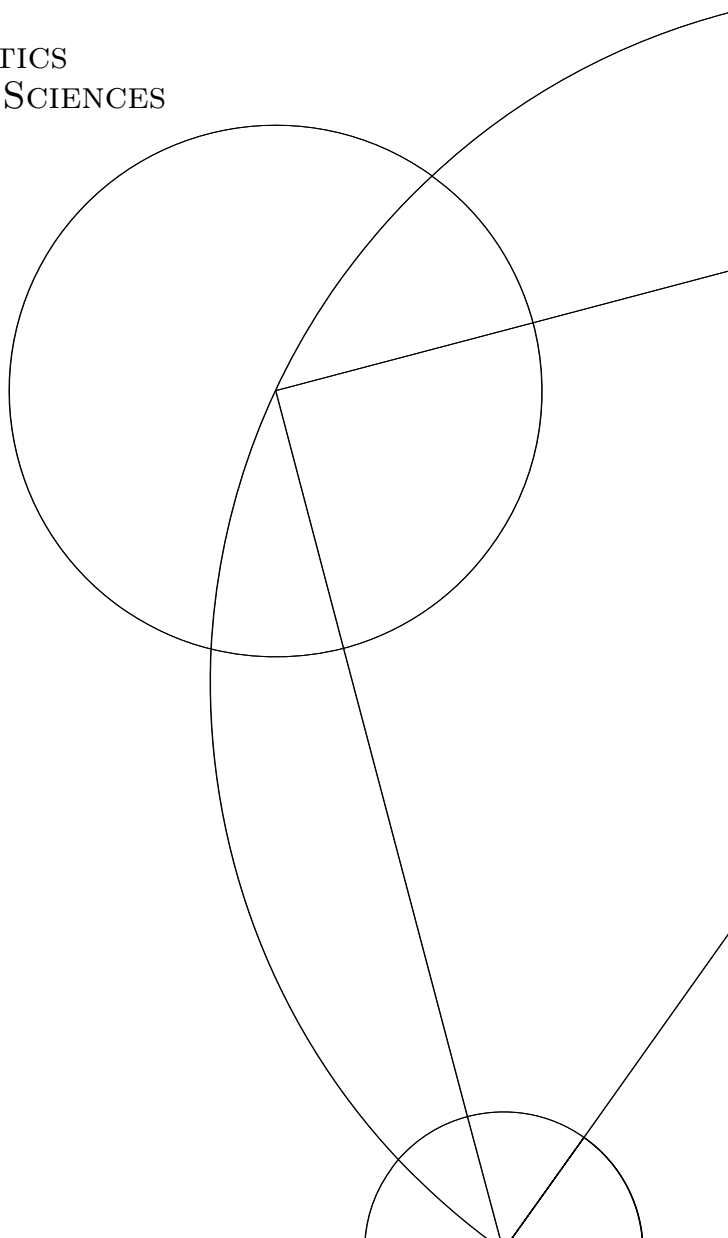
UNIVERSITY OF COPENHAGEN



Quantum Random Access Codes

Bachelor's Thesis in Mathematics
Department of Mathematical Sciences
University of Copenhagen

Sigurd Anker Laursen Storgaard
qmt293



Supervisor: Laura Mančinska

Date: 5th of June 2020

Abstract

In this thesis a communication protocol known as a Quantum Random Access Code (QRAC) is studied. A QRAC is a scheme that encodes n classical bits into m qubits ($m < n$) with the possibility of recovering any of the initial n bits with a worst case success probability of $p > \frac{1}{2}$. Such a code is denoted by (n, m, p)-QRAC. We prove that in any (n, m, p)-QRAC the worst case success probability is bounded by $p \leq \frac{1}{2} + \frac{1}{2}\sqrt{\frac{2^{m-1}}{n}}$ which in the case of $m = 2$ proves the conjecture posed in a recent paper by T. Imamichi and R. Raymond [8]. In particular, this means that the analytically known $(3, 2, \frac{1}{2} + \frac{1}{\sqrt{6}})$, $(4, 2, \frac{1}{2} + \frac{1}{2\sqrt{2}})$ and $(6, 2, \frac{1}{2\sqrt{3}})$-QRACs are optimal. This is done through a study of the geometry of quantum states in the Bloch vector representation. We give a geometric interpretation of the fact that any two quantum states have non-negative overlaps and utilize this to find restrictions on the geometry of the set of Bloch vectors. We show that quantum measurements in the POVM formalism can be associated with Bloch vectors whose norms are then bounded by the geometry of the set of Bloch vectors as well. Also, we discuss our new upper bound on the worst case success probability of any (n, m, p)-QRAC and its relation to the Nayak bound which states that any QRAC satisfies $m \geq (1 - H(p))n$ where $H(p)$ is the binary entropy function, $H(p) = -p\log p - (1-p)\log(1-p)$: When considering $(n, m > 3, p)$ as well as $(n \leq 15, 3, p)$-QRACs our new upper bound is above the upper bound implied by the Nayak bound.

Contents

1 Introduction

The limits of how well information can be stored in a physical system and then retrieved again is of central relevance in quantum information theory. In this thesis we will study some aspects of the information protocol known as a quantum random access code (QRAC, in short). A QRAC is the quantum version of a random access code (or RAC, in short) which will be introduced in this section. In Section 3 we give a proper definition of a QRAC after introducing the necessary mathematical framework of quantum mechanics in Section 2.

Imagine that a sender (Alice) and a recipient (Bob) are given the following task: Alice has to encode a message in the form of an n-bit string into a shorter message - a string of m bits ($m < n$) - and send this to Bob. Bob, upon receiving the m-bit string, has to recover (decode) any one of the initial n bits with a probability of at least $p > \frac{1}{2}$ (this inequality will become clear in the following). Alice and Bob are allowed to make a strategy before Alice receives the input string of n bits, but they are otherwise not allowed to cooperate and they do not know which of the initial n bits Bob will be asked to decode. A RAC, in general, is a solution to this task.

This preliminary description implies that a RAC must contain some joint encoding-decoding *strategy* for Alice and Bob to follow. To make it more clear what we mean by *strategy* we define for some values $n, m \in \mathbb{N}$ with $n > m$ an *encoding function* as a map $e : \{0,1\}^n \to \{0,1\}^m$, and a *decoding function* as a map $D_i : \{0,1\}^m \to \{0,1\}$. With these definitions at hand we make the following definition:

Definition 1.1. A *Classical* (n,m)*-strategy* is an ordered tuple

$$(P_e, P_{D_1}, ..., P_{D_n}), \tag{1.1}$$

where P_e is a probability distribution over encoding functions and for each $i \in \{1, ..., n\}$, P_{D_i} is a probability distribution over decoding functions.

In this setting we allow Alice and Bob to act probabilistically but not to cooperate. A classical (n,m)-strategy yields some probability, $p_{i,x}$, of decoding the ith bit of an n-bit string, $x \in \{0,1\}^n$, correctly. When assesing the performance of a strategy one could have different figures of merit. We will in this thesis consider two: (1) The *worst case success probability* where the performance is assessed by the minimum of $p_{i,x}$ over all possible pairs (i,x),

$$p_{\min} = \min_{i,x} p_{i,x}, \tag{1.2}$$

and (2) the *average success probability* where the performance is assessed by the average of $p_{i,x}$ over all possible pairs (i,x) given by

$$p_{\text{ave}} = \frac{1}{n2^n} \sum_{x \in \{0,1\}^n} \sum_{i=1}^{n} p_{i,x}. \tag{1.3}$$

A notational remark is that when we write a sum over all elements of $\{0,1\}^n$ using the symbol $\sum_{x \in \{0,1\}^n}$, it is to be understood as equivalent with $\sum_{x_1,...,x_n \in \{0,1\}} = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}}$. Also, we use the notation, $\overline{x_i}$, for the bit-flipped of x_i, hence it is 1 if x_i is 0 and vice versa. Thereby also, if $x \in \{0,1\}^n$ has x_i in its ith bit then $\overline{x} \in \{0,1\}^n$ has $\overline{x_i}$ in its ith bit.

Notice now, that the worst case success probability is, for any n and m, at least $\frac{1}{2}$ since this can be achieved by simply guessing. Formally, this corresponds to a strategy in which for every $i \in \{1, ..., n\}$, P_{D_i} is a uniform distribution of the two constant decoding functions, 0 and 1. We say therefore that a RAC exists for certain values of n and m only if it has a worst case success probability stricly larger than $\frac{1}{2}$. Hence the following definition:

Definition 1.2 (RAC)**.** A *RAC* is a classical (n, m)-*strategy* that yields a worst case success probability, p, that is strictly larger than $\frac{1}{2}$. A RAC will henceforth be denoted (n, m, p)-RAC.

If Alice and Bob share a quantum channel, then we have the quantum version of a RAC (or QRAC, in short). This is similar to a RAC except that Alice has to encode n classical bits of information into m qubits and Bob then has to recover any one of the initial bits, with a success probability of at least $p > \frac{1}{2}$, by performing a measurement upon the received quantum state. We will denote a QRAC by (n, m, p)-QRAC. Although we postpone a proper definition of a QRAC to Section 3 we will outline some history of this communication protocol here and then return to a fuller picture in section 3.

The idea behind a QRAC first appeared in a paper that was published in 1983 by Stephen Weisner [17] where it went by the name of *conjugate coding* as also noted in [3, 5]. The QRACs were then re-discovered and popularized by Ambainis et al. in [1, 2]. The original QRACs include a $(2, 1, \frac{1}{2} + \frac{1}{2\sqrt{2}})$-QRAC and a $(3, 1, \frac{1}{2} + \frac{1}{2\sqrt{3}})$-QRAC (found in [1] although the $(3, 1, \frac{1}{2} + \frac{1}{2\sqrt{3}})$-QRAC is attributed to Chuang). These can readily be generalized to $(2m, m, \frac{1}{2} + \frac{1}{2\sqrt{2}})$-QRACs and $(3m, m, \frac{1}{2} + \frac{1}{2\sqrt{3}})$-QRACs as we will see in detail in section 6. The original 1-qubit QRACs have been experimentally realized in 2009 in [16]. In the same year, they were shown to be optimal [3], in that the authors show that in any QRAC with $m = 1$ we have

$$p \leq \frac{1}{2} + \frac{1}{2\sqrt{n}}. \tag{1.4}$$

In [8] the authors propose a method of numerically constructing QRACs for $m > 1$. They use this method to find $(n, 2, p)$-QRACs for $3 \leq n \leq 9$ that perform better than the prior state of the art [13]. They also give an analytical $(3, 2, \frac{1}{2} + \frac{1}{\sqrt{6}})$-QRAC. The QRACs found by the proposed method all satisfy

$$p \leq \frac{1}{2} + \frac{1}{\sqrt{2n}}, \tag{1.5}$$

and for $3 \leq n \leq 6$ this bound is tight. Hence, they do not find $(4, 2, p)$- and $(6, 2, p)$-QRACs that perform better than combining two smaller QRACs in the above sense. This leads them to conjecture that any $(n, 2, p)$-QRAC has an upper bound on the worst case success probability given by (1.5). In this thesis we will prove this conjecture.

This thesis has the following structure: In Section 2 we introduce the necessary mathematical concepts of quantum mechanics. We define what we mean by quantum states and measurements. In Section 3 we give a propor definition of a QRAC and present more prior general findings about these codes than have been presented in this introductory section. A crucial part of our proof of the conjecture posed in [8] depends on the understanding of the geometry of quantum states in the Bloch vector representation. Therefore, in Section 4, we give a review of the Bloch vector representation of a quantum state and in the following Section 5 we study the geometry of the set of Bloch vectors. We give, in particular, a geometric interpretation of the fact that quantum states have non-negative overlaps which we believe has not been given in any prior research. This is used to find bounds on the geometry of the set of Bloch vectors. In Section 6, we utilize the gained knowledge about the geometry of quantum states to show explicit constructions of QRACs. We show also that a general quantum measurement (POVM) can be associated with a set of antiparallel Bloch vectors and utilize non-negativity of overlaps to derive an upper bound on the norms of these. This is followed by Section 7 in which in it shown how our findings in the prior sections lead to a proof of conjecture put forth in [8]. In Section 8 we discuss our new upper bound on the worst case success probability of any (n, m, p)-QRAC and its relation to the Nayak bound which will be presented in Section 3.

2 Quantum States and Measurements

In this section we review the mathematical concepts of pure and mixed quantum states. This is followed by a discussion of quantum measurements. To this end we follow [15]. We start by giving some preliminary remarks about some frequently used quantum mechanical notation for notions from linear algebra. We also make a number of claims that we will use without proof throughout the thesis.

We suppose that the reader is familiar with the concept of a Hilbert space. In this thesis the Hilbert space under consideration will be the finite-dimensional, $\mathbb{C}^N$, equipped with an inner product that will be defined shortly. Elements of this Hilbert space are column vectors denoted by a ket, $|\psi\rangle \in \mathbb{C}^N$. Such an element can be expanded in an orthonormal basis of $\mathbb{C}^N$ given by $\{|i\rangle\}_{i=1}^N$ such that

$$|\psi\rangle = \sum_{i=1}^{N} \alpha_i |i\rangle , \tag{2.1}$$

where $\alpha_i \in \mathbb{C}$.

We use the notation $A^\dagger$ about the Hermitian conjugate of a linear operator, A, acting on $\mathbb{C}^N$. In the matrix representation of A, finding the Hermitian conjugate amounts to tranposing and complex conjugating. An object written as $\langle\psi|$ is called a *bra* and it is an element of the dual space of $\mathbb{C}^N$ which has $\{\langle i|\}_{i=1}^N$ as an orthonormal basis. The dual of the element $|\psi\rangle \in \mathbb{C}^N$ is now defined as $|\psi\rangle^\dagger = \langle\psi|$ and it is therefore represented by a row vector with α_i^* in its ith entry. The bra $\langle\psi|$ can be expanded as a linear combination of elements of the set $\{\langle i|\}_{i=1}^N$ (which itself spans $\mathbb{C}^N$) such that

$$\langle\psi| = \sum_{i=1}^{N} \alpha_i^* \langle i| . \tag{2.2}$$

with $\beta_i \in \mathbb{C}$. The inner product

$$\langle\cdot|\cdot\rangle : \mathbb{C}^N \times \mathbb{C}^N \longrightarrow \mathbb{C}, \tag{2.3}$$

is then for two elements of $\mathbb{C}^N$, such as $|\psi\rangle$ (as in Eq. (2.1)) and $|\phi\rangle = \sum_{i=1}^N \beta_i |i\rangle$, defined as

$$\langle\phi|\psi\rangle = \sum_i \beta_i^* \alpha_i . \tag{2.4}$$

The outer product, i.e. an object given by $|\psi\rangle\langle\phi|$ for two elements of $\mathbb{C}^N$ is given by

$$|\psi\rangle\langle\phi| = \sum_{ij} \alpha_i \beta_j^* |i\rangle\langle j| \tag{2.5}$$

and it is therefore an N by N matrix with $\alpha_i\beta_j^*$ in its (i,j)'th entry. Since finding the Hermitian conjugate of a matrix amounts to transposing and complex conjugating we find that

$$(|\psi\rangle\langle\phi|)^\dagger = \sum_{ij} \alpha_i^* \beta_j |j\rangle\langle i| = |\phi\rangle\langle\psi| . \tag{2.6}$$

An operator, A, acting on $\mathbb{C}^N$, that fulfills $A^\dagger = A$ is called *Hermitian*. Suppose A is Hermitian. Then, by the *spectral decomposition theorem* (see [15] for details) there exists an orthonormal basis of $\mathbb{C}^N$ with respect to which A is diagonal. In fact, one can show that the normalized eigenvectors of A form an orthonormal basis of $\mathbb{C}^N$. Also, the eigenvalues of a Hermitian operator can be shown to be real.

