STATISTICAL ANALYSIS OF THE SINGLE-QUBIT UNITARITY RANDOMIZED BENCHMARKING PROTOCOL

M.SC. THESIS

To obtain the degree Master of Science at Delft University of Technology,

by

Bas DIRKSE

Student of Applied Physics and Applied Mathematics,
Delft University of Technology,
Delft, The Netherlands.

Thesis Committee:

Applied Physics:	
Prof. dr. S. D. C. Wehner	QuTech, supervisor, responsible professor
Dr. ir. M. Veldhorst	QuTech
Dr. M. T. Wimmer	Independent member
Applied Mathematics:	
Dr. ir. W.G.M. Groenevelt	Supervisor
Prof. dr. J. M. A. M. van Neerven	Responsible professor
Dr. M. Möller	Independent member

December 5, 2017

An electronic version of this dissertation is available at
http://repository.tudelft.nl/.

CONTENTS

PREFACE

This thesis was written as the final report of my master's project to obtain the degree of Master of Science in Applied Physics and Applied Mathematics. As this is a combined thesis project, I was looking for a strongly theoretical and mathematical subject. And with this topic, I certainly got what I bargained for. This project turned out to be completely analytical and was the first time I had the opportunity to derive a theorem of my own. Of course, the result still related to applications in quantum computing.

When starting on this project, my knowledge of representation theory was virtually zero and the last time I have seen group theory was over five years ago. I had a decent understanding in the calculus of Hilbert spaces and had followed some courses in quantum information theory as well. I felt that before even being able to thoroughly understanding the problem that we wanted to solve in this thesis, I had to study some of the prerequisite knowledge. I started refreshing up my knowledge on Hilbert spaces and quantum information theory, writing my own summary as I went. Then I refreshed group theory and started learning about the representations of finite groups. All of this learning was essentially done by writing a summary and repeating proofs in my own words. I also studied the theory op superoperators as a descriptive tool for quantum gates. All of this resulted in the extensive chapter 2. In retrospect, I might have spent a little bit too much time on getting my prerequisite knowledge up to the level that I wanted, before moving on to study the actual problem at hand. Perhaps this was due to the fear of not understanding it immediately, which inevitably still happened of course.

Next I went on to understand the randomized benchmarking protocol (and all the preliminaries that preceded them) and completely understand the work that my mentor Jonas Helsen had done to analyze the statistics of this protocol. To get familiar with the notation and the proof techniques, and also for completeness, I started giving a description of the protocol and the proof of work in my own words. When I finally was at the point that I was able to reproduce the protocol and the statistical problem, we were ready to tackle protocols that were related to randomized benchmarking. At first, the interleaved randomized benchmarking protocol seemed a good start, because of its close relation to standard randomized benchmarking. Soon I discovered that the statistics were actually the same, and the result of my mentor already covered the problem. We then decided to try and analyze the unitarity randomized benchmarking protocol. This protocol is slightly different and therefore required a slightly different knowledge on the specific group representations, but I was able to analyze the statistics of this protocol in a similar fashion to what Jonas had done for standard randomized benchmarking.

Many times on the way I discovered mistakes or got lost in some (relevant or irrelevant) detail. This was part of the learning process of course, but sometimes lead to some frustration. In the end I spend a few months working out all the details in order to bound each and every term that arose in my analysis. When I finally had the complete result I was very happy, but I needed to look further and try to understand the implications of my result. This lead to the result-first approach of the presentation of my work in chapter 5.

Altogether this year of graduation was very exciting and I have learned a lot, not only about randomized benchmarking proofs, but also on writing and presenting my own work and collaborating with other people. Being able to do this work in the inspiring environment of QuTech and in particular

in the group of Stephanie Wehner, has sparked my enthusiasm to possibly continue to work in the domain of quantum information theory in the future.

Bas Dirkse
Delft, December 5, 2017

1

INTRODUCTION

The goal of this chapter is to give an introduction to the research carried out and reported in this thesis. It starts in the first section with providing a background and motivation for the unitarity randomized benchmarking protocol. This protocol estimates the unitarity of a noisy quantum gate, an important metric that quantifies the coherence of a noisy gate used for quantum computation. Next it introduces the problem in unitarity randomized benchmarking of how many random sequences are needed to rigorously obtain an estimate of the unitarity. This thesis aims to provide a detailed answer to this problem. The second section continues with a more detailed problem description, after which the main result is presented that allows for the reduction of the number of sequences needed. Comparison is then made with previous and related work in the field. Finally an outline of this thesis is given, providing guidance to the reader as to where and when certain topics are covered in greater detail.

1

1.1. MOTIVATION

Currently great experimental effort is put into improving control over qubit systems to allow for scalable, fault-tolerant quantum computing. These tremendously difficult endeavors are motivated by the fundamental theoretical guarantee that a large-scale quantum computer can be built in principle if noise strengths and correlations are below a certain fault-tolerant threshold [1–4]. It is therefore of great importance that the strength of errors in noisy quantum processes can be quantified in terms of experimentally accessible quantities. A commonly used measure for quantifying the error of a noisy quantum gate $\tilde{G}$ is the average error rate r, which is defined as the infidelity of the output of the noisy gate $\tilde{G}$ with the output of its ideal unitary counterpart G, averaged over all pure input states. This quantity can be estimated efficiently and in a scalable manner (in the dimension of the underlying system) by the **randomized benchmarking** protocol [5–8], in a way that separates state preparation and measurement errors from the gate errors under investigation. These properties make it a very widely implemented protocol to experimentally characterize the error rate [9, 10, and references therein].

However this quantity can not directly be related to fault-tolerant thresholds, since these are formulated using the diamond norm distance [9, 11]. Intuitively, the average error rate r quantifies the average-case error behavior of a single use of a noisy gate, whereas fault-tolerant thresholds are formulated in terms of worst-case error behavior of a gate when used in a quantum computation. Even though there exist inequalities that bound the average error rate r in terms of the diamond norm distance and vice versa, these bounds are prohibitively loose in both r (in the small r regime) and the dimension of the underlying system for r to be a practical measure for fault-tolerant thresholds, even though these inequalities are optimal [9, 12]. Furthermore the average error rate r does not provide any information about the dominant error process in the system, providing little guidance on how to further improve the quality of the gates in an experimental setup.

In order to improve the understanding of noisy quantum gates $\tilde{G}$, the unitarity u has been introduced [13]. The unitarity is a measure of the coherence of the noisy gate and is roughly defined as the purity of output states averaged over all pure states with the identity component subtracted off. Intuitively, the unitarity is a quantity that characterizes how close the gate $\tilde{G}$ is to being unitary (coherent). This quantity is also experimentally accessible via the **unitarity randomized benchmarking** protocol [13], an experimental routine that is similar to standard randomized benchmarking and allows for estimation of u independent of state preparation and measurement errors. This provides a great experimental tool to distinguish whether the error process in the noisy gate is dominated by coherent processes (i.e. over-/under-rotations due to detuning and calibration errors) or by incoherent processes (i.e. relaxation, dephasing or depolarization) and thus allows for easier identification of dominant error contributions in a practical set-up [14]. It also turns out that coherent noise processes account for the large discrepancies between the average-case error behavior and worst-case error behavior in noisy gate implementations. Therefore knowing both the average error rate r and the unitarity u of a noisy gate $\tilde{G}$ can improve the bound on the worst-case error behavior for comparison to fault-tolerant thresholds [9, 11].

It is clear that randomized benchmarking type protocols have become very important experimental tools in quantifying the quality of a quantum gate implementation [9, 10, 14]. Therefore it is important that these protocols have a rigorous theoretical foundation. Randomized benchmarking type protocols essentially consist of (1) sampling multiple random sequences of m noisy gates, (2) applying these random sequences to some prepared state and (3) performing some measurement to obtain different measurement outcomes as a function of the sampled sequences. Averaging these measurement outcomes over the random sequences sampled and doing this for multiple sequence lengths m yields exponential decays in m where the decay parameter can be related to the quantity of interest characterizing the noisy gate. A decisive factor in the experimental feasibility of these protocols is **the number of random sequences** that must be averaged over in order to obtain rigorous

confidence intervals. These random sequences consist of m independently and uniformly sampled gates from a certain gate set $\mathcal{G}$. Exact averaging over all possible sequences is infeasible since there are $|\mathcal{G}|^m$ different sequences, which grows exponentially with the sequence length m. This question has been addressed by various authors for the standard randomized benchmarking protocol [8, 15, 16]. The best known result so far puts a bound on the number of sequences that is asymptotically independent of the system size and the sequence length, and that goes to zero as the average error rate of the noisy gate r goes to zero [16]. This result leads to an experimentally feasible number of sequences needed in realistic scenario's. The **number of sequences required for doing unitarity randomized benchmarking** up to a certain degree of accuracy has never been analyzed before. In this work the statistics of the unitarity randomized benchmarking protocol are analyzed for single-qubit systems. The result here is the first bound on the number of sequences needed for unitarity randomized benchmarking that has the similar property of going to zero in the limit of perfect gates ($u \to 1$), state preparations and measurements. In the regime of nearly perfect operations, the number of sequences is therefore much smaller than previously known results. This is made more precise in the next subsection.

1.2. SUMMARY OF MAIN RESULT

This work provides a rigorous bound on the number of sequences required for the unitarity randomized benchmarking protocol in case of single-qubit gates. The bound has the desirable property that the number of sequences needed goes to zero in the limit of perfect operations (gates, state preparation and measurement), which leads to a small number of sequences needed in the regime of good operational control. The bound is furthermore asymptotically independent of the sequence length m. This result brings rigorous unitarity randomized benchmarking for single qubits closer to the realm of experimental feasibility. Our result is derived under the assumption that the gate set under investigation is the single-qubit Clifford group [17, 18] and that the error model is gate and time-independent. In unitarity randomized benchmarking N different string of m independently and uniformly sampled gates from the Clifford group are composed. A noisy implementation of such sequences is applied to some initial state, after which a certain measurement is performed, yielding an outcome $q_{\mathbf{i_m}}$ that depends on the randomly sampled sequence indexed by the multi-index $\mathbf{i_m}$. Denote $\overline{q}_m$ as the average of the measurement outcomes $q_{\mathbf{i_m}}$ over the N randomly drawn sequences. Using the fact that $q_{\mathbf{i_m}}$ is a discrete and bounded random variable (due to the randomly chosen sequences), a concentration inequality [19] can be applied to bound the number of sequences N required for the average $q_{\mathbf{i_m}}$ to be close to the exact mean of the distribution. This allows for the estimation of the minimum number of sequences required as

$$N \geq \frac{\ln\left(\frac{\delta}{2}\right)}{\left(\frac{1-\epsilon}{\sigma^2+1}\right)\ln\left(\frac{1}{1-\epsilon}\right)+\left(\frac{\sigma^2+\epsilon}{\sigma^2+1}\right)\ln\left(\frac{\sigma^2}{\sigma^2+\epsilon}\right)}, \tag{1.1}$$

where ϵ and δ are parameters quantifying the confidence interval around $\overline{q}_m$ and σ^2 is an upper bound on the variance of the random variable $q_{\mathbf{i_m}}$. Our main contribution to putting a rigorous bound on N is proving a sharp bound on the variance of the random variable $q_{\mathbf{i_m}}$. This bound σ^2 depends essentially on a priori estimate of the unitarity u of the gates in the Clifford group, the sequence length m and relative state preparation and measurement errors. The bound σ^2 is essentially of the form

$$\sigma^2 = \left(\left[\frac{3\sqrt{3}}{2}+\sqrt{2}\right](1-u)^2\frac{1-u^{2(m-1)}}{1-u^2}(1-e_{SP})+e_{SP}\right)(1+e_M), \tag{1.2}$$

where $0 < e_{SP}, e_M < 1$ are measures of the relative state preparation and measurement error respectively. They are defined as the magnitude squared of the error component divided by the magnitude squared of the total operator in the Hilbert-Schmidt norm. Our bound satisfies certain desirable properties that allows us to put a sharp bound on N:

- In the absence of state preparation and measurement errors, $\sigma^2 \to 0$ (and therefore $N \to 0$) as the a priori estimate of the unitarity $u \to 1$;
- The variance bound is asymptotically independent of the sequence length m;
- The variance bound is sufficiently sharp in the experimentally relevant regimes of large a priori estimates of u and small relative state preparation and measurement errors e_{SP}, e_M.

In this regime our bound significantly improves a naive bound using a weaker concentration inequality that does not depend on the variance of the distribution. Similar to the approach of [8], it can be shown that

$$N \geq \frac{\ln(\frac{2}{\delta})}{2\epsilon^2}. \tag{1.3}$$

As a concrete example $\delta = \epsilon = 0.01$ yields $N \geq 26492$, whereas our new bound yields $N \geq 585$ for $u \geq 0.999$ and $e_{SP}, e_M \leq 0.001$ and $N \geq 3532$ for $u \geq 0.99$ and $e_{SP}, e_M \leq 0.01$.

Since our result is similar to the result of [16] for standard randomized benchmarking, it is natural to compare the two results. The bound of [16] for randomized benchmarking has the stronger property that $N \to 0$ as $r \to 0$ even in the presence of state preparation and measurement errors. In our result, these errors contribute a constant factor to the bound on N. We argue that this is the best achievable result, since even in the best case scenario of perfect gates, the random sequences for unitarity randomized benchmarking still differ between different realizations (and therefore $q_{\mathbf{i_m}}$ varies over the random sequences samples), meaning nonzero variance of the random variable $q_{\mathbf{i_m}}$. In contrast the realized sequences for randomized benchmarking are all the identity sequence in the case of ideal gates, due to the inversion step in the end. Therefore the relevant random variable is constant over all sequences and the variance goes to zero. Unitarity randomized benchmarking lacks this inversion step, so the sampled sequences differ from each other even in the limit of perfect gates. We show using an example that state preparation and measurement errors contribute randomness to the protocol even in the case of perfect gates.

1.3. THESIS OUTLINE

This thesis is divided into four main chapters, excluding this introduction chapter. They are structured in the following way. First, a summary of prerequisite knowledge is presented in chapter 2. The goal of this chapter is to familiarize the reader with some of the relevant concepts in quantum information theory and mathematics that are the foundation for understanding the main result of this thesis. All of the topics are standard textbook material and as such serve only to summarize some key concepts. No illustrating examples are given and for many proofs the reader is referred to textbooks. Each section covers a separate topic and is independently readable from the other sections. The reader is invited to skip any sections he/she is familiar with already.

In chapter 3 some more specialized prerequisite knowledge is presented that is essential to understanding randomized benchmarking related protocols and their proofs, as well as understanding the new proofs given here. Key notation is also introduced along the way. Although none of these prerequisite topics are new, most of these topics are outside the scope of standard textbook material or are presented in a way tailored to their application in benchmarking protocols.

The contents of chapter 4 review the randomized benchmarking protocol, the slight modification to interleaved randomized benchmarking and finally the protocol that is analyzed in this thesis, unitarity randomized benchmarking. The goal is to present the latest understanding of randomized benchmarking within the limits of our assumptions and report on the recent similar analysis of the number of sequences required. The chapter sets the stage for our analysis of unitarity randomized benchmarking by first familiarizing the reader with all the notation and the techniques used in proving that these protocols work. Finally the unitarity randomized benchmarking protocol is presented

and proven to work. Most of the material is a review of recent literature, but some slight modifications are proposed and nuances are put on different aspects.

Finally in chapter 5 our main result is stated, discussed and proven. This is a new result as summarized above, improving on previously known work. The chapter is structured in a top-down way, starting with the statement of the main result and a discussion thereof. Next experimental data is used to illustrate the result and compare it to previously known results. It serves to illustrate the dependencies of N on the various parameters involved. Only after this the variance bound, the main ingredient of the proof, is presented. First the ideal scenario of ideal state preparations and measurements is covered, and next the result is extended to include state preparation and measurement errors. The global outline of the proof is presented first, and all of the technical details are captured in separate smaller propositions. This is conform our top-down approach of presenting the result. Finally an outlook for the multi-qubit case is given and conclusions on the significance of the result as well as some remaining open questions are discussed.

2

PREREQUISITE KNOWLEDGE

In this chapter the most important prerequisite knowledge required throughout the rest of this thesis. All material covered in this chapter is standard textbook material, and many references can be used to study this material is summarized. The aim is to give a summary of elementary definitions and theorems, without providing much intuition, illustration or discussion. Each section in this chapter covers a separate topic and they can be read independently from each other. The reader is invited to only read the sections on the topics he/she is unfamiliar with. The first three section introduce strictly mathematical concepts, whereas the last two section introduce the relevant tools of quantum information theory, aimed towards the audience that is less familiar in this topic. The treatment is however still fairly mathematical and concise.

2.1. HILBERT SPACES AND LINEAR OPERATORS

This section is designed to give an overview of the mathematical theory of Hilbert spaces and linear operators, introduce the notation used and state the most important theorems that can be found in classical textbooks on analysis. The content is roughly based on refs [20, 21] and many proofs of statements can be found here.

2.1.1. DEFINITIONS AND RESULTS FOR GENERAL HILBERT SPACES

The concept of Hilbert spaces is absolutely fundamental to the description of quantum mechanics and here the most basic definitions and theorems needed to construct Hilbert spaces are summarized. For a more detailed description see [20]. A Hilbert space is defined as follows:

Definition 2.1.1 (Hilbert space)**.** A complex Hilbert space, usually denoted $\mathcal{H}$, is a vector space over $\mathbb{C}$ equipped with an inner product that is complete with respect to the norm induced by the inner product. □

A normed vector space $\mathcal{H}$ is complete if every Cauchy sequence in $\mathcal{H}$ converges in $\mathcal{H}$ with respect to the norm. To avoid any possible confusion, the inner product is defined as follows:

Definition 2.1.2 (Inner product)**.** An inner product on a complex vector space $\mathcal{H}$ over $\mathbb{C}$ is a function $\langle\cdot,\cdot\rangle : \mathcal{H}\times\mathcal{H}\to\mathbb{C}$ such that:

(i) $\langle\cdot,\cdot\rangle$ is linear in its second argument, i.e. $\langle x, ay+bz\rangle = a\langle x,y\rangle + b\langle x,z\rangle$ for all $x,y,z\in\mathcal{H}$ and all $a,b\in\mathbb{C}$;

(ii) $\langle\cdot,\cdot\rangle$ is conjugate symmetric, i.e. $\langle x,y\rangle = \langle y,x\rangle^*$ for all $x,y\in\mathcal{H}$;

(iii) $\langle\cdot,\cdot\rangle$ is positive definite, i.e. $\langle x,x\rangle \geq 0$ and $\langle x,x\rangle = 0 \Leftrightarrow x = 0$ for all $x\in\mathcal{H}$. □

Note that in most textbooks in mathematics the inner product is defined to be linear in its first argument, but following standards in physics, the definition of linearity in the second argument is adopted in this thesis. The inner product induces a norm on the vector space $\mathcal{H}$ by the function $\|x\|_2 = \sqrt{\langle x,x\rangle}$ for all $x\in\mathcal{H}$. This is usually referred to as the Euclidean norm and the subscript 2 is generally omitted when its clear from the context. A very important theorem regarding the inner product and its induced norm, is the Cauchy-Schwarz inequality, stated below.

Theorem 2.1.1 (Cauchy-Schwarz inequality)**.** *Let $x,y\in\mathcal{H}$. Then $|\langle x,y\rangle| \leq \|x\|\|y\|$, with equality if and only if $x = cy$ for some $c\in\mathbb{C}$.*

Proof. The statement is trivial if $x = 0$, so therefore assume $\langle x,x\rangle > 0$. Then define $z = y - \frac{\langle x,y\rangle}{\langle x,x\rangle}x$. Then $\langle x,z\rangle = \langle x,y\rangle - \frac{\langle x,y\rangle}{\langle x,x\rangle}\langle x,x\rangle = 0$. So

$$\begin{aligned}
\|y\|^2 &= \|z + \frac{\langle x,y\rangle}{\langle x,x\rangle}x\|^2 \\
&= \left\langle z + \frac{\langle x,y\rangle}{\langle x,x\rangle}x, z + \frac{\langle x,y\rangle}{\langle x,x\rangle}x \right\rangle \\
&= \langle z,z\rangle + \frac{\langle x,y\rangle^*}{\langle x,x\rangle}\langle x,z\rangle + \frac{\langle x,y\rangle}{\langle x,x\rangle}\langle z,x\rangle + \frac{|\langle x,y\rangle|^2}{\langle x,x\rangle} \qquad (2.1)\\
&= \|z\|^2 + \frac{|\langle x,y\rangle|^2}{\|x\|^2} \\
&\geq \frac{|\langle x,y\rangle|^2}{\|x\|^2}.
\end{aligned}$$

Multiply by $\|x\|^2$ to obtain the result. Equality is obtained if and only if $\|z\| = 0 \Leftrightarrow z = 0 \Leftrightarrow y = \frac{\langle x,y\rangle}{\langle x,x\rangle} x = cx$. ■

In the context of Hilbert spaces it is natural to consider linear operators between Hilbert spaces. A linear operator is is defined as follows:

Definition 2.1.3 (Linear operator)**.** Let $\mathcal{H}$ and $\mathcal{H}'$ be Hilbert spaces. The mapping $A : \mathcal{H} \to \mathcal{H}'$ is a linear operator if it satisfies $A(ax + by) = aAx + bAy$ for all $x, y \in \mathcal{H}$ and all $a, b \in \mathbb{C}$. The set of all linear operators is denoted as $\mathcal{L}(\mathcal{H}, \mathcal{H}')$. $\mathcal{L}(\mathcal{H})$ is understood to mean $\mathcal{L}(\mathcal{H}, \mathcal{H})$. □

The operator norm is a norm on $\mathcal{L}(\mathcal{H})$ defined by $\|A\|_\infty = \sup_{x\in\mathcal{H}}\{\|Ax\| : \|x\| \leq 1\}$ for $A \in \mathcal{L}(\mathcal{H})$. An operator is called bounded if $\|A\|_\infty < \infty$. The set of bounded linear operators is denoted by $\mathcal{B}(\mathcal{H}) = \{A \in \mathcal{L}(\mathcal{H}) : \|A\|_\infty < \infty\}$. The space $\mathcal{L}(\mathcal{H})$ equipped with the operator norm is in fact also a complete vector space (i.e. a Banach space). The dual space of a Hilbert space $\mathcal{H}$ is the space of all bounded linear functionals on $\mathcal{H}$, defined as $\mathcal{H}^* = \{f \in \mathcal{L}(\mathcal{H}, \mathbb{C}) : |f(x)| < \infty \text{ for all } x \in \mathcal{H}\}$. A very fundamental theorem characterizing linear functionals is given by Riesz's representation theorem:

Theorem 2.1.2 (Riesz's representation theorem)**.** *Let $\mathcal{H}$ be a Hilbert space. For any $y \in \mathcal{H}$ the function $f_y : \mathcal{H} \to \mathbb{C}$ given by $f_y(x) = \langle y, x\rangle$ defines a linear functional on $\mathcal{H}$, i.e. $f_y \in \mathcal{H}^*$ with $\|f\| = \|y\|$. Conversely, for any linear functional $f \in \mathcal{H}^*$ there exists a unique $y \in \mathcal{H}$ such that $f(x) = \langle y, x\rangle$ for all $x \in \mathcal{H}$.*

Proof. See Theorem 33.9 of [20] ■

Note that conform standards in physics, the inner product is defined to be linear in the second argument, making $f_y(x) := \langle y, x\rangle$ a linear functional. In general, the linear functional f_y corresponding to $y \in \mathcal{H}$ is denoted $y^\dagger \in \mathcal{H}^*$, a notation justified by the theorem since there is a one-to-one correspondence between each linear functional and an element of the Hilbert space. The inner product is then sometimes written as $f_y(x) = \langle y, x\rangle = y^\dagger x$. The definition of the adjoint of an operator heavily relies on Riesz's representation theorem.

Definition 2.1.4 (Adjoint)**.** Let $A \in \mathcal{B}(\mathcal{H}, \mathcal{H}')$. The adjoint $A^\dagger \in \mathcal{B}(\mathcal{H}', \mathcal{H})$ is uniquely defined by $\langle Ax, y\rangle = \langle x, A^\dagger y\rangle$ for all $x \in \mathcal{H}$, $y \in \mathcal{H}'$. □

This uniquely defines the adjoint by invoking Riesz's representation theorem. The adjoint of an operator is used to define several important classes of bounded linear operators. The restriction of boundedness is not always necessary but the discussion of unbounded operators is avoided in this text for two reasons. First, in quantum information finite dimensional Hilbert spaces arise naturally, and all linear operators are bounded in that case. Second the treatment of unbounded operators, even though interesting in quantum mechanics, requires the introduction of some other concepts that are of little use in quantum information theory and are therefore omitted from this section. In the definition below, several important classes of bounded linear operators are summarized.

Definition 2.1.5 (Classes of bounded linear operators)**.** Let $A \in \mathcal{B}(\mathcal{H})$ be a bounded linear operator on $\mathcal{H}$. Then A is

(i) *normal* if it commutes with its adjoint $A^\dagger$, i.e. if $AA^\dagger = A^\dagger A$. The set of normal operators is denoted $\mathcal{N}(\mathcal{H})$.

(ii) *unitary* if $AA^\dagger = A^\dagger A = I$ is the identity on $\mathcal{H}$. The set of unitary operators is denoted $\mathcal{U}(\mathcal{H})$.

(iii) *hermitian* if $A = A^\dagger$. This is equivalent to $\langle Ax, x\rangle \in \mathbb{R}$ for all $x \in \mathcal{H}$. The set of hermitian opera-

tors is denoted Herm($\mathcal{H}$).

(iv) *positive semi-definite* (denoted $A \succeq 0$) if A is hermitian and $\langle Ax, x\rangle \geq 0$ for all $x \in \mathcal{H}$. The set of positive semi-definite operators is denoted Pos($\mathcal{H}$).

(v) *an orthogonal projection* if $A^2 = A$ and A is hermitian. The set of orthogonal projections is denoted Proj($\mathcal{H}$). □

By virtue of the definitions of these classes of operators, the set inclusions

$$\text{Proj}(\mathcal{H}) \subset \text{Pos}(\mathcal{H}) \subset \text{Herm}(\mathcal{H}) \subset \mathcal{N}(\mathcal{H}) \subset \mathcal{B}(\mathcal{H}) \subseteq \mathcal{L}(\mathcal{H}), \tag{2.2}$$

as well as $\mathcal{U}(\mathcal{H}) \subset \mathcal{N}(\mathcal{H})$ hold. However it is noteworthy to see that there is no inclusion possible between $\mathcal{U}(\mathcal{H})$ and Herm($\mathcal{H}$), while they are also not disjunct. This means that there exists operators which are hermitian but not unitary, unitary but not hermitian, both or neither.

Normal operators are of great importance because they are diagonalizable by unitary transformation, according to the spectral theorem. Unitary operators preserve the inner product, meaning that $\langle Ux, Uy\rangle = \langle x, y\rangle$ for all $U \in \mathcal{U}(\mathcal{H})$ and all $x, y \in \mathcal{H}$. Hermitian operators are especially important in quantum mechanics, since their spectrum is real. If in addition, the spectrum is nonnegative (strictly positive), the class of positive semi-definite (positive definite) operators is retrieved. They are of importance for measurements in quantum mechanics. Furthermore, the notion of positive semi-definiteness provides a partial ordering on the set Herm($\mathcal{H}$). For two hermitian operators $A, B \in \text{Herm}(\mathcal{H})$ one can order them as $A \succeq B$ if $A - B \succeq 0$ is positive semi-definite. Note that it may happen that $A \not\succeq B$ and $A \not\preceq B$, hence the ordering is partial. Finally, orthogonal projections are an important special type of positive semi-definite operators. A more detailed characterization is given in the next section, applied only to the finite-dimensional case. First however, the notation of commutator and anti-commutator is defined.

Definition 2.1.6 (commutator and anti-commutator)**.** Let $A, B \in \mathcal{B}(\mathcal{H})$ be two bounded operators. The commutator between A and B is then defined as $[A, B] = AB - BA$. Two operators are said to commute with each other if $[A, B] = 0$ (i.e. if $AB = BA$). Similarly, the anti-commutator is defined to be $\{A, B\} = AB + BA$ and the operators A and B are said to anti-commute if the anti-commutator is zero (i.e. if $AB = -BA$). □

In the next subsection, the theory is refined to linear operators on finite-dimensional Hilbert spaces, since these occur most naturally in quantum information theory.

2.1.2. LINEAR OPERATORS ON FINITE DIMENSIONAL HILBERT SPACES

All of the reviewed theory above holds for general Hilbert spaces, in particular also for infinite-dimensional Hilbert spaces. In this thesis almost all Hilbert spaces will be finite dimensional, complex Hilbert space of the form $\mathcal{H} = \mathbb{C}^d$. It is from here on assumed that $\mathcal{H}$ is of finite dimension d unless explicitly specified otherwise. Typically d will be a power of 2, since a q-qubit system is associated with the Hilbert space $\mathcal{H} = \mathbb{C}^d$, with $d = 2^q$. The additional assumption of finite dimension reduces the complexity significantly. When assuming that the dimension of $\mathcal{H}$ is finite, the following additional statements can be made:

1. All linear operators are bounded. This implies $\mathcal{B}(\mathcal{H}) = \mathcal{L}(\mathcal{H})$ and frees us from the additional restriction of boundedness.
2. All norms are equivalent. That is, for all possible norms $\|\cdot\|_a$ and $\|\cdot\|_b$ there exists real numbers K and M such that $K\|x\|_a \leq \|x\|_b \leq M \leq \|x\|_a$ for all $x \in \mathcal{H}$. This means that a finite dimensional Hilbert space is complete in every possible norm.
3. There always exists an orthogonal basis of $\mathcal{H}$.

4. An operator $A \in \mathcal{L}(\mathcal{H})$ is invertible if and only if the range of A is the entire Hilbert space $\mathcal{H}$.
5. The spectrum of an operator $A \in \mathcal{L}(\mathcal{H})$ consists only of d (not necessarily distinct) eigenvalues, defined as the d (possibly complex) roots of the equation $\text{Det}(A-\lambda I) = 0$ where I is the identity.
6. A linear operator $A \in \mathcal{L}(\mathcal{H})$ is usually represented by a $d \times d$ matrix of complex numbers, i.e. $L(\mathbb{C}^d) \cong \mathbb{C}^{d\times d}$. All properties of the operators discussed in the previous subsection carry over to properties of matrices in linear algebra.

Now some properties of certain classes of linear operators will be discussed. This discussion was intentionally postponed until here, since from here the linear operators are assumed to be finite dimensional. This allows for statements about the matrix representation and about the eigenvalues of the operators to be made, without the need to be careful about the subtleties of the infinite-dimensional case. The following four propositions characterize unitary, hermitian, positive semi-definite and projective operators respectively.

Proposition 2.1.3 (characterization of unitary operators)**.** *Let $U \in \mathcal{L}(\mathbb{C}^d)$. Then the following are equivalent:*

(1) U is unitary, i.e. $UU^\dagger = U^\dagger U = I$;

(2) U is nonsingular and $U^\dagger = U^{-1}$;

(3) The columns of U form an orthonormal basis of $\mathbb{C}^n$;

(4) The rows of U form an orthonormal basis of $\mathbb{C}^n$;

(5) $\langle Ux, Uy\rangle = \langle x, y\rangle$ for all $x, y \in \mathbb{C}^d$;

(6) U is normal with all the eigenvalues lying on the unit circle.

Proof. See Theorem 2.1.4 of [22]. ■

Proposition 2.1.4 (characterization of hermitian operators)**.** *Let $A \in \mathcal{L}(\mathbb{C}^d)$. Then the following are equivalent:*

(1) A is hermitian, i.e. $A = A^\dagger$;

(2) $\langle x, Ax\rangle \in \mathbb{R}$ for all $x \in \mathbb{C}$;

(3) A is normal and all eigenvalues of A are real

Proof. See Theorem 4.1.4 of [22]. ■

Proposition 2.1.5 (characterization of positive semi-definite operators)**.** *Let $A \in \mathcal{L}(\mathbb{C}^d)$. Then the following are equivalent:*

(1) A is positive semi-definite ($A \geq 0$), i.e. $\langle x, Ax\rangle$ is real and nonnegative for all $x \in \mathbb{C}$;

(2) A is normal and all eigenvalues of A are real and nonnegative;

(3) $A = B^\dagger B$ for some $B \in \mathcal{L}(\mathbb{C}^d)$;

(4) $\langle B, A\rangle = \text{Tr}[B^\dagger A]$ is real and nonnegative for all positive semi-definite $B \in \text{Pos}(\mathbb{C}^d)$.

Proof. See Theorem 7.2.1 and 7.2.7 of [22]. ■

Proposition 2.1.6 (characterization of orthogonal projections)**.** *Let $P \in \text{Proj}(\mathbb{C}^d)$ be a nonzero orthogonal projection, i.e. $P^2 = P \neq 0$ and $P = P^\dagger$. Then:*

(1) $\mathrm{Rge}(P) \perp \mathrm{Ker}(P)$ *(sometimes, this is the defining property of an orthogonal projection together with $P^2 = P$, but a projection is orthogonal in this sense if and only if it is hermitian).*

(2) *The eigenvalues of P are either* 0 *or* 1.