In the following, an operator, A, is frequently referred to as *positive semi-definite*. By

this mean that the inner product, $\langle\psi| A |\psi\rangle$, is real and non-negative for any vector $|\psi\rangle \in \mathbb{C}^N$. It can be shown (see for example [11]) that an operator acting on $\mathbb{C}^N$ is positive semi-definite if and only if it is Hermitian and its eigenvalues are non-negative. It can also be shown that for any operator, B, $B^\dagger B$ is positive semi-definite.

We will also need to consider the set of all linear operators acting on $\mathbb{C}^N$, denoted $\mathcal{L}(\mathbb{C}^N)$, as a Hilbert space. $\mathcal{L}(\mathbb{C}^N)$ is a vector space since for any two $\alpha, \beta \in \mathbb{C}$ and any two $A, B \in \mathcal{L}(\mathbb{C}^N)$ we hve that $\alpha A + \beta B \in \mathcal{L}(\mathbb{C}^N)$ and it contains 0. $\mathcal{L}(\mathbb{C}^N)$ can be equipped with the *Hilbert-Schmidt* inner product

$$(\cdot,\cdot)_{HS} : \mathcal{L}(\mathbb{C}^N) \times \mathcal{L}(\mathbb{C}^N) \longrightarrow \mathbb{C} \tag{2.7}$$

defined by

$$(A, B)_{HS} = \mathrm{Tr}[A^\dagger B], \tag{2.8}$$

which turns it into a Hilbert space.

2.1 Quantum States - Pure and Mixed

Postulate 1 of quantum mechanics [1] contains the fundamental notion of quantum physical states: The state space of an isolated physical system is a Hilbert space and the system is completely described by its state vector which is a unit vector in the system's state space.

From this postulate we see that a quantum state can be written as a unit column vector, $|\psi\rangle$, in a state space which we take to be $\mathbb{C}^N$. If $\{\alpha_i\}_{i=1}^N$ is the set of expansion coefficients of $|\psi\rangle$ in an orthonormal basis $\{|i\rangle\}_{i=1}^N$ then the normalization requirement can be expressed as

$$\sum_i |\alpha_i|^2 = 1, \tag{2.9}$$

which is equal to $\langle\psi|\psi\rangle$. Hence the following definition

Definition 2.1 (*Pure quantum state*)**.** *A pure quantum state* (or *pure state*, in short) is a column vector denoted by a ket, $|\psi\rangle \in \mathbb{C}^N$ which fulfills the normalization requirement $\langle\psi|\psi\rangle = 1$.

Now, the simplest quantum mechanical system is that of a *qubit*. This corresponds to $N = 2$ such that a quantum state is a superposition of two orthogonal unit vectors, $|0\rangle$ and $|1\rangle$. Here we see the fundamental difference between a classical bit and a qubit. A classical bit is in one of two possible states, 0 or 1. A qubit is a superposition of two possible states $|0\rangle$ and $|1\rangle$. Additionally, just as well as two classical bits have four possible states - 00, 01, 10, and 11 - the state space of a two qubit system is spanned by four orthogonal unit vectors, $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$, spanning $\mathbb{C}^4$. Here $|x_1x_2\rangle = |x_1\rangle \otimes |x_2\rangle$ for $x_1, x_2 \in \{0, 1\}$. In general the state space of an m qubit system is $\mathbb{C}^{2^m}$.

Suppose now that a quantum system is in one of a number of different pure states indexed by i, $|\psi_i\rangle$. Specifically it is in the state $|\psi_i\rangle \in \mathbb{C}^N$ with probability of p_i. Such a probabilistic mixture of pure states is called a *mixed state* and the object $\{p_i, |\psi_i\rangle\}$ is called an *ensemble of pure states*. This brings about the following definition.

Definition 2.2 (*Density operator*)**.** *The density operator* of a mixed quantum state given by an ensemble of pure states, $\{p_i, |\psi\rangle_i\}$ is given by

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| . \tag{2.10}$$

[1] This postulate can be found in different equivalent formulations in the litterature. In this presentation we follow [15].

The following theorem provides us with a necessary and sufficient condition for any operator in $\mathcal{L}(\mathbb{C}^{\mathbb{N}})$ to be a density operator.

Theorem 2.1. *An operator, $\rho \in \mathcal{L}(\mathbb{C}^N)$ is the density operator associated to some ensemble of pure states, $\{p_i, |\psi_i\rangle\}$ if and only if it has trace equal to 1 and it is positive semi-definite.*

Proof. Suppose first that ρ is a density operator. Notice, that for any pure state, $|\psi\rangle \in \mathbb{C}^N$, we have that

$$|\psi\rangle\langle\psi| = \sum_{i,j} \alpha_i \alpha_j^* |i\rangle\langle j|, \tag{2.11}$$

which is an N by N matrix with $\alpha_i \alpha_j^*$ in its (i,j)th entry. Its diagonal elements are $|\alpha_i|^2$ and hence it has a trace equal to 1. The trace of ρ is then

$$\mathrm{Tr}[\rho] = \sum_i p_i \mathrm{Tr}[|\psi_i\rangle\langle\psi_i|] = \sum_i p_i = 1, \tag{2.12}$$

since the trace is a linear. Also, ρ is positive semi-definite since for any $|\phi\rangle \in \mathbb{C}^N$ we have

$$\langle\phi|\rho|\phi\rangle = \sum_i p_i \langle\phi|\psi_i\rangle\langle\psi_i|\phi\rangle = \sum_i p_i \left|\langle\phi|\psi_i\rangle\right|^2 \geq 0. \tag{2.13}$$

Conversely, suppose that ρ has trace equal to 1 and is positive semi-definite. Since ρ, in particular, is Hermitian its normalised eigenvectors, denoted $|\lambda_i\rangle$, form an orthonormal basis of $\mathbb{C}^N$ in which ρ is diagonal such that $\rho = \sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i|$ where λ_i are the eigenvalues of ρ. Since it is assumed that $\mathrm{Tr}[\rho] = 1$ we see that $\sum_i \lambda_i = 1$ and hence ρ is the density operator corresponding to the ensemble of pure states given by $\{\lambda_i, |\lambda_i\rangle\}$. □

Notice that any quantum state - pure or mixed - can be given in terms of a density operator. A pure state, $|\psi\rangle \in \mathbb{C}^N$, corresponds to a probability of 1 that the system is in the state described by $|\psi\rangle \in \mathbb{C}^N$ such that its density matrix is given as in Eq. (2.11). The above Theorem leads us to the following definition of the *density operator space*.

Definition 2.3 (*Density operator space*)**.** *The density operator space* is the following subset of $\mathcal{L}(\mathbb{C}^N)$:

$$\mathcal{L}_{+,1}(\mathbb{C}^N) = \{\rho \in \mathcal{L}(\mathbb{C}^N) | \rho^\dagger = \rho \ , \ \mathrm{eig}_k(\rho) \geq 0 \ , \ \mathrm{Tr}[\rho] = 1\}, \tag{2.14}$$

where $\mathrm{eig}_k(\rho)$ denotes the kth eigenvalue of ρ.

Remark now, that a density operator is idempotent if and only if it is the density operator of a pure state. This can be seen by diagonalizing it or in other words writing it in the basis given by its normalized eigenvectors, say $\{|\psi_i\rangle\}$ such that we get

$$\rho^2 = \sum_i p_i^2 |\psi_i\rangle\langle\psi_i|, \tag{2.15}$$

which is equal to ρ if and only if all the eigenvalues p_i vanish except for one $p_{i'} = 1$ which corresponds to ρ being a pure state. We see therefore that

$$\mathrm{Tr}[\rho^2] = \sum_i p_i^2 \leq 1, \tag{2.16}$$

with equality if and only if ρ is a pure state. Therefore a simple way to check whether a state is pure is to take the trace of its density matrix to the second power.

2.2 Quantum Measurements

Postulate 3 of quantum mechanics[2] provides the fundamental notion of quantum measurements: Quantum measurements are described by a set of measurement operators, $\{M_m\} \subset \mathcal{L}(\mathbb{C}^N)$, fulfilling the following completeness relation

$$\sum_m M_m^\dagger M_m = I. \tag{2.17}$$

These are operators acting on the state space of the system being measured and m refers to the outcome of the measurement. If the state of the system immediately before the measurement is denoted $|\psi\rangle$, then the probability of getting outcome m is given by

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle . \tag{2.18}$$

The postulate also contains a statement about the state of the system after the measurement. This is given by

$$\frac{M_n}{\sqrt{\langle\psi|M_n^\dagger M_n|\psi\rangle}} |\psi\rangle . \tag{2.19}$$

Notice that the completeness relation ensures that the probabilities sum to one,

$$1 = \sum_m p(m) = \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle . \tag{2.20}$$

Since considering mixed states when constructing QRACs is inevitable we follow [15] and give a reformulation of postulate 3 in terms density matrices. First, observe that for an arbitrary operator A and a quantum state, $|\psi\rangle$, we have

$$\mathrm{Tr}[A|\psi\rangle\langle\psi|] = \sum_i \langle\psi|i\rangle\langle i| A |\psi\rangle = \langle\psi| A |\psi\rangle , \tag{2.21}$$

where we have used that $I = \sum_i |i\rangle\langle i|$. This means that if initially the system is in a state $|\psi_i\rangle$, then performing a measurement described by M_m yields a probability

$$p(m||\psi_i\rangle) = \langle\psi_i| M_m^\dagger M_m |\psi_i\rangle = \mathrm{Tr}[M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|] \tag{2.22}$$

of getting result m. Due to the law of total probability we then get

$$p(m) = \sum_i p_i p(m||\psi_i\rangle) = \sum_i p_i \mathrm{Tr}[M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|] = \mathrm{Tr}[M_m^\dagger M_m \rho], \tag{2.23}$$

where we have used that the trace is linear. To see what the density operator is after measurement of m notice first the standard result of probability theory: $p(m||\psi_i\rangle)p(|\psi_i\rangle) = p(|\psi_i\rangle|m)p(m)$. Hence

$$p(|\psi_i\rangle|m) = \frac{\mathrm{Tr}[M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|]}{\mathrm{Tr}[M_m^\dagger M_m \rho]} p_i. \tag{2.24}$$

Therefore, if the system was in the state $|\psi_i\rangle$ before the measurement, then after obtaining the result m it will be in the state given by (2.19). Thus, after performing a measurement that yields m we have an ensemble of states with respective probabilities of $p(|\psi_i\rangle|m)$ such that the corresponding density matrix can be found as

$$\rho_m = \sum_i p(|\psi_i\rangle|m) \frac{M_m |\psi_i\rangle\langle\psi_i| M_m^\dagger}{\langle\psi_i| M_m^\dagger M_m |\psi\rangle} = \sum_i p_i \frac{M_m |\psi_i\rangle\langle\psi_i| M_m^\dagger}{\mathrm{Tr}[M_m^\dagger M_m \rho]} = \frac{M_m \rho M_m^\dagger}{\mathrm{Tr}[M_m^\dagger M_m \rho]}, \tag{2.25}$$

where we used Eqs. (2.21) and (2.24).

For many purposes the state after the measurement is of little interest. This is also the

[2]Same comment as in the previous subsection.

case when considering QRACs. Therefore we will employ the POVM formalism in our analysis of quantum measurements.

Let

$$E_m = M_m M_m^\dagger \tag{2.26}$$

where M_m is an element of a general quantum measurement. Then $\{E_m\}$ is a set of positive semidefinite operators fulfilling the completeness relation

$$\sum_m E_m = I. \tag{2.27}$$

And if a quantum system is in a state given by ρ then the probability of getting outcome m upon measurement is given by

$$p(m) = \mathrm{Tr}[E_m \rho]. \tag{2.28}$$

Hence the set of operators given by $\{E_m\}$ is sufficient to determine the probabilities associated with the quantum measurement given by $\{M_m\}$. On the other hand, if $\{E_m\}$ is any set of positive semidefinite operators fulfilling eq. (2.27) then there is a quantum measurement, $\{M_m\}$, associated with $\{E_m\}$. One can show that positive semidefinite matrices have unique positive semidefinite square roots such that if we let $M_m = \sqrt{E_m}$ we see that the completeness requirement, $\sum_m M_m M_m^\dagger = I$ is fulfilled. Hence the following definition.

Definition 2.4 (*POVM*)**.** A *POVM* is a set of positive semi-definite operators, $\{E_m\}$, fulfilling $\sum_m E_m = I$.

The POVM formalism provides a simple means by which one can study the statistics of general quantum measurements without having to know about the system after the measurement. We will use this formalism in the remainder of the thesis.

3 What is a Quantum Random Access Code?

In this section we will properly introduce what a QRAC is. The preliminary description of a QRAC given in the introduction suggests the following rewriting of a *strategy* in the quantum case.

Definition 3.1 (*Quantum*(n,m)*-strategy*)**.** A *Quantum* (n,m)*-strategy* is an encoding map

$$e : \{0,1\}^n \longrightarrow \mathcal{L}_{+,1}(\mathbb{C}^{2^m}) \tag{3.1}$$

and n POVMs denoted $\{D_i^0, D_i^1\}_{i=1}^n$.

Therefore, suppose that some input string $x \in \{0,1\}^n$ has x_i in its ith bit. Then, based on the discussion in Section 2, the probability that Bob correctly decodes the ith bit to be x_i is given by

$$p_{i,x} = \mathrm{Tr}[e(x) D_i^{x_i}]. \tag{3.2}$$

All the considerations regarding the average and worst case success probabilities are the same as in the classical case. Bob could still just randomly guess. This corresponds to a strategy in which $D_i^0 = D_i^1 = \frac{1}{2} I$ for all $i \in \{1, ..., n\}$ and this yields success probabilities of $\frac{1}{2}$ independent of the input string and bit to be recovered. Hence for a strategy to be non-trivial we require that the worst case success probability is strictly larger than $\frac{1}{2}$ which suggests the following definition.

Definition 3.2 (*QRAC*)**.** A *QRAC* is a quantum (n,m)-strategy that yields a worst case success probability strictly larger than $\frac{1}{2}$.

It is interesting to notice that in the classical setting, Bob, after recovering one bit of the initial string with a probability of at least a half, could go on and try to recover another bit of the original string also with a probability of at least a half. This is not the case in the quantum version since, as we saw in Section 2, measurements disturb the system.

On the other hand, QRACs compared to RACs can exist with longer initial strings. Consider the following theorem that is proved in [9].

Theorem 3.1. *For any $n \in \mathbb{N}$ there exists a $(4^n - 1, n, p)$-QRAC but there does not exist a $(4^n, n, p)$-QRAC. Moreover, there exists a $(2^n - 1, n, p)$-RAC but there does not exist a $(2^n, n, p)$-RAC.*

This theorem implies a quantum advantage in this type of coding. Notice, for example, that a $(2, 1, p)$-RAC does not exist while, as noted in the introduction, there exists a $(2, 1, \frac{1}{2} + \frac{1}{2\sqrt{2}})$-QRAC. In fact, explicit (n, m, p)-QRACs have been constructed for any n and $m \leq 4^n - 1$ [13, 9]. We will reproduce these concrete constructions in Section 6.

A general upper bound on the success probability, p, in a (n, m, p)-QRAC was found by Nayak [14]. Consider the following theorem (see [14] for a proof).

Theorem 3.2. *Any (n, m, p)-QRAC must obey*

$$m \geq (1 - H(p))n, \tag{3.3}$$

where $H(p)$ is the binary entropy function given by

$$H(p) = -p \log p - (1 - p) \log(1 - p). \tag{3.4}$$

However, as already noted, in [3] it is shown that $(n, 1, p)$-QRACs for $n = 2, 3$ have a lower upper bound on the success probabilities of $\frac{1}{2} + \frac{1}{2\sqrt{n}}$, which is approximately equal to 0.85 and 0.79 for n equal to 2 and 3, respectively. These probabilities have a gap to the Nayak bound which when $m = 1$ implies an upper bound of approximately 0.89 and 0.83 when n is equal to 2 and 3, respectively. The original and optimal $(n, 1, \frac{1}{2} + \frac{1}{2\sqrt{n}})$-QRACs use only pure encoding states. Mixed states become useful when $m \geq 2$ as we will see later. For example, in [13] the author, by numerical searches, finds $(n, 2, p)$-QRACs that use only pure encoding states for n up to 12. It is still, to the best of my knowledge, an open question whether n can be 13, 14 or 15 in a $(n, 2, p)$-QRAC with the constraint that one can only use pure encoding states.

In [8] the authors provide a new way of numerically constructing QRACs that perform better than those previously known in [13], as also noted in the introduction. They use see-saw iterations of semidefinite programming switching between keeping either the encoding states or the POVMs fixed and optimizing with respect to the other one (see [8] for details). Going back and forth like this until no improvement in the success probability is gained after several iterations gives a constructive way of finding QRACs that perform well. For $3 \leq n \leq 6$ they find that using pure encoding states gives better performance while for $n > 6$ the worst case success probability grows if they allow the encoding states to be mixed. Besides the analytical $(n, 2, \frac{1}{2} + \frac{1}{\sqrt{2n}})$-QRACs for $n = 3, 4, 6$ they find a $(5, 2, \approx 0.811)$-QRAC that uses pure encoding states and whose worst case success probability is very close to $\frac{1}{2} + \frac{1}{\sqrt{10}}$. Furthermore, they find $(7, 2, \approx 0.702)$-, $(8, 2, \approx 0.690)$- and $(9, 2, \approx 0.671)$-QRACs that all use mixed encoding states. By purifying the encoding states in their $(7, 2, \approx 0.702)$-QRAC the worst case success probability drops to 0.561. On the other hand the average success probability increases from 0.716 to 0.734 [8]. The reason for this is explained by the following proposition.

Proposition 3.1. *For any QRAC using mixed encoding states with an average success probability of p^m_{ave} there exists a QRAC using only pure encoding states with an average success probability of $p^p_{ave} \geq p^m_{ave}$.*

Proof. Suppose we have a QRAC with POVMs given by $\{D^0_i, D^1_i\}$ and a mixed state given by

$$\rho_x = \sum_j q_j \left|\psi^j_x\right\rangle \left\langle\psi^j_x\right| \tag{3.5}$$

for encoding the string $x \in \{0,1\}^n$ with x_i in its ith bit. The average success probability of being correct when trying to recover a bit of x is given by

$$\tfrac{1}{n}\sum_{i=1}^{n} \mathrm{Tr}[D^{x_i}_i \rho_x] = \sum_j q_j \big(\tfrac{1}{n}\sum_{i=1}^{n} \mathrm{Tr}[D^{x_i}_i \left|\psi^j_x\right\rangle \left\langle\psi^j_x\right|]\big). \tag{3.6}$$

Now, the term in the paratheses is the average success probability corresponding to the encoding state being the pure state $\left|\psi^j_x\right\rangle \left\langle\psi^j_x\right|$. This will have a maximum for some j' which means that a QRAC with the same POVMs as above but the pure state

$$\rho'_x = \left|\psi^{j'}_x\right\rangle \left\langle\psi^{j'}_x\right| \tag{3.7}$$

for encoding the string $x \in \{0,1\}^n$ performs at least as well. □

The proof of the conjecture posed in [8] depends upon knowledge of the geometry of quantum states in the Bloch vector representation. In the next section we introduce this.

4 Bloch Vector Representation of a Quantum State

We will in this section see that one can bijectively associate a quantum state, an element of $\mathcal{L}_{+,1}(\mathbb{N}^N)$, with a real vector in $\mathbb{R}^{N^2-1}$. In the following we will be talking about a "set of generators" so we begin by defining exactly what we mean by that.

Definition 4.1. (*Set of generators*) A *set of generators* is a set of linear operators, $\{\tilde{\sigma}_i\}_{i=1}^{N^2-1} \subset \mathcal{L}(\mathbb{C}^N)$, whose elements fulfill

$$(i)\ \tilde{\sigma}_i = \tilde{\sigma}_i^\dagger\ ,\ (ii)\ \mathrm{Tr}[\tilde{\sigma}_i] = 0\ ,\ (iii)\ \mathrm{Tr}[\tilde{\sigma}_i\tilde{\sigma}_j] = 2\delta_{ij}. \tag{4.1}$$

In the remainder of this thesis we will denote a set of generators by a symbol such as $\tilde{\sigma}, \lambda$ or σ and assume that there is some ordering of the set such that we can denote the ith element of a set of generators by $\tilde{\sigma}_i$. We reserve the symbol $\tilde{\sigma}$ for a generic set of generators.

The factor of 2 in (iii) is conventional. In fact, we only strictly need the $\tilde{\sigma}_i$'s to be linearly independent and not necessarily orthogonal (in the sense of the Hilbert-Schmidt inner product). We include the orthogonality requirement since it simplifies the following discussion without loss of generality. Notice, that (ii) implies that the identity, I, is orthogonal with all the $\tilde{\sigma}_i$'s. Hence, the generators, $\tilde{\sigma}_i$, with the identity form a complete orthogonal basis for the set of linear operators $\mathcal{L}(\mathbb{C}^N)$. It is convenient to think of a set of generators in the form of a vector, such that for a vector $\alpha \in \mathbb{C}^{N^2-1}$ that has α_i in its ith entry we define

$$\alpha \cdot \tilde{\sigma} = \sum_{i=1}^{N^2-1} \alpha_i \tilde{\sigma}_i. \tag{4.2}$$

It follows, that if $S \in \mathcal{L}(\mathbb{C}^N)$, then there exist unique $\alpha_0 \in \mathbb{C}$ and $\alpha \in \mathbb{C}^{N^2-1}$ such that

$$S = \alpha_0 I + \tfrac{1}{2}\alpha \cdot \tilde{\sigma}, \tag{4.3}$$

where $\alpha_0 = \frac{1}{N}\mathrm{Tr}[S]$ and $\alpha_i = \frac{1}{2}\mathrm{Tr}[S\tilde{\sigma}_i]$. Now, it is easily verified that $S \in \mathcal{L}(C^N)$ is Hermitian if and only if $\alpha_0 \in \mathbb{R}$ and $\alpha \in \mathbb{R}^{N^2-1}$. Also, S has trace equal to 1 if and only if $\alpha_0 = \frac{1}{N}$. These observations suggest the following definition:

Definition 4.2 (Bloch vector)**.** Given a set of generators, $\tilde{\sigma}$, and a density operator, ρ_β, the unique vector, $\beta \in \mathbb{R}^{N^2-1}$, such that

$$\rho_\beta = \tfrac{1}{N} I + \tfrac{1}{2}\beta \cdot \tilde{\sigma}. \tag{4.4}$$

is called the *Bloch vector* with respect to the set of generators, $\tilde{\sigma}$, associated with the quantum state, ρ_β.

We see from the observations above that the ith component of a Bloch vector with respect to the set of generators, $\tilde{\sigma}$, is given by

$$\beta_i = \mathrm{Tr}[\rho_\beta \tilde{\sigma}_i]. \tag{4.5}$$

The reverse, namely that any element $\beta' \in \mathbb{R}^{N^2-1}$ can be associated with a quantum state is, however, not true. β' is a Bloch vector if and only if, according to Definition (2.3), the eigenvalues of the operator

$$\tfrac{1}{N} I + \tfrac{1}{2}\beta' \cdot \tilde{\sigma}, \tag{4.6}$$

are non-negative. For $k \in \{1, ..., N\}$ we need the kth eigenvalue of (4.6) to be non-negative hence we need

$$\tfrac{1}{N} + \tfrac{1}{2}\mathrm{eig}_k(\beta' \cdot \tilde{\sigma}) \geq 0, \tag{4.7}$$

which entails requirements for a vector in $\mathbb{R}^{N^2-1}$ to be a Bloch vector that will be studied in the following section. Here we give the definition.

Definition 4.3 (*Bloch vector space*)**.** The *Bloch vector space* (henceforth, in short, *Bloch space*) is the following subset of $\mathbb{R}^{N^2-1}$,

$$\mathcal{B}(\mathbb{R}^{N^2-1}) = \{\beta \in \mathbb{R}^{N^2-1} | \forall k \in \{1, ..., N\} : \mathrm{eig}_k(\beta \cdot \tilde{\sigma}) \geq -\tfrac{2}{N}\}. \tag{4.8}$$

Before we turn our attention to a more detailed study of the geometry of the set $\mathcal{B}(\mathbb{R}^{N^2-1})$ we make a few more comments about a set of generators.

Let $[\cdot,\cdot]$ and $\{\cdot,\cdot\}$ be the commutator and anti-commutator, respectively. Then, for any two elements of a set of generators, $\tilde{\sigma}_i, \tilde{\sigma}_j$ we have that $-i[\tilde{\sigma}_i, \tilde{\sigma}_j]$ and $\{\tilde{\sigma}_i, \tilde{\sigma}_j\}$ are Hermitian operators which means that they can be expanded as linear combinations of I and the $\tilde{\sigma}_i$'s with real coefficients, such that

$$[\tilde{\sigma}_i, \tilde{\sigma}_j] = i\alpha_0 I + i\alpha_{ij} \cdot \tilde{\sigma} \tag{4.9}$$

$$\{\tilde{\sigma}_i, \tilde{\sigma}_j\} = \alpha'_0 I + \alpha'_{ij} \cdot \tilde{\sigma}, \tag{4.10}$$

where $\alpha_0, \alpha'_0 \in \mathbb{R}$ and $\alpha_{ij}, \alpha'_{ij} \in \mathbb{R}^{N^2-1}$. Now, notice that taking the trace of the following,

$$\tilde{\sigma}_i\tilde{\sigma}_j \pm \tilde{\sigma}_j\tilde{\sigma}_i = \tfrac{1}{2}([\tilde{\sigma}_i, \tilde{\sigma}_j] + \{\tilde{\sigma}_i, \tilde{\sigma}_j\}) \mp \tfrac{1}{2}([\tilde{\sigma}_i, \tilde{\sigma}_j] - \{\tilde{\sigma}_i, \tilde{\sigma}_j\}), \tag{4.11}$$

yields that $\alpha_0 = 0$ and $\alpha'_0 = \frac{4}{N}\delta_{ij}$ using the relations in Eqs. (4.1). Now we define f_{ijk} to be the kth component of $\frac{1}{2}\alpha_{ij}$ and g_{ijk} to be the kth component of $\frac{1}{2}\alpha'_{ij}$, which therefore means that

$$[\tilde{\sigma}_i, \tilde{\sigma}_j] = 2i \sum_k f_{ijk}\tilde{\sigma}_k \tag{4.12}$$

$$\{\tilde{\sigma}_i, \tilde{\sigma}_j\} = \tfrac{4}{N}\delta_{ij} I + 2\sum_k g_{ijk}\tilde{\sigma}_k \tag{4.13}$$

where $f_{ijk}, g_{ijk} \in \mathbb{R}$ are called the *structure constants* of $\tilde{\sigma}$. If we define a complex structure constant by $z_{ijk} = g_{ijk} + if_{ijk}$, we find the product

$$\tilde{\sigma}_i\tilde{\sigma}_j = \tfrac{2}{N}\delta_{ij} I + \sum_k z_{ijk}\tilde{\sigma}_k \tag{4.14}$$

by adding Eq. (4.12) and Eq. (4.13) and taking half of the result. The structure constants can readily be calculated by multiplying through Eq. (4.12) and Eq. (4.13) by $\tilde{\sigma}_{k'}$ and taking traces to get

$$f_{ijk'} = \tfrac{1}{4i}\mathrm{Tr}[\tilde{\sigma}_i, \tilde{\sigma}_j]\tilde{\sigma}_{k'}, \tag{4.15}$$

$$g_{ijk'} = \tfrac{1}{4}\mathrm{Tr}\{\tilde{\sigma}_i, \tilde{\sigma}_j\}\tilde{\sigma}_{k'}. \tag{4.16}$$

Due to the fact that the trace is invariant under cyclic permutations one can see that f_{ijk} is totally antisymmetric and g_{ijk} is totally symmetric under permutations of the indices.

We round off this section by exhibiting some commonly used sets of generators in the following examples.

Example 4.1 (The Pauli matrices)**.** . A canonical example of a set of generators is that of the *Pauli matrices*. Let $N = 2$ and

$$p_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; p_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; p_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \; p_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{4.17}$$

Then p_1, p_2 and p_3 fulfill the requirements in Definition 4.1 such that these with p_0 form a complete orthogonal basis for $\mathcal{L}(\mathbb{C}^2)$.

Example 4.2 (The Gell-Mann matrices)**.** . Let $\{|1\rangle, |2\rangle, ..., |N\rangle\}$ be the standard orthonormal basis of $\mathbb{C}^N$ and define the following $\frac{N(N-1)}{2}$ symmetric matrices

$$\lambda^s_{jk} = \left\{ |j\rangle\langle k| + |k\rangle\langle j| \;\middle|\; 1 \le j < k \le N \right\} \tag{4.18}$$

and the $\frac{N(N-1)}{2}$ antisymmetric matrices

$$\lambda^a_{jk} = \left\{ -i|j\rangle\langle k| + i|k\rangle\langle j| \;\middle|\; 1 \le j < k \le N \right\} \tag{4.19}$$

and the $N-1$ diagonal matrices

$$\lambda^d_l = \left\{ \sqrt{\tfrac{2}{d(d+1)}} \Big(\sum_{j=1}^{l} |j\rangle\langle j| + l\,|l+1\rangle\langle l+1| \Big) \;\middle|\; 1 \le l \le N-1 \right\}. \tag{4.20}$$

The *Gell-Mann matrices*, denoted λ_i, are then given as the $N^2 - 1$ elements of the set $\lambda^s_{jk} \cup \lambda^a_{jk} \cup \lambda^d$. Notice that when $N = 2$ the Gell-Mann matrices reduce to the Pauli matrices.