(3) *For any $u \in \mathbb{C}^d$ with $\|u\| = 1$, it follows that $0 \leq \langle u, Pu\rangle \leq 1$, with $\langle u, Pu\rangle = 0 \Leftrightarrow Pu = 0$ and $\langle u, Pu\rangle = 1 \Leftrightarrow Pu = u$.*

Proof. (1) For any $x, y \in \mathbb{C}^d$, note that $(I-P)y \in \mathrm{Ker}(P)$ since $P(I-P)y = (P-P^2)y = 0$. Then

$$\langle Px, (I-P)y\rangle = \langle P^2x, (I-P)y\rangle = \langle Px, P(I-P)y\rangle = \langle Px, 0\rangle = 0.$$

So $\mathrm{Rge}(P) \perp \mathrm{Ker}(P)$. To show that an orthogonal projection in this sense is hermitian, note that

$$\langle (I-P)x, Py\rangle = \langle Px, (I-P)y\rangle = 0 \Leftrightarrow \langle Px, y\rangle = \langle Px, Py\rangle = \langle x, Py\rangle .$$

But $\langle Px, y\rangle = \langle x, P^\dagger y\rangle$ and so $P = P^\dagger$.

(2) Suppose $Px = \lambda x$ for some $x \in \mathbb{C}^d$. Then also $P^2x = \lambda^2 x = Px = \lambda x$. Therefore $\lambda^2 = \lambda$. The only solutions to this equation are $\lambda = 0$ or $\lambda = 1$.

(3) Now $\|Pu\|^2 = \langle Pu, Pu\rangle = \langle u, P^2u\rangle = \langle u, Pu\rangle \leq \|Pu\|\|u\|$, where the last expression is due to the Cauchy-Schwarz inequality and it holds with equality if and only if $Pu = cu$ for some $c \in \mathbb{C}$ (Theorem 2.1.1). Since the only eigenvalues of P are 0 and 1, equality holds if and only if $Pu = u$ or $Pu = 0$. Since $\|u\| = 1$ and $P \neq 0$ it follow that $\|Pu\| \leq 1$ and hence $\langle u, Pu\rangle \leq 1$, with equality if and only if $Pu = u$. Furthermore $\langle u, Pu\rangle = \|Pu\|^2 \geq 0$ with equality if and only if $Pu = 0$. ■

The trace is one particularly important linear functional on $\mathcal{L}(\mathcal{H})$. Again, the discussion of the trace is limited to the finite dimensional case, but the trace can under certain conditions be extended to compact operators on infinite-dimensional Hilbert spaces. The trace is defined as follows.

Definition 2.1.7 (Trace)**.** Let $A, B \in \mathcal{L}(\mathcal{H})$ be linear operators and $\{x_i\}_{i=1}^n$ be a orthonormal basis for $\mathcal{H}$. Then $\mathrm{Tr} \in \mathcal{L}(\mathcal{H})^* = \mathcal{L}(\mathcal{L}(\mathcal{H}), \mathbb{C})$ is a linear functional defined by

$$\mathrm{Tr}[A] = \sum_{i=1}^n a_{ii} = \sum_{i=1}^n \lambda_i, \tag{2.3}$$

where $a_{ii} = \langle x_i, Ax_i\rangle$ are the diagonal entries of the matrix representation of A and λ_i are the eigenvalues of A. Moreover, $\mathrm{Tr}[AB] = \mathrm{Tr}[BA]$, which is known as the cyclic property of the trace. □

The cyclic property is mentioned in the definition, because it can be viewed also as a defining property of the trace in the following sense. Any linear functional $f \in \mathcal{L}(\mathcal{H})^*$ that satisfies $f(AB) = f(BA)$ satisfies $f = c\,\mathrm{Tr}$ for some $c \in \mathbb{C}$. In particular, this means that the trace is invariant under similarity transformation PAP^{-1}, since $\mathrm{Tr}[PAP^{-1}] = \mathrm{Tr}[P^{-1}PA] = \mathrm{Tr}[A]$. The fact that the trace is equal to the sum of the eigenvalues follows then from the fact that every operator A is similar to its Jordan normal form. It can also be shown that the definition is independent of the choice of the orthonormal basis in which A is represented. In fact, the trace can be defined without referring to the eigenvalues of A or to any basis of $\mathcal{H}$. This definition holds depends on the tensor product of $\mathcal{H}$ and its dual $\mathcal{H}^*$, and the isomorphism with $\mathcal{L}(\mathcal{H})$.

One of the most important results in the theory of linear operators is the spectral theorem. The theorem can be generalized to bounded linear operators on infinite dimensional Hilbert spaces, as well as to unbounded linear operators, but its statement is easier in the case of finite dimensional Hilbert spaces. There is many different forms to state the spectral theorem, but the bottom line is that every normal operator is diagonalizable by a unitary matrix. The result is summarized in the following theorem with its corollaries.

Theorem 2.1.7 (The Spectral Theorem)**.** *Let $\mathcal{H} = \mathbb{C}^d$ and $N \in \mathcal{N}(\mathcal{H})$. Assume there are $k \leq d$ distinct eigenvalues $\lambda_1, ..., \lambda_k$. Then there exists a unique set of orthogonal projectors $P_1, ..., P_k \in \text{Proj}(\mathcal{H})$ satisfying $P_i P_j = \delta_{ij} P_i$ and $\sum_{i=1}^k P_i = I$, where δ_{ij} is the Kronecker delta and I is the identity on $\mathcal{H}$, such that*

$$N = \sum_{i=1}^{k} \lambda_i P_i. \tag{2.4}$$

$\text{Rank}\, P_i$ is equal to the multiplicity of λ_i for each $i = 1, ..., k$.

Proof. See Theorem 2.5.3 of [22] or Theorem 2.1 of [23]. ■

Corollary. *Eigenvectors belonging to distinct eigenvalues are orthogonal.*

Corollary. *Let $\mathcal{H} = \mathbb{C}^d$ and $N \in \mathcal{N}(\mathcal{H})$ and let $\lambda_1, ..., \lambda_d$ be the eigenvalues of N. Then there exists an orthonormal basis $\{u_1, ..., u_d\}$ of $\mathcal{H}$ such that*

$$N = \sum_{i=1}^{d} \lambda_i u_i u_i^\dagger = U \Lambda U^\dagger, \tag{2.5}$$

where $U = [u_1 \cdots u_d]$ is a unitary matrix and $\Lambda = \text{diag}(\lambda_1, ..., \lambda_d)$.

The second corollary gives rise to the definition of a function of normal operators. Let $f : \mathbb{C} \to \mathbb{C}$ be a complex-valued function. Then the function $f : \mathcal{N}(\mathcal{H}) \to \mathcal{N}(\mathcal{H})$ is defined by $f(N) := \sum_{i=1}^d f(\lambda_i) u_i u_i^\dagger$. If the domain of f is a subset of $\mathbb{C}$ and all eigenvalues are in the subset, then the definition holds naturally. One function that is frequently encountered is the square root of a positive semi-definite operator. If $A \in \text{Pos}(\mathcal{H})$ then by the above definition the operator $\sqrt{A} \in \text{Pos}(\mathcal{H})$ is uniquely defined via $f(z) = \sqrt{z}$. In particular, for any $A \in \mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$ it can easily be seen (observing that $A^\dagger \in \mathcal{L}(\mathcal{H}_2, \mathcal{H}_1)$) that $A^\dagger A \in \mathcal{L}(\mathcal{H}_1)$ is a positive semi-definite operator, since

$$\langle A^\dagger A x, x \rangle = \langle Ax, Ax \rangle = \langle x, A^\dagger A x \rangle = \|Ax\|_2^2 \geq 0, \tag{2.6}$$

for all $x \in \mathcal{H}_1$, where the norm is the 2-norm induced by the inner product on $\mathcal{H}_2$. Therefore for any operator $A \in \mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$ one can define the absolute value of A uniquely as $|A| = \sqrt{A^\dagger A}$. An important application of this is for hermitian operators $A \in \text{Herm}(\mathcal{H})$. As discussed in Proposition 2.1.4, hermitian operators are precisely the normal operators with real eigenvalues. That means, using the absolute value, a hermitian operator can be split into a positive and negative part as follows.

Definition 2.1.8 (Positive/negative part of hermitian operator)**.** Let $A \in \text{Herm}(\mathcal{H})$ and $|A| = \sqrt{A^\dagger A}$. Then the positive part of A is defined as $A^+ = (|A| + A)/2$ and the negative part of A is defined as $A^- = (|A| - A)/2$. Note that A^+ and A^- are both positive semidefinite and $A = A^+ - A^-$. □

Another important consequence of the spectral theorem is presented below. The theorem states that two normal operators can be simultaneously diagonalized if and only if they commute.

Theorem 2.1.8 (Simultaneously diagonalizable)**.** *Let $\mathcal{H} = \mathbb{C}^d$ and $N, M \in \mathcal{N}(\mathcal{H})$ be two normal operators. Then there exists a unitary operator $U \in \mathcal{U}(\mathcal{H})$ such that $N = U \Lambda_N U^\dagger$ and $M = U \Lambda_M U^\dagger$ are the respective spectral decompositions if and only if $[N, M] = 0$.*

Proof. See Theorem 2.5.5 of [22] or Theorem 2.2 of [23]. ■

Next a decomposition is discussed that applies more generally than the spectral theorem, since it also applies to operators that are not normal, or map between Hilbert spaces of different dimension.

Each operator $A \in \mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$, for which $\text{Dim}(\mathcal{H}_1)$ need not be equal to $\text{Dim}(\mathcal{H}_2)$ but are assumed finite here, admits the singular value decomposition. In a sense this is a generalization of the spectral decomposition. However, the two only coincide for positive semi-definite matrices.

Theorem 2.1.9 (Singular Value Theorem)**.** *Let $A \in \mathcal{L}(\mathbb{C}^m, \mathbb{C}^n) \cong \mathbb{C}^{n\times m}$ be a $n \times m$ matrix and let $d = \min(n, m)$ and suppose $\text{Rank}\, A = r \leq d$. Then there exists square unitary matrices $U \in \mathbb{C}^{n\times n}$ and $V \in \mathbb{C}^{m\times m}$, and a real diagonal matrix $S_d = \text{diag}(s_1, s_2, ..., s_d)$ with nonnegative decreasing entries $s_1 \geq s_2 \geq \cdots \geq s_d \geq 0$ (of which exactly the first r are strictly positive and the remaining $d - r$ are zero) such that $A = USV^\dagger$, where*

$$S = \begin{cases} S_d & \text{if } n = m, \\ \begin{bmatrix} S_d & 0 \end{bmatrix} \in \mathbb{C}^{n\times m} & \text{if } m > n, \text{ and} \\ \begin{bmatrix} S_d \\ 0 \end{bmatrix} \in \mathbb{C}^{n\times m} & \text{if } m < n. \end{cases} \tag{2.7}$$

The numbers $s_1, ..., s_d$ are called the singular values of A.

Proof. See Theorem 2.6.3 of [22]. ■

For normal operators $A \in \mathcal{N}(\mathcal{H})$ the singular values of A are the absolute value of the eigenvalues of A. That is to say, if the spectral decomposition of A is $A = U\Lambda U^\dagger$ then $|A| = \sqrt{A^\dagger A} = U|\Lambda|U^\dagger$. Note that this does not say anything about the unitary operators arising in the singular value decomposition of A, just about the diagonal matrix $S = |\Lambda|$.

The space $\mathcal{L}(\mathcal{H})$ is in itself a finite dimensional Hilbert space (of dimension d^2), when equipped an inner product. Most common is the use of the Hilbert-Schmidt inner product, defined by $\langle A, B\rangle = \text{Tr}[A^\dagger B]$. The induced norm by this inner product is then $\|A\|_2 = \sqrt{\text{Tr}|A|^2}$ and $\mathcal{L}(\mathcal{H})$ is complete in this (and any other) norm. Note that this norm differs from the operator norm $\|A\|_\infty$ introduced earlier. Equipping the space $\mathcal{L}(\mathcal{H})$ with the Hilbert-Schmidt inner product is common in quantum information theory.

So far two operator norms have been encountered. In the next section, a complete discussion on the relevant norms on $\mathcal{H}$ and on $\mathcal{L}(\mathcal{H})$ is given.

2.1.3. NORMS ON HILBERT SPACES AND INDUCED NORMS

In the finite-dimensional case, the Euclidean norm $\|\cdot\|_2$ on a Hilbert space $\mathcal{H}$ is a special case of the p-norms. In general, the p-norm on $\mathcal{H}$ is defined as follows.

Definition 2.1.9 (p-norm)**.** Let $\mathcal{H} = \mathbb{C}^d$ be a Hilbert space with an orthonormal basis $\{e_i : i = 1, ..., d\}$. Then, for any $p \in [1, \infty]$, the p-norm on $\mathcal{H}$ is defined by

$$\|x\|_p := (\sum_i |x_i|^p)^{1/p},$$

where $x = \sum_{i=1}^d x_i e_i$ is the expression of x in the given basis. Observe that

$$\|x\|_\infty = \lim_{p\to\infty} \|x\|_p = \max_i |x_i|.$$

All norms except $p = 2$ depend on the choice of basis $\{e_i\}$. □

The p-norms satisfy a monotonicity property, meaning that $\|x\|_p \leq \|x\|_q$ if $p \geq q$ for all $x \in \mathcal{H}$. There is an important inequality for p-norms that is known as Hölder's inequality.

Theorem 2.1.10 (Hölder's inequality)**.** *Let $x, y \in \mathbb{C}^d$ and $p, q \in [1,\infty]$ satisfying $p^{-1} + q^{-1} = 1$ (where $\infty^{-1} = 0$ is to be understood, i.e. $p = 1$ and $q = \infty$ satisfy the condition). Then*

$$\sum_{i=1}^{d} |x_i y_i| \leq \|x\|_p \|y\|_q. \tag{2.8}$$

Proof. See Theorem 31.3 of [20]. ■

Corollary.

$$|\langle x, y\rangle| = \left|\sum_{i=1}^{d} x_i^* y_i\right| \leq \sum_{i=1}^{d} |x_i y_i| \leq \|x\|_2 \|y\|_2, \tag{2.9}$$

for the special case $p = q = 2$, which is the Cauchy-Schwarz inequality of Theorem 2.1.1. Hölders inequality is therefore a generalization of Cauchy-Scharz.

Naturally, the p- and q-norms on $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively induce a norm on linear operators $A \in \mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$ in the following way.

Definition 2.1.10 (Induced pq-norm)**.** Let $\mathcal{H}_1$, $\mathcal{H}_2$ be Hilbert spaces equipped with a p-norm and q-norm respectively. Then these norms induce a norm on the linear operators $A \in \mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$ by

$$\|A\|_{p-q} = \sup_{x \in \mathcal{H}_1} \left\{ \|Ax\|_q : \|x\|_p \leq 1 \right\}. \qquad \square$$

However, this is not the only way a norm on $\mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$ can be defined. In view of $\mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$ being a Hilbert space in itself (with the Hilbert-Schmidt inner product $\langle A, B\rangle = \mathrm{Tr}[A^\dagger B]$), one can also equip the space with an Schatten p-norm, a generalization of the p-norm for the space $\mathbb{C}^d$. The Schatten p-norm is defined as follows.

Definition 2.1.11 (Schatten p-norm)**.** Let $A \in \mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$ be a linear operator and $p \in [1,\infty]$. Then the Schatten p-norm is defined by

$$\|A\|_p = \left(\mathrm{Tr}\left[|A|^p\right]\right)^{\frac{1}{p}} = \left(\mathrm{Tr}\left[(A^\dagger A)^{\frac{p}{2}}\right]\right)^{\frac{1}{p}} = \|s(A)\|_p = \left(\sum_i s_i(A)^p\right)^{\frac{1}{p}},$$

where $s(A)$ is the vector of singular values of A, with components $s_i(A)$. $\square$

The Hilbert-Schmidt norm (also referred to as the Frobenius norm) $\|A\|_2^2 = \langle A, A\rangle = \mathrm{Tr}[A^\dagger A]$ is precisely the Schatten 2-norm, whereas the operator norm (also referred to as the spectral norm) $\|A\|_\infty = \sup_{x \in \mathcal{H}} \{\|Ax\|_2 : \|x\|_2 \leq 1\}$ is the Schatten ∞-norm, which is why this notation was already adopted. Often, the trace norm is also encounters, which is the Schatten 1-norm, then defined as $\|A\|_1 = \mathrm{Tr}\,|A|$. The Schatten p-norm satisfies the following properties (for simplicity here only given for $\mathcal{L}(\mathcal{H})$, but with straightforward extention to $\mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$) [21]:

Proposition 2.1.11 (Schatten p-norm)**.** *Let $A, B \in \mathcal{L}(\mathcal{H})$, $U, V \in \mathcal{U}(\mathcal{H})$ and $p, q \in [1,\infty]$. The following properties then hold:*

(1) $\|UAV\|_p = \|A\|_p$ (Unitary invariance);

(2) If $p^{-1} + q^{-1} = 1$, then $\|AB\|_1 \leq \|A\|_p \|B\|_q$ (Hölder's inequality);

(3) $\|AB\|_p \leq \|A\|_p \|B\|_p$ (Sub-multiplicativity);

(4) If $p \geq q$, then $\|A\|_\infty \leq \|A\|_q \leq \|A\|_p \leq \|A\|_1$ (Monotonicity).

Proof. See [21]. ■

This concludes the subsection on norms in Hilbert spaces and norms on linear operators. The section on Hilbert spaces is concluded with a discussion of the tensor product, since it is widely used in quantum information theory.

2.1.4. THE TENSOR PRODUCT AND KRONECKER PRODUCT

The tensor product is an abstract concept that applies to general vector spaces. Although it is not the intention to capture the full and most general notion of the tensor product, some discussion may be useful since it is so frequently encountered in quantum information theory. Let V and W be vector spaces. Then their tensor product, denoted $V \otimes W$ is by definition a vector space build from the ordered pairs in the Cartesian product $V \times W$ that generalized the outer product of finite-dimensional vectors. The vectors in $V \otimes W$ are defined to be bilinear under the composition $\otimes$. This yields in the following definition.

Definition 2.1.12 (tensor product)**.** Let V, W be vector spaces. Then the space $V \otimes W$ is defined by

$$V \otimes W = \text{Span}\{v \otimes w | v \in V, w \in W\}, \tag{2.10}$$

where $\otimes : V \times W \mapsto V \otimes W$ is a bilinear map $(v, w) \mapsto v \otimes w$ defined by the following properties known as bilinearity:

$$\begin{aligned} (v_1 \otimes w) + (v_2 \otimes w) &= (v_1 + v_2) \otimes w \\ (v \otimes w_1) + (v \otimes w_2) &= v \otimes (w_1 + w_2) \\ c(v \otimes w) &= (cv) \otimes w = v \otimes (cw), \end{aligned} \tag{2.11}$$

for all $v, v_1, v_2 \in V$, all $w, w_1, w_2 \in W$ and $c \in \mathbb{C}$. □

This is, the most general vector space that can be build from $V \times W$, in the sense that only bilinearity is assumed and nothing else. If $\{v_i\}$ and $\{w_j\}$ are orthogonal bases for V and W respectively, then $\{v_i \otimes w_j\}$ forms a basis for $V \otimes W$. In particular if $\text{Dim}(V)$ and $\text{Dim}(W)$ are finite, then $\text{Dim}(V \otimes W) = \text{Dim}(V)\,\text{Dim}(W)$. The tensor product of linear operators on V are then easily defined by their action. If $A \in \mathcal{L}(V)$ and $B \in \mathcal{L}(W)$, then $A \otimes B \in \mathcal{L}(V \otimes W)$ is defined by $v \otimes w \mapsto A(v) \otimes B(w)$. Tensor products also concatenate in a straightforward way. If X is a third vector space, then $(V \otimes W) \otimes X$ is another tensor product. Technically, it is only isomorphic to $V \otimes (W \otimes X)$ due to the ordering, but the isomorphism is canonical and for simplicity the space is just written as $V \otimes W \otimes X$. This then warrants the tensor power notation $V^{\otimes n}$, for $n \in \mathbb{N}$, where n tensor products of V with itself are meant.

The Kronecker product is a matrix operation that corresponds to the general concept of the tensor product. In particular, if the vector spaces are all finite-dimensional, then the Kronecker product is just the tensor product expressed in a particular chosen basis. This applies to vectors in V (or its dual) as well as to linear operators on V. The Kronecker product is defined as follows.

Definition 2.1.13 (Kronecker product)**.** Let $A \in \mathbb{C}^{m \times n}$ and $B \in \mathbb{C}^{p \times q}$ be the matrix (or vector) representation of abstract vectors or linear operators over $\mathbb{C}$ with respect to a certain basis. The Kronecker product (also denoted $\otimes$) is then defined by

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix} \in \mathbb{C}^{mp \times nq}, \tag{2.12}$$

where $A \otimes B$ is the matrix representation of the abstract object $A \otimes B$ (tensor product) with respect to the tensor basis generated by the basis in which A and B were represented. □

Next a brief discussion is given about the relation between $\mathcal{L}(\mathcal{H})$, $\mathcal{H} \otimes \mathcal{H}^*$ and the trace. By no means this is complete, but it is useful to keep in mind later on, especially when the Dirac notation for quantum states is introduced. Let $x_1, x_2, ...x_n \in \mathcal{H}$ be an orthonormal basis. Then $\{x_i^\dagger\}_i$ is an orthonormal basis of $\mathcal{H}^*$ by going back and forth between $\mathcal{H}$ and $\mathcal{H}^*$ using Riesz representation theorem (Theorem 2.1.2) and by linearity of the inner product. Let $t : \mathcal{H} \otimes \mathcal{H}^* \to \mathbb{C}$ be the canonical linear functional defined by the mapping $x \otimes f \mapsto f(x)$. So $t(x \otimes f) = f(x)$. The spaces $\mathcal{L}(\mathcal{H})$ and $\mathcal{H} \otimes \mathcal{H}^*$ are then isomorphic by the following linear map $\alpha : \mathcal{L}(\mathcal{H}) \to \mathcal{H} \otimes \mathcal{H}^*$ given by

$$\alpha : A \mapsto \sum_{i,j} t(Ax_j \otimes x_i^\dagger)(x_i \otimes x_j^\dagger) = \sum_{i,j} x_i^\dagger(Ax_j) x_i \otimes x_j^\dagger = \sum_{i,j} \langle x_i, Ax_j \rangle \, x_i \otimes x_j^\dagger,$$

which together with linearity of α and bilinearity of $\otimes$ defines the map. Here $x_j^\dagger$ is the linear functional corresponding to $x_j \in \mathcal{H}$ by Riesz representation theorem. It is this isomorphism on which the Dirac notation is built. Its inverse is given by $\alpha^{-1} : \mathcal{H} \otimes \mathcal{H}^* \to \mathcal{L}(\mathcal{H})$ that maps

$$\alpha^{-1} : x \otimes f \mapsto t(x \otimes f) P_x = f(x) P_x,$$

where P_x is the orthogonal projection onto $\mathrm{Span}\{x\}$. Again α^{-1} is then defined by linearity. Now using these two maps, it is easily verified that for any $A \in \mathcal{L}(\mathcal{H})$ it holds that $\mathrm{Tr}[A] = t(\alpha(A))$. This definition is the way in which the basis free definition of the trace is formulated. Also, the isomorphism α is very often used implicitly.

2.2. INTRODUCTION INTO GROUP THEORY

This sections provides a brief and concise introduction into elementary group theory, requiring little to no prerequisite knowledge in the topic. In the spirit of the chapter, no examples are provided. The content is loosely based on ref. [24] and the reader who wishes a more extensive introduction in the topic is encouraged to consult this source. The logical point of departure is the definition of a group.

Definition 2.2.1 (Group)**.** A group is an ordered pair $(G, *)$ where G is a set and $* : G \times G \mapsto G$ is a binary operation on G that satisfies the following group axioms:

(i) $*$ is associative, i.e. $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$;

(ii) There exists an $e \in G$, called the identity on G, such that $a * e = e * a = a$ for all $a \in G$;

(iii) For each $a \in G$ there exists an element $a^{-1} \in G$, called the inverse of a, such that $a * a^{-1} = a^{-1} * a = e$.

A group is said to be Abelian if in addition to the above

(iv) the group is commutative, i.e. if $a * b = b * a$ for all $a, b \in G$.

Finally a group is called finite is the set G is finite. Generally G is informally called a group if the operation $*$ is understood from the context and the operation $*$ is omitted, writing $a * b$ just as ab. □

The identity element is unique since if e and e' are identities, then $e = ee' = e'$ by applying (ii) twice. The inverse of an element $a \in G$ is also unique. To see this, assume b and c are both inverses of a. Then $c = ce = c(ab) = (ca)b = eb = b$, by virtue of the group axioms. Define the order of a group $|G|$ as the number of elements in the underlying set, which may be infinite. The order of an element $a \in G$ is the smallest natural number n such that $a^n = e$ is the identity on G. If no such n exists, the

order of a is infinite. Finally a subset $H \subseteq G$ of G is called a subgroup of $(G, *)$ if $(H, *)$ is also a group and is denoted $H \leq G$. In particular this means that the operation $*$ restricted to $H \times H$ has an image in H, i.e. H is closed under multiplication. There is a proposition that makes it easier to verify when a subset is a subgroup.

Proposition 2.2.1 (Subgroup Criterion)**.** *Let $H \subseteq G$ be a subset of a group G. Then $H \leq G$ if and only if*

(1) $H \neq \emptyset$, and

(2) $\forall a, b \in H$, $ab^{-1} \in H$.

Proof. If $H \leq G$ then $e \in H$ so $H \neq \emptyset$ and also $b^{-1} \in H$ and therefore $ab^{-1} \in H$ by the group axioms. Conversely, suppose that H satisfies (1) and (2). First note that the associativity of the operation is directly inherited from G. Now pick a $x \in H$ (which exists by (1)) and apply (2) using $a = b = x$ to find $xx^{-1} = e \in H$. Then apply (2) using $a = e$ and $b = x$ to find that $ex^{-1} = x^{-1} \in H$. Finally pick $x, y \in H$. By what was just proved, $y^{-1} \in H$ and apply (2) to $a = x$ and $b = y^{-1}$ to obtain that $x(y^{-1})^{-1} = xy \in H$, so H is closed under multiplication. ■

Subgroups can be defined in terms of a generating set, a subset of a group. Suppose $S \subset G$ is a subset of G and let $S^{-1} := \{s^{-1} : s \in S\}$. Then the subgroup generated by S, denoted $\langle S \rangle$, is defined as the set of finitely many products of elements from $S \cup S^{-1}$. Clearly $e \in \langle S \rangle$, since e is by definition the empty product. Furthermore, if $s, t \in \langle S \rangle$, then also $st^{-1} \in \langle S \rangle$ and by Proposition 2.2.1 $\langle S \rangle \leq G$. In fact, it is the smallest subgroup containing S. To see this, let $S \subset H \leq G$. Then $S^{-1} \subset H$ by group axiom (iii), and $S \cup S^{-1} \subset H$ implies $\langle S \rangle \subset H$, since H must be closed under the multiplication.

It is natural to consider maps between groups next, in particular maps that respect the group operations. Such maps are referred to as group homomorphisms and isomorphisms, and are defined as follows:

Definition 2.2.2 (Homomorphism, isomorphism of groups)**.** Let $(G_1, *)$ and $(G_2, \diamond)$ be two groups. A map $f : G_1 \to G_2$ is called a homomorphism if it satisfies $f(a * b) = f(a) \diamond f(b)$ for all $a, b \in G_1$. If in addition f is a bijection, then it is called a isomorphism. When there exists an isomorphism between G_1 and G_2, the groups are called isomorphic, denoted $G_1 \cong G_2$. □

The kernel of a homomorphism $f : G_1 \to G_2$ is defined as $\mathrm{Ker}(f) := \{x \in G_1 : f(x) = e_2\}$, where e_2 is the identity on G_2, and the range is defined as $\mathrm{Rge}(f) := \{f(g) : g \in G_1\}$. The following proposition states useful properties of homomorphisms.

Proposition 2.2.2. *Let $f : G_1 \to G_2$ be a homomorphism. Also let e_1 and e_2 denote the identity elements in G_1 and G_2 respectively. Then*

(1) f is injective $\Leftrightarrow \mathrm{Ker}(f) = \{e_1\}$;

(2) $f(e_1) = e_2$;

(3) $f(g^{-1}) = f(g)^{-1}$ for all $g \in G_1$;

(4) $\mathrm{Ker}(f) \leq G_1$;

(5) $\mathrm{Rge}(f) \leq G_2$.

Proof.

(1) For $a, b \in G_1$: $f(a) = f(b) \Leftrightarrow f(a)^{-1} f(b) = e_2 \Leftrightarrow f(a^{-1}b) = e_2 \Leftrightarrow a^{-1}b \in \mathrm{Ker}(f)$. So if f is injective then $f(a) = f(b)$ implies $a = b$ and therefore $a^{-1}b = e_1$ can be the only element in

Ker(f). Conversely if Ker(f) = $\{e_1\}$ then $a = b$ and by the stated relation it follows that $f(a) = f(b) \Rightarrow a = b$, i.e. f is injective.

(2) $f(e_1) = f(e_1e_1) = f(e_1)f(e_1)$, so $f(e_1) = e_2$.

(3) $e_2 = f(e_1) = f(g^{-1}g) = f(g^{-1})f(g)$, so $f(g)^{-1} = f(g^{-1})$.

(4) Clearly Ker(f) $\subseteq G_1$ by definition and Ker(f) $\neq \emptyset$ by (2). Let $a, b \in$ Ker(f), i.e. $f(a) = f(b) = e_2$. Then $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e_2e_2^{-1} = e_2$, making use of (3). So $ab^{-1} \in$ Ker(f). By Proposition 2.2.1 then Ker(f) $\leq G_1$.

(5) Clearly Rge(f) $\subseteq G_2$ by definition and Ker(f) $\neq \emptyset$ by (2). Let $a, b \in$ Rge(f), i.e. there exists $x, y \in G_1$ such that $f(x) = a$ and $f(y) = b$. Then $b^{-1} = f(y)^{-1} = f(y^{-1})$ by (3) and $ab^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$ so since $xy^{-1} \in G$ this shows that $ab^{-1} \in$ Rge(f). By Proposition 2.2.1 then Rge(f) $\leq G_2$. ■

Cayley's Theorem is an important characterization of finite groups in terms of subgroups of the permutation group. The permutation group (or symmetric group) S_n is the group of all bijections of a set of n elements to itself with composition as its operation, and therefore has $n!$ elements.

Theorem 2.2.3 (Cayley's Theorem)**.** *Let G be a finite group. Then G is isomorphic with a subgroup of S_n, where $n = |G|$.*

Proof. Consider the left multiplication $\lambda_g : G \to G$ given by $\lambda_g(a) = ga$ for all $a \in G$. This mapping is, for any g, a bijection from G to itself, since $ga = x$ has one and only one solution in G, namely $a = g^{-1}x$. That is to say, $(\lambda_g)^{-1} = \lambda_{g^{-1}}$. Therefore $\lambda_g \in S_n$, with $n = |G|$. Now let $K = \{\lambda_g : g \in G\} \subset S_n$ and consider the mapping $T : G \to K$ given by $g \mapsto \lambda_g$. Now T is a homomorphism, since $\lambda_g \circ \lambda_h(a) = \lambda_g(ha) = g(ha) = (gh)a = \lambda_{gh}(a)$. Furthermore T is injective, because if $\lambda_g = \lambda_h$ then $ga = ha$ for all $a \in G$ and thus $g = h$. By construction T is surjective onto K and hence $G \cong K$. ■

An important result from this theorem and its proof is that left (and right) multiplications are bijections, a result that is useful in many settings. Next the concept of cosets, normal subgroups and quotient groups are presented and connected with the notion of homomorphisms and isomorphisms.

Definition 2.2.3 (cosets)**.** Let $H \leq G$. Then for any $g \in G$ the sets $gH = \{gh : h \in H\}$ and $Hg = \{hg : h \in H\}$ are called a left coset and right coset of H in G respectively. Any element (in particular g) of a coset is called a representative of the coset. Denote G/H ($G\backslash H$) the set of all different left (right) cosets of H in G. □

The left (right) cosets of H in G are the equivalence classes of the equivalence relation $a \equiv b$ if $a^{-1}b \in H$ ($ab^{-1} \in H$) for all $a, b \in G$. The fact that this is an equivalence relation follows from the group properties of H. Therefore the sets aH and bH (similarly for Ha and Hb) are equal if $a \equiv b$ and otherwise disjoint but of equal size due to Cayley's Theorem, stating that the left multiplication with g is a bijection from H to gH. The size of G is related to the size of H by Lagrange's Theorem

Theorem 2.2.4 (Lagrange's Theorem)**.** *Let $H \leq G$. Then $|G| = |G/H||H|$.*

Proof. Every coset of H in G is disjoint and of equal number of elements $|H|$ (since $eH = H$ has $|H|$ elements). Every element $g \in G$ is in one and only one coset gH and therefore G is the disjoint union of all different cosets from which the result follows. ■

Corollary. *The order of a subgroup of a finite group divides the order of that group.* ■

In general aH and Ha are different sets, unless H is a normal subgroup.