Example 4.3. Another set of generators can be found for $N = 2^m$ with $m \in \mathbb{N}$ by appropriately tensoring Pauli matrices as in [13]:

$$\sigma_k = \tfrac{1}{\sqrt{2^{m-1}}} \bigotimes_{i=1}^{m} p_{c_i(k_4)}, \tag{4.21}$$

where p_i is the ith Pauli matrix as in Example 4.1. $c_i(k_4)$ is the ith digit from the right in the base four representation of k.

5 Bloch Space Geometry

We begin this section with some preliminary well-known (see for example [6, 4]) facts about the geometry of Bloch space. First of all, notice that $\mathcal{B}(\mathbb{R}^{N^2-1})$ must be a convex set: This follows from the fact that $\mathcal{L}_{+,1}(\mathbb{C}^N)$ is certainly a convex set in the sense that if $\rho_1, \rho_2 \in \mathcal{L}_{+,1}(\mathbb{C}^N)$, then a probabilitistic mixture ,

$$\theta\rho_1 + (1-\theta)\rho_2, \tag{5.1}$$

is also a density operator (one can check by using the definition). Therefore, if $a_1, a_2 \in \mathcal{B}(\mathbb{R}^{N^2-1})$, then when taking a probabilistic mixture of their corresponding density matrices we get

$$\frac{1}{N}I + (\frac{\theta}{2}a_1 + \frac{1-\theta}{2}a_2) \cdot \tilde{\sigma}, \tag{5.2}$$

such that a probabilitistic mixture of Bloch vectors is also a valid Bloch vector.

Also, the set $\mathcal{B}(\mathbb{R}^{N^2-1})$ must be closed: A boundary point, $b \in \mathcal{B}(\mathbb{R}^{N^2-1})$, must correspond to an operator that has at least one eigenvalue equal to 0, making it infinitesimally close to an invalid state. But since we only require positive semi-definiteness this boundary itself corresponds to a quantum state and therefore $b \in \mathcal{B}(\mathbb{R}^{N^2-1})$.

Furthermore, in the following we will make use of the fact that an overlap between two states, $\rho_a, \rho_b \in \mathcal{L}_{+,1}(\mathbb{C}^N)$ is given by $\mathrm{Tr}[\rho_a\rho_b]$ and by using that the trace is a linear operator we can express this in terms of their corresponding Bloch vectors as

$$\mathrm{Tr}[\rho_a\rho_b] = \frac{1}{N} + \frac{1}{2}a \cdot b. \tag{5.3}$$

Orthogonal Bloch vectors correspond to states with an overlap of $\frac{1}{N}$. We call such states *unbiased*.

Now we find restrictions on the norm of an element of $\mathcal{B}(\mathbb{R}^{N^2-1})$ in the following proposition. This proposition is also well-known (see for example [10, 13]) but since it is of much importance in our further investigations, we include a proof here.

Proposition 5.1. *Let* $r_N = \sqrt{\frac{2}{N(N-1)}}$ *and* $R_N = \sqrt{2\frac{N-1}{N}}$ *and let*

$$\mathcal{D}_s(\mathbb{R}^{N^2-1}) = \{\beta \in \mathbb{R}^{N^2-1} \,|\, |\beta| \leq r_N\}, \tag{5.4}$$

and

$$\mathcal{D}_l(\mathbb{R}^{N^2-1}) = \{\beta \in \mathbb{R}^{N^2-1} \,|\, |\beta| \leq R_N\}. \tag{5.5}$$

Then following inclusions

$$\mathcal{D}_s(\mathbb{R}^{N^2-1}) \subseteq \mathcal{B}(\mathbb{R}^{N^2-1}) \subseteq \mathcal{D}_l(\mathbb{R}^{N^2-1}) \tag{5.6}$$

hold. Moreover, any $\beta \in \mathcal{B}(\mathbb{R}^{N^2-1})$ *has norm equal to* R_N *if and only if it corresponds to a pure state.*

Proof. From the observations above and in Section 2 we notice that if $\beta \in \mathcal{B}(\mathbb{R}^{N^2-1})$ then for its corresponding density operator, ρ_β, we have that

$$\mathrm{Tr}[\rho_\beta^2] = \frac{1}{N} + \frac{1}{2}|\beta|^2 = \sum_k \mathrm{eig}_k(\rho_\beta)^2, \tag{5.7}$$

such that

$$|\beta| = \sqrt{2\mathrm{Tr}[\rho_\beta^2] - r_N R_N} = \sqrt{-r_N R_N + 2\sum_k \mathrm{eig}_k(\rho_\beta)^2} \tag{5.8}$$

since $r_N R_N = \frac{2}{N}$. Now, from Section 2, we know that $\mathrm{Tr}[\rho_\beta] \leq 1$ with equality if and only if ρ_β is pure. This means that $|\beta| \leq \sqrt{2 - r_N R_N} = R_N$ with equality if and only if β is the Bloch vector of a pure state. This shows the second inclusion and the last part of the proposition.

Now, any boundary point of $\mathcal{B}(\mathbb{R}^{N^2-1})$ must correspond to a density operator that has at least one eigenvalue equal to 0, as remarked above. We can find the shortest distance from the origin to any boundary point by the following consideration. We think of the

eigenvalues as entries of a vector, $\overline{\text{eig}(\rho_\beta)} = (\text{eig}_1(\rho), ...) \in \mathbb{R}^{N-l}$ where $l \geq 1$ is the number of eigenvalues that are equal to 0. Define now $x = (1, ..., 1) \in \mathbb{R}^{N-l}$ and the Cauchy-Schwarz inequality (i.e. $a \cdot b \leq |a||b|$ for any $a, b \in \mathbb{R}^n$ with $n \in \mathbb{N}$) therefore gives

$$1 = \overline{\text{eig}(\rho_\beta)} \cdot x \leq \left|\overline{\text{eig}(\rho_\beta)}\right||x| = \sqrt{N-l}\sqrt{\sum_k \text{eig}_k(\rho_\beta)^2}. \tag{5.9}$$

Thereby the sum of the squares of the eigenvalues is lower bounded by $\frac{1}{N-1}$ corresponding to exactly one eigenvalue being 0. Using this in Eq. (5.8) yields a Bloch vector length of r_N which shows the first inclusion. □

Notice that the above proposition is independent of the choice of set of generators. For the remainder of this thesis we refer to R_N as the radius of the *outsphere* and r_N as the radius of the *insphere*. Notice that for $N = 2$ the inclusive relations in (5.6) coincide and Bloch space becomes a Ball of radius $r_2 = R_2 = 1$.

Remark also that a boundary Bloch vector has norm equal to r_N if and only if its corresponding density matrix has exactly one eigenvalue equal to 0 and $N-1$ eigenvalues equal to $\frac{1}{N-1}$ which can be confirmed in the following way. We know already that exactly one eigenvalue must be 0 from the above proof. Suppose, without loss of generality that $\text{eig}_N(\rho_\beta) = 0$ and $\text{eig}_i(\rho_\beta) > 0$ for $i \in \{1, ..., N-1\}$. Then

$$\sum_{i=1}^{N-1} \text{eig}_i(\rho_\beta)^2 = \sum_{i=1}^{N-1} \left(\tfrac{1}{N-1} + \text{eig}_i(\rho_\beta) - \tfrac{1}{N-1}\right)^2 = \tfrac{1}{N-1} + \sum_{i=1}^{N-1} \left(\text{eig}_i(\rho_\beta) - \tfrac{1}{N-1}\right)^2 \tag{5.10}$$

where we have used that

$$\sum_{i=1}^{N-1} \tfrac{1}{N-1}(\text{eig}_i(\rho_\beta) - \tfrac{1}{N-1}) = 0. \tag{5.11}$$

Then it is clear that the left-hand side of Eq. 5.10 is equal to $\frac{1}{N-1}$ if and only if all the other $N-1$ eigenvalues of ρ_β are $\frac{1}{N-1}$.

In [10] the author finds the set $\mathcal{B}(\mathbb{R}^{N^2-1})$ explicitly by the following Theorem which we present without proof. The Theorem, as we will see, allows us to plot two-dimensional regions of Bloch space.

Theorem 5.1. *The Bloch vector space for N-level systems is*

$$\mathcal{B}(\mathbb{R}^{N^2-1}) = \{a \in \mathbb{R}^{N^2-1} | b_i(a) \geq 0\}, \tag{5.12}$$

where $b_i(a)$ are the coefficients of the characteristic polynomial $\det(xI - \rho_a) = 0$ *where ρ_a is given as in Eq. (4.4).*

This theorem implies that one can investigate the geometry of Bloch space by using, for example, the Faddeev-LeVerrier algorithm to calculate the coefficients of the characteristic polynomial,

$$\det(xI - \rho_a) = \sum_{j=0}^{N} (-1)^j b_j x^{N-j} \tag{5.13}$$

with $b_0 = 1$, and require that all of them be positive. One gets

$$j! b_j = -(j-1)! \sum_{k=1}^{j} (-1)^k b_{j-k} \text{Tr}[\rho^k]. \tag{5.14}$$

When calculating the coefficient it is therefore necessary to calculate the trace of powers of the density matrix. This quickly becomes tedious but can in general be done by using, for

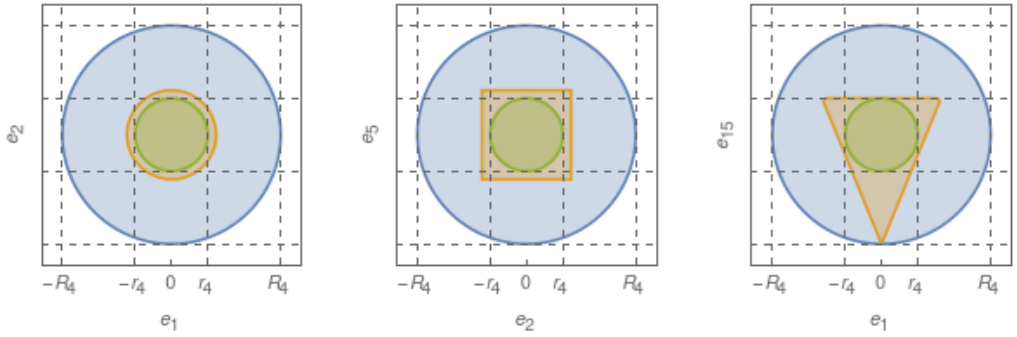


Figure 1: Intersection of $\mathbb{R}^{15}$ with plane spanned by $\{e_1, e_2\}$, $\{e_2, e_5\}$ and $\{e_1, e_{15}\}$ on the left, in the middle and on the right respectively. The orange area is the intersection with Bloch space, the blue, the intersection with a ball of radius R_N and the green, the intersection with a ball of radius r_N.

example, the binomial expansion formula in the following way

$$\mathrm{Tr}[\rho_a^k] = \left(\tfrac{1}{N}\right)^k \sum_{n=0}^{k} \binom{k}{n} \left(\tfrac{N}{2}\right)^n \mathrm{Tr}[(a\cdot\tilde{\sigma})^n]. \tag{5.15}$$

We omit the concrete expansions of the sum given Eq. (5.14) and refer the reader to [10] for details. Here, as an example, we just present the requirements one gets in the case of $N = 4$.

Example 5.1. A vector $a \in \mathbb{R}^{15}$ is a valid Bloch vector with respect to a set of generators, $\tilde{\sigma}$, with the totally symmetric structure constants, g_{ijk}, as given in Eqs. (4.15), if and only if it satisfies

$$\begin{gathered}(1)\ \tfrac{3}{2} \geq |a|^2\ ,\ (2)\ \tfrac{1}{2} + \tfrac{2}{3} g_{ijk} a_i a_j a_k \geq |a|^2\ , \\ (3)\ \tfrac{1}{4} + \tfrac{4}{3} g_{ijk} a_i a_j a_k - 2 g_{ijm} g_{klm} a_i a_j a_k a_l \geq |a|^2 \left(1 - |a|^2\right).\end{gathered} \tag{5.16}$$

with a repeated index summation implied. These requirements can be used to plot two-dimensional intersections of Bloch space. As an example we choose the Gell-Mann matrices and plot intersections of $\mathbb{R}^{15}$ with the plane spanned by $\{e_1, e_2\}$, $\{e_2, e_5\}$ and $\{e_1, e_{15}\}$ where e_i is the unit vector with 1 in its ith entry. These can be seen in Figure 1.

Only the first of the requirements in (5.16) is easy to grasp visually. This states that Bloch vectors have norms smaller than the radius of the outsphere. The two other requirements are more difficult due to the assymmetric nature of the structure constants. We see though that there could exist a subspace of a lower dimension in which Bloch space is a Ball of radius $\frac{1}{\sqrt{2}}$. For $N = 4$ this happens if there is a subset of the set of generators that consists only of anticommuting operators such that the terms including a structure constant vanish. For $N = 4$ there are up to 5 anticommuting generators [13].

If we restrict to anti-parallel directions, then we can derive a dependence on how far Bloch space reaches in the one direction given a valid Bloch vector in the other direction. We give here an adaptation and further development of an argument given in [12]:

Proposition 5.2. *For any Bloch vector, $0 \neq \beta \in \mathcal{B}(\mathbb{R}^{N^2-1})$, whose correspoding density matrix ρ_β has $eig_1(\rho_\beta)$ as its largest eigenvalue,*

$$-\frac{\beta}{N\, eig_1(\rho_\beta) - 1} \tag{5.17}$$

is a surface Bloch vector. In particular:

- *Surface points on the insphere and the outsphere obtain in dual pairs.*
- *$-\beta$ is a valid Bloch vector if and only if $eig_1(\rho_\beta) \leq r_N R_N$ with equality if and only if $-\beta$ is a surface Bloch vector.*

Proof. Let β be a Bloch vector whose corresponding density matrix, ρ_β, has eigenvalues that we list as

$$\mathrm{eig}_1(\rho_\beta) \geq ... \geq \mathrm{eig}_N(\rho_\beta) \geq 0. \tag{5.18}$$

Then, we know that the eigenvalues of $\beta \cdot \tilde{\sigma}$ are $2\mathrm{eig}_i(\rho_\beta) - r_N R_N$ and hence, if we consider for some $0 < \gamma \in \mathbb{R}$, a vector, $-\gamma\beta$, pointing in the opposite direction, then the eigenvalues of its corresponding density matrix, $\rho_{-\gamma\beta}$ can be listed as

$$\tfrac{1+\gamma}{N} - \gamma\mathrm{eig}_N(\rho_\beta) \geq ... \geq \tfrac{1+\gamma}{N} - \gamma\mathrm{eig}_1(\rho_\beta) \geq 0 \tag{5.19}$$

such that the largest eigenvalue in one direction determines the smallest eigenvalue in the other direction and $-\gamma\beta$ is a surface vector if it has at least one eigenvalue that is 0 which means that the surface is reached for

$$\gamma = \tfrac{1}{N\mathrm{eig}_1(\rho_\beta)-1}, \tag{5.20}$$

which shows the first part.