Definition 2.2.4 (Normal subgroup)**.** Let $H \leq G$. Then H is called a normal subgroup if $gH = Hg$ for all $g \in G$. Equivalently, H is normal if $gHg^{-1} := \{ghg^{-1} : h \in H\} = H$ for all $g \in G$. Normal subgroups are denoted $H \lhd G$. □

From the definition it is clear that each subgroup of an Abellian group is normal, however in regular (even finite) groups most subgroups need not be normal. Normal subgroups are important because of the following theorems.

Theorem 2.2.5. *Let $N \leq G$. Then the following are equivalent:*

(1) there exists a homomorphism $f : G \to G'$ with $\mathrm{Ker}(f) = N$*;*

(2) $N \lhd G$;

(3) G/N is a group with the operation defined by $aN \cdot bN := abN$;

Proof. (1) ⇒ (2): For all $h \in \mathrm{Ker}(f) = N$ and $g \in G$ it follows that

$$f(ghg^{-1}) = f(g)e'f(g^{-1}) = f(g)e'f(g)^{-1} = e'$$

and therefore $ghg^{-1} \in \mathrm{Ker}(f)$. This implies $gNg^{-1} \subseteq N$. Since left and right multiplication are bijections, so is conjugation, i.e. the map $T_g : N \to gNg^{-1}$ given by $T_g(n) = gng^{-1}$ for $n \in N$ is a bijection. Therefore $|gNg^{-1}| = |N|$ and since $gNg^{-1} \subseteq N$ this implies $gNg^{-1} = N$.
(2) ⇒ (3): The first thing is checking that the operation is well-defined. That is, if $aN = a'N$ and $bN = b'N$ it must hold that $(ab)N = (a'b')N$. From the assumptions it follows that $a' = an_1$ and $b' = bn_2$ for some $n_1, n_2 \in N$. Then

$$a'b'N = an_1bn_2N = a(bb^{-1})n_1bn_2N = ab(b^{-1}n_1b)n_2N = abN,$$

since $b^{-1}n_1b \in N$ by normality of N, making the operation well-defined. The group axioms are inherited from G. For any $a, b, c \in G$ and identity $e \in G$ it follows that the three group axioms are satisfied:

(i): $aN(bNcN) = aN(bcN) = a(bc)N = (ab)cN = (abN)cN = (aNbN)(cN)$;

(ii): $eNaN = eaN = aN = aeN = aNeN$, so $eN = N$ is the identity in G/N;

(iii): $a^{-1}NaN = a^{-1}aN = N = aa^{-1}N = eN = aNa^{-1}N$, so $a^{-1}N$ is the inverse of aN in G/N.

(3) ⇒ (1): Let $f : G \to G/N$ be defined by $g \mapsto gN$ for all $g \in G$. Then $f(ab) = abN = aNbN = f(a)f(b)$ for all $a, b \in G$, showing that f is a homomorphism. Its kernel is then

$$\mathrm{Ker}(f) = \{g \in G : f(g) = eN\} = \{g \in G : gN = eN\} = \{g \in G : g \in N\} = N,$$

and therefore f is an explicit construction of a homomorphism from G to G/N with kernel N. ■

In the case that G/N is a group it is called the quotient group. Strictly speaking it is a group of which each element is a coset. But since all cosets are disjoint, each coset is uniquely identified by a representative. Therefore the group G/N can be viewed as a (non-unique) group of representatives in G of the different cosets. The final result presented here is the isomorphism theorem, which connects the kernel and the range of a homomorphism.

Theorem 2.2.6 (Isomorphism Theorem)**.** *Let $f : G \to G'$ be a homomorphism with $N := \mathrm{Ker}(f)$. Then $G/N \cong \mathrm{Rge}(f)$ by the isomorphism $\varphi : G/N \to \mathrm{Rge}(f)$ defined by $gN \mapsto f(g)$.*

Proof. $G/\operatorname{Ker}(f)$ is a group by Theorem 2.2.5 and $\operatorname{Rge}(f)$ is a group by Proposition 2.2.2. φ is well-defined, in the sense that the image of a coset gN does not depend on its representative g. To see this, take $a, b \in G$. Then

$$f(a) = f(b) \Leftrightarrow f(a)^{-1}f(b) = e' \Leftrightarrow f(a^{-1}b) = e' \Leftrightarrow a^{-1}b \in N \Leftrightarrow b \in aN \Leftrightarrow aN = bN,$$

so each representative of a coset has the same image. Because $f(a) = f(b)$ if and only if $aN = bN$, it is also clear that each different coset in G/N is mapped to a different point in $\operatorname{Rge}(f)$, making φ a bijection. It remains to show that φ is a homomorphism, a property that it inherits from f:

$$\varphi(aNbN) = \varphi(abN) = f(ab) = f(a)f(b) = \varphi(aN)\varphi(bN),$$

making φ an isomorphism between G/N and $\operatorname{Rge}(f)$. ■

So far, most of the theory discussed has been focused on the left (or right) regular action of a group G on itself or on a subgroup $H \leq G$. This action was used to define left (or right) cosets and it has been discussed that the left (or right) cosets of H in G are equivalence classes and therefore partition the group G. Whenever $gH = Hg$ for all g the subgroup H was defined to be normal. Now our focus is turned to the conjugation action of G on itself, defined by the map $g \mapsto hgh^{-1}$ for some fixed $h \in G$. This action gives rise to the following definitions.

Definition 2.2.5 (Conjugacy classes)**.** Let G be a group. Then the conjugacy classes of G are the sets $\sigma_G(g) := \{hgh^{-1} : h \in G\}$ for all $g \in G$. It contains all elements that commute with g. Any element (in particular g) is called a representative of $\sigma_G(g)$. □

Again, the conjugation classes are equivalence classes of the equivalence relation $g \cong h$ if $hgh^{-1} = g$. Hence the conjugation classes are disjoint subsets of G and can uniquely be identified by a representative. Next the normalizer and centralizer of sets are defined.

Definition 2.2.6 (Normalizer and centralizer)**.** Let $S \subseteq G$ be a subset of a group G. Then the normalizer is defined as $N_G(S) := \{g \in G : gSg^{-1} = S\}$ and the centralizer is defined as $C_G(S) := \{g \in G : gsg^{-1} = s, \quad \forall s \in S\}$. □

The next proposition states some subgroup inclusions about the normalizer and centralizer.

Proposition 2.2.7. *Let $H \leq G$ and $S \subseteq G$. Then*

1. *$N_G(S) \leq G$, $C_G(S) \leq G$ and $C_G(S) \triangleleft N_G(S)$.*
2. *$H \triangleleft N_G(H)$.*

Proof. (1) First observe that $e \in N_G(S)$ and $e \in C_G(S)$ since all elements commute with the identity. For $a, b \in N_G(S)$ then it follows that $(ab^{-1})S(ab^{-1})^{-1} = ab^{-1}Sba^{-1} = aSa^{-1} = S$, so $ab^{-1} \in N_G(S)$. By Proposition 2.2.1 then $N_G(S) \leq G$. Similarly for $a, b \in C_G(S)$, $ab^{-1}sba^{-1} = asa^{-1} = s$ for all $s \in S$ so $ab^{-1} \in C_G(H)$ and again by the proposition $C_G(S) \leq G$. From the definition it is clear that $C_G(S) \subseteq N_G(S)$, and since both are subgroups of G then $C_G(S) \leq N_G(S)$. But $gC_G(S)g^{-1} = C_G(S)$ for all $g \in N_G(S)$. To see this pick any $g \in N_G(S)$ and $h \in C_G(S)$. Then by definition of $N_G(S)$ it follows that for all $s \in S$ there exists a $t \in S$ such that $gtg^{-1} = s$, and therefore $(ghg^{-1})s(ghg^{-1})^{-1} = ghg^{-1}sgh^{-1}g^{-1} = ghth^{-1}g^{-1} = gtg^{-1} = s$ for all $s \in S$, so $ghg^{-1} \in C_G(S)$ for all $h \in C_G(S)$ and all $g \in N_G(S)$. The conclusion $C_G(S) \triangleleft N_G(S)$ follows.
(2) Since $H \leq G$, H is a group. Furthermore $H \subseteq N_G(H)$ since $gHg^{-1} = H$ for all $g \in H$. So $H \leq N_G(H)$. But $gHg^{-1} = H$ for all $g \in N_G(H)$ by definition so $H \triangleleft N_G(H)$. ■

Finally the definition of group algebra is given, which connects the concept of an algebra to the concept of a group. It generates a vector space over a finite group that inherits the bilinear form (the group product) from the group, making it an associative algebra with unit.

Definition 2.2.7 (Group algebra)**.** Let $G = \{g_1, ..., g_n\}$ be a finite group. The group algebra $\mathbb{C}[G]$ is then defined as $\mathbb{C}[G] := \{c_1 g_1 + \cdots + c_n g_n : c_i \in \mathbb{C} \text{ for all } i\}$, where the bilinear product is inherited from G by letting $g_i g_j = g_k$ in $\mathbb{C}[G]$ if $g_i g_j = g_k$ in G with its linear extension. □

2.3. REPRESENTATION THEORY OF FINITE GROUPS

This section provides the reader with basic notions of representation theory of finite groups, continues with the most important theorems and concludes with a section on characters. This section is by no means a complete review, but aims to introduce the necessary concepts for this thesis to a reader that is unfamiliar with the subject. Throughout this section a group G is considered to be finite and representations are assumed to be on finite-dimensional vector spaces over the complex numbers $\mathbb{C}$, unless explicitly stated otherwise. Some results may be presented in a more general way, but for the purpose of its application in this thesis, the attention is restricted to finite-dimensional vector spaces over $\mathbb{C}$. The contents of this section are roughly based on [25, 26]

2.3.1. DEFINITIONS AND GENERAL FRAMEWORK

The natural point of departure is the definition of a formal representation.

Definition 2.3.1 (representation)**.** A representation of a group G is a pair (V, R) where V is a vector space and $R : G \to \mathcal{GL}(V) = \mathrm{Aut}(V)$ is a group homomorphism, i.e. $R(g)R(h) = R(gh)$ for all $g, h \in G$. If in addition the space V is equipped with an inner product and $R(g)$ is a unitary operator for all $g \in G$ with respect to the inner product on V, then the representation (V, R) is said to be a unitary representation. If R is injective, then the representation is said to be faithful. □

The space V is said to carry the representation of G. Each $g \in G$ defines a linear operator on V that can act on an element $v \in V$. When there is no confusion about the homomorphism R, an operator $R(g)$ is usually denoted as just g, i.e. $R(g)v = gv$, and V is referred to as the representation of G. For any representation (V, R) of G, it holds that $R(e) = I$ where e is the identity in G and I is the identity on V by Proposition 2.2.2. Furthermore, since $g \in G$ has a unique inverse $g^{-1} \in G$, so does $R(g)$ in $\mathcal{L}(V)$: $I = R(e) = R(gg^{-1}) = R(g^{-1}g) = R(g)R(g^{-1}) = R(g^{-1})R(g)$. Therefore $R(g^{-1}) = R(g)^{-1}$. Finally (V, R) is a unitary representation of G if and only if $R(g^{-1}) = R(g)^{-1} = R(g)^\dagger$ for all $g \in G$ by Proposition 2.1.3.

Each group has a trivial representation on every vector space V, corresponding to the homomorphism that maps each element of G to the identity I on V. Each group G also has a (left) regular representation: $V = \mathbb{C}[G]$ and $R : G \to \mathcal{L}(\mathbb{C}[G])$ defined by $R(g)(\sum_i c_i g_i) = \sum_i c_i (g g_i)$, where $c_i \in \mathbb{C}$ and $g, g_i \in G$. The action of $R(g)$ is thus fully determined by the left regular action (or left multiplication) $\lambda_g : h \mapsto gh$ on G.

Any representation (V, R_V) of G has a dual representation (V^*, R_{V^*}) on the dual space V^*. Note that since dual vectors are represented by row vectors, the representation acts via matrix multiplication from the right. By Riesz representation theorem (Theorem 2.1.2), there is a unique one-to-one correspondence between elements $v \in V$ and $v^\dagger \in V^*$ via the inner product on V. The relation between the two representations is that they respect the natural paring of Riesz representation theorem. That is for any $u^\dagger \in V^*$ and $v \in V$, it is required that

$$\langle u, v \rangle = u^\dagger v = (u^\dagger R_{V^*}(g))(R_V(g)v) = \langle R_{V^*}(g)^\dagger u, R_V(g)v \rangle , \tag{2.13}$$

for all $g \in G$. This then defines $R_{V^*}(g)R_V(g) = I$ or equivalently $R_{V^*}(g) := R_V(g)^{-1} = R_V(g^{-1})$.

Our next definition regards subrepresentations and defines the term irreducible representation.

Definition 2.3.2 (subrepresentation, irreducible representation)**.** Let (V, R) be a representation of a group G. Then a subrepresentation of G is a subspace $W \subseteq V$ which is invariant under the operators $R(g)$, for all $g \in G$, meaning that $R(g)w \in W$ for all $w \in W$, $g \in G$. $W = 0$ and $W = V$ are always subrepresentations. The representation V is said to be irreducible (sometimes called simple) if these are the only subrepresentations of V. □

Note that any one-dimensional representation is automatically irreducible. It is also natural to consider mappings between representations of a single group. Again of particular interest are the mappings that preserve the action of $g \in G$. The next definition makes this notion precise.

Definition 2.3.3 (Homomorphism of representations)**.** Let V_1, V_2 be two representations of a group G. Then a homomorphism of representations (also called intertwining operator or G-linear map) $\phi : V_1 \to V_2$ is a linear map such that $\phi(gv) = g\phi(v)$ for all $g \in G$ and $v \in V_1$. One says that ϕ is an isomorphism of representation if in addition to being a homomorphism of representation it is also an isomorphism of vector spaces, i.e. if ϕ is a linear bijection between the vector spaces V_1 and V_2. If such an isomorphism exists, V_1 and V_2 are said to be equivalent representations (sometimes also called isomorphic representations), denoted $V_1 \cong V_2$. □

More explicitly, if the representations are (V_1, R_1) and (V_2, R_2), then a map $\phi : V_1 \to V_2$ is a homomorphism of representations if $\phi R_1(g) = R_2(g)\phi$ for all $g \in G$. In other words, the diagram of Figure 2.1 commutes for any $g \in G$.

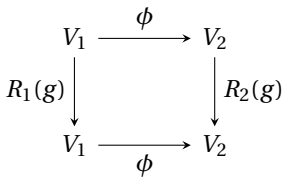

Figure 2.1: Commutative diagram for a homomorphism of representations ϕ.

Similarly to group homomorphisms, the kernel and range of a homomorphism of representations are subrepresentations.

Proposition 2.3.1. *Let V_1 and V_2 be representations of a group G and $\phi : V_1 \to V_2$ be a homomorphism of representations. Then* $\mathrm{Ker}(\phi)$ *is a subrepresentation of V_1 and* $\mathrm{Rge}(\phi)$ *is a subrepresentation of V_2.*

Proof. Let $v \in \mathrm{Ker}(\phi)$ and $g \in G$, then $\phi(gv) = g\phi(v) = 0$. So $gv \in \mathrm{Ker}(\phi)$. Therefore $\mathrm{Ker}(\phi)$ is a subrepresentation of V_1. Similarly, let $v \in V_1$. Then also $gv \in V_1$ and hence $\phi(v), \phi(gv) \in \mathrm{Rge}(\phi)$. Now $g\phi(v) = \phi(gv) \in \mathrm{Rge}(\phi)$, making $\mathrm{Rge}(\phi)$ a subrepresentation of V_2. ■

Our next definition extends the direct sum of vector spaces and defines the direct sum of representations.

Definition 2.3.4 (direct sum and tensor product representations)**.** Let (V_1, R_1) and (V_2, R_2) be two representations of a group G. Then $V_1 \oplus V_2$ has the structure of a representation, defined by $(R_1 \oplus R_2)(g) := R_1(g) \oplus R_2(g)$ for all $g \in G$. Similarly $V_1 \otimes V_2$ is a representation via the identification $(R_1 \otimes R_2)(g) := R_1(g) \otimes R_2(g)$ for all $g \in G$. □

Definition 2.3.5 (indecomposable)**.** A nonzero representation $V \neq 0$ is said to be indecomposable if it is not isomorphic to a direct sum of two nonzero representations. □

It is clear that any irreducible representation is indecomposable. On the other hand, it is not immediately clear that indecomposable representations are irreducible. In fact, it is an important theorem that this holds for finite group representations. For general representations of associative algebras, this does not hold. For an example of an indecomposable and reducible representation of an associative algebra, see [26]. When indecomposable also implies irreducible, the representation is called completely reducible, as formalized in the following definition:

Definition 2.3.6 (completely reducible representation)**.** A representation V is said to be completely reducible (also called semisimple) if it is the direct sum of irreducible representations. □

The important result, stated in the next section, is then that every representation of a finite group is completely reducible. That means that knowing all the (inequivalent) irreducible representations of a group, provides all the information there is on any representation of that group. Typical problems in representation theory therefore include classifying the irreducible representations of a given group (which may be very hard to do) or at least finding the irreducible subrepresentations of a particular representation.

2.3.2. RESULTS FOR FINITE GROUP REPRESENTATIONS

This section provides some essential results for finite dimensional representations of finite groups. The first theorem is an important characterization of group representations. It says that every group representation is completely reducible. Equivalently, every indecomposable representation of a group is irreducible. In order to prove this theorem, a small lemma is first required.

Lemma 2.3.2 (Finite-dimensional group representation can be chosen unitary)**.** *Let (V,R) be a finite-dimensional group representation. Then there exists an inner product on V such that $R(g)$ is unitary for all $g \in G$.*

Proof. Let $\langle\cdot,\cdot\rangle$ be an arbitrary inner product on V. For $x, y \in V$ define the inner product

$$\langle x, y\rangle_* := \frac{1}{|G|}\sum_{g\in G}\langle R(g)x, R(g)y\rangle\,. \tag{2.14}$$

Then for all $h \in G$ and $x, y \in V$ it follows that

$$\begin{aligned}\langle R(h)x, R(h)y\rangle_* &= \frac{1}{|G|}\sum_{g\in G}\langle R(h)R(g)x, R(h)R(g)y\rangle = \frac{1}{|G|}\sum_{g\in G}\langle R(hg)x, R(hg)y\rangle \\ &= \frac{1}{|G|}\sum_{a\in G}\langle R(a)x, R(a)y\rangle = \langle x, y\rangle_*\,,\end{aligned} \tag{2.15}$$

where in the last step the change of variables $a = hg$ is used by Cayley's Theorem, Theorem 2.2.3. By Proposition 2.1.3 then $R(h)$ is unitary with respect to the inner product $\langle\cdot,\cdot\rangle_*$. ■

Theorem 2.3.3 (Maschke's Theorem)**.** *Every finite dimensional representation (over $\mathbb{C}$) of a finite dimensional group is completely reducible.*

Proof. Let G be a finite group and (V,R) be its n-dimensional group representation. By Lemma 2.3.2, V can be equipped with an inner product such that R is unitary. If V is irreducible, the statement trivially holds. Therefore suppose $W \subset V$ is a proper subrepresentation of G (of dimension $0 < m < n$), i.e. $R(g)w \in W$ for all $w \in W$ and all $g \in G$. Then $W^\perp$ is also a subrepresentation (of dimension

$n-m$), since for all $g \in G$, $x \in W$ and $y \in W^{\perp}$ one has

$$\langle x, R(g)y\rangle = \langle R(g)^{\dagger}x, y\rangle = \langle R(g^{-1})x, y\rangle = 0. \tag{2.16}$$

The subrepresentations W and $W^{\perp}$ need not be irreducible at this point, but since their dimensions are strictly smaller than n, the above procedure can be repeated on W and $W^{\perp}$ to eventually decompose V into the direct sum of irreducible representations. The procedure ends after finite steps since each time the dimension strictly reduces and a sub-representation of dimension 1 is always irreducible.

■

Corollary. *Let (V,R) be a finite-dimensional, nonzero representation of a finite group G. Then (V,R) decomposes uniquely (up to isomorphisms and ordering) as*

$$V = \bigoplus_{i=1}^{k}\left(\mathbb{C}^{n_i}\otimes V_i\right) = \bigoplus_{i=1}^{k} V_i^{\oplus n_i} \qquad \text{and} \qquad R = \bigoplus_{i=1}^{k}\left(I_{n_i}\otimes R_i\right) = \bigoplus_{i=1}^{k} R_i^{\oplus n_i}, \tag{2.17}$$

where the set $\{(V_i,R_i) : i = 1,...,k\}$ contains mutually inequivalent, nonzero, irreducible representations occurring with multiplicity n_i in the decomposition of (V,R) and I_{n_i} is the identity on a n_i-dimensional vector space.

Proof. See Proposition 1.8 of [25]. ■

Note that the Maschke's Theorem (Theorem 2.3.3) is false over $\mathbb{R}$ and therefore it is crucial that the representation is over $\mathbb{C}$. The uniqueness of the above decomposition makes use of Schur's Lemma, one of the most fundamental results from representation theory. It is applicable to many different problems. Here Schur's Lemma is presented in a general form. In later chapters, a particular form suitable for the thesis is presented.

Theorem 2.3.4 (Schur's Lemma)**.** *Let V_1 and V_2 be representations of a group G and let $\phi : V_1 \to V_2$ be a nonzero homomorphism of representations (intertwining operator). Then*

(1) if V_1 is irreducible, ϕ is injective;

(2) if V_2 is irreducible, ϕ is surjective.

Thus, if both V_1 and V_2 are irreducible, then ϕ is an isomorphism.

Proof.

(1) $\mathrm{Ker}(\phi)$ is a subrepresentation of V_1 by Proposition 2.3.1. Since $\phi \neq 0$, $\mathrm{Ker}(\phi) \neq V_1$. So if V_1 is irreducible, then $\mathrm{Ker}(\phi) = 0$ is the only possible subrepresentation and if $\mathrm{Ker}(\phi) = 0$ then ϕ is injective. To see this, take $v, w \in V_1$ such that $\phi(v) = \phi(w)$, then $0 = \phi(v) - \phi(w) = \phi(v-w)$, so $v - w \in \mathrm{Ker}(\phi)$. Since $\mathrm{Ker}(\phi) = 0$, $v - w = 0$ and so $v = w$.

(2) $\mathrm{Rge}(\phi)$ is a subrepresentation of V_2 by Proposition 2.3.1. Since $\phi \neq 0$, $\mathrm{Rge}(\phi) \neq 0$. So if V_2 is irreducible, then $\mathrm{Rge}(\phi) = V_2$ is the only possible subrepresentation and thus ϕ is surjective.

■

Corollary. *Let V be a finite dimensional, irreducible representation of a group G and $\phi : V \to V$ be a homomorphism of representations. Then $\phi = \lambda I$ for some $\lambda \in \mathbb{C}$, where I is the identity on V.*

Proof. Let λ be an eigenvalue of ϕ (possibly 0), which exists since $\mathbb{C}$ is algebraically closed. Then $\phi - \lambda I$ is a homomorphism of representations (because every operator commutes with the identity)

that is not a bijection, since the eigenvector belonging to eigenvalue λ is in $\text{Ker}[\phi - \lambda I]$. By Schur's Lemma then $\phi - \lambda I = 0$, proving the result. ■

Corollary. *Let V_1 and V_2 be finite-dimensional, irreducible representations of a group G, and $\phi : V_1 \to V_2$ be a homomorphism of representations. Then all homomorphisms of representations between V_1 and V_2 are of the form $\lambda\phi$, for some nonzero $\lambda \in \mathbb{C}\backslash\{0\}$. That is,*

$$\text{Dim}(\text{Hom}(V_1, V_2)_G) := \text{Dim}(\{\phi : V_1 \to V_2 | \phi g = g\phi \; \forall g \in G\}) = \begin{cases} 1 & \text{if } V_1 \cong V_2 \\ 0 & \text{if } V_1 \ncong V_2 \end{cases}.$$

Proof. By Schur's Lemma, if V_1 and V_2 are irreducuble, then ϕ must be an isomorphism of representations or $\phi = 0$. So if $V_1 \ncong V_2$ then the only homomorphism of representations is $\phi = 0$ so then $\text{Dim}(\text{Hom}(V_1, V_2)_G) = 0$. On the other hand, if $V_1 \cong V_2$ then all homomorphisms of representations must in fact be isomorphisms of representations, and at least one exists since $V_1 \cong V_2$. Let $\phi_1, \phi_2 : V_1 \to V_2$ be isomorphisms of representations. Then $\phi_1 \circ \phi_2^{-1} : V_1 \to V_1$ is an isomorphism of representations from V_1 to itself. By the above corollary then $\phi_1 \circ \phi_2^{-1} = \lambda I$, so that $\phi_1 = \lambda\phi_2$, where $\lambda \neq 0$. ■

Corollary. *Let (V, R) be a nonzero, irreducible representation of an Abelian group G. Then* $\text{Dim}(V) = 1$.

Proof. For any $g \in G$, $R(g) : V \to V$ is an homomorphism of representations, since for $g, h \in G$ and $v \in V$

$$R(g)R(h)v = R(gh)v = R(hg)v = R(h)R(g)v, \tag{2.18}$$

making use of the commutativity of G in the second equality. Then by the above corollary $R(g) = \lambda_g I$. Hence every subspace of V is a subrepresentation. But since V is irreducible, 0 and V are the only subrepresentations. Because $V \neq 0$ it must be that $\text{Dim}(V) = 1$. ■

Finally, the projection formula onto the trivial subrepresentations that occur in the decomposition of any representation into irreducible ones is given. This projection formula is simple, elegant and a powerful tool to classify the trivial representations contained in the decomposition of any representation. It is a building block for character theory (discussed in the next subsection), although the proofs are omitted for brevity. This projection formula can be generalized to a projection onto the all copies of any specific irreducible subrepresentation contained in the decomposition of an arbitrary representation. For details, see [25].

Let (V, R) be a representation of G and define $V^G := \{v \in V : R(g)v = v, \; \forall g \in G\}$ to be the subspace of V on which G acts trivially. Note that V^G need not be irreducible, in fact $V^G = V_{tr}^{\oplus n_{tr}}$ is the direct sum of n_{tr} trivial irreducible representations, where n_{tr} is the number of occurrences of the trivial representation in the representation V. The following lemma gives a projection of V onto V^G.

Lemma 2.3.5 (Projection onto trivial subrepresentations)**.** *Let (V, R) be any representation of a group G and let V^G denote the subspace on which G acts trivially. Define the map $\phi : V \to V$ by*

$$\phi = \frac{1}{|G|} \sum_{g \in G} R(g). \tag{2.19}$$

Then ϕ is a homomorphism of representations and moreover ϕ is the orthogonal projection of V onto V^G.

Proof. To show that ϕ is a homomorphism of representations, consider

$$\phi R(h) = \frac{1}{|G|} \sum_{g \in G} R(g)R(h) = \frac{1}{|G|} \sum_{g \in G} R(gh) = \frac{1}{|G|} \sum_{k \in G} R(hk) = R(h)\phi, \tag{2.20}$$

where the change of variables $k = h^{-1}gh$ is used since conjugation is a group isomorphism from G to itself. Now consider an arbitrary $w \in V$ and $h \in G$, and let $v = \phi(w)$. Then

$$R(h)v = \frac{1}{|G|}\sum_{g\in G} R(h)R(g)w = \frac{1}{|G|}\sum_{g\in G} R(hg)w = \frac{1}{|G|}\sum_{k\in G} R(k)w = v, \tag{2.21}$$

so $v \in V^G$. Therefore $\mathrm{Rge}(\phi) \subseteq V^G$. Next, consider any $v \in V^G$. Then

$$\phi(v) = \frac{1}{|G|}\sum_{g\in G} R(g)v = \frac{1}{|G|}\sum_{g\in G} v = v, \tag{2.22}$$

by definition of V^G. Therefore $\phi^2 = \phi$. The projection is orthogonal with respect to any inner product on V in which the representation (V, R) is unitary (which always exists by Lemma 2.3.2), since

$$\phi^\dagger = \frac{1}{|G|}\sum_{g\in G} R(g)^\dagger = \frac{1}{|G|}\sum_{g\in G} R(g^{-1}) = \frac{1}{|G|}\sum_{h\in G} R(h) = \phi. \qquad \blacksquare$$

2.3.3. CHARACTER THEORY

Character theory is an essential tool for classifying the representations of finite groups. It provides a simple and straightforward way to determine if a representation is irreducible or whether it is equivalent to some other representation. Furthermore it has a nice structure with respect to direct sums and tensor products, meaning that it is enough to study the characters of irreducible representations. A character is a function from the group G to the complex numbers, defined as follows:

Definition 2.3.7 (Character)**.** Let (V, R) be a finite-dimensional representation of a finite group. Then the character is a function $\chi_V : G \to \mathbb{C}$ defined by $g \mapsto \mathrm{Tr}[R(g)]$. □

A first observation that can be made about characters is that $\chi_V(e) = \mathrm{Tr}[I] = \mathrm{Dim}(V)$, since $R(e) = I$ for the identity element $e \in G$. The following proposition shows that the character has nice structure with respect to direct sums and tensor products.

Proposition 2.3.6. *Let (V, R_V) and (W, R_W) be finite, unitary group representations. Then*

$$\chi_{V\oplus W} = \chi_V + \chi_W, \quad \chi_{V\otimes W} = \chi_V\chi_W \quad \textit{and} \quad \chi_{V^*} = \chi_V^*. \tag{2.23}$$

Proof. By direct computation,

$$\begin{aligned}
\chi_{V\oplus W}(g) &= \mathrm{Tr}[R_V(g)\oplus R_W(g)] = \mathrm{Tr}[R_V(g)] + \mathrm{Tr}[R_W(g)] = \chi_V(g) + \chi_W(g),\\
\chi_{V\otimes W}(g) &= \mathrm{Tr}[R_V(g)\otimes R_W(g)] = \mathrm{Tr}[R_V(g)]\,\mathrm{Tr}[R_W(g)] = \chi_V(g)\chi_W(g),\\
\chi_{V^*}(g) &= \mathrm{Tr}[R_{V^*}(g)] = \mathrm{Tr}[R_V(g^{-1})] = \mathrm{Tr}[R_V(g)^\dagger] = \mathrm{Tr}[R_V(g)]^* = \chi_V^*(g),
\end{aligned}$$

for all $g \in G$. $\blacksquare$

As a consequence, the character of any representation is determined by the character of the irreducible representations into which it can be decomposed. Furthermore note that from the properties of R and the cyclic property of the trace it follows that

$$\chi_V(hgh^{-1}) = \mathrm{Tr}[R(hgh^{-1})] = \mathrm{Tr}[R(h)R(g)R(h)^{-1}] = \mathrm{Tr}[R(h)^{-1}R(h)R(g)] = \mathrm{Tr}\,R(g) = \chi_V(g).$$

This means that the character is constant on the conjugacy classes of G. Such functions are called class functions. Let us denote the set of all class function on G as $F_{\mathrm{class}}(G, \mathbb{C})$. Now one can define an inner product on the space $F_{\mathrm{class}}(G, \mathbb{C})$ as follows

Definition 2.3.8 (character inner product)**.** Let G be a finite group, (V,R) be a finite-dimensional representation of G and $F_{\text{class}}(G,\mathbb{C})$ be the space of class function on G. Then for $\alpha,\beta \in F_{\text{class}}(G,\mathbb{C})$ the character inner product is defined by

$$\langle \alpha,\beta\rangle = \frac{1}{|G|}\sum_{g\in G}\alpha(g)^*\beta(g). \qquad \square$$

Now that the required definitions are given, the main result of character theory is summarized in a single theorem. A number of different corollaries is directly stated. For a proof or more detailed explanation, the reader may refer to [25].

Theorem 2.3.7. *Let G be a finite group. Then the characters of the (non-isomorphic) irreducible representations of G form an orthonormal basis of $F_{\text{class}}(G,\mathbb{C})$ with respect to the character inner product.*

Corollary. *The following statements are all directly a result from the above theorem. Let G be a finite group and (V,R) be a finite-dimensional representation of G, with decomposition $V=\bigoplus_{i=1}^{k} V_i^{\oplus n_i}$ into all mutually inequivalent irreducible representations (possibly with multiplicity $n_i=0$).*

(1) The number of irreducible representations of G, is equal to the number of conjugacy classes of G.

(2) Any representation V is determined by its character, since $\chi_V=\sum_{i=1}^{k} n_i\chi_{V_i}$, where all χ_{V_i} are linearly independent.

(3) The multiplicities n_i in the decomposition of V are related to the character by $n_i=\langle\chi_V,\chi_{V_i}\rangle$. Therefore $\langle\chi_V,\chi_V\rangle=\sum_{i=1}^{k} n_i^2$.

(4) Also by the above, a representation W of G is irreducible if and only if $\langle\chi_W,\chi_W\rangle=1$.

(5) Application to the regular representation, i.e. the representation on the space $\mathbb{C}[G]$ identified with the left regular action of G on itself $\lambda_g : h\mapsto gh$, yields

$$\sum_{i=1}^{k}(\text{Dim}(V_i))^2 = |G|.$$

Proof. See Sections 2.2 and 2.4 of [25]. ■

The above results are very powerful tools to analyze representations, proof irreducibility or determine multiplicities. In the following lemma, characters are used to computed the multiplicity of the trivial subrepresentation in a particular situation. However, as stated here, the lemma does more than that, namely explicitly giving a method to find a trivial subrepresentation. The details are given below.

Lemma 2.3.8. *Let (V,R_V) be a unitary, irreducible representation with character χ_V and let $\{v_i\}$ be an orthonormal basis for V. Then the trivial representation is a subrepresentation of $(V\otimes V^*,R_{V\otimes V^*})$ with multiplicity one and it is spanned by the vector*

$$\sum_i v_i\otimes v_i^\dagger. \tag{2.24}$$

Proof. Since (V,R) is irreducible, its character has inner product 1. Therefore

$$1=\langle\chi_V,\chi_V\rangle=\frac{1}{|G|}\sum_{g\in G}\chi_V(g)^*\chi_V(g)=\frac{1}{|G|}\sum_{g\in G}\chi_V(g)\chi_{V^*}(g)=\frac{1}{|G|}\sum_{g\in G}\chi_{V\otimes V^*}(g)=\langle\chi_{V\otimes V^*},\chi_1\rangle,$$

where χ_1 is the character of the trivial subrepresentation, therefore satisfying $\chi_1(g)=1$ for all $g\in G$. The subspace is found using the isomorphism $\alpha:\mathcal{L}(V)\to V\otimes V^*$ given by $v_iv_i^\dagger\mapsto v_i\otimes v_i^\dagger$ and its

inverse (see subsection 2.1.4 for details). Then

$$\begin{aligned} R_{V\otimes V^*}(g)\left(\sum_i v_i\otimes v_i^\dagger\right) &= \sum_i (R_V(g)v_i)\otimes(v_i^\dagger R_{V^*}(g)) \\ &= \sum_i (R_V(g)v_i)\otimes(v_i^\dagger R_V(g)^\dagger) \\ &= \alpha\left(\sum_i R_V(g)v_i v_i^\dagger R_V(g)^\dagger\right) \\ &= \alpha\left(R_V(g)\left[\sum_i v_i v_i^\dagger\right]R_V(g)^\dagger\right) \\ &= \alpha\left(\sum_i v_i v_i^\dagger\right) \\ &= \sum_i v_i\otimes v_i^\dagger, \end{aligned}$$

for all $g\in G$, showing that indeed the claimed vector is invariant under the action of G. ■

Corollary. *For a real, orthogonal representation (V,R) of a group G with decomposition $V=\bigoplus_{i=1}^k V_i^{\oplus n_i}$ into mutually inequivalent irreducible representations, one has*

$$\sum_{i=1}^k n_i^2 = \langle\chi_V,\chi_V\rangle = \langle\chi_{V\otimes V},\chi_1\rangle\,. \tag{2.25}$$

Denote V_{i_s} the s-th copy of the space V_i ($s=1,\dots,n_i$) and denote $\{v_j^{(i_s)} : j=1,\dots,\mathrm{Dim}(V_i)\}$ an orthonormal basis of V_{i_s} that respect the isomorphisms between equivalent spaces (meaning that $v_j^{(i_s)}\mapsto v_j^{(i_{s'})}$ under the isomorphism between V_{i_s} and $V_{i_{s'}}$ that commutes with the representation). Then write

$$V\otimes V = \bigoplus_{i=1}^k\left(\bigoplus_{s,s'=1}^{n_i}(V_{i_s}\otimes V_{i_{s'}})\right). \tag{2.26}$$

Applying Lemma 2.3.8 to each term, using that $V_{i_s}\cong V_{i_{s'}}$ are equivalent, one finds the trivial subrepresentations of $(V\otimes V,R^{\otimes 2})$ as

$$\sum_{j=1}^{\mathrm{Dim}(V_i)} v_j^{(i_s)}\otimes v_j^{(i_{s'})}, \qquad \forall s,s'=1,\dots,n_i,\ \forall i=1,\dots,k. \tag{2.27}$$

These are precisely the $\sum_{i=1}^k n_i^2=\langle\chi_{V\otimes V},\chi_1\rangle$ trivial subrepresentations that are present.

2.4. BRIEF INTRODUCTION INTO QUANTUM MECHANICS

Quantum mechanics is currently the most accurate and complete description of the world available, but still it remains difficult to fully grasp the philosophical implications of the theory. This section is restricted to a concise treatment of the most essential concepts of quantum mechanics, focusing primarily on its postulates without considering the interpretation of the theory or any practical examples. For a more detailed introduction, the reader may consult standard textbooks in the topic (e.g. [27]). The approach taken here is rather formal and mathematical in order to set up powerful tools and notation that is commonly used in quantum information and computation. The contents of this section is roughly based on refs [21, 27, 28].

2.4.1. THE POSTULATES OF QUANTUM MECHANICS

Quantum mechanics is a mathematical framework developed to describe the physical theory of (quantum mechanical) systems. The postulates form a basis for this framework and are motivated by a century of experiments. It forms the connection between the full mathematical framework and the real physical world. The postulates can be formulated as follows:

1. With each isolated physical system a complex Hilbert space $\mathcal{H}$ is associated, known as the state space of the system. The system is then fully described by a state vector $\psi \in \mathcal{H}$ with unit length $\|\psi\| = 1$.
2. The evolution of closed quantum systems is described by a unitary transformation $U \in \mathcal{U}(\mathcal{H})$. If a system evolves from state ψ to state ψ' between times t_1 and t_2, its evolution is described by the unitary transformation $\psi' = U\psi$, where U only depends on t_1 and t_2, but not on ψ and ψ'.
3. Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These operators are linear operators on the state space of the system being measured. The subscript m refers to a (real valued) measurement outcome. The collection of measurement operators must satisfy $\sum_m M_m^\dagger M_m = I$, with I the identity. If a system is in state $\psi \in \mathcal{H}$ immediately before the measurement then the probability of obtaining the outcome m is given by

$$\mathbb{P}(m) = \langle M_m\psi, M_m\psi\rangle = \langle \psi, M^\dagger M\psi\rangle \tag{2.28}$$

   and the post-measurement state is given by

$$\psi_m = \frac{M_m\psi}{\sqrt{\mathbb{P}(m)}}. \tag{2.29}$$

   The requirement on the measurement operators above ensure that the outcome probabilities sum to one:

$$\sum_m \mathbb{P}(m) = \sum_m \langle \psi, M^\dagger M\psi\rangle = \langle \psi, (\sum_m M^\dagger M)\psi\rangle = \langle \psi, I\psi\rangle = \|\psi\|^2 = 1.$$

4. The state space of a composite physical system is the tensor product of the state spaces of the component systems. In particular, if the state spaces of system A and B are $\mathcal{H}_\mathsf{A}$ and $\mathcal{H}_\mathsf{B}$ respectively, the state space of the composite system is $\mathcal{H} = \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$.

The first postulate simply states that the state space of any physical system is a complex Hilbert space, but it does not tell us anything about what Hilbert space is associated with a particular physical system nor what the state vector of a that system in a specific state is. These things are determined by the laws of physics. The normalization condition $\|\psi| = 1$ ensures that measurement outcome probabilities sum to one. Similarly, the second postulate does not give any information on which unitary transformation describes real world quantum transformations. Interestingly, on qubit systems, all unitary operators are valid real world transformations. The second postulate can be formulated in an equivalent and more refined way, which may be more familiar to the reader:

2'. The time evolution of the state ψ of a closed quantum system is described by the Schrödinger equation,

$$i\hbar\frac{\partial\psi}{\partial t} = H\psi, \tag{2.30}$$

   where i is the imaginary unit, $\hbar$ a physical constant (Planck's constant) and where $H \in \mathrm{Herm}(\mathcal{H})$ is a hermitian operator on the state space of ψ known as the systems Hamiltonian. Therefore the systems state, if known at some initial time t_0, is determined for all times t if the Hamiltonian is known.

The equivalence between the two postulates (especially in the case of unbounded Hamiltonians) is governed by Stone's theorem. It provides a one-to-one correspondence between strongly continuous one-parameter (typically identified as time t) unitary groups and the hermitian operators on the Hilbert space. Its construction rests on the spectral theorem for hermitian operators. The solution of (2.30) can easily be verified to be $\psi(t_1) = \exp(-iH(t_1 - t_0)/\hbar)\psi_0$. Now the operator $U = \exp(-iH(t_1 - t_0)/\hbar)$ is defined by the function of normal operators via the spectral theorem. Stone's theorem basically says that any unitary operator U can be written in the form $U = \exp(iH)$ for some hermitian operator H and conversely that any hermitian operator H defines a unitary operator by the definition $U := \exp(iH)$. Now the problem has translated into finding the hermitian operator H, the Hamiltonian of a system, that correctly describes its time evolution.

The second postulate describes the evolution of closed systems, but does not tell us anything about what happens upon interaction with an other system, say an observer. In practice, experimentalists perform measurements on quantum systems. The third postulate governs the act of measurement of a quantum system, and is by far the most widely debated postulate of all. The debate is mostly about its interpretation and philosophical implication, and not about its correctness. For an excellent discussion on the interpretation of quantum mechanics and its postulates, the reader may consult [29].

The final postulate seems innocent, but why should the tensor product describe the composition of state space? The tensor product encapsulates the principles of superposition and entanglement in quantum mechanics. The superposition principle follows already from the first postulate: if $u, v \in \mathcal{H}$ are valid quantum states, then so is $au + bv$ for all $a, b \in \mathbb{C}$ such that $|a|^2 + |b|^2 = 1$. This follows from the fact that $\mathcal{H}$ is a linear vector space. Consider two different systems A and B with state spaces $\mathcal{H}_\mathsf{A}$ and $\mathcal{H}_\mathsf{B}$. Then if system A is in state $u \in \mathcal{H}_\mathsf{A}$ and system B is in state $v \in \mathcal{H}_\mathsf{B}$, the state of the composite system may be viewed as $\begin{bmatrix} u \\ v \end{bmatrix}$. Applying the superposition principle to different states of this form yields the state space $\mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$. This gives a motivation for the postulate, but is no derivation since the superposition principle is not taken as a postulate in itself.

2.4.2. THE DIRAC NOTATION

The Dirac notation is frequently used in all fields of quantum mechanics and quantum information. It is a powerful way to represent states, linear operators and functionals in a finite or infinite dimensional Hilbert space. Its justification makes use of Riesz's representation theorem (Theorem 2.1.2). Dirac proposed to chop the brackets of the inner product into two pieces. Consider $\langle u, v\rangle$ with $u, v \in \mathcal{H}$. This consists of the so called 'bra' part $\langle u|$ and the 'ket' part $|v\rangle$. Here $|v\rangle$ is then viewed as the vector v in the Hilbert space, i.e. $|v\rangle \in \mathcal{H}$. A linear operator $A \in \mathcal{L}(\mathcal{H})$ can operate on a ket, denoted $|w\rangle = A|v\rangle$. The bra part $\langle u|$ can be seen as a linear functional on $\mathcal{H}$, i.e. $\langle u| \in \mathcal{H}^*$, since $\langle u| : \mathcal{H} \to \mathbb{C}$ can be uniquely defined as $\langle u|v\rangle := \langle u, v\rangle$ by Riesz's representation theorem. This is so natural, that from here on out in this thesis, the inner product will be written as $\langle u|v\rangle$. Invoking the Riesz's representation theorem, the linear functional $\langle u|$ can be uniquely identified with an element $|u\rangle \in \mathcal{H}$ and vice versa with each element $|u\rangle \in \mathcal{H}$ a linear functional $\langle u|$ can be identified. In other words, $(|u\rangle)^\dagger = \langle u|$. Depending on the context, a state is written as $|u\rangle$ or just u and a linear functional as $\langle u|$ or $u^\dagger$. Finally note that $(\alpha|u\rangle)^\dagger = \langle u|\alpha^*$, for any $\alpha \in \mathbb{C}$, where a^* denotes the complex conjugate of a, which follows from the conjugate symmetry of the inner product.

Using the isomorphism between $\mathcal{L}(\mathcal{H}) \cong \mathcal{H} \otimes \mathcal{H}^*$, a linear operator $A \in \mathcal{L}(\mathcal{H})$ can be represented as $\sum_{i,j} A_{ij}|i\rangle\otimes\langle j|$, where $\{|i\rangle\}_i$ is an orthonormal basis of $\mathcal{H}$ and $A_{ij} = \langle i|(A|j\rangle)$. It is customary in Dirac notation to omit the tensor symbol, such that $|i\rangle \otimes \langle j| = |i\rangle\langle j|$ and $|i\rangle \otimes |j\rangle = |i\rangle|j\rangle = |i, j\rangle$ (similarly for bras). Another important observation is that $(A|u\rangle)^\dagger|v\rangle = \langle Au|v\rangle = \langle u|A^\dagger v\rangle = \langle u|(A^\dagger|v\rangle)$ for all $u, v \in \mathcal{H}$, giving rise to the definition $\langle u|A^\dagger := (A|u\rangle)^\dagger$. For a general linear operator A, the notation $\langle u|A|v\rangle$ is ambiguous, but generally understood to mean $\langle u|(A|v\rangle)$. However if A is hermitian, then $(A|u\rangle)^\dagger = \langle v|A$. Therefore, one can write $\langle u|A|v\rangle$ without ambiguity.

Explicitly in the finite dimensional case, an element $|u\rangle \in \mathcal{H} = \mathbb{C}^n$ and its dual $\langle u| \in \mathcal{H}^*$ can be identified as (with respect to some orthonormal basis $\{x_i\}_{i=1}^n$)

$$|u\rangle = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} \qquad \text{and} \qquad \langle u| = \begin{pmatrix} u_1^* & u_2^* & \cdots & u_n^* \end{pmatrix},$$

where u_i^* is the complex conjugate of u_i. The tensor product is then the outer product between vectors and Kronecker product between matrices. In general the tensor product of a $m \times n$ matrix A and a $p \times q$ matrix B is a $mp \times nq$ matrix defined as

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix}, \tag{2.31}$$

which also holds in the special case of vectors where m, n, p or q may be one.

2.5. ESSENTIAL TOOLS FOR QUANTUM INFORMATION

This section is devoted to the discussion of the tools required in quantum information. This section is divided into several subsections, each discussing a single topic. In this section, and the rest of this thesis, Dirac notation is used. The contents of this section are based on refs [21, 27, 28].

2.5.1. THE DENSITY OPERATOR

The density operator is a powerful tool to describe classical ensembles of quantum states. Suppose that a classical ensemble of states are given $\{p_i, |\psi_i\rangle\}$, each state $|\psi_i\rangle$ occurring with probability $p_i \in [0,1]$, such that $\sum_i p_i = 1$. Then the density operator corresponding to this ensemble is defined as

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| . \tag{2.32}$$

Note that ρ is not an element of $\mathcal{H}$, but can rather be viewed as an element of $\mathcal{L}(\mathcal{H})$. It turns out that all four postulates of quantum mechanics can be formulated in the density operator language. Then $\mathcal{L}(\mathcal{H})$ is viewed as a Hilbert space in its own right, and quantum operations are linear maps from that Hilbert space onto itself that map density operators to density operators. This is made precise later. First the formal definition of a density operator is given. A density operator is a positive semidefinite operator operator, denoted $\rho \geq 0$, with $\mathrm{Tr}[\rho] = 1$. In particular this means that all the eigenvalues of ρ are contained in the interval $[0,1]$.

Definition 2.5.1 (Density operator)**.** A density operator is a linear operator $\rho \in \mathrm{Pos}(\mathcal{H}) \subset \mathcal{L}(\mathcal{H})$ such that $\mathrm{Tr}[\rho] = 1$. The space of density operators is denoted $\mathcal{D}(\mathcal{H})$. □

Note that the same density operator can be obtained from different ensembles. Two different ensembles $\{p_i |\psi_i\rangle\}$ and $\{q_j |\phi_j\rangle\}$ produce the same density matrix if and only if

$$\sqrt{q_j}|\phi_j\rangle = \sum_i u_{ij}\sqrt{p_i}|\psi_i\rangle ,$$

where u_{ij} is the (i,j)-th entry of a unitary matrix $U \in \mathcal{U}(\mathcal{H})$.

All postulates of quantum mechanics can equivalently be written in terms of density operator language. Postulate 1 then just says that density operator $\rho \in \mathcal{D}(\mathcal{H})$ is a valid quantum state. The

evolution of a density operator is still governed by a unitary evolution mapping $\rho \mapsto U\rho U^\dagger$, where $U \in \mathcal{U}(\mathcal{H})$. Alternatively, the Schrödinger equation for the explicit time evolution can be formulated for density operators as

$$i\hbar \frac{\partial \rho}{\partial t} = [H, \rho] = H\rho - \rho H, \tag{2.33}$$

where H is again the system Hamiltonian. This equation is known as the Liouville-Von Neumann equation and is equivalent to the Schrödinger equation. In quantum information this description is hardly ever used and states are just evolved by applying some unitary operation U (related to the Hamiltonian H by Stone's theorem, see subsection 2.4.1). Measurements, as formulated in the third postulate, are also easily described in the density operator language. Suppose $\{M_m\}$ is a collection of measurement operators, then the probability to obtain outcome m on the mixed state ρ is given by

$$\mathbb{P}(m) = \sum_i \mathbb{P}(m|i)p_i = \sum_i p_i \operatorname{Tr}[M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|] = \operatorname{Tr}[M_m^\dagger M_m \rho] \tag{2.34}$$

and the post-measurement state is then given by

$$\rho_m = \frac{M_m \rho M_m^\dagger}{\sqrt{\mathbb{P}(m)}}. \tag{2.35}$$

The fourth postulate carries over in a straightforward way and $\rho_{\mathsf{AB}} \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}})$ is a valid density operator on the state space of a composite system A and B. Completely analogous to the state vector description, systems A and B are said to be entangled if ρ_{AB} can not be written as $\rho_{\mathsf{AB}} = \rho_{\mathsf{A}} \otimes \rho_{\mathsf{B}}$ for some $\rho_{\mathsf{A}} \in \mathcal{D}(\mathcal{H}_{\mathsf{A}})$ and $\rho_{\mathsf{B}} \in \mathcal{D}(\mathcal{H}_{\mathsf{B}})$. A state of the form $\rho_{\mathsf{A}} \otimes \rho_{\mathsf{B}}$ is called a product state or separable state.

One of the most powerful applications of the density operator, aside from describing classical ensembles over quantum states, is that it provides a descriptive tool for subsystems of a composite system. A subsystem is described by the reduced density operator, obtained by tracing out (taking the partial trace over) the rest of the system.

Definition 2.5.2 (Partial trace)**.** Suppose $\rho \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}})$ is a density operator of a composite system A and B and that $\{|i\rangle_{\mathsf{A}}\}_i$, $\{|i\rangle_{\mathsf{B}}\}_i$ are orthonormal bases of $\mathcal{H}_{\mathsf{A}}$ and $\mathcal{H}_{\mathsf{B}}$ respectively, such that $\rho = \sum_{ijkl} a_{ijkl} |i\rangle\langle j|_{\mathsf{A}} \otimes |k\rangle\langle l|_{\mathsf{B}}$ in the tensor product basis for $a_{ijkl} \in \mathbb{C}$. Then the partial trace of ρ over system B is defined as

$$\rho_{\mathsf{A}} = \operatorname{Tr}_{\mathsf{B}} \rho = \sum_{ijkl} a_{ijkl} |i\rangle\langle j|_{\mathsf{A}} \otimes \operatorname{Tr}[|k\rangle\langle l|_{\mathsf{B}}] = \sum_{ij} \left(\sum_k a_{ijkk} \right) |i\rangle\langle j|_{\mathsf{A}} \tag{2.36}$$

and ρ_{A} is called the reduced density operator of system A. □

Interestingly enough, any density operator can be viewed as the reduced density operator of a pure state of a composite system. Suppose ρ_{A} is given, with its spectral decomposition $\rho_{\mathsf{A}} = \sum_i \lambda_i |v_i\rangle\langle v_i|$. Then introducing a reference system R with a state space of the same dimension as system A and orthonormal basis $\{|i\rangle\langle i|_{\mathsf{R}}\}$, the desired pure state is then simply

$$|\Psi\rangle_{\mathsf{AR}} = \sum_i \sqrt{\lambda_i} |v_i\rangle_{\mathsf{A}} \otimes |i\rangle_{\mathsf{R}}. \tag{2.37}$$

To verify this statement, let us compute

$$\begin{aligned} \operatorname{Tr}_{\mathsf{R}} |\Psi\rangle\langle\Psi|_{\mathsf{AR}} &= \sum_{ij} \sqrt{\lambda_i \lambda_j} |v_i\rangle\langle v_j|_{\mathsf{A}} \operatorname{Tr} |i\rangle\langle j|_{\mathsf{R}} \\ &= \sum_{ij} \sqrt{\lambda_i \lambda_j} |v_i\rangle\langle v_j|_{\mathsf{A}} \delta_{ij} \\ &= \sum_i \lambda_i |v_i\rangle\langle v_i|_{\mathsf{A}} = \rho_{\mathsf{A}}. \end{aligned} \tag{2.38}$$

The state $|\Psi\rangle_{\mathsf{AR}}$ is referred to as the purification of ρ_{A}.

Definition 2.5.3 (Purification)**.** Let $\rho_{\mathsf{A}} \in \mathcal{D}(\mathcal{H}_{\mathsf{A}})$ be density operator. Then a pure state $|\Psi\rangle \in \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{R}}$ is called a purification of ρ_A if $\mathrm{Tr}_{\mathsf{R}} |\Psi\rangle \langle\Psi| = \rho_{\mathsf{A}}$, where $\mathcal{H}_{\mathsf{R}}$ is an arbitrary (not necessarily physical) reference space. □

2.5.2. PROJECTIVE MEASUREMENTS AND POVM'S

The most general form of a measurement is a collection of operators $M_m \in \mathcal{L}(\mathcal{H})$ such that

$$\sum_m M_m^\dagger M_m = I.$$

The probability of obtaining outcome m on a general state ρ is then $\mathbb{P}(m) = \mathrm{Tr}[M_m^\dagger M_m \rho]$ and the post-measurement state is the normalized state

$$\rho_m = \frac{M_m \rho M_m^\dagger}{\sqrt{\mathrm{Tr}[M_m^\dagger M_m \rho]}},$$

as discussed in the previous section. In the special case that each M_m in a measurement collection is an orthogonal projector onto mutually disjoint subspaces, then the collection is said to be a projective measurement or Von Neumann measurement.

Definition 2.5.4 (Projective measurement)**.** A measurement collection $\{P_m\}$ is called a projective measurement or Von Neumann measurement if it satisfies the following conditions:

(i) $P_m^2 = P_m$ and $P_m = P_m^\dagger$ (orthogonal projection);

(ii) $P_m P_n = \delta_{mn} P_m$ for all m, n (projecting onto mutually disjoint subspaces);

(iii) $\sum_m P_m = I$ (completeness of measurement collection). □

The probability of observing outcome m can then be simplified to $\mathbb{P}(m) = \mathrm{Tr}[P_m \rho]$.

Often one is only interested in outcome probability and not in the post-measurement state. In that case a measurement collection can be simplified by setting $E_m = M_m^\dagger M_m$. Then $\sum_m E_m = I$ and $\mathbb{P}(m) = \mathrm{Tr}[E_m \rho]$. As discussed in subsection 2.1.2, $E_m \succeq 0$ for all m. The collection $\{E_m\}$ is called a POVM.

Definition 2.5.5 (POVM)**.** A collection $\{E_m\}$ is called a POVM (Positive Operator-Value Measure) if it satisfies $E_m \succeq 0$ for all m and $\sum_m E_m = I$. □

Note that a projective measurement is also a POVM, since $E_m = P_m^\dagger P_m = P_m$, with the additional advantage that the post-measurement state can also be found. One very important feature of POVM measurements is that one can optimize over them using semidefinite programming to find the POVM element that maximizes the outcome of a certain measurement. This can for example be used to find the measurement that maximizes the probability of distinguishing two quantum states.

2.5.3. QUANTUM CHANNELS

A quantum channel is a linear map that sends quantum states (density operators) to quantum states, possibly on a different state space. Two special cases were already encountered in the previous, namely the unitary evolution and the measurement. Both can be viewed as a quantum channel, but here a quantum channel will be defined to map density operators to density operators with certainty,

which excludes measurements from the definition. However, the power of a quantum channel is that it can also describe the evolution of an open system, i.e. a system of interest that is coupled to some environment system. Therefore a quantum channel is much more general than just unitary evolution.

Before giving the formal definition of a quantum channel, some notions need introduction. Quantum channels are a subset of the linear operators between two spaces of linear operators on a Hilbert space. That is, a quantum channel is a linear map $\mathcal{E} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ with some additional conditions. Let us denote the space of all linear operators $\mathcal{E} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ as $\mathcal{T}(\mathcal{H}_A, \mathcal{H}_B)$. Again $\mathcal{T}(\mathcal{H})$ is then understood to mean the linear maps from $\mathcal{L}(\mathcal{H})$ to itself. Of course, there is nothing special here, since $\mathcal{L}(\mathcal{H})$ can just be viewed as a Hilbert space in itself (with the Hilbert-Schmidt inner product). Then $\mathcal{T}(\mathcal{H}_A, \mathcal{H}_B) = \mathcal{L}(\mathcal{L}(\mathcal{H}_A), \mathcal{L}(\mathcal{H}_B))$. This means that all properties discussed in section 2.1 can be applied to elements of $\mathcal{T}(\mathcal{H})$.

In the context of quantum information, an element $\mathcal{E} \in \mathcal{T}(\mathcal{H}_A, \mathcal{H}_B)$ is referred to as a linear superoperator (or simply superoperator). To distinguish superoperators $\mathcal{E} \in \mathcal{T}(\mathcal{H})$ from operators in $A \in \mathcal{L}(\mathcal{H})$, the notation $\mathcal{E} : A \mapsto \mathcal{E}(A)$ is used when the superoperator $\mathcal{E}$ is applied to an element of its domain. This is in contrast with the linear operator A, for which the notation $A : x \mapsto Ax$ is used for $x \in \mathcal{H}$. That is, brackets shall be used whenever a superoperator is applied and brackets are omitted whenever a linear operator is applied to an element of the underlying Hilbert space. Furthermore, the composition of superoperators shall be made explicit with the $\circ$ symbol, whereas the composition of operators is just regarded as the regular (matrix) product, with any symbol omitted.

Next, some properties that superoperators may posses are defined.

Definition 2.5.6 (Positive, completely positive, trace-preserving and unital maps)**.** A linear superoperator $\mathcal{E} \in \mathcal{T}(\mathcal{H}_A, \mathcal{H}_B)$ is said to be

(a) positive if $\mathcal{E}(P) \in \mathrm{Pos}(\mathcal{H}_B)$ for all $P \in \mathrm{Pos}(\mathcal{H}_A)$;

(b) completely positive if $\mathcal{E} \otimes I_{\mathcal{L}(\mathcal{H}_C)} \in \mathcal{T}(\mathcal{H}_A \otimes \mathcal{H}_C, \mathcal{H}_B \otimes \mathcal{H}_C)$ is positive for any complex Hilbert space $\mathcal{H}_C$;

(c) trace-preserving if $\mathrm{Tr}[\mathcal{E}(A)] = \mathrm{Tr}[A]$ for all $A \in \mathcal{L}(\mathcal{H}_A)$;

(d) unital if $\mathcal{E}(I_{\mathcal{L}(\mathcal{H}_A)}) = I_{\mathcal{L}(\mathcal{H}_B)}$. □

These properties can now be used to formally define a quantum channel.

Definition 2.5.7 (Quantum channel)**.** A quantum channel is a linear map $\mathcal{E} \in \mathcal{T}(\mathcal{H}_A, \mathcal{H}_B)$, satisfying

(i) $\mathcal{E}$ is completely positive, and

(ii) $\mathcal{E}$ is trace-preserving.

For this reason, quantum channels are also commonly referred to as CPTP (Completely Positive Trace Preserving) maps. Let us denote the space of of quantum channels as $\mathcal{S}(\mathcal{H}_A, \mathcal{H}_B) \subset \mathcal{T}(\mathcal{H}_A, \mathcal{H}_B)$. □

In some text, quantum channels are defined to be trace-decreasing, completely positive, linear map between $\mathcal{L}(\mathcal{H}_A)$ and $\mathcal{L}(\mathcal{H}_B)$. Trace-decreasing means $\mathrm{Tr}[\mathcal{E}(A)] \leq \mathrm{Tr}[A]$ for all $A \in \mathcal{L}(\mathcal{H}_A)$. This allows the incorporations of measurements in the framework of quantum channels. Then $0 \leq \mathrm{Tr}[\mathcal{E}(\rho)] \leq 1$ for all $\rho \in \mathcal{D}(\mathcal{H})$ and $\mathrm{Tr}[\mathcal{E}(\rho)]$ is associated with the probability that the channel $\mathcal{E}$ acted on initial state ρ. In this thesis however, measurements are treated separately, and a quantum channel occurs with certainty, i.e. $\mathrm{Tr}[\mathcal{E}(\rho)] = \mathrm{Tr}[\rho] = 1$.

Precisely the conditions of trace-preserving and complete positivity assure that if a quantum channel $\mathcal{E}$ is applied to a density operator $\rho \in \mathcal{D}(\mathcal{H})$, then $\mathcal{E}(\rho) \in \mathcal{D}(\mathcal{H})$ is also a density operator. Clearly by the trace-preserving property $\mathrm{Tr}[\mathcal{E}(\rho)] = \mathrm{Tr}[\rho] = 1$. But at first it may seem unclear why positivity is not enough. This is because ρ may be part of a larger composite system $\rho_{\mathsf{AB}} \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}})$. Then the map $\mathcal{E} \otimes I$ must also be a valid density state. See Example 2.5.1 for a positive map that is not completely positive.

Example 2.5.1. The transpose $T : \mathcal{L}(\mathbb{C}^2) \to \mathcal{L}(\mathbb{C}^2)$ given by $A \mapsto A^T$ is a positive operator, i.e. if $A \geq 0$ then also $T(A) = A^T \geq 0$, because $\mathrm{Det}[A - \lambda I] = \mathrm{Det}[A - \lambda I]^T = \mathrm{Det}[A^T - \lambda I]$ so A and A^T have the same eigenvalues. However, the superoperator $T \otimes I \in \mathcal{T}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ is not positive. To see this, suppose it acts on $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Then $\rho = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$ and so

$$\sigma := (T \otimes I)(\rho) = \frac{1}{2}(|00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10| + |11\rangle\langle 11|), \tag{2.39}$$

which is not a positive operator since it has an eigenvalue $-\frac{1}{2}$ corresponding to the eigenstate $|\phi\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$. Thus σ is not a valid quantum state. □

First let us characterize the set of quantum channels in the following way.

Proposition 2.5.1 (The set of quantum channels is convex)**.** *The set of quantum channels $\mathcal{S}(\mathcal{H}_{\mathsf{A}}, \mathcal{H}_{\mathsf{B}})$ is a convex set.*

Proof. Let $\mathcal{E}_1, \mathcal{E}_2 \in \mathcal{S}(\mathcal{H}_{\mathsf{A}}, \mathcal{H}_{\mathsf{B}})$ be two quantum channels and let $\alpha_1, \alpha_2 \geq 0$ such that $\alpha_1 + \alpha_2 = 1$. Then $\mathcal{E} = \alpha_1\mathcal{E}_1 + \alpha_2\mathcal{E}_2$ is completely positive, since for all $P \in \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{C}}$

$$(\mathcal{E} \otimes \mathcal{I})(P) = \alpha_1(\mathcal{E}_1 \otimes \mathcal{I})(P) + \alpha_2(\mathcal{E}_2 \otimes \mathcal{I})(P) \tag{2.40}$$

is positive by linearity and the fact that $\mathcal{E}_1$ and $\mathcal{E}_2$ are CP. Here $\mathcal{I}$ is the identity on the auxiliary Hilbert space $\mathcal{H}_{\mathsf{C}}$. Furthermore, $\mathcal{E}$ is trace-preserving, since for all $A \in \mathcal{H}_{\mathsf{A}}$

$$\mathrm{Tr}[\mathcal{E}(A)] = \alpha_1 \mathrm{Tr}[\mathcal{E}_1(A)] + \alpha_2 \mathrm{Tr}[\mathcal{E}_2(A)] = (\alpha_1 + \alpha_2)\mathrm{Tr}[A] = \mathrm{Tr}[A], \tag{2.41}$$

by the trace-preserving property of $\mathcal{E}_1$ and $\mathcal{E}_2$. Hence $\mathcal{S}(\mathcal{H}_{\mathsf{A}}, \mathcal{H}_{\mathsf{B}})$ is a convex set. ■

A quantum channel $\mathcal{E} \in \mathcal{S}(\mathcal{H}_{\mathsf{A}_1} \otimes \cdots \otimes \mathcal{H}_{\mathsf{A}_n}, \mathcal{H}_{\mathsf{B}_1} \otimes \cdots \otimes \mathcal{H}_{\mathsf{B}_n})$ is said to be a product channel if $\mathcal{E} = \mathcal{E}_1 \otimes \cdots \otimes \mathcal{E}_n$ for some $\mathcal{E}_i \in \mathcal{S}(\mathcal{H}_{\mathsf{A}_i}, \mathcal{H}_{\mathsf{B}_i})$ for all $i = 1, ..., n$. A product channel represents the independent application of channel $\mathcal{E}_i$ on a state in $\mathcal{D}(\mathcal{H}_{\mathsf{A}_i})$ mapping it into a valid state in $\mathcal{D}(\mathcal{H}_{\mathsf{B}_i})$. At the end of this section, it is shown that any tensor product of quantum channels is in fact a quantum channel itself. The proof makes use of some concepts that are introduced below.