Now, suppose β reaches the outsphere. Then it is the Bloch vector of a pure state and hence the largest eigenvalue of its corresponding density matrix is 1 yielding $\gamma = \frac{1}{N-1}$ which means that $|\gamma\beta| = \frac{1}{N-1}R_N = r_N$. Let β be a surface point on the insphere. This, as we have seen, means that its largest eigenvalue is $\frac{1}{N-1}$ yielding $\gamma = N-1$ and hence $|\gamma\beta| = (N-1)r_N = R_N$.

For a valid Bloch vector β, we see from (5.19) by inserting $\gamma = 1$, that $-\beta$ is also a valid Bloch vector if and only if $\mathrm{eig}_1(\rho_\beta) \leq r_N R_N$ with equality if and only if $-\beta$ is a surface Bloch vector. □

Notice that we require that $\beta \neq 0$ in the above. This is because γ would not be defined for $\beta = 0$. If the largest eigenvalue of β is $\frac{1}{N}$ then the denominator of Eq. (5.20) becomes 0. But if the largest eigenvalue is $\frac{1}{N}$ then all the eigenvalues are $\frac{1}{N}$ corresponding to $\beta = 0$.

The following Lemma provides another way of finding restrictions on the geometry of Bloch space. Even though the proof of the Lemma is simple the geometric interpretation is important for our further investigations. Also, this geometric interpretation is, to the best of my knowledge, not given in any prior research within this field. This justifies stating this observation as a Lemma.

Lemma 5.1. *Let $b \in \mathbb{R}^{N^2-1}$. Then $b \in \mathcal{B}(\mathbb{R}^{N^2-1})$ if and only if for all $a \in \mathcal{B}(\mathbb{R}^{N^2-1})$ we have*

$$\tfrac{1}{N} + \tfrac{1}{2}a \cdot b \geq 0. \tag{5.21}$$

Proof. Suppose first that b is a valid Bloch vector. The overlap between quantum states can be calculated in terms of Bloch vectors as Eq. (5.3) and this is non-negative. Hence for any $a \in \mathcal{B}(\mathbb{R}^{N^2-1})$ we have

$$\tfrac{1}{N} + \tfrac{1}{2}a \cdot b \geq 0. \tag{5.22}$$

Now, we prove the other implication by contraposition. Recall, that any $b \in \mathbb{R}^{N^2-1}$ is a valid Bloch vector if and only if for all $k \in \{1, ..., N\}$, we have $\mathrm{eig}_k(\rho_b) \geq 0$ where $\rho_b = \frac{1}{N}I + \frac{1}{2}b \cdot \tilde{\sigma}$. Also, ρ_b is Hermitian and we denote its normalized, orthogonal eigenvectors by $\{|\psi_k\rangle\}_{k=1}^N$ and these span $\mathbb{C}^N$. We can then write

$$\rho_b = \sum_{k=1}^{N} \mathrm{eig}_k(\rho_b)\, |\psi_k\rangle \langle\psi_k| \tag{5.23}$$

Assume now that there exists $k' \in \{1, ..., N\}$ such that $\mathrm{eig}_{k'}(\rho_b) < 0$. This implies that there exists a Bloch vector, $\tilde{a} \in \mathcal{B}(\mathbb{R}^{N^2-1})$, namely the one corresponding to the pure quantum state

$$\rho_{\tilde{a}} = |\psi_{k'}\rangle\langle\psi_{k'}| = \tfrac{1}{N}I + \tfrac{1}{2}\tilde{a}\cdot\tilde{\sigma}, \tag{5.24}$$

such that

$$\mathrm{Tr}[\rho_b\rho_{\tilde{a}}] = \tfrac{1}{N} + \tfrac{1}{2}\tilde{a}\cdot b = \mathrm{eig}_{k'}(\rho_b) < 0. \tag{5.25}$$

This shows the other implication and we can conclude the desired. □

This Lemma entails that, for every valid Bloch vector, $a \in \mathcal{B}(\mathbb{R}^{N^2-1})$, we have a necessary condition for any $b \in \mathbb{R}^{N^2-1}$ to be a valid Bloch vector. For the rest of this section we interpret the consequences of this geometrically.

Let $a \in \mathcal{B}(\mathbb{R}^{N^2-1})$ be any valid Bloch vector with $\hat{a} = \frac{a}{|a|}$, and with a corresponding quantum state, ρ_a. Consider (5.21) with equality and let $z \in \mathbb{R}^{N^2-1}$ be a variable, i.e.

$$\hat{a}\cdot z + \tfrac{r_N R_N}{|a|} = 0. \tag{5.26}$$

This defines a hyperplane with the unit normal vector $\hat{a}$ and a distance of $\frac{r_N R_N}{|a|}$ to the origin. For every valid Bloch vector, a, there is such a hyperplane and any quantum state, ρ, is orthogonal to ρ_a only if its corresponding Bloch vector is given by a point in this plane. We know then, by Lemma 5.1, that every valid Bloch vector gives a restriction to the geometry of Bloch space, in that it divides $\mathbb{R}^{N^2-1}$ into two parts, one where we find other valid Bloch vectors and one where there are no valid Bloch vectors. The geometric interpretation of Lemma 5.1 is therefore that any $b \in \mathbb{R}^{N^2-1}$ is a Bloch vector if and only if for every $a \in \mathcal{B}(\mathbb{R}^{N^2-1})$ we have that b lies on the same side of the hyperplane, defined by a as in Eq. (5.26), as a itself.

Notice, for example, that if the vector a corresponds to a pure state, then the hyperplane we get by using it in Eq. (5.26) is tangent to the insphere. This means, in particular, that Bloch space in the opposite direction of a reaches no further than the insphere, i.e. $-\frac{r_N}{R_N}a$ is a surface vector which we have already seen in Proposition 5.2. Non-negativity of overlaps allows us to upper bound the product of the norms of to antiparallel Bloch vectors in general by

$$|a||b| \leq r_N R_N = \tfrac{2}{N}. \tag{5.27}$$

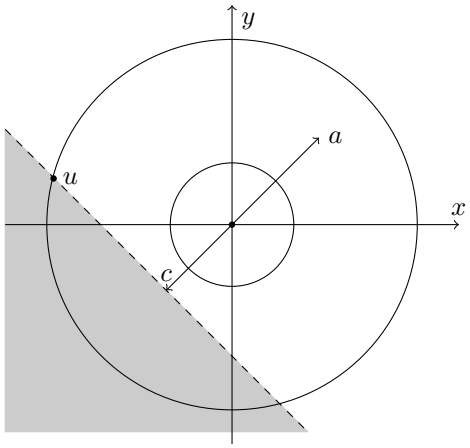


Figure 2: Bloch space intersected with the plane spanned by $\hat{x}$ and $a \in \mathcal{B}(\mathbb{R}^{N^2-1})$ (as in Eq. 5.28). The grey area is inaccesible for Bloch space vectors.

To grasp this geometric interpretation visually we have included Figure 2. We consider here a Bloch vector, $0 \neq a \in \mathcal{B}(\mathbb{R}^{N^2-1})$, and some unit vector $\hat{x} \in \mathbb{R}^{N^2-1}$ such that $0 < a \cdot \hat{x} < |a|$. Figure 2 then shows the intersection of $\mathbb{R}^{N^2-1}$ with the plane spanned by a and $\hat{x}$. The vertical axis corresponds to some unit vector, $\hat{y}$, with $\hat{x} \cdot \hat{y} = 0$ such that

$$a = a_x\hat{x} + a_y\hat{y} \ , \ 0 < a_x \leq R_N \ , \ |a_y| \leq \sqrt{R_N^2 - a_x^2}. \tag{5.28}$$

The vector denoted c in Figure 2 is given by $-\frac{r_N R_N}{|a|}a$ and the grey area is according to Lemma 5.1 inaccesible for Bloch vectors since a is assumed to be a valid Bloch vector. The demarcation line between the white area and the grey area is the intersection between the hyperplane given by a used in Eq. (5.26) and the plane spanned by $\hat{x}$ and a. The Bloch vector a in this way upper bounds the component of any Bloch vector in the direction of $-\hat{x}$. This upper bound is reached, if the point marked by u in Figure 2 corresponds to a valid Bloch vector. These considerations lead to the following Lemma.

Lemma 5.2. *Let $a, u \in \mathcal{B}(\mathbb{R}^{N^2-1})$ and consider two antiparallel directions $\{-\hat{x}, \hat{x}\}$ in $\mathbb{R}^{N^2-1}$. If the component of a in the direction of $\hat{x}$ is given by a_x and the component of u in the direction of $-\hat{x}$ is given by u_x then*

$$\tfrac{1}{2}(a_x + u_x) \leq 1, \tag{5.29}$$

for any $N \geq 2$.

Proof. Let $a \in \mathcal{B}(\mathbb{R}^{N^2-1})$ be decomposed as in Eq. (5.28) and let $u' \in \mathbb{R}^{N^2-1}$ with $|u'| \leq R_N$ have u'_x along $-\hat{x}$ and u'_y along $\hat{y}$. We find then the largest possible value of u'_x such that u' satifies the necessary condition from Lemma 5.1 for being a valid Bloch vector, given by $a \in \mathcal{B}(\mathbb{R}^{N^2-1})$. Then, since u is assumed to be a valid Bloch vector we must have $u_x \leq u'_x$.

First, notice that if we suppose that $a_x \leq r_N$ then the vector $-R_N\hat{x}$ fulfills the necessary condition from Lemma 5.1 for being a Bloch vector such that the average of a_x and u_x would be bounded by

$$\tfrac{1}{2}(r_N + R_N) = \tfrac{1}{R_N} \leq 1 \quad \forall N \geq 2, \tag{5.30}$$

and thus, in the following we assume that $a_x \geq r_N$.

By Lemma 5.1, a necessary condition for u' to be a valid Bloch vector is that

$$u'_x \leq \tfrac{r_N R_N + a_y u'_y}{a_x} \leq \tfrac{r_N R_N + \sqrt{R_N^2 - a_x^2}\sqrt{R_N^2 - u_x'^2}}{a_x} \tag{5.31}$$

where the upper bound on the right hand side of (5.31) can only be reached for two pure states whose Bloch vectors both lie in the plane spanned by $\hat{x}$ and $\hat{y}$, i.e. a situation as in Figure 3. Now, the right hand side of (5.31) is the upper semi-ellipse with semi-major axis equal R_N and semi-minor axis equal to $\frac{R_N}{a_x}\sqrt{R_N^2 - a_x^2}$ that has been shifted $\frac{r_N R_N}{a_x}$ upwards. The left-hand side of (5.31) is a straight line that, for any $a_x \geq r_N$, will have a point of intersection, u'_{x_m}, with the semi-ellipse such that any $u'_x \in [-R_N, u'_{x_\mathrm{m}}]$ satisfies the inequality in (5.31). This point of intersection is found by the larger of the two solutions of (5.31) with equality with respect to u'_x. The other solution is the intersection with the lower semi-ellipse which corresponds to the point o in figure 3. The two solutions of are given by

$$(1) \ \tfrac{r_N}{R_N}a_x - \eta(a_x) \text{ and } (2) \ \tfrac{r_N}{R_N}a_x + \eta(a_x) \tag{5.32}$$

with

$$\eta(a_x) = R_N\sqrt{(1 - \tfrac{a_x^2}{R_N^2})(1 - \tfrac{r_N^2}{R_N^2})} \geq 0. \tag{5.33}$$

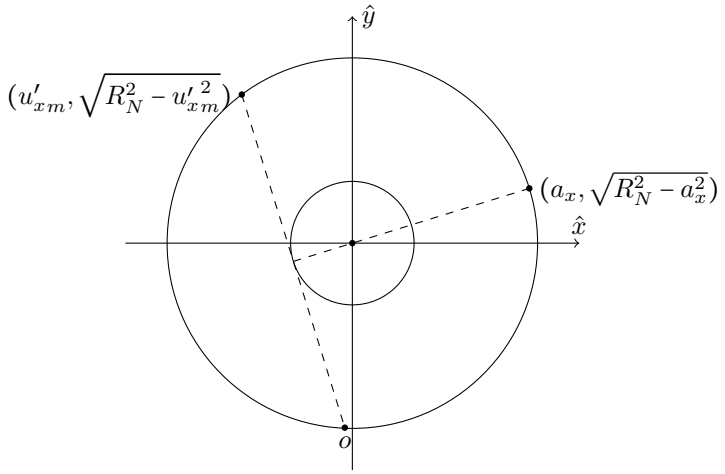


Figure 3: Bloch space intersected with the plane spanned by $\hat{x}$ and a (pure state). Any quantum state has a component smaller than u'_{x_m} in the direction of $-\hat{x}$.

Notice, that $\eta(r_N) = R_N - \frac{r_N^2}{R_N}$ and $\eta(R_N) = 0$ such that the upper bound on u_x becomes $u_x \leq R_N$ and $u_x \leq r_N$ for $a_x = r_N$ and $a_x = R_N$, respectively, as expected.

This means that for any $a_x \in [r_N, R_N]$ we have an upper bound on u'_x (and therefore on u_x) given by (2) in Eq. (5.32) such that the average $\frac{1}{2}(a_x + u_x)$ is upper bounded by

$$\tfrac{1}{R_N^2} a_x + \tfrac{1}{2}\eta(a_x) \tag{5.34}$$

since $1 + \frac{r_N}{R_N} = \frac{2}{R_N^2}$. This can by standard methods be shown to be less than or equal to 1 for all $a_x \in [r_N, R_N]$ independently of $N \geq 2$. So we can conclude the desired. □

Remark that this upper bound is reached only for $a_x = u_x = 1$ such that it can be reached if and only if there exists some two-dimensional section of Bloch space spanned by orthogonal unit vectors, say $(\hat{x}, \hat{y})$, where both

$$\pm\, \hat{x} + \sqrt{R_N^2 - 1}\hat{y}, \tag{5.35}$$

are valid Bloch vectors. This Lemma will be crucial for the main argument of this thesis as will be apparent later. We turn now to concrete constructions of QRACs.

6 Constructing QRACs

In this section we utilize the knowledge about the geometry of Bloch space to construct QRACs. We consider general (n, m, p)-QRACs and since we are encoding a string of length n into m qubits we need $N = 2^m$.