Here a property of the adjoint of a quantum channel is presented in a small proposition, that will be used at a later stage in this thesis. The adjoint of a channel is uniquely defined by $\langle \mathcal{E}_1^\dagger(A)|B\rangle = \langle A|\mathcal{E}_1(B)\rangle$ for all $A, B \in \mathcal{L}(\mathcal{H})$.

Proposition 2.5.2 (The adjoint of a quantum channel is CPU)**.** *Let $\mathcal{E} \in \mathcal{T}(\mathcal{H})$. Then*

(1) $\mathcal{E}$ is completely positive (CP) if and only if $\mathcal{E}^\dagger$ is completely positive, and

(2) $\mathcal{E}$ is trace-preserving (TP) if and only if $\mathcal{E}^\dagger$ is unital (U).

Hence $\mathcal{E}$ is a quantum channel if and only if $\mathcal{E}^\dagger$ is completely positive and unital (CPU).

Proof. (1) The superoperator $\mathcal{E}$ is positive if and only if $\mathcal{E}(P) \geq 0$ for all $P \geq 0$. This is equivalent to $\langle \mathcal{E}(P)|Q\rangle = \langle P|\mathcal{E}^\dagger(Q)\rangle \geq 0$ for all $P, Q \geq 0$. But this is then equivalent to $\mathcal{E}^\dagger(Q) \geq 0$ for all $Q \geq 0$ and

therefore equivalent to $\mathcal{E}^\dagger$ being positive. Then $\mathcal{E}\otimes\mathcal{I}_{\mathcal{L}(\mathcal{H}_\mathsf{R})}$ is positive for any reference Hilbert space $\mathcal{H}_\mathsf{R}$ if and only if $(\mathcal{E}\otimes\mathcal{I}_{\mathcal{L}(\mathcal{H}_\mathsf{R})})^\dagger = \mathcal{E}^\dagger\otimes\mathcal{I}_{\mathcal{L}(\mathcal{H}_\mathsf{R})}$ is positive by the above. Hence $\mathcal{E}$ is CP if and only if $\mathcal{E}^\dagger$ is CP.
(2) Let $A\in\mathcal{L}(\mathcal{H})$. Suppose $\mathcal{E}$ is TP. Then

$$\langle I|A\rangle = \mathrm{Tr}[A] = \mathrm{Tr}[\mathcal{E}(A)] = \langle I|\mathcal{E}(A)\rangle = \langle\mathcal{E}^\dagger(I)|A\rangle\,, \tag{2.42}$$

so that $\langle I-\mathcal{E}^\dagger(I)|A\rangle = 0$ for all $A\in\mathcal{L}(\mathcal{H})$. Therefore then $\mathcal{E}^\dagger(I) = I$, that is, $\mathcal{E}^\dagger$ is unital. Conversely, suppose $\mathcal{E}^\dagger$ is unital. Then for any $A\in\mathcal{L}(\mathcal{H})$,

$$\mathrm{Tr}[\mathcal{E}(A)] = \langle I|\mathcal{E}(A)\rangle = \langle\mathcal{E}^\dagger(I)|A\rangle = \langle I|A\rangle = \mathrm{Tr}[A], \tag{2.43}$$

so $\mathcal{E}$ is trace-preserving (TP). ■

Next some forms in which superoperators are encountered are discussed. There exists several different forms and their use depend on the application. There are four common forms in which a superoperator can be presented. To facilitate the discussion of these representation, first a simple operation called vectorization is introduced.

Definition 2.5.8 (Vectorization)**.** Let $\mathcal{H}$ be a Hilbert space with orthonormal basis $\{|i\rangle\}$. Then the vectorization operation is a linear map $\eta:\mathcal{L}(\mathcal{H})\mapsto\mathcal{H}\otimes\mathcal{H}$ defined (with respect to a chosen basis) by $\eta:|i\rangle\langle j|\mapsto|i\rangle|j\rangle$. It is called vectorization because it can be thought of as the column stacking of the matrix representation of a linear operator, forming a vector in $\mathcal{H}\otimes\mathcal{H}$. □

Returning to the discussion of representations of superoperators, the natural representation is discussed first. The superoperator $\mathcal{E}\in\mathcal{T}(\mathcal{H}_\mathsf{A},\mathcal{H}_\mathsf{B})$ maps linear operators from $\mathcal{L}(\mathcal{H}_\mathsf{A})$ to $\mathcal{L}(\mathcal{H}_\mathsf{B})$. The idea of the natural representation is to pick a basis for $\mathcal{H}_\mathsf{A}$ and $\mathcal{H}_\mathsf{B}$, and column stack the matrix representations of linear operators in $\mathcal{L}(\mathcal{H}_\mathsf{A})$ and $\mathcal{L}(\mathcal{H}_\mathsf{B})$ as to make them resemble ordinary column vectors. Then a linear superoperator $\mathcal{E}\in\mathcal{T}(\mathcal{H}_\mathsf{A},\mathcal{H}_\mathsf{B})$ can be given a matrix representation with respect to the chosen bases. This is made precise in the following definition

Definition 2.5.9 (Natural representation of superoperators)**.** Let $\mathcal{H}_\mathsf{A}$ and $\mathcal{H}_\mathsf{B}$ be two Hilbert spaces with orthonormal bases $\{|e_i\rangle\}$ and $\{|f_i\rangle\}$ respectively. Let $\mathcal{E}\in\mathcal{T}(\mathcal{H}_\mathsf{A},\mathcal{H}_\mathsf{B})$ be a linear superoperator, mapping $\mathcal{L}(\mathcal{H}_\mathsf{A})$ into $\mathcal{L}(\mathcal{H}_\mathsf{B})$. Then the natural representation of the superoperator $\mathcal{E}$ is the matrix representation of size $(\mathrm{Dim}(\mathcal{H}_\mathsf{A}))^2\times(\mathrm{Dim}(\mathcal{H}_\mathsf{B}))^2$ defined by its action on the basis elements $|e_i\rangle\langle e_j|$ as

$$\mathcal{E}(|e_i\rangle\langle e_j|) = \sum_{k,l=1}^{\mathrm{Dim}(\mathcal{H}_\mathsf{B})}\alpha_{ijkl}|f_k\rangle\langle f_l|\,. \tag{2.44}$$

The complex numbers α_{ijkl} form the matrix representation of $\mathcal{E}$ in the given basis. In terms of the vectorization operation η, this equation can be written as

$$K(\mathcal{E})\eta_\mathsf{A}(A) = \eta_\mathsf{B}(\mathcal{E}(A)), \tag{2.45}$$

for some $A\in\mathcal{L}(\mathcal{H}_\mathsf{A})$, where $K:\mathcal{T}(\mathcal{H}_\mathsf{A},\mathcal{H}_\mathsf{B})\to\mathcal{L}(\mathcal{H}_\mathsf{A}\otimes\mathcal{H}_\mathsf{A},\mathcal{H}_\mathsf{B}\otimes\mathcal{H}_\mathsf{B})$, given by

$$K:\mathcal{E}\mapsto\sum_{i,j=1}^{\mathrm{Dim}(\mathcal{H}_\mathsf{A})}\eta_\mathsf{B}(\mathcal{E}(|e_i\rangle\langle e_j|))\eta_\mathsf{A}(|e_i\rangle\langle e_j|)^\dagger = \sum_{i,j=1}^{\mathrm{Dim}(\mathcal{H}_\mathsf{A})}\sum_{k,l=1}^{\mathrm{Dim}(\mathcal{H}_\mathsf{B})}\alpha_{ijkl}|f_k\rangle|f_l\rangle\langle e_i|\langle e_j|, \tag{2.46}$$

is the mapping that maps a superoperator to its natural representation. □

The natural representation K is a bijection and $\mathcal{E}(A)$ can be obtained by

$$\mathcal{E}(A) = \eta_\mathsf{B}^{-1}\big(K(\mathcal{E})\eta_\mathsf{A}(A)\big).$$

It has some desirable operational properties. First, it respects the product (composition). That is, if $\mathcal{E}_1 \in \mathcal{T}(\mathcal{H}_A, \mathcal{H}_B)$ and $\mathcal{E}_2 \in \mathcal{T}(\mathcal{H}_B, \mathcal{H}_C)$ then $K(\mathcal{E}_2 \circ \mathcal{E}_1) = K(\mathcal{E}_2)K(\mathcal{E}_1)$. In particular if all spaces are the same, i.e. $K : \mathcal{T}(\mathcal{H}) \to \mathcal{L}(\mathcal{H} \otimes \mathcal{H})$, then $(K, \mathcal{H} \otimes \mathcal{H})$ is a representation in the strict sense of representation theory, since in addition to $K(\mathcal{E}_2 \circ \mathcal{E}_1) = K(\mathcal{E}_2)K(\mathcal{E}_1)$, the identity is also mapped to the identity by K. Furthermore it respects the adjoint. That is $K(\mathcal{E})^\dagger = K(\mathcal{E}^\dagger)$, where the adjoint of a superoperator is uniquely defined by $\langle \mathcal{E}(A)|B\rangle = \langle A|\mathcal{E}^\dagger(B)\rangle$ for all $A, B \in \mathcal{L}(\mathcal{H})$. Finally, it also respects the tensor product: $K(\mathcal{E}_1 \otimes \mathcal{E}_2) = K(\mathcal{E}_1) \otimes K(\mathcal{E}_2)$. However, there is no property on $K(\mathcal{E})$ that characterizes if $\mathcal{E}$ is a completely positive or trace-preserving channel. This makes it hard in this representation to distinguish arbitrary superoperators from quantum channels. For a continued discussion on this representation, see section 3.6, where a specific basis is chosen.

The next way a superoperator can be presented is known as its Choi form (also called Choi-Jamiolkowski representation). This is done via the Choi map, defined as follows.

Definition 2.5.10 (Choi form of superoperators)**.** Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be two Hilbert spaces with orthonormal bases $\{|e_i\rangle\}$ and $\{|f_i\rangle\}$ respectively. Let $\mathcal{E} \in \mathcal{T}(\mathcal{H}_A, \mathcal{H}_B)$ be a linear superoperator, mapping $\mathcal{L}(\mathcal{H}_A)$ into $\mathcal{L}(\mathcal{H}_B)$. Then the Choi representation $J(\mathcal{E})$ (or Choi operator) of $\mathcal{E}$ is defined by the mapping $J : \mathcal{T}(\mathcal{H}_A, \mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_B \otimes \mathcal{H}_A)$:

$$\mathcal{E} \mapsto J(\mathcal{E}) = \sum_{i,j=1}^{\mathrm{Dim}(\mathcal{H}_A)} \mathcal{E}(|e_i\rangle\langle e_j|) \otimes |e_i\rangle\langle e_j| = (\mathcal{E} \otimes \mathcal{I}_A)(|\phi\rangle\langle\phi|), \tag{2.47}$$

where $|\phi\rangle = \sum_{i=1}^{\mathrm{Dim}(\mathcal{H}_A)} |e_i\rangle|e_i\rangle = \eta(I_A)$ is the unnormalized maximally entangled state over $\mathcal{H}_A \otimes \mathcal{H}_A$, $\mathcal{I}_A$ is the identity superoperator on $\mathcal{L}(\mathcal{H}_A)$ and I_A is the identity operator on $\mathcal{H}_A$. □

The Choi map J is also a bijection and $\mathcal{E}(A)$ can be retrieved by

$$\mathcal{E}(A) = \mathrm{Tr}_A\left[J(\mathcal{E})(I_B \otimes A^T)\right],$$

where A^T is the transpose of A with respect to the basis $|e_i\rangle$. This can be verified by direct computation

$$\begin{aligned}\mathcal{E}(A) = \mathrm{Tr}_A\left[J(\mathcal{E})(I_B \otimes A^T)\right] &= \mathrm{Tr}_A\left[\left(\sum_{i,j=1}^{\mathrm{Dim}(\mathcal{H}_A)} \mathcal{E}(|e_i\rangle\langle e_j|) \otimes |e_i\rangle\langle e_j|\right)(I_B \otimes A^T)\right] \\ &= \sum_{i,j=1}^{\mathrm{Dim}(\mathcal{H}_A)} \mathcal{E}(|e_i\rangle\langle e_j|)\,\mathrm{Tr}\left[|e_i\rangle\langle e_j|\,A^T\right] = \sum_{i,j=1}^{\mathrm{Dim}(\mathcal{H}_A)} \mathcal{E}(|e_i\rangle\langle e_j|)\langle e_j|\,A^T\,|e_i\rangle \\ &= \mathcal{E}\left(\sum_{i,j=1}^{\mathrm{Dim}(\mathcal{H}_A)} \langle e_i|A|e_j\rangle\,|e_i\rangle\langle e_j|\right) = \mathcal{E}(A).\end{aligned} \tag{2.48}$$

The Choi form does not have the property of respecting the product (composition). In particular for $\mathcal{E}_1 \in \mathcal{T}(\mathcal{H}_A, \mathcal{H}_B)$ and $\mathcal{E}_2 \in \mathcal{T}(\mathcal{H}_B, \mathcal{H}_C)$ the Choi forms live in completely different spaces: $J(\mathcal{E}_1) \in \mathcal{L}(\mathcal{H}_B \otimes \mathcal{H}_A)$, $J(\mathcal{E}_2) \in \mathcal{L}(\mathcal{H}_C \otimes \mathcal{H}_B)$ and $J(\mathcal{E}_2 \circ \mathcal{E}_1) \in \mathcal{L}(\mathcal{H}_C \otimes \mathcal{H}_A)$. The benefit is that in the Choi representation one can easily verify if a superoperator $\mathcal{E}$ is completely positive and/or trace-preserving by checking simple properties of $J(\mathcal{E})$. This is made precise in Theorem 2.5.5. The Choi form can also be used to evaluate inner products and this is shown in the following proposition.

Proposition 2.5.3 (Choi form evaluation of inner products)**.** *Let $\mathcal{E} \in \mathcal{T}(\mathcal{H}_A, \mathcal{H}_B)$ be a linear superoperator. Then for all $A \in \mathcal{L}(\mathcal{H}_A)$ and $B \in \mathcal{L}(\mathcal{H}_B)$, the following holds*

$$\langle B, \mathcal{E}(A)\rangle = \mathrm{Tr}\left[B^\dagger \mathcal{E}(A)\right] = \mathrm{Tr}\left[J(\mathcal{E})(B^\dagger \otimes A^T)\right]. \tag{2.49}$$

Proof. By direct computation, it follows that

$$\begin{aligned} \mathrm{Tr}\left[B^\dagger \mathcal{E}(A)\right] &= \mathrm{Tr}\left[B^\dagger \mathrm{Tr}_{\mathsf{A}}[J(\mathcal{E})(I_{\mathsf{B}} \otimes A^T)]\right] = \mathrm{Tr}\left[(B^\dagger \otimes I_{\mathsf{A}}) J(\mathcal{E})(I_{\mathsf{B}} \otimes A^T)\right] \\ &= \mathrm{Tr}\left[J(\mathcal{E})(I_{\mathsf{B}} \otimes A^T)(B^\dagger \otimes I_{\mathsf{A}})\right] = \mathrm{Tr}\left[J(\mathcal{E})(B^\dagger \otimes A^T)\right], \end{aligned} \tag{2.50}$$

by the cyclic property of the trace. ∎

Finally there are two different forms of presenting a superoperator that are mostly convenient in operational use. They provide an explicit way to apply the superoperator to a density operator in its domain and compute the resulting operator. One is the Kraus form. Let $\mathcal{E} \in \mathcal{T}(\mathcal{H}_{\mathsf{A}}, \mathcal{H}_{\mathsf{B}})$, then there exists an indexed set of operators $A_i, B_i \in \mathcal{L}(\mathcal{H}_{\mathsf{A}}, \mathcal{H}_{\mathsf{B}})$ such that $\mathcal{E}(X) = \sum_i A_i X B_i^\dagger$ for all $X \in \mathcal{L}(\mathcal{H}_{\mathsf{A}})$. This is called the Krauss form. The sets $\{A_i\}$ and $\{B_i\}$ are called the Krauss operators of $\mathcal{E}$. These are however not uniquely defined for any $\mathcal{E}$. Closely related is the Stinespring form, where $\mathcal{E} \in \mathcal{T}(\mathcal{H}_{\mathsf{A}}, \mathcal{H}_{\mathsf{B}})$ is represented by two Stinespring operators $A, B \in \mathcal{L}(\mathcal{H}_{\mathsf{A}}, \mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}})$ as $\mathcal{E}(X) = \mathrm{Tr}_{\mathcal{H}_{\mathsf{C}}}[AXB^\dagger]$ for all $X \in \mathcal{L}(\mathcal{H}_{\mathsf{A}})$. Here $\mathcal{H}_{\mathsf{C}}$ is some arbitrary Hilbert space.

Two theorems are presented characterizing the representations discussed. The first related all discussed forms and the second characterizes quantum channels in the different representations.

Theorem 2.5.4 (Equivalence of superoperator forms)**.** *Let $\mathcal{H}_{\mathsf{A}}$ and $\mathcal{H}_{\mathsf{B}}$ be complex Hilbert spaces and let $\{A_i\}_{i\in I}, \{B_i\}_{i\in I} \subset \mathcal{L}(\mathcal{H}_{\mathsf{A}}, \mathcal{H}_{\mathsf{B}})$ be indexed sets (with index set I) of linear operators. Finally let $\mathcal{E} \in \mathcal{T}(\mathcal{H}_{\mathsf{A}}, \mathcal{H}_{\mathsf{B}})$ be a linear superoperator. Then the following statements are equivalent:*

(1) $K(\mathcal{E}) = \sum_{i\in I} A_i \otimes B_i^T$ (natural representation);

(2) $J(\mathcal{E}) = \sum_{i\in I} \eta(A_i) \otimes \eta(B_i)^\dagger$ (Choi form);

(3) $\mathcal{E}(X) = \sum_{i\in I} A_i X B_i^\dagger$ for all $X \in \mathcal{L}(\mathcal{H}_{\mathsf{A}})$ (Kraus form);

(4) For $\mathcal{H}_{\mathsf{C}} = \mathrm{Span}\{e_i\}_{i\in I}$, define $A = \sum_{i\in I} A_i \otimes e_i$ and $B = \sum_{i\in I} B_i \otimes e_i$. Then $\mathcal{E}(X) = \mathrm{Tr}_{\mathcal{H}_{\mathsf{C}}}[AXB^\dagger]$ (Stinespring form).

Proof. See Proposition 2.20 of [21]. ∎

Theorem 2.5.5. *Let $\mathcal{H}_{\mathsf{A}}$ and $\mathcal{H}_{\mathsf{B}}$ be complex Hilbert spaces and let $\mathcal{E} \in \mathcal{T}(\mathcal{H}_{\mathsf{A}}, \mathcal{H}_{\mathsf{B}})$ be a linear superoperator. Then the following statements are equivalent:*

(1) $\mathcal{E}$ is a quantum channel, i.e. it is completely positive (CP) and trace-preserving (TP);

(2) $J(\mathcal{E}) \in \mathrm{Pos}(\mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{A}})$ (equivalent to CP) and $\mathrm{Tr}_{\mathcal{H}_{\mathsf{B}}} J(\mathcal{E}) = I_{\mathcal{H}_{\mathsf{A}}}$ (equivalent to TP);

(3) There exists a single indexed set $\{A_i\}_{i\in I} \subset \mathcal{L}(\mathcal{H}_{\mathsf{A}}, \mathcal{H}_{\mathsf{B}})$ such that $\mathcal{E}(X) = \sum_{i\in I} A_i X A_i^\dagger$ for all $X \in \mathcal{L}(\mathcal{H}_{\mathsf{A}})$ (equivalent to CP) and $\sum_{i\in I} A_i^\dagger A_i = I_{\mathcal{H}_{\mathsf{A}}}$ (equivalent to TP)

(4) There exists a complex Hilbert space $\mathcal{H}_{\mathsf{C}}$ and an isometry $U \in \mathcal{L}(\mathcal{H}_{\mathsf{A}}, \mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}})$ (i.e. $U^\dagger U = I_{\mathcal{H}_{\mathsf{A}}}$) such that $\mathcal{E}(X) = \mathrm{Tr}_{\mathcal{H}_{\mathsf{C}}}[UXU^\dagger]$ for all $X \in \mathcal{L}(\mathcal{H}_{\mathsf{A}})$.

Proof. See Theorems 2.22 and 2.26 of [21]. ∎

Now that the Choi form of a quantum channel is introduced and characterized by the above theorem, it can be applied to prove that the tensor product of quantum channels is also a quantum channel. Here the proof is constricted to channels mapping into the same space for notational purposes, but it can easily be generalized to arbitrary channels.

Proposition 2.5.6 (Tensor product of CPTP maps is CPTP)**.** *Let $\mathcal{E}_1, ..., \mathcal{E}_n \in \mathcal{S}(\mathcal{H})$ be a finite number of*

quantum channels (CPTP maps). Then $\mathcal{E} = \mathcal{E}_1 \otimes \cdots \otimes \mathcal{E}_n$ is also a quantum channel (on the space $\mathcal{H}^{\otimes n}$).

Proof. It suffices to this for $n = 2$, since it then holds for arbitrarily large, but finite n by repeated application. By Theorem 2.5.5 $\mathcal{E} = \mathcal{E}_1 \otimes \mathcal{E}_2$ is completely positive if and only if $J(\mathcal{E}) \geq 0$. Let $|i\rangle$ denote an orthonormal basis for $\mathcal{H}$. Then

$$\begin{aligned} J(\mathcal{E}_1 \otimes \mathcal{E}_2) &= \sum_{i,j,k,l=1}^{\mathrm{Dim}(\mathcal{H})} (\mathcal{E}_1 \otimes \mathcal{E}_2)(|i\rangle|k\rangle\langle j|\langle l|) \otimes |i\rangle|k\rangle\langle j|\langle l| \\ &= \sum_{i,j,k,l=1}^{\mathrm{Dim}(\mathcal{H})} \mathcal{E}_1(|i\rangle\langle j|) \otimes \mathcal{E}_2(|k\rangle\langle l|) \otimes |i\rangle\langle j| \otimes |k\rangle\langle l| \\ &= P\left(\sum_{i,j,k,l=1}^{\mathrm{Dim}(\mathcal{H})} \mathcal{E}_1(|i\rangle\langle j|) \otimes |i\rangle\langle j| \otimes \mathcal{E}_2(|k\rangle\langle l|) \otimes |k\rangle\langle l|\right) P^\dagger \\ &= P\left(\left[\sum_{i,j=1}^{\mathrm{Dim}(\mathcal{H})} \mathcal{E}_1(|i\rangle\langle j|) \otimes |i\rangle\langle j|\right] \otimes \left[\sum_{k,l=1}^{\mathrm{Dim}(\mathcal{H})} \mathcal{E}_2(|k\rangle\langle l|) \otimes |k\rangle\langle l|\right]\right) P^\dagger \\ &= P\left(J(\mathcal{E}_1) \otimes J(\mathcal{E}_2)\right) P^\dagger, \end{aligned} \tag{2.51}$$

where P is the permutation of basis in $\mathcal{H}^{\otimes 4}$ that swaps the second and third copy of the Hilbert space, defined by

$$P = \sum_{i,j,k,l=1}^{\mathrm{Dim}(\mathcal{H})} |i\rangle|k\rangle|j\rangle|l\rangle\langle i|\langle j|\langle k|\langle l|. \tag{2.52}$$

Now since $J(\mathcal{E}_1)$ and $J(\mathcal{E}_2)$ are positive semi-definite by Theorem 2.5.5, so is $J(\mathcal{E}_1) \otimes J(\mathcal{E}_2)$. And since similarity transforms (and in particular permutations) leave the eigenvalues invariant, $J(\mathcal{E}_1 \otimes \mathcal{E}_2)$ is also positive. Then again by Theorem 2.5.5, $\mathcal{E}_1 \otimes \mathcal{E}_2$ is completely positive. To show that $\mathcal{E}_1 \otimes \mathcal{E}_2$ is also trace preserving, let $X \in \mathcal{L}(\mathcal{H} \otimes \mathcal{H})$ and decompose it as $X = \sum_{i,j,k,l=1}^{\mathrm{Dim}(\mathcal{H})} x_{ijkl}|i\rangle|j\rangle\langle k|\langle l|$. Then

$$\begin{aligned} \mathrm{Tr}[(\mathcal{E}_1 \otimes \mathcal{E}_2)(X)] &= \sum_{i,j,k,l=1}^{\mathrm{Dim}(\mathcal{H})} x_{ijkl}\,\mathrm{Tr}[\mathcal{E}_1(|i\rangle\langle k|) \otimes \mathcal{E}_2(|j\rangle\langle l|)] \\ &= \sum_{i,j,k,l=1}^{\mathrm{Dim}(\mathcal{H})} x_{ijkl}\,\mathrm{Tr}[\mathcal{E}_1(|i\rangle\langle k|)]\,\mathrm{Tr}[\mathcal{E}_2(|j\rangle\langle l|)] \\ &= \sum_{i,j,k,l=1}^{\mathrm{Dim}(\mathcal{H})} x_{ijkl}\,\mathrm{Tr}[|i\rangle\langle k|]\,\mathrm{Tr}[|j\rangle\langle l|] \\ &= \sum_{i,j,k,l=1}^{\mathrm{Dim}(\mathcal{H})} x_{ijkl}\,\mathrm{Tr}[|i\rangle|j\rangle\langle k|\langle l|] = \mathrm{Tr}[X], \end{aligned} \tag{2.53}$$

Showing also that $\mathcal{E}_1 \otimes \mathcal{E}_2$ is trace-preserving. Therefore $\mathcal{E}_1 \otimes \mathcal{E}_2$ is CPTP (i.e. a quantum channel). ■

A quantum channel $\mathcal{E} \in \mathcal{S}(\mathcal{H})$, analogous to the definition for linear operators, is unitary if $\mathcal{E}^\dagger \circ \mathcal{E} = \mathcal{E} \circ \mathcal{E}^\dagger = \mathcal{I}$, where $\mathcal{I}$ is the identity superoperator on $\mathcal{L}(\mathcal{H})$. If there exists a unitary operator $U \in \mathcal{U}(\mathcal{H})$ such that a quantum channel has a Kraus form $\mathcal{E}(A) = UAU^\dagger$, then it is unitary, since $(\mathcal{E}^\dagger \circ \mathcal{E})(A) = U^\dagger(UAU^\dagger)U = A = \mathcal{I}(A)$ for any $A \in \mathcal{L}(\mathcal{H})$. In particular superoperator $\mathcal{E}(X) \in \mathcal{T}(\mathcal{H})$ with Kraus form $\mathcal{E}(A) = UAU^\dagger$ for some $U \in \mathcal{U}(\mathcal{H})$ is a (unitary) quantum channel by Theorem 2.5.5. Using Theorem 2.5.4 it has natural representation $K(\mathcal{E}) = U \otimes U^T$ and Choi representation $J(\mathcal{E}) = \eta(U) \otimes \eta(U)^\dagger$. So it is clear that, with every $U \in \mathcal{U}(\mathcal{H})$ a unitary superoperator can be associated, defined by $A \mapsto UAU^\dagger$. This operation is commonly referred to as conjugation. The symbol U shall also be used to identify the corresponding superoperator and the context will make clear whether U means the unitary operator or unitary superoperator. To make it clear from context which is meant, the superoperator is still applied with brackets and composition is still indicated with the $\circ$ symbol. As an example, let $U, V \in \mathcal{U}(\mathcal{H})$ and $\rho \in \mathcal{D}(\mathcal{H})$, then $(U \circ V)(\rho) = U(V\rho V^\dagger) = UV\rho V^\dagger U^\dagger$.

2.5.4. METRICS IN INFORMATION THEORY

This section addresses the questions 'how close are two quantum states?' and 'how close are two quantum channels?'. This section discusses some of the most common ways that these questions are addressed. However, it is by no means clear what the best answer is to these question. The underlying problem at heart is that typical distance measures like norms and induced metrics are not experimentally accessible, due to the inherent fact that measurements only provide partial information on a system. As a result, in the theoretical analysis of quantum information, typical distance measures like norms on the state space are used. On the other hand experiments and experimental protocols typically make statements about the fidelity between states, a quantity related to the measurable overlap between two quantum states. First a discussion is given about distinguishing two quantum states and next about the distinguishing quantum channels.

Suppose two quantum states are given, ρ and σ. Then naturally the question arises how close those two states are. In particular it is useful if this notion of 'distance' between two quantum states is a metric, such that it satisfies the natural axioms that are usually identified with distances. Therefore it seems natural to build distance metric from a norm on the space $\mathcal{L}(\mathcal{H})$. One frequently used metric based on this idea is the trace distance, which is build on the Schatten 1-norm on $\mathcal{L}(\mathcal{H})$.

Definition 2.5.11 (Trace distrance)**.** The trace distrance is a function $D : \mathcal{D}(\mathcal{H}) \times \mathcal{D}(\mathcal{H}) \to [0,1]$ given by $D(\rho,\sigma) := \frac{1}{2}\|\rho-\sigma\|_1 = \frac{1}{2}\operatorname{Tr}|\rho-\sigma|$, where $\|\cdot\|_1$ is the Schatten 1-norm (or Trace norm) on $\mathcal{L}(\mathcal{H})$. □

The factor $\frac{1}{2}$ is only introduced such that the distance between two quantum states is between 0 and 1. This follows from the triangle inequality, since $D(\rho,\sigma) = \frac{1}{2}\|\rho-\sigma\|_1 \leq \frac{1}{2}(\|\rho\|_1 + \|\sigma\|_1) = 1$, since $\|\rho\|_1 = \sum_i |\lambda_i| = \sum_i \lambda_i = \operatorname{Tr}[\rho] = 1$, by positivity of ρ and the requirement that it has trace 1. A trace distance one is attained for example if ρ and σ are pure states that are orthogonal (or more generally if they are convex combinations of pure states from orthogonal subspaces of $\mathcal{H}$).

The trace distance is unitarily invariant, i.e. $D(U\rho U^\dagger, U\sigma U^\dagger) = D(\rho,\sigma)$ for all $U \in \mathcal{U}(\mathcal{H})$. To see this, decompose $\rho-\sigma = \sum_i \lambda_i P_i$. Then $D(\rho,\sigma) = \frac{1}{2}\sum_i |\lambda_i|$. Using the decomposition then $U(\rho-\sigma)U^\dagger = \sum_i \lambda_i UPU^\dagger$. Now $UPU^\dagger$ is also an orthogonal projection, since

$$(UPU^\dagger)^2 = UPU^\dagger UPU^\dagger = UPPU^\dagger = UPU^\dagger$$

and $(UPU^\dagger)^\dagger = UPU^\dagger$. So in fact, $U(\rho-\sigma)U^\dagger = \sum_i \lambda_i UPU^\dagger$ is its spectral decomposition and

$$D(U\rho U^\dagger, U\sigma U^\dagger) = \sum_i |\lambda_i| = D(\rho,\sigma).$$

In the theorem below the trace distance is characterized more intuitively. The theorem states that the trace distance between two density matrices is exactly the maximum probability of distinguishing the two states by any POVM measurement. Unfortunately, this does not provide an experimental way to measure the trace distance between two quantum states.

Theorem 2.5.7. *Let $\rho,\sigma \in \mathcal{D}(\mathcal{H})$. Then $D(\rho,\sigma) = \max_{0\leq M\leq I} \operatorname{Tr}[M(\rho-\sigma)]$, where the maximization is over all positive semi-definite operators M, such that $I-M$ is also positive semi-definite.*

Proof. See Theorem 9.1 of [28]. ■

Finally, the trace distance is a useful measure on the set of density matrices since any CPTP quantum channel is contractive with respect to this measure (this is not the case for a distance based on any Schatten p-norm; see [30] for an excellent discussion on contractivity of superoperators). That is, after applying the channel to both states, their trace distance has not increased.

Theorem 2.5.8. *Let $\mathcal{E}$ be a CPTP map and $\rho,\sigma\in\mathcal{D}(\mathcal{H})$. Then $D(\mathcal{E}(\rho),\mathcal{E}(\sigma))\leq D(\rho,\sigma)$.*

Proof. See theorem 9.2 of [28] or Theorem 3.1 of [30]. ■

As discussed in the introduction of this section, there is no experimental procedure to access the trace distance. Therefore the fidelity is introduced, a quantity that is directly measurable. The fidelity quantifies the overlap between two states, i.e. the angle between the purifications of two density operators. First, the general definition is given.