First, consider a POVM for measuring in the ith bit, $\{D_i^0, D_i^1\}$. Since these operators are Hermitian and fulfill the completeness relation, $D_i^0 + D_i^1 = I$, we can write them as

$$D_i^0 = \alpha_{0_i} I + \alpha_i \cdot \tilde{\sigma} \tag{6.1}$$

$$D_i^1 = (1 - \alpha_{0_i}) I - \alpha_i \cdot \tilde{\sigma}, \tag{6.2}$$

for some set of generators, $\tilde{\sigma}$, and for some $\alpha_{0_i} \in \mathbb{R}$ and $\alpha_i \in \mathbb{R}^{4^m - 1}$. The fact that D_i^0 and D_i^1 have to be positive semi-definite gives restrictions to α_{0_i} and α_i in a similar vein as in

our discussion of the Bloch vector. Since $\mathrm{Tr}[\alpha_i \cdot \tilde{\sigma}] = 0$ the minimum of the eigenvalues of $\alpha_i \cdot \tilde{\sigma}$ cannot be positive as well as the maximum of the eigenvalues cannot be negative. This means that $\alpha_{0_i} \in (0,1)$ since a value outside this interval would result in negative eigenvalues of either D_i^0 or D_i^1. We find also an upper bound on the norm of α_i in the following Lemma.

Lemma 6.1. *If a POVM is given as in Eqs. (6.1)-(6.2) then* $|\alpha_i| \leq \frac{1}{2}\sqrt{2^{m-1}}$.

Proof. We rewrite Eqs. (6.1)-(6.2) to get

$$D_i^0 = \alpha_{0_i} 2^m \left(\tfrac{1}{2^m} I + \tfrac{1}{2} \tfrac{1}{\alpha_{0_i} 2^{m-1}} \alpha_i \cdot \tilde{\sigma}\right) \tag{6.3}$$

$$D_i^1 = (1-\alpha_{0_i}) 2^m \left(\tfrac{1}{2^m} I - \tfrac{1}{2} \tfrac{1}{(1-\alpha_{0_i}) 2^{m-1}} \alpha_i \cdot \tilde{\sigma}\right), \tag{6.4}$$

such that the elements of the POVM are proportional to quantum states with Bloch vectors given by $\frac{1}{\alpha_{0_i} 2^{m-1}} \alpha_i$ and $-\frac{1}{(1-\alpha_{0_i}) 2^{m-1}} \alpha_i$. These are antiparallel and the product of their norms is therefore bounded by $R_{2^m} r_{2^m} = \frac{1}{2^{m-1}}$ as we saw in (5.27), i.e.

$$|\alpha_i|^2 \leq \alpha_{0_i}(1-\alpha_{0_i}) 2^{m-1} \leq \tfrac{1}{4} 2^{m-1} \ , \ \forall \alpha_{0_i} \in (0,1). \tag{6.5}$$

Thus, we can conclude the desired. □

Remark, that this upper bound is reached for $\alpha_{0_i} = \frac{1}{2}$. Therefore it is useful to search for valid pairs of Bloch vectors given by

$$\pm \tfrac{1}{\sqrt{2^{m-1}}} \hat{\alpha}_i, \tag{6.6}$$

for some unit vector, $\hat{\alpha}_i \in \mathbb{R}^{4^m-1}$, and associate the POVM with such a pair. Notice that such a pair would reach the upper bound given in (5.27) and hence correspond to orthogonal quantum states. Also, by Proposition 5.2 searching for such pairs implies searching for surface points in Bloch space in a distance of $\frac{1}{\sqrt{2^{m-1}}}$ from the origin corresponding to a density operator with $r_{2^m} R_{2^m}$ as its largest eigenvalue.

We see now, that the set of generators given in Eq. (4.21) is particularly well-suited for constructing QRACs since the eigenvalues of any σ_i are 2^{m-1}-fold degenerate with values $\pm\frac{1}{\sqrt{2^{m-1}}}$. This means that the eigenvalues of the operators

$$D_i^{x_i} = \tfrac{1}{2} I + (-1)^{x_i} \tfrac{1}{2} \sqrt{2^{m-1}} \sigma_i \tag{6.7}$$

are 0 and 1 (both 2^{m-1}-fold degenerate) and these are therefore a natural choice as POVMs. The pair of antiparallel Bloch vectors with which we associate the POVM for decoding the ith bit is simply

$$\pm \tfrac{1}{\sqrt{2^{m-1}}} e_i, \tag{6.8}$$

where e_i is the unit vector with 1 in its ith entry and 0 in the other entries. Next, we can choose

$$\beta_x = \tfrac{r_{2^m}}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} e_i \tag{6.9}$$

as the Bloch vector for decoding the string with x_i in its ith bit. This lies within the insphere to ensure that it corresponds to a valid quantum states. This construction gives the success probability

$$\tfrac{1}{2} + \tfrac{1}{2} \sqrt{\tfrac{2^{m-1}}{n}} r_{2^m}, \tag{6.10}$$

for correctly decoding the ith bit to be x_i. Since it is independent of x and i the average and worst case success probabilties coincide. These explicit constructions of $(4^m > n, m, p > \frac{1}{2})$-QRACs were derived in [9, 13] and show that the upper bound of $n < 4^m$ in any (n,m,p)-QRAC derived in [7] is tight as mentioned earlier. When $m = 1$ this construction yields the

optimal $(n, 1, \frac{1}{2} + \frac{1}{2\sqrt{n}})$-QRACs.

To improve upon the QRACs found by this insphere based method one could try to extend the encoding Bloch vector lengths. In Section 5 above we have derived an upper bound on two antiparallel Bloch vectors of $r_{2^m} R_{2^m}$ and from the discussion here it is evident that given a pair of antiparallel Bloch vectors $\{\alpha_i, -\alpha_i\}$ with which we can associate the POVM for decoding the ith bit, the task is to find a Bloch vector for encoding a string, $x \in \{0,1\}^n$ with x_i in its ith bit with a large component in the same direction as

$$\alpha_x = \sum_{i=1}^{n} (-1)^{x_i} \alpha_i. \tag{6.11}$$

But we need also an encoding Bloch vector to encode the string $\overline{x} \in \{0,1\}^n$ with a large component in the direction of $-\alpha_x$ since $(-1)^{\overline{x_i}} = -(-1)^{x_i}$. Therefore, one might think that a natural way to proceed would be to search for suitable decoding Bloch vectors such that the directions $\{\alpha_x, -\alpha_x\}$ allow the upper bound of $r_{2^m} R_{2^m}$ to be reached symmetrically, i.e in such a way that r_{2^m} in Eq. (6.9) could be replaced by $\sqrt{r_{2^m} R_{2^m}} = \frac{1}{\sqrt{2^{m-1}}}$, resulting in the worst case success probability,

$$\frac{1}{2} + \frac{1}{2\sqrt{n}} \tag{6.12}$$

similar to the optimal success probability in the smaller QRACs with $m = 1$. However, in the light of what we know from Lemma 5.2 it might be possible to extend the components of the encoding Bloch vectors for the strings $x, \overline{x} \in \{0,1\}^n$, in the direction of α_x and $-\alpha_x$, respectively, by adding a component in some orthogonal direction. This leads us to the following definition.

Definition 6.1 (Residual vector)**.** Let $r_x, \tilde{\beta}_x \in \mathbb{R}^{4^m-1}$. r_x is called a *residual vector* of $\tilde{\beta}_x$ if and only if

$$\tilde{\beta}_x \notin \mathcal{B}(\mathbb{R}^{4^m-1}) \text{ and } \tilde{\beta}_x + r_x \in \mathcal{B}(\mathbb{R}^{4^m-1}). \tag{6.13}$$

This means that if we denote the component of the encoding Bloch vector in the direction of α_x by $\tilde{\beta}_x$ which is not itself a valid Bloch vector, then we can find improvements to a QRAC if there exists a residual vector, r_x, such that $\beta_x = \tilde{\beta}_x + r_x$ is a valid Bloch vector. We will look at some examples shortly but first we briefly review the optimal $(n, 1, \frac{1}{2} + \frac{1}{2\sqrt{n}})$-QRACs.

Example 6.1. For $m = 1$ the geometrical understanding of the constructions of QRACs given above is straightforward. Bloch space is a three dimensional ball with radius equal to $r_2 = R_2 = 1$ as we have seen. Orthogonal pure states correspond to antipodal points on the sphere and both the Gell-Mann matrices and the ones given in (4.21) are just the Pauli matrices. The encoding states correspond to the vertices of a square and of a cube when $n = 2$ and $n = 3$, respectively, in accordance with eq. (6.9). Furthermore, in accordance with eq. (6.7), the POVM for decoding the ith bit to be x_i is

$$d_i^{x_i} = \tfrac{1}{2} I + (-1)^{x_i} \tfrac{1}{2} p_i, \tag{6.14}$$

where, for later reference, we use lower case d to indicate that these POVMs stem from the case of $m = 1$. These are proportional to pure quantum states with corresponding Bloch vectors equal to $(\pm 1, 0, 0)$, $(0, \pm 1, 0)$ and $(0, 0, \pm 1)$ when decoding the 1st, the 2nd and the 3rd bit, respectively. Hence, they are the three mutually unbiased bases of $\mathbb{C}^N$ given by $\{|-\rangle, |+\rangle\}$, $\{|-i\rangle, |+i\rangle\}$ and $\{|0\rangle, |1\rangle\}$.

These QRACs can readily be generalized to $(2m, m, \frac{1}{2} + \frac{1}{2\sqrt{2}})$- and $(3m, m, \frac{1}{2} + \frac{1}{2\sqrt{3}})$-QRACs which we will see in the next example.

Example 6.2. The encoding state for encoding the string $x \in \{0,1\}^{2m}$ we write as copies of the encoding states from the $(2, 1, \frac{1}{2} + \frac{1}{2\sqrt{2}})$-QRAC, denoted $\rho'_{x_i x_j}$, in the following way,

$$\rho_x = \rho'_{x_1 x_2} \otimes \ldots \otimes \rho'_{x_{2m-1} x_{2m}}. \tag{6.15}$$

The POVMs for decoding the $2s-k$th bit to be x_i can then be written as

$$D_{2s-k}^{x_i} = I^{\otimes s-1} \otimes d_k^{x_i} \otimes I^{\otimes m-s}, \tag{6.16}$$

where s is a number from 1 to m and k is 0 or 1 if we are interested in an even or uneven bit, respectively. One can readily check that these are valid POVMs. This means that the probability of correctly decoding the ith bit to be x_i is indeed $\frac{1}{2} + \frac{1}{2\sqrt{2}}$.

Now, notice that since $d_i^{x_i}$ is written in terms of the Pauli matrices the POVMs in the bigger $(2m, m, \frac{1}{2} + \frac{1}{2\sqrt{2}})$-QRAC are written in terms of the set of generators given in Eq. (4.21). One can easily check that (with respect to these generators) they are equivalent to pairs of antiparallel Bloch vectors as in (6.8), or, in other words, they reach the upper limit as in Lemma 6.1. For $m = 2$ we find that decoding the 1st, 2nd, 3rd and 4th bit are associated with $\pm\frac{1}{\sqrt{2^{m-1}}}e_j$ for j being 1, 2, 4 and 8, respectively. The corresponding Bloch vector for encoding the string $x \in \{0,1\}^4$ with x_i in its ith bit is $\beta_x = \tilde{\beta}_x + r_x$ where

$$\tilde{\beta}_x = \tfrac{1}{2}\big((-1)^{x_1}e_1 + (-1)^{x_2}e_2 + (-1)^{x_3}e_4 + (-1)^{x_4}e_8\big), \tag{6.17}$$

is not itself a valid Bloch vector, and

$$r_x = \tfrac{1}{2\sqrt{2}}\big((-1)^{x_1+x_3}e_5 + (-1)^{x_2+x_3}e_6 + (-1)^{x_1+x_4}e_9 + (-1)^{x_2+x_4}e_{10}\big). \tag{6.18}$$

is the residual vector that makes β_x valid.

One can also, similarly, generalize the $(3, 1, \frac{1}{2} + \frac{1}{2\sqrt{3}})$-QRAC to a $(3m, m, \frac{1}{2} + \frac{1}{2\sqrt{3}})$-QRAC. Using again the set of generators given in Eq. (4.21) then if $m = 2$ the POVMs are equivalent with $\pm\frac{1}{\sqrt{2^{m-1}}}e_j$ with j being 1, 2, 3, 4, 8 and 12 and the Bloch vector for encoding the string $x \in \{0,1\}^6$ with x_i in its ith bit is $\beta_x = \tilde{\beta}_x + r_x$ where

$$\tilde{\beta}_x = \tfrac{1}{\sqrt{6}}\big((-1)^{x_1}e_1 + (-1)^{x_2}e_2 + (-1)^{x_3}e_3 + (-1)^{x_4}e_4 + (-1)^{x_5}e_8 + (-1)^{x_6}e_{12}\big) \tag{6.19}$$

is not itself a valid Bloch vector, and

$$\begin{aligned} r_x = \tfrac{1}{3\sqrt{2}}\big((-1)^{x_1+x_4}e_5 + (-1)^{x_2+x_4}e_6 + (-1)^{x_3+x_4}e_7 + (-1)^{x_1+x_5}e_9 \\ + (-1)^{x_2+x_5}e_{10} + (-1)^{x_3+x_5}e_{11} + (-1)^{x_1+x_6}e_{13} + (-1)^{x_2+x_6}e_{14} + (-1)^{x_3+x_6}e_{15}\big). \end{aligned} \tag{6.20}$$

is the residual vector that makes β_x valid.

In [8], as mentioned earlier, the authors find a $(3, 2, \frac{1}{2} + \frac{1}{\sqrt{6}})$-QRAC. We rewrite the POVMs and two encoding states in terms of Bloch vectors in the next example.