Definition 2.5.12 (Fidelity)**.** Given two density matrices $\rho,\sigma\in\mathcal{D}(\mathcal{H})$, the fidelity between the states is defined as

$$F(\rho,\sigma):=\operatorname{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}=\left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1. \qquad \square$$

At first, this definition seems of little use. It is not even obvious that it is symmetric in its inputs. However, as will be shown in a moment, the fidelity has many properties that make it useful as a distance measure. This definition simplifies in the case that ρ is pure. Then

$$F(|\psi\rangle\langle\psi|,\sigma)=\operatorname{Tr}\sqrt{|\psi\rangle\langle\psi|\sigma|\psi\rangle\langle\psi|}=\sqrt{\langle\psi|\sigma|\psi\rangle}.$$

If in addition, σ is also pure, then $F(|\psi\rangle\langle\psi|,|\phi\rangle\langle\phi|)=\sqrt{\langle\psi|\phi\rangle\langle\phi|\psi\rangle}=|\langle\psi|\phi\rangle|$. Here it already appears that the fidelity is cosine of the angle between the states ϕ and ψ. Equivalently it can be interpreted as the square root of the probability of getting the outcome 1 associated with the measurement $Q=|\phi\rangle$ on the system ψ (or vice versa). These concepts are fundamental to the statistical interpretation of the theory of quantum mechanics. In light of this probabilistic interpretation, the quantity was originally defined as $F'(\rho,\sigma)=F^2(\rho,\sigma)$, i.e. as the square of the current (most frequently) used definition. This then has a direct statistical interpretation, but loses the geometrical interpretation of an angle. Unfortunately, both quantities are still in use and both are referred to as the fidelity.

The fidelity also takes values between 0 and 1, which follows from Hölder's inequality (Theorem 2.1.10):

$$0\leq F(\rho,\sigma)=\left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1\leq\left\|\sqrt{\rho}\right\|_2\left\|\sqrt{\sigma}\right\|_2=\sqrt{\sum_i\lambda_i(\sqrt{\rho})^2}\sqrt{\sum_i\lambda_i(\sqrt{\sigma})^2}=\sqrt{\sum_i\lambda_i(\rho)}\sqrt{\sum_i\lambda_i(\sigma)}=1,$$

due to the fact that $0\leq\lambda_i(\rho)\leq 1$ and $\sum_i\lambda_i(\rho)=1$ for all density matrices $\rho\in\mathcal{D}(\mathcal{H})$. In contrast to the trace distance however, $F(\rho,\rho)=1$. Therefore. the fidelity is not a metric. The fidelity can be turned into a metric via $A(\rho,\sigma):=\frac{2}{\pi}\arccos F(\rho,\sigma)$, although this is a rarely used metric.

Now the discussion is turned to the useful properties of the fidelity. It is also, just like the trace distance, unitarily invariant. This is the case since $\sqrt{U\rho U^\dagger}=U\sqrt{\rho}U^\dagger$, which follows from the spectral decomposition of ρ and the fact that $UPU^\dagger$ is also an orthogonal projection:

$$\begin{aligned}F(U\rho U^\dagger,U\sigma U^\dagger)&=\operatorname{Tr}\sqrt{U\sqrt{\rho}U^\dagger U\sigma U^\dagger U\sqrt{\rho}U^\dagger}=\operatorname{Tr}\sqrt{U\sqrt{\rho}\sigma\sqrt{\rho}U^\dagger}\\&=\operatorname{Tr}[U\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}U^\dagger]=\operatorname{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}=F(\rho,\sigma).\end{aligned}\tag{2.54}$$

An important characterization of the fidelity similar to Theorem 2.5.7 is given by Uhlmann's theorem.

Theorem 2.5.9 (Ulmann's theorem)**.** *Suppose $\rho,\sigma\in\mathcal{D}(\mathcal{H})$. Then*

$$F(\rho,\sigma)=\max_{\{|\psi\rangle,|\phi\rangle\in\mathcal{H}\otimes\mathcal{H}\}}|\langle\psi|\phi\rangle|,$$

where the maximization is over all purifications $|\psi\rangle$ of ρ and $|\phi\rangle$ of σ into $\mathcal{H}\otimes\mathcal{H}$.

Proof. See Theorem 9.4 of [28]. ■

From this theorem it is immediately clear that the fidelity is in fact symmetric. Also, it is related to the angle between the purifications. Similarly to the trace distance, the fidelity increases after application of a CPTP map. This is called the monotonicity of the fidelity.

Theorem 2.5.10. *Let $\mathcal{E}$ be a CPTP map and $\rho,\sigma \in \mathcal{D}(\mathcal{H})$. Then $F(\mathcal{E}(\rho),\mathcal{E}(\sigma) \geq F(\rho,\sigma)$.*

Proof. See Theorem 9.6 of [28]. ■

It seems like the trace distance and the fidelity satisfy similar properties that make it useful as a distance measure. As already discussed, the fidelity is of more experimental value. Unfortunately, it turns out to be really that to use the fidelity in proofs or use it to rigorously bound certain quantities. This is why in theoretical proofs, the trace distance is typically used. A natural question in this context then is how the two are related. This answer is provided in general by the Fuchs–Van de Graaf inequalities.

Theorem 2.5.11 (Fuchs-Van de Graaf inequalities)**.** *Let $\rho,\sigma \in \mathcal{D}(\mathcal{H})$ be two density matrices. Then*

$$1 - F(\rho,\sigma) \leq D(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)^2}. \tag{2.55}$$

Proof. See Theorem 3.33 of [21]. ■

Unfortunately, the relationship is nonlinear. This causes great difficulty in converting trace distance bounds into fidelity bounds.

Now the question is addressed how close two quantum channels $\mathcal{E}_1$ and $\mathcal{E}_2$ are. Again, there are norm based distances and fidelity based distances, with the similar trade-offs in theoretical rigidity and experimental accessibility. One frequently used norm is the pq-induced norm for $p = q = 1$, following the trace norm on the space of density matrices. This is often referred to as the induced trace norm on superoperators, and it should be noted that it is in fact not a Schatten 1-norm.

Definition 2.5.13 (Induced trace norm on superoperators)**.** Let $\mathcal{E} \in \mathcal{T}(\mathcal{H})$ be any superoperator. Then the induced trace norm on $\mathcal{T}(\mathcal{H})$ is the norm induced by the trace norm on $\mathcal{L}(\mathcal{H})$, defined by

$$\|\mathcal{E}\|_1 := \|\mathcal{E}\|_{1-1} = \sup_{A \in \mathcal{L}(\mathcal{H})} \{\|\mathcal{E}(A)\|_1 : \|A\|_1 \leq 1\} \qquad \square$$

The induced trace norm distance between two channels $\mathcal{E}_1,\mathcal{E}_2 \in \mathcal{T}(\mathcal{H})$ is then $\|\mathcal{E}_1 - \mathcal{E}_2\|_1$ (apparently without a factor $\frac{1}{2}$). This distance measure inherits some useful properties from the trace norm, but not all. It may seem like, just as in the case of the trace norm, it might have the physical interpretation of maximum discrimination between two channels. However, this turns out not to be the case (see [21] for a more elaborate discussion). The reason for this is that in general, one can prepare a state $\rho \in \mathcal{D}(\mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B})$ and let the two channels $\mathcal{E}_1 \otimes \mathcal{I}$ and $\mathcal{E}_2 \otimes \mathcal{I}$ act on the state and then perform an optimal measurement (on $\mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$) that discriminates between the output states $(\mathcal{E}_1 \otimes \mathcal{I})(\rho)$ and $(\mathcal{E}_1 \otimes \mathcal{I})(\rho)$. The point is that entanglement between the system of interest A and an auxiliary system B can help discriminate between the channels. In principle the dimension of $\mathcal{H}_\mathsf{B}$ can be unbounded, but it can be shown that $\mathrm{Dim}(\mathcal{H}_\mathsf{B}) > \mathrm{Dim}(\mathcal{H}_\mathsf{A})$ yields no further improvement in channel discrimination. In order to have a useful norm that has this interpretation, the diamond norm was introduced.

Definition 2.5.14. Let $\mathcal{E} \in \mathcal{T}(\mathcal{H})$ be a superoperator. Then the diamond norm is defined by

$$\|\mathcal{E}\|_\diamond := \|\mathcal{E} \otimes \mathcal{I}\|_1, \tag{2.56}$$

where $\mathcal{I}$ is the identity channel on $\mathcal{L}(\mathcal{H})$. □

This definition does turn out to satisfy this maximum discrimination property. Many other possible norms exists, but these are most commonly encountered in current literature.

The discussion is resumed with some fidelity related distance measures between superoperators. Again, there is even a wider range of possible quantities and only the few most commonly encountered are presented here. The most used is the so called average gate fidelity. It is defined as the fidelity between the output of two channels squared, averaged over all input states.

Definition 2.5.15 (Average gate fidelity)**.** Let $\mathcal{E}_1, \mathcal{E}_2 \in \mathcal{S}(\mathcal{H})$ be two quantum channels. Then the average gate fidelity between $\mathcal{E}_1$ and $\mathcal{E}_2$ is defined as

$$\overline{F}(\mathcal{E}_1, \mathcal{E}_2) = \int_{\{\psi \in \mathcal{H} : \|\psi\|_2 = 1\}} F(\mathcal{E}_1(\psi), \mathcal{E}_2(\psi))^2 \, \mathrm{d}\psi, \tag{2.57}$$

where with some abuse of notation $\mathcal{E}_1(\psi)$ is understood to mean $\mathcal{E}(|\psi\rangle\langle\psi|)$ and where $\mathrm{d}\psi$ is the normalized Haar measure on the set of normalized pure states $\{\psi \in \mathcal{H} : \|\psi\|_2 = 1\}$. Furthermore $\overline{F}(\mathcal{E})$ is understood to mean $\overline{F}(\mathcal{E}, \mathcal{I})$, where $\mathcal{I} \in \mathcal{S}(\mathcal{H})$ is the identity channel. □

First note that the average is only over pure states, which is sufficient since the set of density operators is convex, with pure states as its boundary. Also note that in this definition, as is common in literature (see [8] for example), the fidelity squared is used. Similar to the state fidelity, the evaluation simplifies is one of the channels is unitary, say $\mathcal{E}_2 = \mathcal{U}$. Then $F(\mathcal{E}_1(\psi), \mathcal{U}(\psi)) = F(\mathcal{U}^\dagger \circ \mathcal{E}_1, \mathcal{I}(\psi))$ and so $\overline{F}(\mathcal{E}_1, \mathcal{U}) = \overline{F}(\mathcal{U}^\dagger \circ \mathcal{E}_1)$. Now for any channel $\mathcal{E}$, $\overline{F}(\mathcal{E})$ is explicitly evaluated as

$$\overline{F}(\mathcal{E}) = \int_{\{\psi \in \mathcal{H} : \|\psi\|_2 = 1\}} F(\mathcal{E}(\psi), I(\psi))^2 \, \mathrm{d}\psi = \int_{\{\psi \in \mathcal{H} : \|\psi\|_2 = 1\}} \langle\psi|\mathcal{E}(\psi)|\psi\rangle \, \mathrm{d}\psi. \tag{2.58}$$

It has the interpretation of the average overlap between $|\psi\rangle\langle\psi|$ and $\mathcal{E}(|\psi\rangle\langle\psi|)$, averaged over pure states. The average gate fidelity is also unitarily invariant in the following sense.

Proposition 2.5.12 (Average gate fidelity is unitarily invariant)**.** *Let $\mathcal{E} \in \mathcal{S}(\mathcal{H})$ and $U \in \mathcal{U}(\mathcal{H})$. Then*

$$\overline{F}(\mathcal{E}) = \overline{F}(U^\dagger \circ \mathcal{E} \circ U). \tag{2.59}$$

Proof.

$$\begin{aligned}
\overline{F}(U^\dagger \circ \mathcal{E} \circ U) &= \int_{\{\psi \in \mathcal{H} : \|\psi\|_2 = 1\}} \langle\psi|(U^\dagger \circ \mathcal{E} \circ U)(\psi)|\psi\rangle \, \mathrm{d}\psi \\
&= \int_{\{\psi \in \mathcal{H} : \|\psi\|_2 = 1\}} \langle\psi|U\mathcal{E}\left(U^\dagger|\psi\rangle\langle\psi|U\right)U^\dagger|\psi\rangle \, \mathrm{d}\psi \\
&= \int_{\{\phi \in \mathcal{H} : \|\psi\|_2 = 1\}} \langle\phi|\mathcal{E}\left(|\phi\rangle\langle\phi|\right)|\phi\rangle \, \mathrm{d}\phi = \overline{F}(\mathcal{E}),
\end{aligned} \tag{2.60}$$

using the change of variables $\phi = U^\dagger\psi$ and the fact that the Haar measure is unitarily invariant ($\mathrm{d}\psi = \mathrm{d}\phi$). ■

3

PRELIMINARIES TO BENCHMARKING PROTOCOLS

This chapter provides a summary of more specialized prerequisite concepts directly related to randomized benchmarking protocols and introduces some of the important notation and definitions used throughout the rest of the thesis. Some topics in subsequent sections are connected and build upon each other. The goal is provide the reader with all the tools available in literature to understand the description and proof of randomized benchmarking type protocols. None of the topics covered here are new results, but most of them are outside the scope of main textbooks in the fields. The presentation of the topics is tailored to their application to benchmarking protocols.

3.1. CONCENTRATION INEQUALITIES IN STATISTICS

This section briefly discusses upper bounds for the probability that the empirical average of N independent and identically distributed random variables (denoted $\overline{X}$) deviates from its expectation value (denoted μ) by a certain amount $\epsilon > 0$. The results are due to Hoeffding [19]. The first bound only depends on N and ϵ, and in particular is independent of the variance.

Theorem 3.1.1 (Hoeffding's first inequality)**.** *Let $X_1, ..., X_N$ be N independent and identically distributed random variables with $a \leq X_i \leq b$ almost surely, where $a < b$, and with the expectation value satisfying $\mathbb{E}\left[\frac{X_i}{b-a}\right] = \mu$. Furthermore denote the empirical average $\overline{X} = \frac{1}{N}\sum_{i=1}^{N}\frac{X_i}{b-a}$. Then for $\epsilon > 0$*

$$\mathbb{P}\left[|\overline{X} - \mu| \geq \epsilon\right] \leq 2e^{-2N\epsilon^2}. \tag{3.1}$$

Proof. See [19]. ■

The second inequality also depends on the variance (denoted σ^2) of the distribution and is generally more stringent than the first. However, it requires a bound on σ^2.

Theorem 3.1.2 (Hoeffding's second inequality)**.** *Let $X_1, ..., X_N$ be N independent and identically distributed random variables with $a \leq X_i \leq b$ almost surely, where $a < b$, with the expectation value satisfying $\mathbb{E}\left[\frac{X_i}{b-a}\right] = \mu$ and with the variance satisfying $\mathbb{V}\left[\frac{X_i}{b-a}\right] = \sigma^2$. Furthermore denote the empirical average $\overline{X} = \frac{1}{N}\sum_{i=1}^{N}\frac{X_i}{b-a}$. Then for $0 < \epsilon < 1$*

$$\mathbb{P}\left[|\overline{X} - \mu| \geq \epsilon\right] \leq 2\left(\left(\frac{1}{1-\epsilon}\right)^{\frac{1-\epsilon}{\sigma^2+1}}\left(\frac{\sigma^2}{\sigma^2+\epsilon}\right)^{\frac{\sigma^2+\epsilon}{\sigma^2+1}}\right)^N. \tag{3.2}$$

Proof. See [19]. ■

3.2. TELESCOPING SERIES

In this section, the telescoping series for an associative algebra is presented [16]. Let us begin with the definition of an associative algebra.

Definition 3.2.1 (Associative algebra)**.** An associative algebra is a vector space A over $\mathbb{C}$ equipped with a bilinear map $A \times A \to A$, $(a, b) \mapsto ab$ (the product) such that $(ab)c = a(bc)$ for all $a, b, c \in A$ (associativity). If there exists a unit $1 \in A$ such that $1a = a1 = a$ for all $a \in A$, then A is an associative algebra with unit. □

For an element $a \in A$ of an algebra it is customary to denote a^m, $m \in \mathbb{N}$, as the m-fold product of the elements a and define $a^0 = 1$, where 1 is the unit. The telescoping series for an associative algebra with unit is given below.

Lemma 3.2.1 (Telescoping Series)**.** *Let A be an associative algebra with unit. Then for $a, b \in A$ and $m \in \mathbb{N}_+$,*

$$a^m - b^m = \sum_{j=1}^{m} a^{m-j}(a-b)b^{j-1}. \tag{3.3}$$

Proof. By direct computation, it follows that

$$\sum_{j=1}^{m} a^{m-j}(a-b)b^{j-1} = \sum_{j=1}^{m} a^{m-j+1}b^{j-1} - a^{m-j}b^{j} = \sum_{j=0}^{m-1} a^{m-j}b^{j} - \sum_{j=1}^{m} a^{m-j}b^{j}$$
$$= a^m b^0 - a^0 b^m = a^m - b^m. \qquad \blacksquare$$

3.3. SCHUR'S LEMMA IN ALTERNATE FORM

Here a restatement of Schur's Lemma (Theorem 2.3.4) is given. It is equivalent to the theorem presented in the previous chapter, but is of a form that is more applicable to randomized benchmarking. First, a lemma is presented that characterizes homomorphisms of representations.

Lemma 3.3.1. *Let (V,R) be a finite-dimensional unitary representation (over $\mathbb{C}$) of a finite group G, and let $\phi : V \to V$ be a linear map. Then ϕ is a homomorphism of representations if and only if it is of the form*

$$\phi = \frac{1}{|G|}\sum_{g\in G} R(g)AR(g)^\dagger \tag{3.4}$$

for some $A \in \mathcal{L}(V)$. Note that this form need not be unique.

Proof. First suppose ϕ is a homomorphism of representations. Then $\phi R(g) = R(g)\phi$, or equivalently $\phi = R(g)\phi R(g)^\dagger$ for all $g \in G$. Hence

$$\phi = \frac{1}{|G|}\sum_{g\in G}\phi = \frac{1}{|G|}\sum_{g\in G} R(g)\phi R(g)^\dagger,$$

which is of the above form with $A = \phi$. Conversely define for some $A \in \mathcal{L}(V)$ the map ϕ as in (3.4). Then for any $h \in G$ it follows that

$$\phi R(h) = \sum_{g\in G} R(g)AR(g)^\dagger R(h) = \sum_{g\in G} R(g)AR(g^{-1}h) = \sum_{k\in G} R(hk)AR(k^{-1}) = R(h)\phi, \tag{3.5}$$

where the change of variables $k = h^{-1}g$ is used by Cayley's Theorem, Theorem 2.2.3. Therefore ϕ is a homomorphism of representations. $\blacksquare$

Using Lemma 3.3.1 together with Lemma 2.3.2 and Machke's theorem (Theorem 2.3.3) a restatement of Schur's lemma (Theorem 2.3.4) is presented for finite-dimensional, unitary representations of a finite group G [31, 32].

Theorem 3.3.2 (Schur's Lemma, twirl form)**.** *Let G be a finite group and let $(\mathcal{H},R)$ be a finite-dimensional, unitary representation of G on the Hilbert space $\mathcal{H}$ with decomposition*

$$\mathcal{H} = \bigoplus_{i=1}^{p} \mathcal{H}_i^{\oplus n_i} \qquad \text{and} \qquad R = \bigoplus_{i=1}^{p} R_i^{\oplus n_i}$$

into irreducible and mutually inequivalent representations $(\mathcal{H}_i, R_i)$ which occur with multiplicity n_i. Let $\mathcal{B} = \{v_{i,k,l} | i = 1,...,\mathrm{Dim}(\mathcal{H}), k = 1,...,n_i, l = 1,...,\mathrm{Dim}(\mathcal{H}_i)\}$ be an orthonormal basis of $\mathcal{H}$ such that for fixed i and k, the subset $\mathcal{B}_{i,k} = \{v_{i,k,l} | l = 1,...,\mathrm{Dim}(\mathcal{H}_i)\}$ is an orthonormal basis of the subspace carrying the k-th copy of the i-th representation. Define the operators

$$P_{i,k,k'} := \sum_{l=1}^{\mathrm{Dim}(\mathcal{H}_i)} v_{i,k,l}(v_{i,k',l})^\dagger,$$

which in case that $k = k'$ are orthogonal projectors on k-th copy of the space $\mathcal{H}_i$ and otherwise are isomorphisms between the k-th copy and k'-th copy of $\mathcal{H}_i$ (for fixed i). Then for any $A \in \mathcal{L}(\mathcal{H})$,

$$\frac{1}{|G|}\sum_{g\in G} R(g)AR(g)^\dagger = \sum_{i=1}^{p}\left(\sum_{k,k'=1}^{n_i}\xi_{k,k'}P_{i,k,k'}\right), \tag{3.6}$$

where

$$\xi_{k,k'} = \frac{1}{\mathrm{Dim}(\mathcal{H}_i)}\mathrm{Tr}[AP^T_{i,k,k'}] = \frac{1}{\mathrm{Dim}(\mathcal{H}_i)}\sum_{j_i=1}^{\mathrm{Dim}(\mathcal{H}_i)}\langle v^{k_i}_{j_i}, Av^{k'}_{j_i}\rangle .$$

For notational convenience, define the $n_i \times n_i$ matrix $\xi_i := \left[\xi_{k,k'}\right]_{k,k'}$ for $i = 1,\ldots,p$.

Proof. First note that by Maschke's Theorem, the representation permits the stated decomposition into irreducible and mutually inequivalent representations. The left-hand-side of (3.6) is a homomorphism of representations by Lemma 3.3.1 and in fact all homomorphisms of representations are of this form. Now each space $\mathcal{H}_i$ carries (possibly multiple copies of) irreducible and mutually inequivalent representations, meaning that there does not exist an isomorphism between any pair of spaces $\mathcal{H}_i, \mathcal{H}_{i'}$ that is a homomorphism of representations, whenever $i \neq i'$. By Schur's Lemma then, the only homomorphism of representations between any pair of different spaces $\mathcal{H}_i$ is the trivial map $\phi = 0$. This is expressed on the right-hand-side by fact that the resulting operator is block diagonal with respect to the spaces $\mathcal{H}_i$, since it is the sum of isomorphisms only between (possibly different) copies of the i-th subspace $\mathcal{H}_i$. Between two copies k and k' of a single space $\mathcal{H}_i$ there exists isomorphisms, which in case $k = k'$ must be of the form $\phi = \xi_{k,k}P_{i,k,k}$ by Schur's Lemma and in case $k \neq k'$ may be chosen in the form $\xi_{k,k'}P_{i,k,k'}$. Note that $P_{i,k,k}$ is just the projector onto the k-th copy of $\mathcal{H}_i$ and is therefore the identity when restricted to this subspace. This proves the validity of (3.6).

In order to compute $\xi_{\hat{k},\hat{k}'}$, note that

$$P_{i,k,k'}P^T_{\hat{i},\hat{k},\hat{k}'} = \delta_{k'\hat{k}'}\delta_{i,\hat{i}}P_{i,k,\hat{k}'}.$$

Now multiply (3.6) from the right with $P^T_{\hat{i},\hat{k},\hat{k}'}$ and take the trace,

$$\begin{aligned}
\mathrm{Tr}\left[\frac{1}{|G|}\sum_{g\in G} R(g)AR(g)^\dagger P^T_{\hat{i},\hat{k},\hat{k}'}\right] &= \mathrm{Tr}\left[\sum_{i=1}^{p}\left(\sum_{k,k'=1}^{n_i}\xi_{k,k'}P_{i,k,k'}\right)P^T_{\hat{i},\hat{k},\hat{k}'}\right]\\
\frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}\left[R(g)AP^T_{\hat{i},\hat{k},\hat{k}'}R(g)^\dagger\right] &= \mathrm{Tr}\left[\sum_{i=1}^{p}\sum_{k,k'=1}^{n_i}\xi_{k,k'}\delta_{k'\hat{k}'}\delta_{i\hat{i}}P_{i,k,\hat{k}'}\right]\\
\frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}\left[R(g)^\dagger R(g)AP^T_{\hat{i},\hat{k},\hat{k}'}\right] &= \sum_{k=1}^{n_i}\xi_{k,\hat{k}'}\,\mathrm{Tr}\left[P_{\hat{i},k,\hat{k}'}\right]\\
\frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}\left[AP^T_{\hat{i},\hat{k},\hat{k}'}\right] &= \sum_{k=1}^{n_i}\xi_{k,\hat{k}'}\delta_{k\hat{k}}\,\mathrm{Dim}(\mathcal{H}_i)\\
\mathrm{Tr}\left[AP^T_{\hat{i},\hat{k},\hat{k}'}\right] &= \xi_{\hat{k},\hat{k}'}\,\mathrm{Dim}(\mathcal{H}_i),
\end{aligned} \tag{3.7}$$

from which $\xi_{\hat{k},\hat{k}'}$ is easily computed. In the second line it was used that $P^T_{\hat{i},\hat{k},\hat{k}'} = P_{\hat{i},\hat{k}',\hat{k}}$ is a homomorphism of representations, i.e. $P^T_{\hat{i},\hat{k},\hat{k}'}R(g) = R(g)P^T_{\hat{i},\hat{k},\hat{k}'}$ for all $g \in G$. ∎

3.4. THE PAULI MATRICES AND THE PAULI GROUP

The Pauli matrices and the Pauli group form a fundamental set of operators in quantum information and in particular in benchmarking protocols. In order to even understand the Clifford group, one

needs to first understand the Pauli group. In this thesis, both groups are limited to their respective multi-qubit cases, but work has been done [17] in generalizing this to arbitrary qudit systems.

The Pauli matrices are special in several ways. They are both unitary and hermitian, having eigenvalues ± 1 only. Furthermore, the Pauli matrices either commute or anti-commute. The multi-qubit Pauli group can be thought of as defined by their commutation relations. Here, the definition is just given in terms of their matrix representation.

Definition 3.4.1 (Set Pauli matrices)**.** The single-qubit Pauli matrices, elements of $\mathcal{L}(\mathbb{C}^2)$ are defined by

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3.8}$$

Denote $P_1 = \{X, Y, Z, I\}$ as the set of single-qubit Pauli matrices. Let $\mathcal{H} = \mathbb{C}^{2^q}$ be the state space of a q-qubit system. Then the set of q-qubit Pauli matrices $\mathcal{P}_q \subset \mathcal{L}(H)$ are defined as $\mathcal{P}_q := \{I, X, Y, Z\}^{\otimes q}$. Furthermore denote $\mathcal{P}_q^* := \mathcal{P}_q \backslash \{I^{\otimes q}\}$ as all non-identity Pauli matrices. Finally, define $\mathcal{Q}_q = 2^{-\frac{q}{2}} \mathcal{P}_q$ and $\mathcal{Q}_q^* = 2^{-\frac{q}{2}} \mathcal{P}_q^*$ as the same set of matrices, scaled by a factor $\frac{1}{\sqrt{2^q}}$. This scaling serves the purpose of being normalized in the Hilbert-Schmidt norm. For notational convenience, the subscript q is dropped when it is clear from the context. □

In the Liouville representation (see section 3.6), the normalized Pauli matrices form an operator basis of $\mathcal{L}(\mathcal{H})$ so therefore it is convenient that they are orthonormal (with respect to the Hilbert-Schmidt inner product). For that reason, the sets $\mathcal{Q}$ and $\mathcal{Q}^*$ have been introduced. In summary of this notation, $\mathcal{P}$ means regular Pauli matrices, $\mathcal{Q}$ means normalized counterpart and a superscript * is used to indicate the non-identity Pauli matrices from their respective sets. From here on out, the subscript q will be dropped to indicate that it concerns the set of (normalized) q-qubit Pauli matrices. For the set of (normalized) single-qubit Pauli's, the notation $\mathcal{P}_1$ or $\mathcal{Q}_1$ will be used to emphasize this. In the single-qubit case, all Pauli elements commute with themselves and with the identity, and anti-commute with the other two. This is easily verified by direct matrix multiplication. The commutation properties of the multi-qubit Pauli matrices are more difficult. Two lemma's regarding the commutation properties are presented.

Lemma 3.4.1 (Non-identity Pauli's commute with precisely half of all Pauli's)**.** *Let $\sigma \in \mathcal{P}^*$. Then σ commutes with precisely half of the elements of $\mathcal{P}$ and anti-commutes with the other half.*

Proof. Write $\sigma = \bigotimes_{j=1}^q \sigma_j$ and choose a k such that $\sigma_k \neq I$. Let $\tau_\nu \in \mathcal{P}$ and write it as $\tau_\nu = \bigotimes_{j=1}^q \tau_j$, such that τ_j can be any element of $\mathcal{P}_1$ for $j \neq k$, but fix $\tau_k = \nu$. Now either τ_I (that is, $\nu = I$) commutes or anti-commutes with σ. If it commutes with σ, then so does τ_ν for $\nu = \sigma_k$ and τ_ν will anti-commute with σ for $\nu \in \mathcal{P}_1^* \backslash \{\sigma_k\}$, and vice versa. This follows from the single-qubit commutation relations. Therefore, half of all elements $\tau \in \mathcal{P}$ commute with σ and half anti-commute. ■

Now that it is clear that half of the elements commute and the other half anti-commutes with every non-identity Pauli, one can ask the question if for each pair of different non-identity Pauli's, there exists a third that commutes with the one and anti-commutes with the other. The next lemma answers this question in the positive.

Lemma 3.4.2. *For all $\tau, \hat{\tau} \in \mathcal{P}^*$, such that $\tau \neq \hat{\tau}$, there exists a $\sigma \in \mathcal{P}^*$ such that*

$$\sigma\tau\sigma^\dagger = -\tau \quad \textit{and} \quad \sigma\hat{\tau}\sigma^\dagger = \hat{\tau}. \tag{3.9}$$

Proof. The proof is by induction on q. For $q = 1$, simply take $\sigma = \hat{\tau}$, since any element of $\mathcal{P}_1^*$ commutes only with itself and anti-commutes with all others from the set. Suppose, as the induction

hypothesis, that for all $\tau, \hat{\tau} \in \mathcal{P}_q^*$, $\tau \neq \hat{\tau}$, there exists a $\sigma \in \mathcal{P}_q^*$ such that $\sigma\tau\sigma^\dagger = -\tau$ and $\sigma\hat{\tau}\sigma^\dagger = \hat{\tau}$, for a certain q. To proof that is then also holds for $q+1$, pick a $\tau, \hat{\tau} \in \mathcal{P}_{q+1}^*$ such that $\tau \neq \hat{\tau}$ and write them as $\tau = \tau_q \otimes \tau_1$ and $\hat{\tau} = \hat{\tau}_q \otimes \hat{\tau}_1$, where $\tau_q, \hat{\tau}_q \in \mathcal{P}_q$ (including the identity) and $\tau_1, \hat{\tau}_1 \in \mathcal{P}_1$. There are five cases to distinguish:

1) $\tau_q, \hat{\tau}_q \in \mathcal{P}_q^*$ and $\tau_q \neq \hat{\tau}_q$. Then by the induction hypothesis there exists a $\sigma_q \in \mathcal{P}_q^*$ that anti-commutes τ_q and commutes $\hat{\tau}_q$. But then $\sigma := \sigma_q \otimes I$ anti-commutes with τ and commutes with $\hat{\tau}$.

2) $\tau_q, \hat{\tau}_q \in \mathcal{P}_q^*$ and $\tau_q = \hat{\tau}_q$. Then $\tau_1 \neq \hat{\tau}_1$. Note that either τ_1 or $\hat{\tau}_1$ may be the identity. By Lemma 3.4.1 there exists $\sigma_q^+ \in \mathcal{P}_q^*$ that commutes with $\tau = \hat{\tau}$ and a $\sigma_q^- \in \mathcal{P}_q^*$ that anti-commutes with $\tau = \hat{\tau}$. Now if $\tau_1 \neq I$ and $\hat{\tau}_1 \neq I$, then $\sigma = \sigma_q^+ \otimes \hat{\tau}_1$ satisfies the commutation properties of (3.9). If $\hat{\tau}_1 = I$, then pick any $\sigma_1 \in \mathcal{P}_1^* \setminus \{\tau_1\}$ so that $\sigma = \sigma_q^+ \otimes \sigma_1$ satisfies condition (3.9). Finally if $\tau_1 = I$, then pick any $\sigma_1 \in \mathcal{P}_1^* \setminus \{\hat{\tau}_1\}$ so that $\sigma = \sigma_q^- \otimes \sigma_1$ satisfies condition (3.9).

3) $\tau_q \in \mathcal{P}_q^*$ and $\hat{\tau}_q = I$. Then by Lemma 3.4.1, there exists an $\sigma_q \in \mathcal{P}_q^*$ that anti-commutes with τ_q. Since $\hat{\tau}_q = I$, σ_q also commutes with $\hat{\tau}_q$. Thus $\sigma = \sigma_q \otimes I$ satisfies (3.9).

4) $\hat{\tau}_q \in \mathcal{P}_q^*$ and $\tau_q = I$. Then $\tau_1 \neq I$. By Lemma 3.4.1 there exists $\sigma_q^+ \in \mathcal{P}_q^*$ that commutes with $\hat{\tau}$ and a $\sigma_q^- \in \mathcal{P}_q^*$ that anti-commutes with $\hat{\tau}$. Since $\tau = I$, both will commute with τ. Now if $\hat{\tau}_1 = \tau_1 \neq I$, then pick any $\sigma_1 \in \mathcal{P}_1^* \setminus \{\tau_1\}$ so that $\sigma = \sigma_q^- \otimes \sigma_1$ satisfies (3.9). If $\hat{\tau}_1 = I$ pick any $\sigma_1 \in \mathcal{P}_1^* \setminus \{\tau_1\}$ so that $\sigma = \sigma_q^+ \otimes \sigma_1$ satisfies (3.9). Finally if $\hat{\tau}_1 \in \mathcal{P}_1^* \setminus \{\tau_1\}$, then $\sigma = \sigma_q^+ \otimes \hat{\tau}$ satisfies (3.9).

5) $\tau_q = \hat{\tau}_q = I$. Then $\tau_1, \hat{\tau}_1 \in \mathcal{P}_1^*$ with $\tau_1 \neq \hat{\tau}_1$. Then $\sigma = I \otimes \hat{\tau}_1 \in \mathcal{P}_{q+1}^*$ satisfies (3.9) for τ and $\hat{\tau}$.

In all cases, an explicit $\sigma \in \mathcal{P}_{q+1}^*$ was constructed such that (3.9) was satisfied for arbitrary $\tau, \hat{\tau} \in \mathcal{P}_{q+1}^*$, completing the induction. ■

The set $\mathcal{P}$ does not form a group under matrix multiplication, since $XZ = -iY \notin \mathcal{P}_1$. To remedy this situation, one needs to add all multiples of $i^n\sigma$, $n = 1,2,3,4$, $\sigma \in \mathcal{P}$ of the Pauli's to the set. This closes the set under multiplication. The group is therefore defined as follows.

Definition 3.4.2 (Multi-qubit Pauli Group)**.** The multi-qubit Pauli group $\overline{\mathcal{P}}_q$ is defined as

$$\overline{\mathcal{P}}_q = \pm\mathcal{P}_q \cup \pm i\mathcal{P}_q, \tag{3.10}$$

making it a group under matrix multiplication. □

Note that $\mathcal{P}_q$ contains exactly one representative from the quotient group $\overline{\mathcal{P}}_q/\mathcal{U}(1)$ and are therefore isomorphic. However, to think of $\overline{\mathcal{P}}_q \cong \mathcal{P}_q/\mathcal{U}(1)$ as a group is not useful, since it disregards the commutation relations between the Pauli elements.

3.5. THE CLIFFORD GROUP

The Clifford group has first arisen in quantum information in the context of stabilizer codes and fault tolerant quantum computing [33, 34]. In this context, the group was (implicitly) defined by the set of generators $\{H_i, S_i, CNOT_{ij}\}$, where H_i and S_i are the gates H and S on qubit i and identity on the rest, whereas $CNOT_{ij}$ is a CNOT gate between qubit i and j with the identity on all others. These gates are explicitly given as

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}; \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}; \qquad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{3.11}$$

Even in this definition, it was realized that there was some connection between the Clifford group and the normalizer of the Pauli group in the unitary group. However, the normalizer is of infinite size, since the centralizer of the Pauli group in the unitary group is the set $\{e^{i\theta}I : \theta \in [0, 2\pi)\}$. Later, the Clifford group was then defined as the normalizer of the Pauli group in the unitary group, divided out to global phase, and each coset is given a representative with zero global phase [17, 18]. This is formalized in the definition below, that will be used in this thesis.

Definition 3.5.1 (Clifford group)**.** The (complex) Clifford group on q-qubits is defined by

$$\mathcal{C}_q = \{U \in \mathcal{U}(2^q) |\ U\sigma U^\dagger \in \overline{\mathcal{P}}_q \text{ for all } \sigma \in \overline{\mathcal{P}}_q\} / \mathcal{U}(1), \tag{3.12}$$

where $\mathcal{U}(d)$ denotes the unitary group of $d \times d$ unitary matrices over $\mathbb{C}$. Again the subscript q is dropped when clear from the context. □

The global phase may be ignored since U and $e^{i\phi}U$ conjugate a Pauli in the same way, and it is convenient to do so since it makes the Clifford group a finite group. This definition is slightly different that the generating definition above. To see this, note that $(HS)^3 = \alpha I$, with $\alpha = \frac{1+i}{\sqrt{2}} = e^{\frac{\pi i}{4}}$. Therefore the set generated by the Hadamard (H), phase (S) and CNOT gates is actually the set $\bigcup_{a=0}^{7} \alpha^a \mathcal{C}_q$, therefore containing 8 times as many elements. In [17] it was shown that H, S and $CNOT$ form a necessary and sufficient generating set for the Clifford group up to global phase for any q-qubit system (in fact they generalize it to arbitrary qudit systems), and they provide a constructive proof, showing how to decompose any Clifford into the product of its generators (up to global phase). That is to say

$$\mathcal{C}_q = \langle \{H_i, S_i, CNOT_{ij} | i, j = 1, ..., q, \quad i \neq j\} \rangle / \mathcal{U}(1). \tag{3.13}$$

Next it is of interest what the size of the Clifford group is, following Definition 3.5.1. From this definition, it is not even clear that it is finite. However, the discussion above about the generators of $\mathcal{C}$ made it clear that the group is finite, since it is finitely generated and each element has finite order ($H^2 = S^4 = I_2$ and $CNOT^2 = I_2 \otimes I_2 = I_4$). Clifford elements are defined to be unitary matrices that send Pauli matrices to Pauli matrices under conjugation. Conjugation must preserve the structure of the group $\overline{\mathcal{P}}$. Take two elements $\sigma, \tau \in \overline{\mathcal{P}}$ and $C \in \mathcal{C}$. Then $\sigma \mapsto C\sigma C^\dagger$ and $\tau \mapsto C\tau C^\dagger$. But the product is then respected under conjugation, since

$$\sigma\tau \mapsto C\sigma\tau C^\dagger = (C\sigma C^\dagger)(C\tau C^\dagger). \tag{3.14}$$

In particular, the identity Pauli I must be mapped to itself, since $I \mapsto CIC^\dagger = CC^\dagger = I$. Finally, by linearity, if it is defined where σ is sent under conjugation, then so is $i^n\sigma$, for $n = 1, 2, 3$. So, conjugation preserves the group structure and in particular preserves commutation and anti-commutation relations in $\overline{\mathcal{P}}$. Let us consider the single-qubit Clifford group $\mathcal{C}_1$. Taking all previous considerations into account, it is enough to know where X and Z are sent under conjugation by a Clifford element $C \in \mathcal{C}_1$. This is because then the images of iX and iZ are also determined and $\overline{\mathcal{P}}_1 = \langle \{X, Z, iX, iZ\} \rangle$. Because group structure is preserved, it is then determined where every Pauli is sent. This uniquely defined the Clifford element $C \in \mathcal{C}$, since global phase is divided out. In conclusion, there are 6 possible elements that X can be sent to under conjugation by $C \in \mathcal{C}_1$: $\pm X, \pm Y, \pm Z$. Now X can not be sent to iY for example, since then $X^2 = I$ must be sent to $(iY)^2 = -I$ under conjugation by C, which can not be done. Since X and Z anti-commute, so must their images under conjugation. Therefore Z can not be sent to $\pm CXC^\dagger$, leaving only 4 options remaining. Hence, $|\mathcal{C}_1| = 6 \cdot 4 = 24$.

This reasoning can be generalized to $\mathcal{C}_q$, yielding the following result [18].

Theorem 3.5.1 (Size of the Clifford group)**.** *Let $\mathcal{C}_q$ be the q-qubit Clifford group defined as in Defini-*

tion 3.5.1. Then

$$|\mathcal{C}_q| = \prod_{j=1}^{q} 2(4^j-1)4^j = 2^{q^2+2q}\prod_{j=1}^{q}(4^j-1) \leq 2^{q^2+2q}\prod_{j=1}^{q}4^j = 2^{2q^2+3q} \tag{3.15}$$

Proof. As discussed in the text above, conjugation respects the group structure, since for any $\sigma,\tau \in \overline{\mathcal{P}}$ one has $\sigma\tau \mapsto C\sigma\tau C^\dagger = (C\sigma C^\dagger)(C\tau C^\dagger)$. This is a restriction to all possible bijections on $\overline{\mathcal{P}}_q$. Denote $X_j \in \overline{\mathcal{P}}_q$ as the element with all identities and a X on qubit j. Explicitly, $X_j := I^{\otimes(j-1)} \otimes X \otimes I^{\otimes(q-j)}$, and define Z_j similarly. It is sufficient to know where all X_j and Z_j are sent under conjugation by $C \in \mathcal{C}_q$ to uniquely identify C, since $\overline{\mathcal{P}}_q = \langle \{X_j, Z_j, iX_j, iZ_j\}_{j=1}^q \rangle$. Of course, knowing where X_j is sent, also means knowing where iX_j is sent. Again X_j can not be sent to $i\sigma$, for any $\sigma \in \mathcal{P}_q$, since then $X_j^2 = I$ must be sent to $(i\sigma)^2 = -I$, which can not be done. Finally, X_j can not be sent to I, since I commutes with everything and X_j does not commute with Z_j. Also, I is already being sent to I and conjugation is a bijection from $\overline{\mathcal{P}}$ to itself. Thus, X_q can be sent to precisely every element of $\pm\mathcal{P}_q^*$. There are thus $|\pm\mathcal{P}_q^*| = 2(4^q-1)$ possibilities. Now Z_q can only go to elements that anti-commute with the image of X_q. By Lemma 3.4.1, X_q commutes with exactly half of the elements of $\mathcal{P}_q$ (including the identity) and anti-commutes with the other half. Therefore, there are $\frac{2|\mathcal{P}_q|}{2} = 4^q$ elements in $\pm\mathcal{P}_q^*$ where Z_q can be sent to that anti-commute with the image of X_q. Let $H_q := \{C \in \mathcal{C}_q : CX_qC^\dagger = X_q,\ CZ_qC^\dagger = Z_q\} \leq \mathcal{C}_q$ be the subgroup that leaves X_q and Z_q invariant. Then H_q is isomorphic to $\mathcal{C}_{q-1}$ (by just 'forgetting' about the final qubit) and H_q has precisely $2(4^q-1)\cdot 4^q$ cosets in $\mathcal{C}_q$. By Theorem 2.2.4 and $|H_q| = |\mathcal{C}_{q-1}|$ it then follows that $|\mathcal{C}_q| = 2(4^q-1)4^q|\mathcal{C}_{q-1}|$, yielding the conclusion. ■

Evaluating the above result, already yields $|\mathcal{C}_2| = 11520$ and $|\mathcal{C}_3| = 92897280$. The size of the Clifford group grows rapidly in the number of qubits, as $|\mathcal{C}_q| = 2^{\mathcal{O}(q^2)}$.

The Clifford group is a very important group in quantum information theory. Two important results will be given that serve to illustrate the importance of the Clifford group. The first is the fact that Clifford elements can be efficiently simulated on a classical computer. This is known as the Gottesman-Knill theorem [35] and is stated as follows.

Theorem 3.5.2 (Gottesman-Knill Theorem)**.** *A quantum circuit consisting only of the following elements can be simulated efficiently on a classical computer:*

1. *preparation of qubits in the computational basis;*
2. *quantum gates from the Clifford group $\mathcal{C}$;*
3. *measurements of qubits in the computational basis;*
4. *classical control based on measurement outcomes.*

Proof. See [35]. ■

For a more recent discussion of why this is so, the reader may refer to [17]. The main idea is that the set $\mathcal{P}_q$ (as a group via multiplication modulo global phase, which is then generated by X_i, Z_i) is isomorphic to a $2q$-dimensional vector space V over $\mathbb{Z}_2$ via the identification $Z \mapsto (0,1)$ and $X \mapsto (1,0)$. Since Clifford elements send Pauli's to Pauli's, they can be represented as permutations over this vector space V. Applying Clifford gates then just amounts to keeping track of where the basis vectors of V (corresponding to the generators X_i, Z_i) are sent (up to global phase). This is referred to as the sympletic representation of the Clifford group [17, 36]. This then requires only $\mathcal{O}(2q)$ recourses, instead of the $\mathcal{O}(2^q)$ required for the direct matrix multiplication. As a consequence of this sympletic representation, it is also computationally efficient to sample uniformly from the Clifford group, even though it is exponentially large is size. Also see [8] for an excellent discussion on this.

The second result is that, although the Clifford group is not sufficient for universal quantum computing, it is 'as close as it can get'. This will be made precise below. Universal quantum computing means that every possible quantum algorithm can be implemented from gates of the group to arbitrary precision (up to global phase). More precisely one says that a gate set W is a universal gate set if for all $\epsilon > 0$ and all $U \in \mathcal{U}(2^q)$, there exists a unitary operation $V \in \langle W \rangle$ such that $\|U - e^{i\phi}V\| < \epsilon$ for some global phase ϕ (in some norm that need specification). Ideally, the gate set W is small and consists of elements easily implemented in the lab. Furthermore one hopes that the operation V can be decomposed into products of elements from W efficiently (in time on a classical computer as well as in the number of gates in the decomposition for experimental application). Several gate sets that satisfy these properties are known, and the most important one is the set $W = \{H_i, T_i, CNOT_{ij}\}$ [23], where T_i is the T-gate on qubit i, defined by

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{\pi i}{4}} \end{bmatrix}. \tag{3.16}$$

Since $T^2 = S$, it is clear to see that $\langle \mathcal{C} \cup_i \{T_i\} \rangle = \langle W \rangle$. In [23] it is shown that this set W is universal, but it does not provide a means of compiling any unitary into the product of elements from W. This is provided by the Solovay-Kitaev theorem [37]. It states that any element $V \in \langle W \rangle$ that approximates the target unitary U to arbitrary precision $\epsilon > 0$ can be found in $\mathcal{O}(\log_c(\epsilon^{-1}))$ for some fixed constant c both in time and in number of gates. The proof is constructive and therefore provides an explicit way of doing the desired compilation. In a sense this means that "adding T to the Clifford group" results in an efficient, discrete universal gate set. This is what was meant by the statement that the Clifford group is 'almost' universal. This result can in fact be generalized to the following: For any gate $R \in \mathcal{U}(2^1) \backslash \mathcal{C}_1$, the gate set $W_R = \{H_i, S_i, CNOT_{ij}, R_i\}$ is a universal, discrete gate set [38]. However, this proof is very complicated and non-constructive, providing no means to decompose (let alone decompose efficiently). Therefore in practice $R = T$ is always chosen.

3.6. THE LIOUVILLE REPRESENTATION

In this section a particular form of the natural representation of quantum channels (see subsection 2.5.3), known as the Liouville representation, (Pauli) transfer matrix representation of affine representation, will be presented [15, 16] and some notation for it will be introduced. For simplicity of notation this section is restricted to quantum channels $\mathcal{E} \in \mathcal{S}(\mathcal{H})$, i.e. CPTP linear maps from $\mathcal{L}(\mathcal{H})$ into itself, but can be extended without any problem to CPTP maps from $\mathcal{L}(\mathcal{H}_\mathsf{A})$ to $\mathcal{L}(\mathcal{H}_\mathsf{B})$. For a q-qubit system, the underlying Hilbert space is of dimension $d = 2^q$. After introduction of the representation, it is applied to the Clifford group. This section contains some important results regarding the Liouville representation of the Clifford group and it is the foundation of most benchmarking protocols.

3.6.1. DEFINITION OF THE LIOUVILLE REPRESENTATION

Recall that the natural representation consists of picking a basis $\{E_i : i = 0, ..., d^2 - 1\}$ of $\mathcal{L}(\mathcal{H})$ that is orthonormal with respect to the Hilbert-Schmidt inner product $\langle E_i | E_j \rangle = \mathrm{Tr}[E_i^\dagger E_j] = \delta_{ij}$ and a mapping $\eta : \mathcal{L}(\mathcal{H}) \to \mathcal{H} \otimes \mathcal{H}$ defined by $E_i \mapsto |e_i\rangle$, where $\{|e_i\rangle\}$ is the an orthonormal basis of $\mathcal{H} \otimes \mathcal{H}$. A quantum channel $\mathcal{E} \in \mathcal{S}(\mathcal{H})$ then has the natural matrix representation in $\mathcal{L}(\mathcal{H} \otimes \mathcal{H})$ via $K : \mathcal{T}(\mathcal{H}) \to \mathcal{L}(\mathcal{H} \otimes \mathcal{H})$ defined by

$$\mathcal{E} \mapsto K(\mathcal{E}) = \sum_{i,j=0}^{d^2-1} \langle E_i | \mathcal{E}(E_j) \rangle \, \eta(E_i) \eta(E_j)^\dagger = \sum_{i,j=0}^{d^2-1} \langle E_i | \mathcal{E}(E_j) \rangle \, |e_i\rangle \langle e_i| \,. \tag{3.17}$$

This is all very similar to the matrix representation of linear operators on a Hilbert space. For that situation, the Dirac notation was introduced as a convenient way to represent vectors and matrices. The exact same thing can be done for the natural representation of quantum channels. Let us identify

$|\cdot\rangle\rangle : \mathcal{L}(\mathcal{H}) \to \mathcal{H}\otimes\mathcal{H}$ with the map η, then $|E_i\rangle\rangle = |e_i\rangle$. Also define $\langle\langle E_i| = |E_i\rangle\rangle^\dagger$. Any operator $A \in \mathcal{L}(\mathcal{H})$ can be expanded in the basis $\{E_i\}$ as $A = \sum_i \langle E_i|A\rangle |E_i\rangle\rangle$. Note that in this notation $\langle\langle A|B\rangle\rangle = \langle A|B\rangle = \mathrm{Tr}[A^\dagger B]$ for $A, B \in \mathcal{L}(\mathcal{H})$. Therefore the natural representation (3.17) can be expressed using this notation as

$$\boldsymbol{\mathcal{E}} := K(\mathcal{E}) = \sum_{i=0}^{d^2-1} |\mathcal{E}(E_i)\rangle\rangle\langle\langle E_i|, \tag{3.18}$$

where the boldface is used to distinguish the matrix representation from the actual abstract channel. As discussed in subsection 2.5.3, this representation will respect the action of vectorization (by the definition above), the product (composition), the adjoint and the tensor product. In equation form this becomes the following. For $\mathcal{E}_1, \mathcal{E}_2 \in \mathcal{T}(\mathcal{H})$, $A, B, Q \in \mathcal{L}(\mathcal{H})$

$$\begin{aligned}
&|\mathcal{E}_2 \circ \mathcal{E}_1(A)\rangle\rangle = \boldsymbol{\mathcal{E}_2}\,|\mathcal{E}_1(A)\rangle\rangle = \boldsymbol{\mathcal{E}_2}\boldsymbol{\mathcal{E}_1}\,|A\rangle\rangle,\\
&|\mathcal{E}_2 \otimes \mathcal{E}_1(A\otimes B)\rangle\rangle = \boldsymbol{\mathcal{E}_2}\otimes\boldsymbol{\mathcal{E}_1}\,|A\otimes B\rangle\rangle = \boldsymbol{\mathcal{E}_2}\otimes\boldsymbol{\mathcal{E}_1}\,|A\rangle\rangle\,|B\rangle\rangle = \boldsymbol{\mathcal{E}_2}\,|A\rangle\rangle \otimes \boldsymbol{\mathcal{E}_1}\,|B\rangle\rangle,\\
&|\mathcal{E}_1^\dagger(A)\rangle\rangle = \boldsymbol{\mathcal{E}_1}^\dagger\,|A\rangle\rangle\\
&\mathrm{Tr}[Q\mathcal{E}_1(A)] = \langle Q|\mathcal{E}_1(A)\rangle = \langle\langle Q|\boldsymbol{\mathcal{E}_1}|A\rangle\rangle,
\end{aligned} \tag{3.19}$$

where $|A\rangle\rangle\,|B\rangle\rangle$ is understood to mean $|A\rangle\rangle \otimes |B\rangle\rangle$. Note that the final expression is again ambiguous, inherited from the Dirac notation, since $\mathcal{E}_1$ is not necessarily hermitian. Typically $\langle\langle Q|\boldsymbol{\mathcal{E}_1}|A\rangle\rangle$ is understood to mean $\langle\langle Q|\,(\boldsymbol{\mathcal{E}_1}\,|A\rangle\rangle)$. When confusion may arise, the notation $\langle\langle Q|\mathcal{E}_1(A)\rangle\rangle = \langle Q|\mathcal{E}_1(A)\rangle$ is preferred, where the last inner product is just the Hilbert-Schmidt inner product. In case that $\mathcal{E}_1$ is hermitian, i. e. if $\langle\mathcal{E}_1(A)|B\rangle = \langle A|\mathcal{E}_1(B)\rangle$ for all $A, B \in \mathcal{L}(\mathcal{H})$, then there is no ambiguity in this notation.

In the previous section, the orthonormal basis of $\mathcal{L}(\mathcal{H})$ for the natural representation was implicitly chosen as the canonical basis, the basis identified with the outer product of the canonical basis of $\mathcal{H}$. A priori there is however no reason to choose that basis, and in the Liouville representation, a different basis is chosen, namely the normalized Pauli basis. The normalized Pauli basis is defined as follows.

Definition 3.6.1 (Normalized Pauli basis)**.** Let $\mathcal{H}$ be a Hilbert space of dimension $d = 2^q$. Then the normalized Pauli basis is an orthonormal basis of $\mathcal{L}(\mathcal{H})$ with respect to the Hilbert-Schmidt inner product, and is defined as $\mathcal{Q}_q := \{\sigma_0\} \cup \mathcal{Q}_q^*$, where

$$\begin{aligned}
\sigma_0 &= \frac{1}{\sqrt{d}} I_2^{\otimes q} = \frac{1}{\sqrt{d}} I_d,\\
\mathcal{Q}_q^* &= \frac{1}{\sqrt{d}} \{I_2, X, Y, Z\}^{\otimes q} \setminus \{\sigma_0\}.
\end{aligned} \tag{3.20}$$

In this definition I_n is the $n \times n$ identity matrix and X, Y, Z are the Pauli matrices, given by

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

For notational convenience, the subscript q is dropped when clear from the context. □

There are $4^q = 2^{2q} = d^2$ basis elements, which can easily be shown to be complete and mutually orthonormal. At this point, there is nothing special about σ_0 compared to the elements of $\mathcal{Q}_q^*$; this is at the moment just a notation that is already being set up for later purposes. However do note that σ_0 is proportional to the identity and the only element of the basis with non-vanishing trace. In fact $\langle\langle\sigma_0|A\rangle\rangle = \frac{\mathrm{Tr}[A]}{\sqrt{d}}$ for any $A \in \mathcal{L}(\mathcal{H})$, such that $\langle\langle\sigma_0|\rho\rangle\rangle = \frac{\mathrm{Tr}[\rho]}{\sqrt{d}} = \frac{1}{\sqrt{d}}$ for all $\rho \in \mathcal{D}(\mathcal{H})$.

Next, two basic properties of the Liouville representation will be discussed for trace preserving and positive channels. The first property is that if the channel is trace preserving then the top row of the Liouville matrix satisfies $\boldsymbol{\mathcal{E}}_{0j} = \delta_{0j}$. The second proposition establishes that if the channel is positive, then the entries of the Liouville matrix are real and between -1 and 1.

Proposition 3.6.1. *Let $\mathcal{E} \in \mathcal{T}(\mathcal{H})$ be a superoperator and denote $d = \mathrm{Dim}(\mathcal{H})$. Then the following statements hold for the corresponding Liouville matrix $\boldsymbol{\mathcal{E}}$:*

(1) $\mathcal{E}$ is trace preserving if and only if $\boldsymbol{\mathcal{E}}_{0j} = \delta_{0j}$ for all $j = 0, ..., d^2-1$;

(2) If $\mathcal{E}$ is positive, then $\boldsymbol{\mathcal{E}}_{ij} \in \mathbb{R}$;

(3) If $\mathcal{E}$ is completely positive and trace preserving, then $-1 \leq \boldsymbol{\mathcal{E}}_{ij} \leq 1$ for all $i, j = 0, ..., d^2-1$.

Proof. (1). Let us start by computing the top row of $\boldsymbol{\mathcal{E}}$.

$$\begin{aligned} \boldsymbol{\mathcal{E}}_{00} &= \langle\langle \sigma_0 | \boldsymbol{\mathcal{E}} | \sigma_0 \rangle\rangle = \mathrm{Tr}[\frac{I}{\sqrt{d}} \mathcal{E}(\sigma_0)] = \frac{\mathrm{Tr}[\mathcal{E}(\sigma_0)]}{\sqrt{d}} = \frac{\mathrm{Tr}[\mathcal{E}(I)]}{d}, \\ \boldsymbol{\mathcal{E}}_{0j} &= \langle\langle \sigma_0 | \boldsymbol{\mathcal{E}} | \tau \rangle\rangle = \mathrm{Tr}[\frac{I}{\sqrt{d}} \mathcal{E}(\tau)] = \frac{\mathrm{Tr}[\mathcal{E}(\tau)]}{\sqrt{d}}, \quad \forall \tau \in \mathcal{Q}^* \ (j = 1, ..., d^2-1). \end{aligned} \tag{3.21}$$

Now if $\mathcal{E}$ is trace preserving, then $\boldsymbol{\mathcal{E}}_{00} = \frac{\mathrm{Tr}[\mathcal{E}(I)]}{d} = \frac{\mathrm{Tr}[I]}{d} = 1$ and $\boldsymbol{\mathcal{E}}_{0j} = \frac{\mathrm{Tr}[\mathcal{E}(\tau)]}{\sqrt{d}} = \frac{\mathrm{Tr}[\tau]}{\sqrt{d}} = 0$ for all $\tau \in \mathcal{Q}^*$ or $j = 1, ..., d^2-1$. On the other hand, if $\boldsymbol{\mathcal{E}}_{0j} = \delta_{0j}$, then $\mathrm{Tr}[\mathcal{E}(\sigma_0)] = \sqrt{d} = \mathrm{Tr}[\sigma_0]$ and $\mathrm{Tr}[\mathcal{E}(\tau)] = 0 = \mathrm{Tr}[\tau]$ for all $\tau \in \mathcal{Q}^*$ or $j = 1, ..., d^2-1$. Since $\mathcal{Q}$ is a basis for $\mathcal{L}(\mathcal{H})$, one can express any $A \in \mathcal{L}(\mathcal{H})$ as $A = \sum_{j=0}^{d^2-1} a_j \sigma_j$. Then

$$\mathrm{Tr}[\mathcal{E}(A)] = \mathrm{Tr}\left[\mathcal{E}\left(\sum_{j=0}^{d^2-1} a_j \sigma_j\right)\right] = \sum_{j=0}^{d^2-1} a_j \mathrm{Tr}[\mathcal{E}(\sigma_j)] = \sum_{j=0}^{d^2-1} a_j \mathrm{Tr}[\sigma_j] = \mathrm{Tr}\left[\sum_{j=0}^{d^2-1} a_j \sigma_j\right] = \mathrm{Tr}[A],$$

so $\mathcal{E}$ is trace preserving.
(2). If $\mathcal{E}$ is positive, then it maps hermitian operators to hermitian operators. To see this, write $A = A^\dagger \in \mathrm{Herm}(\mathcal{H})$ and use the spectral theorem to decompose it as $A = \sum_i \lambda_i P_i$. Then $(\mathcal{E}(A))^\dagger = \sum_i \lambda_i^* (\mathcal{E}(P_i))^\dagger = \sum_i \lambda_i \mathcal{E}(P_i) = \mathcal{E}(A)$, since $\lambda_i \in \mathbb{R}$ because of the fact that A is hermitian and $\mathcal{E}(P_i) \in \mathrm{Pos}(\mathcal{H}) \subset \mathrm{Herm}(\mathcal{H})$ by positivity of $\mathcal{E}$. In particular, this means that $(\mathcal{E}(\sigma))^\dagger = \mathcal{E}(\sigma)$ for all $\sigma \in \mathcal{Q}$, since $\sigma = \sigma^\dagger$. Therefore it follows that

$$\langle\langle \sigma | \mathcal{E} | \tau \rangle\rangle^* = \langle \sigma | \mathcal{E}(\tau) \rangle^* = \langle \mathcal{E}(\tau) | \sigma \rangle = \mathrm{Tr}[\mathcal{E}(\tau)^\dagger \sigma] = \mathrm{Tr}[\sigma \mathcal{E}(\tau)^\dagger] = \mathrm{Tr}[\sigma^\dagger \mathcal{E}(\tau)] = \langle\langle \sigma | \mathcal{E} | \tau \rangle\rangle,$$

meaning that $\boldsymbol{\mathcal{E}}_{ij} = \langle\langle \sigma | \mathcal{E} | \tau \rangle\rangle \in \mathbb{R}$.
(3). By Proposition 2.5.3, one has that $\boldsymbol{\mathcal{E}}_{ij} = \langle\langle \sigma | \mathcal{E} | \tau \rangle\rangle = \mathrm{Tr}[J(\mathcal{E})(\sigma \otimes \tau^T)]$. Since $\mathcal{E}$ is CPTP, Theorem 2.5.5 implies that $J(\mathcal{E}) \geq 0$ and $\mathrm{Tr}[J(\mathcal{E})] = d$. Furthermore $-\sigma_0 \otimes \sigma_0 \preceq \sigma \otimes \tau^T \preceq \sigma_0 \otimes \sigma_0$. Equivalently, $\sigma_0 \otimes \sigma_0 \pm \sigma \otimes \tau^T \geq 0$. By Proposition 2.1.5, for any two positive semi-definite matrices $A, B \geq 0$ it holds that $\langle A | B \rangle \geq 0$. Using this it follows that

$$\mathrm{Tr}[J(\mathcal{E})(\sigma_0 \otimes \sigma_0 \pm \sigma \otimes \tau^T)] = \langle J(\mathcal{E}) | \sigma_0 \otimes \sigma_0 \pm \sigma \otimes \tau^T \rangle \geq 0$$

This is equivalent to

$$\pm \mathrm{Tr}[J(\mathcal{E})(\sigma \otimes \tau^T)] \leq \mathrm{Tr}[J(\mathcal{E})(\sigma_0 \otimes \sigma_0)] = \mathrm{Tr}[J(\mathcal{E}) \frac{I}{d}] = 1,$$

yielding the result. ∎

Item (1) of the above proposition is sometimes written slightly differently. Suppose $\mathcal{E}$ is a trace preserving map. Now defining the vector $\alpha(\mathcal{E})$ with entries $[\alpha(\mathcal{E})]_\tau = \langle\langle \tau | \boldsymbol{\mathcal{E}} | \sigma_0 \rangle\rangle$, the Liouville representation of $\mathcal{E}$ can be written as

$$\boldsymbol{\mathcal{E}} = \begin{bmatrix} 1 & 0 \\ \alpha(\mathcal{E}) & \boldsymbol{\mathcal{E}}_{\mathrm{u}} \end{bmatrix}, \tag{3.22}$$

where $\boldsymbol{\mathcal{E}}_{\mathrm{u}}$ is referred to as the unital block. This directly follows from item (1) of the proposition. Often in the analysis of benchmarking protocols, the quantity $\|\alpha(\mathcal{E})\|^2$ is encountered, where $\|\cdot\|$

denotes the Euclidean norm (2-norm). This quantity, known as the nonunitality of a superoperator $\mathcal{E}$, then equals (assuming $\mathcal{E}$ is positive, so that the entries of $\alpha(\mathcal{E})$ are real)

$$\|\alpha(\mathcal{E})\|^2 = \sum_{\tau\in\mathcal{Q}^*} \langle\langle\tau|\mathcal{E}|\sigma_0\rangle\rangle^2. \tag{3.23}$$

Finally a simple lemma is presented that is frequently used in the analysis of benchmarking protocols.