Example 6.3. Let the POVMs be given by

$$D_i^{x_i} = \tfrac{1}{2}I + (-1)^{x_i}\alpha_i \cdot \sigma \tag{6.21}$$

where σ are the generators given in Eq. (4.21) and

$$\alpha_1 = \tfrac{1}{\sqrt{3}}e_3 + \tfrac{1}{2\sqrt{3}}e_5 + \tfrac{1}{2\sqrt{3}}e_{13}\ ,\ \alpha_2 = \tfrac{1}{2\sqrt{3}}e_4 + \tfrac{1}{2\sqrt{3}}e_{10} + \tfrac{1}{\sqrt{3}}e_{12} \tag{6.22}$$

$$\alpha_3 = -\tfrac{1}{2\sqrt{3}}e_1 - \tfrac{1}{2\sqrt{3}}e_7 + \tfrac{1}{\sqrt{3}}e_{15}, \tag{6.23}$$

such that all of these meet the upper bound implied by Lemma 6.1. We give here the encoding Bloch vectors for the strings 000 and 111:

$$\beta_{000} = \tfrac{1}{\sqrt{2}}e_3 + \tfrac{1}{\sqrt{2}}e_{12} + \tfrac{1}{\sqrt{2}}e_{15} \tag{6.24}$$

$$\beta_{111} = \tfrac{\sqrt{2}}{3}e_1 - \tfrac{1}{3\sqrt{2}}e_3 - \tfrac{\sqrt{2}}{3}e_4 - \tfrac{\sqrt{2}}{3}e_5 + \tfrac{\sqrt{2}}{3}e_7 - \tfrac{\sqrt{2}}{3}e_{10} - \tfrac{1}{3\sqrt{2}}e_{12} - \tfrac{\sqrt{2}}{3}e_{13} - \tfrac{1}{3\sqrt{2}}e_{15}. \tag{6.25}$$

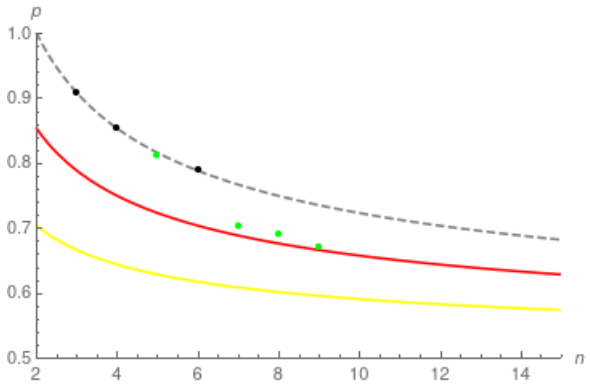


Figure 4: The grey dashed curve is $\frac{1}{2}+\frac{1}{\sqrt{2n}}$ which in the next section will be shown to be an upper bound of $(n,2,p)$-QRACs. The red curve is $\frac{1}{2}+\frac{1}{2\sqrt{n}}$ which are the success probabilities one would get if one succeded in finding encoding states whose Bloch vectors pairwise reach the upper bound in Eq. (5.27). The yellow curve is (6.10), hence the success probability one gets with the insphere based method. The black points are the success probabilities of the known analytical QRACs that reach the upper bound and the green points are the success probabilities of the QRACs found by numerical searches in [8].

In this example one cannot directly read off the component of the encoding Bloch vectors in the same direction as $\sum_{i=0}^{3}(-1)^{x_i}\alpha_i$ and the residual vector. But by inspection we find for example for β_{000} that it is given by $\tilde{\beta}_{000}+r_{000}$ where

$$\tilde{\beta}_{000} = -\frac{1}{3\sqrt{2}}e_1+\frac{\sqrt{2}}{3}e_3+\frac{1}{3\sqrt{2}}e_4+\frac{1}{3\sqrt{2}}e_5-\frac{1}{3\sqrt{2}}e_7+\frac{1}{3\sqrt{2}}e_{10}+\frac{\sqrt{2}}{3}e_{12}+\frac{1}{3\sqrt{2}}e_{13}+\frac{\sqrt{2}}{3}e_{15} \quad (6.26)$$

is not itself a valid Bloch vector, and

$$r_{000} = \frac{1}{3\sqrt{2}}e_1+\frac{1}{3\sqrt{2}}e_3-\frac{1}{3\sqrt{2}}e_4-\frac{1}{3\sqrt{2}}e_5+\frac{1}{3\sqrt{2}}e_7-\frac{1}{3\sqrt{2}}e_{10}+\frac{1}{3\sqrt{2}}e_{12}-\frac{1}{3\sqrt{2}}e_{13}+\frac{1}{3\sqrt{2}}e_{15} \quad (6.27)$$

is orthogonal to $\tilde{\beta}$ and is the residual vector that makes β_{000} valid.

In this last example it becomes clear that constructing QRACs that perform well is a non-trivial problem. Only when we know certain smaller QRACs certain bigger ones can be constructed as tensor products, as we have seen. Thus, we also have $(3m,2m,\frac{1}{2}+\frac{1}{\sqrt{6}})$-QRACs after the findings in [8] since these could be constructed similarly as in Example 6.2.

Notice, that in all the above examples of $(n,2,p)$-QRACs the components of the encoding vectors along the same direction as the sum of the Bloch vectors with which we associate the POVMs (those denoted by $\tilde{\beta}$) all have norms equal to 1. We have in Figure 5, as an example, plotted the intersection of $\mathbb{R}^{15}$ with the plane spanned $\tilde{\beta}_{0000}$ and r_{0000} from the above examples. Here we see that both $\pm\tilde{\beta}_{0000}+r_{0000}$ are valid Bloch vectors of pure states. Therefore they meet the upper bound given by Lemma 5.2 and this gives us a first hint as to why these QRACs might be optimal. In the next section we give a formal proof that they are optimal. In figure 4 we have made an overview of the content of this section focusing on QRACs with $m=2$. We will return to a discussion of these results in Section 8.

7 Upper Bounds

In this section we utilize the findings we have made throughout this thesis to derive an upper bound of $\frac{1}{2}+\frac{1}{2}\sqrt{\frac{2^{m-1}}{n}}$ on the worst case (and average) success probability in any

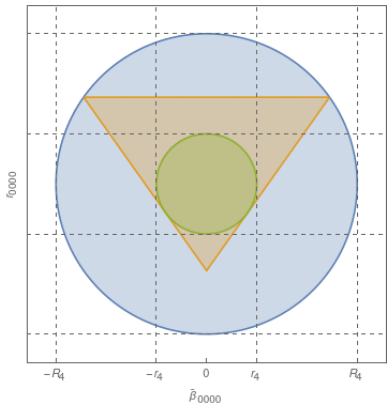


Figure 5: Plot of the intersection of $\mathbb{R}^{15}$ with the plane spanned by $\tilde{\beta}_{0000}$ and r_{0000} as given in Example 6.2. The orange area is the intersection with Bloch space, the blue, the intersection with the outsphere and the green, the intersection with the insphere.

(n, m, p)-QRAC. We start by stating and proving the following Lemma which is a slight generalization of a Lemma given in [3].

Lemma 7.1. *Let $N \in \mathbb{N}$. For any set of vectors, $\{\alpha_i\}_{i=1}^n \subset \mathbb{R}^N$, the inequality*

$$\sum_{x\in\{0,1\}^n} \left| \sum_{i=1}^{n} (-1)^{x_i} \alpha_i \right| \leq 2^n \sqrt{\sum_{i=0}^{n} |\alpha_i|^2} \tag{7.1}$$

holds.

Proof. The inequality in (7.1) holds true if all the α_i's are 0, so we assume they are not all 0. We can interpret[3] the sum on the left hand side of (7.1) as an inner product of $y_1 = (1, ..., 1) \in \mathbb{R}^{2^n}$ and a vector, $y_2 \in \mathbb{R}^{2^n}$, that in its jth entry has the number

$$\left| \sum_{i=1}^{n} (-1)^{x_i} \alpha_i \right|, \tag{7.2}$$

where x_i is the ith bit of the jth element of the set $\{0,1\}^n$, ordered in some way. A natural ordering would be to have the jth element be the number $j-1$ in its binary representation. We get, then, by the Cauchy-Schwartz inequality, $y_1 \cdot y_2 \leq |y_1||y_2|$, that the left hand side of (7.1) is less than or equal to

$$\sqrt{2^n} \sqrt{\sum_{x\in\{0,1\}^n} \left| \sum_{i=1}^{n} (-1)^{x_i} \alpha_i \right|^2}. \tag{7.3}$$

We claim now that

$$\sum_{x\in\{0,1\}^n} \left| \sum_{i=1}^{n} (-1)^{x_i} \alpha_i \right|^2 = 2^n \sum_{i=1}^{n} |\alpha_i|^2. \tag{7.4}$$

This can be justified by induction (again we follow [3]) with respect to n. Eq. (7.4) holds for $n = 1$ since

$$|\alpha_1|^2 + |-\alpha_1|^2 = 2|\alpha_1|^2. \tag{7.5}$$

[3] This idea is taken directly from [3].

Let us assume that Eq. (7.4) holds true for $n = k$. By explicitly carrying out the sum on the left hand side of Eq. (7.4) over $x_{k+1} \in \{0,1\}$ when $n = k+1$ we get

$$\sum_{x\in\{0,1\}^k}\left[\left|\left((-1)^{x_1}\alpha_1 + ... + (-1)^{x_k}\alpha_k\right) + \alpha_{k+1}\right|^2 + \left|\left((-1)^{x_1}\alpha_1 + ... + (-1)^{x_k}\alpha_k\right) - \alpha_{k+1}\right|^2\right]. \quad (7.6)$$

Then, by the parallelogram identity, i.e. $|u_1 + u_2|^2 - |u_1 - u_2|^2 = 2(|u_1|^2 + |u_2|^2)$, we get

$$2\sum_{x\in\{0,1\}^k}\left(\,|\sum_{i=1}^k(-1)^{x_i}\alpha_i\,|^2 + |\alpha_{k+1}|^2\,|\,\right), \quad (7.7)$$

such that the induction hypothesis implies that this is equal to

$$2\left(2^k\sum_{i=1}^k|\alpha_i|^2 + 2^k|\alpha_{k+1}|^2\right) = 2^{k+1}\sum_{i=1}^{k+1}|\alpha_i|^2 \quad (7.8)$$

thereby proving the induction step. Now, by inserting (7.4) in (7.3) we can conclude the desired. □

Notice that we have equality in (7.1) if and only if all the α_i's are orthogonal. This is a consequence of the Cauchy-Schwarz inequality since for the $y_1, y_2 \in \mathbb{R}^{2^n}$ we defined during the proof we have that $y_1 \cdot y_2 = |y_1||y_2|$ if and only if $\gamma y_1 = y_2$ for some positive real number, γ. This would imply that we, for all $x \in \{0,1\}^n$, have

$$\left|\sum_{i=1}^n(-1)^{x_i}\alpha_i\right| = \sqrt{\sum_{i=1}^n|\alpha_i|^2 + \sum_{i\neq j}^n(-1)^{x_i+x_j}\alpha_i\cdot\alpha_j} = \gamma \quad (7.9)$$

where the second term in the square root can only be constant over all $x \in \{0,1\}^n$ if for all $i, j \in \{1, ..., n\}$ with $i \neq j$ we have $\alpha_i \cdot \alpha_j = 0$.

We are now ready to prove the main theorem of this thesis.

Theorem 7.1. *For any (n, m, p)-QRAC, the inequality*

$$p \leq \tfrac{1}{2} + \tfrac{1}{2}\sqrt{\tfrac{2^{m-1}}{n}} \quad (7.10)$$

holds

Proof. The strategy of the proof is to show that the average success probability for any (n, m, p)-QRAC cannot exceed the right hand side of (7.10). If this is true, then, in particular, the worst case success probablity cannot exceed the right hand side of (7.10).

Consider an (n, m, p)-QRAC with POVMs with respect to some set of generators, $\tilde{\sigma}$, given by

$$D_i^{x_i} = \alpha_{0_i} I + (-1)^{x_i}\alpha_i \cdot \tilde{\sigma} \quad (7.11)$$

$$D_i^{\overline{x_i}} = (1 - \alpha_{0_i})I + (-1)^{\overline{x_i}}\alpha_i \cdot \tilde{\sigma}, \quad (7.12)$$

where $\alpha_{0_i} \in \mathbb{R}$ and $\alpha_i \in \mathbb{R}^{4^m-1}$ for any $i \in \{1, ...n\}$ since the elements of a POVM are Hermitian. We denote the encoding Bloch vector for encoding the string $x \in \{0,1\}^n$ by β_x with corresponding density operator ρ_x. $p_{i,x}$ is the probability of correctly decoding the ith bit to be x_i and $p_{i,\overline{x}}$ is the probability of correctly decoding the ith bit of $\overline{x}$ to be $\overline{x_i}$. These are given by

$$p_{i,x} = \mathrm{Tr}[D_i^{x_i}\rho_x] = \alpha_{0,i} + (-1)^{x_i}\alpha_i \cdot \beta_x \quad (7.13)$$

$$p_{i,\overline{x}} = \mathrm{Tr}[D_i^{\overline{x_i}}\rho_{\overline{x}}] = (1 - \alpha_{0_i}) + (-1)^{\overline{x_i}}\alpha_i \cdot \beta_{\overline{x}} \quad (7.14)$$

Now, the average success probability is found by Eq. (1.3). We can use the fact that the sum in Eq. (1.3) does not change if we use $p_{i,\overline{x}}$ instead of $p_{i,x}$ to write

$$p_{\text{ave}} = \frac{1}{n2^n} \sum_{x\in\{0,1\}^n} \sum_{i=1}^{n} \frac{1}{2}(p_{i,x} + p_{i,\overline{x}}). \tag{7.15}$$

Use Eqs. (7.13)-(7.14) this becomes equal to

$$\frac{1}{n2^n} \sum_{x\in\{0,1\}^n} \sum_{i=1}^{n} \frac{1}{2} + \frac{1}{2}\big((-1)^{x_i}\alpha_i \cdot \beta_x + (-1)^{\overline{x_i}}\alpha_i \cdot \beta_{\overline{x}}\big). \tag{7.16}$$

If we set

$$V_x = \sum_{i=1}^{n}(-1)^{x_i}\alpha_i, \tag{7.17}$$

then (7.16) becomes

$$\frac{1}{2} + \frac{1}{n2^n} \sum_{x\in\{0,1\}^n} \frac{1}{2}\big(\hat{V}_x \cdot \beta_x + (-\hat{V}_x) \cdot \beta_{\overline{x}}\big)|V_x|\,, \tag{7.18}$$

where we have taken out the norm of V_x such that $\hat{V}_x$ is a unit vector. We can now use Lemma 5.2 to see that for all pairs $\{\beta_x, \beta_{\overline{x}}\}$ and for all strings $x \in \{0,1\}^n$ we have

$$\frac{1}{2}(\hat{V}_x \cdot \beta_x + (-\hat{V}_x) \cdot \beta_{\overline{x}}) \leq 1 \tag{7.19}$$

such that 7.18 is upper bounded by

$$\frac{1}{2} + \frac{1}{n2^n} \sum_{x\in\{0,1\}^n} |V_x|\,. \tag{7.20}$$

Reinserting the expression for V_x and using Lemma 7.1 gives an upper bound of this expression of

$$\frac{1}{2} + \frac{1}{n}\sqrt{\sum_{i=0}^{n}|\alpha_i|^2}. \tag{7.21}$$

We can now use Lemma 6.1 to upper bound this expression by using the fact that for all $i \in \{1,..,n\}$ we have $|\alpha_i|^2 \leq \frac{1}{4}2^{m-1}$. This means that any (n,m,p)-QRAC must have an average success probability, and, in particular, a worst case success probability which is less than or equal to

$$\frac{1}{2} + \frac{1}{2}\sqrt{\frac{2^{m-1}}{n}}, \tag{7.22}$$

as desired. □

Notice that if $m = 1$, (7.22) reduces to the same upper bound as found in [3] which means that the $(n, 1, \frac{1}{2} + \frac{1}{2\sqrt{n}})$-QRACs are optimal. For $m = 2$ we have hereby found that the worst case success probablity is upper bounded by

$$\frac{1}{2} + \frac{1}{\sqrt{2n}}, \tag{7.23}$$

and hence we have proved the conjecture put forth in [8]. In particular, we have shown that the $(4, 2, \frac{1}{2} + \frac{1}{2\sqrt{2}})$- and $(6, 2, \frac{1}{2} + \frac{1}{2\sqrt{3}})$-QRACs found in the examples above are optimal as well as the analytical $(3, 2, \frac{1}{2} + \frac{1}{\sqrt{6}})$-QRAC found in [8] is optimal.

8 Discussion

We begin this section by remarking that in the known and optimal QRACs with $m = 1, 2$ the average and worst case success probabilities coincide. In order to see why, we make the following summary of our findings.

Any (n, m, p)-QRAC saturates the bound given in (7.10) with respect to the average success probability if and only if the following two requirements are fulfilled: (1) The n POVMs can be associated with a set of n orthogonal (Lemma 7.1) unit vectors $\{\hat{\alpha}_i\}_{i=1}^n \subset \mathbb{R}^{4^m-1}$ where for all $i \in \{1, ..., n\}$ we have $\pm\frac{1}{\sqrt{2^{m-1}}}\hat{\alpha}_i \in \mathcal{B}(\mathbb{R}^{4^m-1})$ as seen in Lemma 6.1. When this is the case, the POVMs of measuring different bits are defined by unbiased quantum states and the elements of every POVM correspond to orthogonal quantum states since the two Bloch vectors $\pm\frac{1}{\sqrt{2^{m-1}}}\hat{\alpha}_i$ reach the upper bound in (5.27). And (2) For any $x \in \{0,1\}^n$ the encoding Bloch vectors, $\beta_x, \beta_{\overline{x}}$, simultaneously satisfy that $\beta_x \cdot \hat{V}_x = \beta_{\overline{x}} \cdot (-\hat{V}_x) = 1$ (saturating the upper bound in Lemma 5.2) where $\hat{V}_x$ (since the $\hat{\alpha}_i$'s are orthogonal) is given by

$$\hat{V}_x = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} \hat{\alpha}_i. \tag{8.1}$$

Lemma 5.2 then implies that β_x and $\beta_{\overline{x}}$ have the same residual vector, r_x, which is orthogonal to $\hat{V}_x$ and has norm equal to $\sqrt{R_{2^m}^2 - 1}$ so they are given by the pure state Bloch vectors

$$\beta_x = \hat{V}_x + r_x \ , \ \beta_{\overline{x}} = -\hat{V}_x + r_x. \tag{8.2}$$

When these two requirements are fulfilled the quantum state, ρ_x, for encoding the string $x \in \{0,1\}^n$ is

$$\rho_x = \frac{1}{2^m} I + \frac{1}{2}(\hat{V}_x + r_x) \cdot \tilde{\sigma}, \tag{8.3}$$

and hence the probability of correctly decoding the ith bit of x to be x_i is found to be

$$\frac{1}{2} + \frac{1}{2}\sqrt{\frac{2^{m-1}}{n}} + \frac{\sqrt{2^{m-1}}}{2} r_x \cdot \alpha_i. \tag{8.4}$$

We know that a QRAC that fulfills the two above requirements must have an average success probability of (7.22) which means that when averaging over all possible pairs (i, x) in (8.4) we get (7.22). Therefore, the average and worst case success probabilities coincide for such a construction if and and only for all pairs (i, x) we have $r_x \cdot \alpha_i = 0$ which means that encoding Bloch vectors consist of a superposition of two components of different orthogonal subspaces of $\mathcal{B}(\mathbb{R}^{4^m-1})$ - one which contributes to the success probability and one which does not but allows an extension of the other component. We summarize the above in the following definition.

Definition 8.1 (*Perfect quantum* (n, m)*-strategy*)**.** A *perfect quantum* (n, m)*-strategy* is a set of $2n$ Bloch vectors $\{\pm\frac{1}{\sqrt{2^{m-1}}}\hat{\alpha}_i\}_{i=1}^n \subset \mathcal{B}(\mathbb{R}^{4^m-1})$ fulfilling $\hat{\alpha}_i \cdot \hat{\alpha}_j = \delta_{ij}$ with which we can associate n POVMs such that there for all $x \in \{0,1\}^n$ exists a residual vector, r_x, fulfilling $r_x \cdot \hat{\alpha}_i = 0$ for all $i \in \{1, .., n\}$, that makes

$$\beta_x = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} \hat{\alpha}_i + r_x \tag{8.5}$$

a valid Bloch vector which can be used for encoding the string $x \in \{0,1\}^n$.

We define a perfect quantum (n, m)-strategy in this way to emphasize the particular construction in Bloch space. When considering $(n, 2, p)$-QRACs the upper bound we have just shown is lower than the upper bound on the worst case success probabilities implied by the Nayak bound. Unfortunately, for $m \geq 3$ the upper bound that we have just found is above the

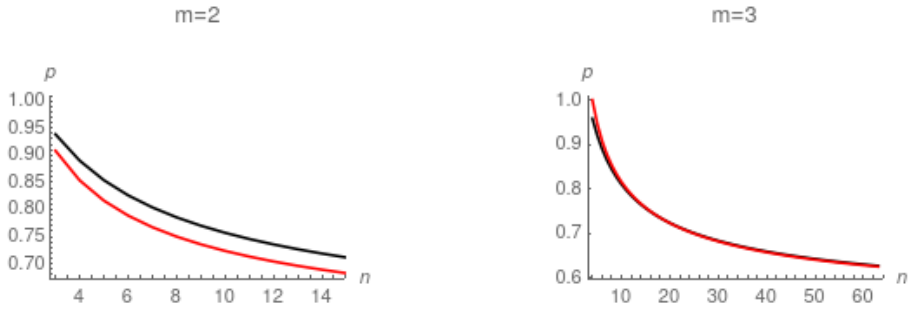


Figure 6: The red curve is corresponds to our new upper bound of $\frac{1}{2}+\frac{1}{2}\sqrt{\frac{2^{m-1}}{n}}$ and the black curve is the upper bound implied by the Nayak bound for $m = 2$ (on the left) and $m = 3$ (on the right).

Nayak bound, so theorem 7.1 is only interesting for $m \leq 2$ (and some values of n when $m = 3$ as we will see). Consider Figure 6. Here we have plotted the upper bound on the success probability implied by the Nayak bound (black curve) and the upper bound we just found in theorem 7.1 (red curve) for QRACs with $m = 2, 3$ (on the left and on the right, respectively) as a function of $n \in [m+1, 4^m - 1]$, where we have connected the points to make it easier for the eye. Notice that for $m = 3$ our new upper bound is below the upper bound implied by the Nayak bound for $n \geq 16$. Hence for $(n \geq 16, 3, p)$-QRACs we have a new and lower upper bound on the worst case success probability than what is implied by the Nayak bound.

From this we can conclude that only for certain pairs (n, m) there exist perfect quantum (n, m)-strategies. For $m = 2$ we already know perfect quantum $(n, 2)$-strategies for $n = 3, 4, 6$ and the data obtained in [8] strongly suggests that there exists one also for $n = 5$ although finding it analytically is still an open problem. Since the numerical method of constructing QRACs in [8] actually produces optimal $(n, 2, \approx \frac{1}{2}+\frac{1}{\sqrt{2n}})$-QRACs for $n = 3, 4, 5, 6$ one might suspect that perfect quantum $(n, 2)$-strategies do not exist for $n > 6$ (see Figure 4). For $n > 6$ they find improved worst case success probabilities when allowing the encoding states to be mixed. Giving a rigorous explanation of this phenomenon is also left open but we expect that one might find similar but stricter conditions for the geometry of Bloch space than the one given in Lemma 5.2. Also, we notice that in the known perfect quantum $(n, 2)$-strategies the encoding Bloch vectors span an increasing number of the 15 dimensions of $\mathbb{R}^{15}$ for increasing n. For $n = 6$ the encoding Bloch vectors span all of $\mathbb{R}^{15}$. Based on these considerations, we conjecture that perfect quantum $(n > 15, 3)$-strategies do not exist, even though our new upper bound is stricter than the upper bound implied by the Nayak bound for these values.

Also, in Proposition 3.1 we show that if one takes the average success probability as the figure of merit, choosing pure encoding states will always be preferable. Therefore, it would be interesting to run a similar optimization procedure as the one in [8] only allowing pure encoding states and optimizing with regards to the average success probability in order to see how close this comes to our new upper bound. Finding quantum (n, m)-strategies that yield an average success probability of the optimal $\frac{1}{2}+\frac{1}{2}\sqrt{\frac{2^{m-1}}{n}}$ is similar to finding perfect quantum (n, m)-strategies except we can loose the additional requirement that $r_x \cdot \alpha_i = 0$ for all pairs (i, x). This means a less restricted choice of residual vectors.

One could also investigate the possibilities of finding a general upper bound on the worst case success probability of a $(n, m > 2, p)$-QRAC which is similar to the $\frac{1}{2}+\frac{1}{2\sqrt{n}}$ and $\frac{1}{2}+\frac{1}{\sqrt{2n}}$

that we have for m equal to 1 and 2 respectively. So far, the most restricitve upper bound we know on p in any (n, m, p)-QRAC is the minimum of $\frac{1}{2} + \frac{1}{2}\sqrt{\frac{2^{m-1}}{n}}$ and the upper bound implied by the Nayak bound. This again, we suspect, would require that one finds similar but more restrictive bounds on Bloch space than the one given in Lemma 5.2.

9 Conclusion

We have found a new and lower upper bound on the worst case success probabilities of $(n, 2, p)$-QRACs and $(n \geq 16, 3, p)$-QRACs given by $p \leq \frac{1}{2} + \frac{1}{2}\sqrt{\frac{2^{m-1}}{n}}$. When $m = 2$ this reduces to $p \leq \frac{1}{2} + \frac{1}{\sqrt{2n}}$ and we have therefore proved the conjecture given in [8] and showed that the known $(3, 2, \frac{1}{2} + \frac{1}{\sqrt{6}})$- $(4, 2, \frac{1}{2} + \frac{1}{2\sqrt{2}})$- and $(6, 2, \frac{1}{2} + \frac{1}{2\sqrt{3}})$-QRACs are optimal. This was done by studying the geometry of quantum states in the Bloch vector representation. Specifically, through giving a geometric interpretation of the fact that quantum states do not have negative overlaps, we found restrictions on the components of any two Bloch vectors in opposing directions in Lemma 5.2. Also, we found that any POVM is determined by a number $\alpha_{0_i} \in \mathbb{R}^{4^m-1}$ and a vector $\alpha_i \in \mathbb{R}^{4^m-1}$ and we showed that $|\alpha_i| \leq \frac{1}{2}\sqrt{2^{m-1}}$. We saw that a POVM that reaches this upper bound can be associated with a pair of antiparallel Bloch vectors whose norms reach the upper bound of $r_{2^m} R_{2^m}$ implied by non-negativity of overlaps. Utilizing the fact that quantum states have non-negative overlaps therefore turned out to be crucial, and we expect that one might find a generalized upper bound on the worst case success probability of any (n, m, p)-QRAC that reduces to the known $\frac{1}{2} + \frac{1}{2\sqrt{n}}$ and $\frac{1}{2} + \frac{1}{\sqrt{2n}}$ for m equal to 1 and 2 respectively, by finding similar but more restrictive bounds on Bloch space than the one given in Lemma 5.2.

Acknowledgement

I would like to sincerely thank my supervisor, Laura Mančinska, for introducing me to the fascinating world of quantum information theory and for all the help she gave me through this process. My sincerest gratitude goes to my partner, Alice Manganaro, for always being by my side.

References

[1] Ambainis, A., Nayak, A., Ta-Shma, A., Vazirani, U. (1999). 'Dense quantum coding and a lower bound for 1-way quantum automata', Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC'99), pp. 376–383, arXiv:quant-ph/9804043.

[2] Ambainis, A., Nayak, A., Ta-Shma, A. and Vazirani, U. (2002). 'Dense Quantum Coding and Quantum Finite Automata', *Journal of the ACM*, vol. 49, Iss. 4, pp. 496–511. `https://dl.acm.org/doi/10.1145/581771.581773`.

[3] Ambainis, A., Leung, D., Mancinska, L. and M. Ozols. (2008). 'Quantum Random Access Codes with Shared Randomness', arXiv:0810.2937

[4] Bengtsson, I., Weis, S., Zyczkowski, K. (2011). 'Geometry of the set of mixed quantum states: An apophatic approach', arXiv:1112.2347

[5] Galvao, E. (2002). 'Foundations of quantum theory and quantum information applications', arXiv:quant-ph/0212124

[6] Goyal, S. K., Simon, B. N., Singh, R. and Simon, S. (2011). 'Geometry of the generalized Bloch sphere for qutrits' arXiv:1111.4427

[7] Hayashi, M., Iwama, K., Nishimura, H., Raymond, R. and Yamashita, S. (2006) '(4,1)-quantum random access coding does not exist – one qubit is not enough to recover one of four bits', *New J. Phys*, Vol. 8, Article no. 129. 10.1088/1367-2630/8/8/129 .

[8] Imamichi, T. and Raymond, R. (2018). 'Constructions of Quantum Random Access Codes'. AQIS 2018. Available at `http://www.ngc.is.ritsumei.ac.jp/~ger/static/AQIS18/OnlineBooklet/`. PDF No. 122. (Accessed June 4th 2020). Data available at github repository - `https://github.com/rraymondhp/qrac` (Accessed June 5th 2020).

[9] Iwama, K., Nishimura H., Raymond R. and Yamashita, S. (2007). 'Unbounded-Error One-Way Classical and Quantum Communication Complexity', Proc. of the 34th International Colloquium on Automata, Languages and Programming, LNCS 4596, pp. 110-121.

[10] Kimura, G. (2003). 'The Bloch Vector for N -Level Systems'. *Phys. Lett. A 314, 339*, arXiv:quant-ph/0301152v2.

[11] Kimura, G. (2003). 'The Bloch Vector for N-Level Systems' *Journal of the Physical Society of Japan*, Vol. 72, Issue suppl. C, pp. 185-188, 10.1143/JPSJS.72SC.185

[12] Kimura, G. (2004). 'The Bloch-vector space for N-level systems – the spherical-coordinate point of view' arXiv:quant-ph/0408014.

[13] Liabøtrø, O. (2016). 'Improved Classical and Quantum Random Access Codes', arXiv:1607.02667v2..

[14] Nayak, A. (1999). 'Optimal lower bounds for quantum automata and random access codes', Proceedings of the 40th IEEE Symposium on Foundations of Computer Science (FOCS'99), pp. 369–376, arXiv:quant-ph/9904093.

[15] Nielsen, M. A. and Chuang, I. L. (2000) *Quantum Computation and Quantum Information*, 10th Anniversary Edition published 2010, Printed in the United Kingdom by Clays, St Ives plc., Cambridge University Press.

[16] Spekkens, R. W., Buzacott, D. H., Keehn, A. J., Toner, B. and Pryde, G. J. (2009). 'Preparation Contextuality Powers Parity-Oblivious Multiplexing', arXiv:0805.1463.

[17] Wiesner, S. (1983). 'Conjugate coding', *SIGACT News*, vol. 15, Issue 1, pp. 78–88.