Lemma 3.6.2. *Let $\mathcal{E}_1, \mathcal{E}_2 \in \mathcal{T}(\mathcal{H})$ be any superoperator and $A_1, A_2, B_1, B_2 \in \mathcal{L}(\mathcal{H})$. Then*

$$\langle\langle A_1\otimes A_2|\boldsymbol{\mathcal{E}_1}\otimes\boldsymbol{\mathcal{E}_2}|B_1\otimes B_2\rangle\rangle = \langle\langle A_1|\boldsymbol{\mathcal{E}_1}|B_1\rangle\rangle\langle\langle A_2|\boldsymbol{\mathcal{E}_2}|B_2\rangle\rangle. \tag{3.24}$$

Proof.

$$\begin{aligned}
\langle\langle A_1\otimes A_2|\boldsymbol{\mathcal{E}_1}\otimes\boldsymbol{\mathcal{E}_2}|B_1\otimes B_2\rangle\rangle &= \mathrm{Tr}[(A_1\otimes A_2)((\mathcal{E}_1\otimes\mathcal{E}_2)(B_1\otimes B_2))]\\
&= \mathrm{Tr}[(A_1\otimes A_2)(\mathcal{E}_1(B_1)\otimes\mathcal{E}_2(B_2))]\\
&= \mathrm{Tr}[(A_1\mathcal{E}_1(B_1))\otimes(A_2\mathcal{E}_2(B_2))]\\
&= \mathrm{Tr}[A_1\mathcal{E}_1(B_1)]\,\mathrm{Tr}[A_2\mathcal{E}_2(B_2)]\\
&= \langle\langle A_1|\boldsymbol{\mathcal{E}_1}|B_1\rangle\rangle\langle\langle A_2|\boldsymbol{\mathcal{E}_2}|B_2\rangle\rangle.
\end{aligned}$$

■

3.6.2. THE LIOUVILLE REPRESENTATION OF THE CLIFFORD GROUP

In this section, the Liouville representation of the Clifford group is discussed. The first result is to decompose this representation into irreducible ones. Next, something is said about tensor powers of the Liouville representation. These notions are building blocks for benchmarking protocols over the Clifford group.

Theorem 3.6.3 (Liouville representation of the Clifford Group)**.** *Let $\mathcal{C}\subset\mathcal{U}(\mathcal{H})$ be the Clifford group, acting on the d-dimensional Hilbert space $\mathcal{H}$, with $d = 2^q$ and $\mathcal{Q}$ be the normalized Pauli matrices. Let $V = \mathrm{Span}\{|\sigma\rangle\rangle : \sigma\in\mathcal{Q}\}$ and $R : \mathcal{U}\to\mathcal{L}(V)$ given by $U\mapsto\mathbf{U}$. Then (V,R) is indeed a representation in the sense of Definition 2.3.1 and $V = V_{\mathrm{id}}\oplus V_{\mathrm{adj}}$ is its decomposition into irreducible and inequivalent representations, where $V_{\mathrm{id}} := \mathrm{Span}\{|\sigma_0\rangle\rangle\}$ and $V_{\mathrm{adj}} = V_{\mathrm{id}}^{\perp} = \mathrm{Span}\{|\sigma\rangle\rangle : \sigma\in\mathcal{Q}^*\}$.*

Proof. (V,R) is a formal representation, since $R(I) = \mathbf{I}$ is in fact the identity on V and $R(AB) = \mathbf{AB} = R(A)R(B)$ for $A, B\in\mathcal{C}$. To see that V_{id} is a subrepresentation, note that all Cliffords leave $|\sigma_0\rangle\rangle$ invariant, since $\mathbf{C}|\sigma_0\rangle\rangle = |C(\sigma_0)\rangle\rangle = |C\sigma_0C^\dagger\rangle\rangle = |\frac{1}{\sqrt{d}}CIC^\dagger\rangle\rangle = |\frac{I}{\sqrt{d}}\rangle\rangle = |\sigma_0\rangle\rangle$ for all $C\in\mathcal{C}$. Because $\mathrm{Dim}(V_{\mathrm{id}}) = 1$ it must be irreducible.

By Maschke's theorem V_{adj} is also a subrepresentation. The main effort of this proof is showing that it is irreducible. First, let us note that $\mathcal{P}\subset\mathcal{C}$, since for all $\sigma,\tau\in\mathcal{P}$ one has $\sigma\tau\sigma^\dagger = \pm\tau$, because Pauli's either commute or anti-commute. Moreover this means that the Liouville representation of any $\sigma\in\mathcal{P}$, $\boldsymbol{\sigma}$, is diagonal in the normalized Pauli basis $\mathcal{Q}$ (that is $\boldsymbol{\sigma}|\tau\rangle\rangle = \pm|\tau\rangle\rangle$ for all $\sigma\in\mathcal{P}$ and all $\tau\in\mathcal{Q}$), with entries ±1. As a result, the representations commute! That is for all $\sigma,\hat{\sigma}\in\mathcal{P}$ it holds that $\boldsymbol{\sigma}\hat{\boldsymbol{\sigma}} = \hat{\boldsymbol{\sigma}}\boldsymbol{\sigma}$.

Now suppose $W\subseteq V_{\mathrm{adj}}$ is an irreducible subrepresentation and let P_W denote the orthogonal projection onto W. Then $\mathbf{C}P_W = P_W\mathbf{C}$ for all $C\in\mathcal{C}$. So in particular P_W commutes with every element of $\boldsymbol{\mathcal{P}^*} := \{\boldsymbol{\sigma} : \sigma\in\mathcal{P}^*\subset\mathcal{C}\}$ and therefore must also be diagonal in the same basis $\mathcal{Q}^*$. Lemma 3.4.2 shows that for all $\tau,\hat{\tau}\in\mathcal{Q}^*$ satisfying $\tau\neq\hat{\tau}$, there exists an $\sigma\in\mathcal{P}^*$ such that $\boldsymbol{\sigma}|\tau\rangle\rangle = -|\tau\rangle\rangle$ and $\boldsymbol{\sigma}|\hat{\tau}\rangle\rangle = |\hat{\tau}\rangle\rangle$. Therefore the set $\boldsymbol{\mathcal{P}^*}$ of $4^q-1 = d^2-1$ Liouville operators is a complete set of commuting operators on V_{adj}, meaning if ones specifies an eigenvalue (±1) for each operator in $\boldsymbol{\mathcal{P}^*}$ this uniquely defines a

simultaneous eigenvector $|\tau\rangle\rangle \in \mathcal{Q}^*$. Therefore $\mathcal{Q}^*$ is the only basis that simultaneously diagonalizes all elements of $\boldsymbol{\mathcal{P}^*}$. Since P_W commutes with all elements of $\boldsymbol{\mathcal{P}^*}$, it is diagonal in the basis $\mathcal{Q}^*$. As a consequence of this result, the space W must be of the form $W = \mathrm{Span}\, S$ for some subset $S \subseteq \mathcal{Q}^*$. To illustrate this, suppose that a linear combination of elements $|v\rangle\rangle = \alpha|\tau\rangle\rangle + \beta|\hat{\tau}\rangle\rangle$, with $\tau, \hat{\tau} \in \mathcal{Q}^*$ and $\alpha, \beta \in \mathbb{C}$ is in W. Then there exists a $\sigma \in \mathcal{P}^* \subset \mathcal{C}$ such that $|v'\rangle\rangle = \boldsymbol{\sigma}|v\rangle\rangle = \alpha|\tau\rangle\rangle - \beta|\hat{\tau}\rangle\rangle$ is also in W. Since $\mathrm{Span}\{|v\rangle\rangle, |v'\rangle\rangle\} = \mathrm{Span}\{|\tau\rangle\rangle, |\hat{\tau}\rangle\rangle\}$, W must be of the claimed form.

By the definition of the Clifford group as the normalizers of the Pauli group in the unitary group, one has for all $\tau \in \mathcal{Q}^*$ and all $C \in \mathcal{C}$ that $\mathbf{C}|\tau\rangle\rangle = |\hat{\tau}\rangle\rangle$ for some $\hat{\tau} \in \mathcal{Q}^*$. Moving $\mathbf{C}$ over to the other side yields $|\tau\rangle\rangle = \mathbf{C}^\dagger|\hat{\tau}\rangle\rangle$, showing that for all τ there exists an Clifford element $C^\dagger \in \mathcal{C}$ and a $\hat{\tau} \in \mathcal{Q}^*$ that sends a basis function $\hat{\tau}$ to τ under conjugation. Therefore $V_{\mathrm{adj}} = W$ is irreducible. Finally since $\mathrm{Dim}(V_{\mathrm{adj}}) = |\mathcal{Q}^*| = 4^q - 1 > 1 = \mathrm{Dim}(V_{\mathrm{id}})$ for all $q = 1, 2, \ldots$, the two representations are inequivalent. ■

In the analysis of various benchmarking protocols, higher tensor powers of the Liouville representations are encountered. In general however, it is not easy to find the irreducible subrepresentations of a representation $\varphi^{\otimes n}$ given the irreducible subrepresentations of φ, even for the simplest case of $n = 2$. The study of tensor power representations of the Clifford group has been done very recently, and is connected to the concept of unitary t-designs [39, 40]. Only recently, the full characterization of the tensor-2 Liouville representation has been found [41]. The full result is not quoted here, but some intermediate results along the way are presented. First of all, Lemma 2.3.8 can be applied to find the trivial subrepresentations of the tensor-2 Liouville representation. Since the Liouville representation decomposes into two inequivalent irreducible subrepresentations, there are two trivial subrepresentations present in the tensor-2 Liouville representations.

Proposition 3.6.4 (Trivial subreps of Liouville tensor-2)**.** *Let (V, R) be the Liouville representation of the Clifford group $\mathcal{C}$ (i.e. $\varphi(C) = \mathbf{C}$ for $C \in \mathcal{C}$) on the space $V = \mathrm{Span}\{|\sigma\rangle\rangle : \sigma \in \mathcal{Q}\}$. Then the tensor-2 Liouville representation $R^{\otimes 2}$ has two trivial subrepresentations (on $V \otimes V$) spanned by*

$$|\sigma_0 \otimes \sigma_0\rangle\rangle \quad \textit{and} \quad \sum_{\sigma \in \mathcal{Q}^*} |\sigma \otimes \sigma\rangle\rangle, \tag{3.25}$$

respectively.

Proof. In Theorem 3.6.3 it was shown that V decomposes into irreducible representations as $V = V_{\mathrm{id}} \oplus V_{\mathrm{adj}}$, where $V_{\mathrm{id}} = \mathrm{Span}\{|\sigma_0\rangle\rangle\}$ and $V_{\mathrm{adj}} = \mathrm{Span}\{|\sigma\rangle\rangle : \sigma \in \mathcal{Q}^*\}$. The task is now to find the trivial subspaces of

$$V \otimes V = (V_{\mathrm{id}} \otimes V_{\mathrm{id}}) \oplus (V_{\mathrm{id}} \otimes V_{\mathrm{adj}}) \oplus (V_{\mathrm{adj}} \otimes V_{\mathrm{id}}) \oplus (V_{\mathrm{adj}} \otimes V_{\mathrm{adj}}).$$

The first space in this decomposition is of dimension 1, so therefore

$$V_{\mathrm{id}} \otimes V_{\mathrm{id}} = \mathrm{Span}\{|\sigma_0 \otimes \sigma_0\rangle\rangle\}$$

is a trivial subrepresentation of $R^{\otimes 2}$. The second and third spaces are equivalent to V_{adj} via the identification $\sigma \mapsto \sigma_0 \otimes \sigma$ and $\sigma \mapsto \sigma \otimes \sigma_0$ respectively. Since V_{adj} is irreducible and of dimension greater than one, it does not contribute any trivial subrepresentations. Now the subrepresentation on $(V_{\mathrm{adj}} \otimes V_{\mathrm{adj}})$ is reducible, and it is not easy to find all of its irreducible subrepresentations. However, there is one and only one trivial subrepresentation present and it is easily found using Lemma 2.3.8, using the fact that (V, R) is a real-valued representation (Proposition 3.6.1) so that $V^* \cong V$, yielding the second trivial subrepresentation

$$\mathrm{Span}\{\sum_{\sigma \in \mathcal{Q}^*} |\sigma \otimes \sigma\rangle\rangle\} \subset V_{\mathrm{adj}} \otimes V_{\mathrm{adj}}.$$

It can also be seen that these are all trivial subrepresentation by considering the character inner product $\langle \chi_{V \otimes V}, \chi_1 \rangle = \langle \chi_V, \chi_V \rangle = \sum_i n_i^2 = 1^2 + 1^2 = 2$. ■

Furthermore there has been work done in finding the value of the character inner product $\langle \chi_{R^{\otimes 2}}, \chi_{R^{\otimes 2}} \rangle$, which provides information on the decomposition of $V^{\otimes 2}$ by Theorem 2.3.7.

Lemma 3.6.5. *Let (V, R) be the Liouville representation of the q-qubit Clifford group $\mathcal{C}$. Then*

$$\langle \chi_{R^{\otimes 2}}, \chi_{R^{\otimes 2}} \rangle = \begin{cases} 15, & \text{if } q = 1, \\ 29, & \text{if } q = 2, \\ 30, & \text{if } q \geq 3. \end{cases} \tag{3.26}$$

Proof. See [39]. ■

The full characterization of the Liouville tensor-2 representation $(V \otimes V, R^{\otimes 2})$ has been carried out in [41] for all qubit systems. The single-qubit results are quoted as needed.

3.7. DEPOLARIZING CHANNEL

In this section the depolarizing channel is defined and some of its most basic properties are discussed. A depolarizing channel is a particular CPTP quantum channel that only depends on a single parameter. It is defined as follows.

Definition 3.7.1 (Depolarizing channel)**.** A depolarizing channel $\Theta_f \in \mathcal{S}(\mathcal{H})$ is a quantum channel, characterized by a single parameter $f \in [-\frac{1}{d-1}, 1]$, defined by

$$\Theta_f(X) := fX + (1-f)\,\mathrm{Tr}[X]\frac{I}{d}, \tag{3.27}$$

for all $X \in \mathcal{L}(\mathcal{H})$, where $I \in \mathcal{L}(\mathcal{H})$ is the identity on $\mathcal{H}$ and d is the dimension of $\mathcal{H}$. □

It is easily verified that this channel is trace preserving (for any f). The restriction $f \in [-\frac{1}{d-1}, 1]$ is to ensure the complete positivity of the channel. Usually, quantum channels are applied to density operators $\rho \in \mathcal{D}(\mathcal{H})$, satisfying $\mathrm{Tr}[\rho] = 1$. The first lemma states that the m-fold composition of a depolarizing channel is also a depolarizing channel, and it gives its depolarizing parameter.

Lemma 3.7.1 (m-fold composition of depolarizing channel is depolarizing)**.** *Let Θ_f be a depolarizing channel and $m \in \mathbb{N}_+$. Then for any $\rho \in \mathcal{D}(\mathcal{H})$*

$$\bigcirc_{s=1}^{m} \Theta_f(\rho) = \Theta_{f^m}(\rho). \tag{3.28}$$

Proof. The proof is by induction to m. For $m = 1$ the statement is trivial. Suppose that $\bigcirc_{s=1}^{k} \Theta_f = \Theta_{f^k}$ for some integer k. Then

$$\begin{aligned} \left(\bigcirc_{s=1}^{k+1} \Theta_f\right)(\rho) &= \Theta_f\left(\bigcirc_{s=1}^{k} \Theta_f(\rho)\right) = \Theta_f\left(\Theta_{f^k}(\rho)\right) \\ &= \Theta_f\left(f^k\rho + (1-f^k)\frac{I}{d}\right) = f^k\Theta_f(\rho) + (1-f^k)\Theta_f\left(\frac{I}{d}\right) \\ &= f^k[f\rho + (1-f)\frac{I}{d}] + (1-f^k)\frac{I}{d} = f^{k+1}\rho + \left[f^k(1-f) + (1-f^k)\right]\frac{I}{d} \\ &= f^{k+1}\rho + (1-f^{k+1})\frac{I}{d} = \Theta_{f^{k+1}}(\rho), \end{aligned} \tag{3.29}$$

using the fact that $\Theta_f\left(\frac{I}{d}\right) = \frac{I}{d}$. This proves the lemma by induction to m. ■

The second lemma relates the depolarizing parameter to the average gate fidelity.

Lemma 3.7.2. *Let $\Theta_f \in \mathcal{S}(\mathcal{H})$ be a depolarizing channel. Then $\overline{F}(\Theta_f) = f + \frac{1-f}{d}$, where d is the dimension of $\mathcal{H}$.*

Proof.

$$\begin{aligned}\overline{F}(\Theta_f) &= \int_{\{\psi\in\mathcal{H}:\|\psi\|_2=1\}} \langle\psi|\Theta_f(|\psi\rangle\langle\psi|)|\psi\rangle \, \mathrm{d}\psi \\ &= \int_{\{\psi\in\mathcal{H}:\|\psi\|_2=1\}} f\langle\psi|\psi\rangle\langle\psi|\psi\rangle + (1-f)\langle\psi|\frac{I}{d}|\psi\rangle \, \mathrm{d}\psi \\ &= \left(f + \frac{1-f}{d}\right)\int_{\{\psi\in\mathcal{H}:\|\psi\|_2=1\}} \mathrm{d}\psi = f + \frac{1-f}{d}.\end{aligned}$$

■

Finally, the Liouville representation of a depolarizing channel is given.

Lemma 3.7.3. *Let Θ_f be a depolarizing channel. Then is has Liouville representation*

$$\boldsymbol{\Theta}_f = |\sigma_0\rangle\rangle\langle\langle\sigma_0| + f\sum_{\tau\in\boldsymbol{\sigma}_q} |\tau\rangle\rangle\langle\langle\tau|. \tag{3.30}$$

Proof. Let us pick an arbitrary $\rho \in \mathcal{D}(\mathcal{H})$. Then in Louiville representation

$$|\rho\rangle\rangle = |\sigma_0\rangle\rangle\langle\langle\sigma_0|\rho\rangle\rangle + \sum_{\tau\in\sigma_q} |\tau\rangle\rangle\langle\langle\tau|\rho\rangle\rangle \tag{3.31}$$

so that

$$\begin{aligned}\boldsymbol{\Theta}_f|\rho\rangle\rangle &= |\sigma_0\rangle\rangle\langle\langle\sigma_0|\rho\rangle\rangle + f\sum_{\tau\in\boldsymbol{\sigma}_q} |\tau\rangle\rangle\langle\langle\tau|\rho\rangle\rangle \\ &= |\sigma_0\rangle\rangle\langle\langle\sigma_0|\rho\rangle\rangle + f|\rho\rangle\rangle - f|\sigma_0\rangle\rangle\langle\langle\sigma_0|\rho\rangle\rangle \\ &= (1-f)|\sigma_0\rangle\rangle\langle\langle\sigma_0|\rho\rangle\rangle + f|\rho\rangle\rangle \\ &= |\frac{1-f}{d}I + f\rho\rangle\rangle = |\Theta_f(\rho)\rangle\rangle,\end{aligned} \tag{3.32}$$

using the fact that $|\sigma_0\rangle\rangle\langle\langle\sigma_0|\rho\rangle\rangle = \frac{1}{\sqrt{d}}|\sigma_0\rangle\rangle = |\frac{I}{d}\rangle\rangle$, proving the claim. ■

3.8. TWIRLING OVER THE CLIFFORD GROUP

In this section, twirling over a quantum channel is introduced. The definition is given for general, finite subgroups of the unitary group. It can easily be extended to infinite groups such as $\mathcal{U}(d)$. For a complete discussion of twirling, the reader may refer to [31, 42, 43]. The twirl of a quantum channel is defined as follows

Definition 3.8.1 (Twirl over a finite group)**.** Let G be a finite-dimensional subgroup of $\mathcal{U}(\mathcal{H})$, the group of unitary operators on $\mathcal{H}$ under composition, (that is $G \leq \mathcal{U}(\mathcal{H}) \leq \mathcal{GL}(\mathcal{H}) \subset \mathcal{L}(\mathcal{H})$) and let $\Lambda \in \mathcal{S}(\mathcal{H})$ be a quantum channel. Then the twirl over G is a map $T_G : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H})$ given by

$$T_G(\Lambda(\rho)) := \frac{1}{|G|}\sum_{g\in G} g\Lambda(g^\dagger\rho g)g^\dagger. \tag{3.33}$$

for all $\rho \in \mathcal{D}(\mathcal{H})$. When no confusion can arise, the notation $\Lambda_T = T_G(\Lambda)$ is adopted for notational clarity. Identifying with each $U \in \mathcal{U}(\mathcal{H})$ the unitary superoperator $U \in \mathcal{S}(\mathcal{H})$ given by $U : X \mapsto UXU^\dagger$, the definition can equivalently by written as

$$T_G(\Lambda) := \frac{1}{|G|}\sum_{g\in G} g\circ\Lambda\circ g^\dagger. \tag{3.34}$$

This second form is usually more convenient since it omits the use of an argument and is notationally more clear. □

As a first result, it is shown that twirling over a group leaves the average gate fidelity invariant [23].

Lemma 3.8.1 (Twirling leaves average gate fidelity invariant)**.** *Let $\Lambda \in \mathcal{S}(\mathcal{H})$ and $G \leq \mathcal{U}(\mathcal{H})$ be a finite group. Then $\overline{F}(\Lambda) = \overline{F}(\Lambda_T)$.*

Proof.

$$\begin{aligned}
\overline{F}(\Lambda_T) &= \int \mathrm{d}\psi \, \langle\psi| \frac{1}{|G|} \sum_{g\in G} g\Lambda(g^\dagger|\psi\rangle \langle\psi| g) g^\dagger |\psi\rangle \\
&= \frac{1}{|G|} \sum_{g\in G} \int \mathrm{d}\psi \, \langle\psi| g\Lambda(g^\dagger|\psi\rangle \langle\psi| g) g^\dagger |\psi\rangle \\
&= \frac{1}{|G|} \sum_{g\in G} \int \mathrm{d}\phi \, \langle\phi|\Lambda(|\phi\rangle \langle\phi|)|\phi\rangle \\
&= \frac{1}{|G|} \sum_{g\in G} \int \mathrm{d}\phi \, \langle\phi|\Lambda(|\phi\rangle \langle\phi|)|\phi\rangle \\
&= \frac{1}{|G|} \sum_{g\in G} \overline{F}(\Lambda) = \overline{F}(\Lambda),
\end{aligned} \tag{3.35}$$

where in the third line the change of variables $|\phi\rangle = g^\dagger|\psi\rangle$ is used together with the fact that the Haar measure on the state space is unitarily invariant ($\mathrm{d}\psi = \mathrm{d}(U\psi)$ for any unitary U). ■

The main result, on which randomized benchmarking is based, shows that $T_{\mathcal{C}}(\Lambda) = \Theta_f$ for some $f \in [-\frac{1}{d+1}, 1]$ that depends on the channel Λ. By Lemma 3.8.1 and Lemma 3.7.2 then, $\overline{F}(\Lambda) = \overline{F}(\Theta_f) = f + \frac{1-f}{d}$, where d is the dimension of the underlying Hilbert space $\mathcal{H}$. Hence, if an experimental procedure exists to twirl over the Clifford group and obtain a value for f, the associated depolarizing channel, then the average gate fidelity of the average error map Λ associated with the Clifford group can be computed.

The proof given below makes use of the Liouville representation. The statement is then representation theoretical, and the proof follows by applying Schur's Lemma. In order to do so, the irreducible representations of the Liouville representation is needed. Alternative proofs exist, usually constructed on the concept of a unitary 2-design. In order not to obscure the result, this route is avoided here, but first some historical context will be given. In [23] it was first shown that the twirl over the unitary group $\mathcal{U}(\mathcal{H})$ produces a depolarizing channel, with the same average gate fidelity. That is, it shows that

$$T_{\mathcal{U}}(\Lambda) := \int \mathrm{d}U U \circ \Lambda \circ U^\dagger = \Theta_f, \tag{3.36}$$

where the integral is over the uniform Haar measure on $\mathcal{U}(\mathcal{H})$, and furthermore that $\overline{F}(T_{\mathcal{U}}(\Lambda)) = \overline{F}(\Lambda)$ (the proof of this goes identical to the proof of Lemma 3.8.1). Then [5] showed that this provides a scalable protocol to estimate the average gate fidelity of Λ^{avg}, the Haar-averaged error map over the unitaries. Drawbacks at the time were the fact that decomposition of a unitary was not known to be efficient in the number of 1- and 2-qubit gates, as well as sampling uniformly according to the Haar measure and inverting. Then [43] was the first to generally proof that the Clifford group is a unitary 2-design, which is defined to be a group $G \leq \mathcal{U}(\mathcal{H})$ such that

$$T_{\mathcal{U}}(\Lambda) = \int \mathrm{d}U U \circ \Lambda \circ U^\dagger = \frac{1}{|G|} \sum_{g\in G} g \circ \Lambda \circ g^\dagger = T_G(\Lambda). \tag{3.37}$$

Alternative, but equivalent definitions for a unitary 2-design exist, as well as generalizations to unitary t-designs. A good summary of this is given in [42, 43]. Since uniform sampling and inverting in the Clifford group can be efficiently done by using the sympletic representation, it was realized that this provides a fully scalable benchmarking procedure. Finally [7, 8] was the first to provide an explicit protocol together with a full analysis, expanding to the case of gate and time dependent error channels which deviate only a little from the average Λ.

As discussed above, the underlying theorem of randomized benchmarking ($T_{\mathcal{C}}(\Lambda) = \Theta_f$) was historically worked out it different steps and using different proving techniques, neither of which depended on representation theory. Here, a more direct approach is taken based on [31]. In order to do so, the irreducible subrepresentation of the Liouville representation of the Clifford group are needed.

Finally all the lemma's have been discussed in order to prove the main result.

Theorem 3.8.2 (Twirl of a quantum channel over $\mathcal{C}$ is depolarizing)**.** *Let $\Lambda \in \mathcal{S}(\mathcal{H})$ be a quantum channel and $\mathcal{C}$ be the Clifford group over the Hilbert space $\mathcal{H}$. Then the twirl of Λ over $\mathcal{C}$ is a depolarizing channel,*

$$\Lambda_T = \frac{1}{|\mathcal{C}|} \sum_{C \in \mathcal{C}} C \circ \Lambda \circ C^\dagger = \Theta_f \tag{3.38}$$

for some f depending on Λ.

Proof. The idea of the proof is to write this in Liouville representation and characterize the irreducible subrepresentations such that Schur's Lemma in the form of Theorem 3.3.2 can be applied to obtain the result. In Liouville representation, (3.38) becomes

$$\mathbf{\Lambda}_T = \frac{1}{|\mathcal{C}_q|} \sum_{C \in \mathcal{C}_q} \mathbf{C}\mathbf{\Lambda}\mathbf{C}^\dagger = |\sigma_0\rangle\rangle\langle\langle\sigma_0| + f \sum_{\tau \in \mathcal{Q}_q^*} |\tau\rangle\rangle\langle\langle\tau| = \mathbf{\Theta}_f. \tag{3.39}$$

Let $V = \mathrm{Span}\{|\sigma\rangle\rangle : \sigma \in \mathcal{Q}\}$ and $R : \mathcal{C} \to \mathcal{L}(V)$ given by $C \mapsto \mathbf{C}$. Then (V, R) is a representation and decomposes into irreducible and inequivalent representations as $V = V_{\mathrm{id}} \oplus V_{\mathrm{adj}}$, where $V_{\mathrm{id}} = \mathrm{Span}\{\sigma_0\}$ and $V_{\mathrm{adj}} = \mathrm{Span}\,\mathcal{Q}^*$ by Theorem 3.6.3. By Schur's Lemma (Theorem 3.3.2) then

$$\mathbf{\Lambda}_T = \frac{1}{|\mathcal{C}_q|} \sum_{C \in \mathcal{C}_q} \mathbf{C}\mathbf{\Lambda}\mathbf{C}^\dagger = \xi_{\mathrm{id}} P_{V_{\mathrm{id}}} + \xi_{\mathrm{adj}} P_{V_{\mathrm{adj}}} = \xi_{\mathrm{id}} |\sigma_0\rangle\rangle\langle\langle\sigma_0| + \xi_{\mathrm{adj}} \sum_{\tau \in \mathcal{Q}_q^*} |\tau\rangle\rangle\langle\langle\tau|, \tag{3.40}$$

where $\xi_{\mathrm{id}} = \mathrm{Tr}[\mathbf{\Lambda}\,|\sigma_0\rangle\rangle\langle\langle\sigma_0|] = \langle\langle\sigma_0|\Lambda(\sigma_0)\rangle\rangle = 1$, since Λ is trace preserving and $\sigma_0 = \frac{I}{\sqrt{d}}$, and where $\xi_{\mathrm{adj}} = \sum_{\tau \in \mathcal{Q}_q^*} \langle\langle\tau|\Lambda(\tau)\rangle\rangle =: f(\Lambda)$ is some parameter depending on Λ. Therefore the conclusion that $\mathbf{\Lambda}_T = \mathbf{\Theta}_f$ follows.

■

4

REVIEW OF BENCHMARKING PROTOCOLS

This chapter reviews three benchmarking protocols that I have studied in the course of this thesis. These protocols have been developed over the last ten years and are now important experimental tools for estimating gate errors independent of state preparation and measurement errors in an efficient and scalable manner. Most of this chapter closely follows important literature on the protocols, but slight modifications and different nuances have been made. The purpose of this chapter is twofold. Firstly it shows the protocols we have studied in order to understand the statistical analyses of randomized benchmarking that have been performed previously. Secondly it sets a foundation to build on, providing the necessary understanding for the statistical analysis of unitarity randomized benchmarking in the next chapter.

4.1. INTRODUCTION

This chapter reviews some of the current literature on randomized benchmarking protocols. In particular it aims to set up a framework for the statistical analysis of the unitarity randomized benchmarking protocol in chapter 5. In order to do so, the standard randomized benchmarking protocol is reviewed first in section 4.2. This section provides a complete description of the protocol as well as a proof of why the protocol works, under the assumption of a gate and time independent error model. This model can be extended using gate and time dependent perturbations, as is done in [8]. The assumption of gate and time independence may not be very realistic, but it is made here since it is a required assumption in the thorough analysis of the number of random sequences needed to perform the protocol [16]. Furthermore, the analysis is restricted to the Clifford group, even though the proof shows that it works for any finite subgroup of the unitary group, that is a unitary 2-design [8]. The restriction to the Clifford group is again done since the statistical analysis of [16] is specific to the Clifford group only. The results of this analysis are briefly summarized.

The goal of this thesis, as stated in chapter 1, is to perform similar statistical analysis for protocols related to randomized benchmarking. Interleaved randomized benchmarking, as discussed in section 4.3, is such a related protocol. The review in this section is based on the original proposal of [8, 44] and provides a description of the protocol as well as a proof of how it works. Furthermore the section reviews how various other authors improved upon the original proposition of this protocol [45, 46], summarizing for the first time an optimal estimation procedure for this protocol in one place. Finally it is argued that the statistical analysis of randomized benchmarking as done in [16] can be directly applied to the interleaved randomized benchmarking protocol.

In the last section, section 4.4, the unitarity randomized benchmarking protocol is reviewed. This section is based on [13], although some slight modifications are proposed here. The goal of this section is to introduce the reader to the protocol and give a proof of why it works as claimed. Extra emphasis is put on two different implementations of the protocol, which differ both in scalability in the number of qubits as well as in their statistical analysis. Finally a first order concentration inequality is applied to put a preliminary bound on the number of sequences needed in this protocol. Throughout the section and the rest of this thesis, the presentation of the unitarity randomized benchmarking protocol is done under the assumption of gate and time independent errors. The protocol is also presented using the Clifford group. The reasons for this is that our statistical analysis, similar to that of [16], is carried out under these assumptions. In contrast to randomized benchmarking however, the unitarity randomized benchmarking protocol has never been analyzed for the more general gate and/or time dependent error model yet.

4.2. RANDOMIZED BENCHMARKING

In this section, the randomized benchmarking (RB) protocol on the Clifford group is presented under the assumption of gate and time independent errors. The analysis follows closely the original paper [8], but here the analysis is restricted to gate and time independent errors. The paper also treats the gate and time dependent error scenario by perturbation around the average. Furthermore it should be noted that the randomized benchmarking protocol works in general for any finite subgroup of the unitary group that is a unitary 2-design. Both the restriction to gate/time independent errors and the restriction to the Clifford group are done in order to apply and build on the variance analysis result of [16].

In the error model used here, it is assumed that instead of perfectly implementing a Clifford gate $C \in \mathcal{C}$, the noisy counterpart $\tilde{C} = \Lambda \circ C$ is implemented. Here $\tilde{C}$ represents the noisy implementation of C and Λ is an unknown CPTP map characterizing the error. Randomized benchmarking is a scalable protocol that characterizes the error channel Λ by a single figure of merit: the average gate fidelity of Λ with the identity map $\overline{F}(\Lambda)$. The algorithm consists of choosing N sequences of m inde-

pendent and uniformly distributed gates from the Clifford group and computing the average survival probability of the sequences of fixed length m. This is then repeated for various m and the measured average fidelity as a function of m is fitted to a suitable model to yield an estimate for the average gate fidelity the error map with the identity. The RB protocol [7, 8] is fully stated in Algorithm 1.

The two main benefits of this protocol are its robustness against state preparation and measurement errors (SPAM) and its scalability. Robustness against SPAM means that the single figure of merit $\overline{F}(\Lambda)$ obtained from the protocol does not depend in any way on the quality of state preparation or the measurements required in the protocol. Scalability means that the amount of state preparations, gates, measurements and classical computation time needed to perform the algorithm scales polynomially in the number of qubits q comprising the system under investigation. In particular, this means that the uniform sampling can be done in polynomial time $\mathcal{O}(q^4)$ (on a classical machine), even though the size of the Clifford group scales exponentially in q (Theorem 3.5.1). Furthermore, any Clifford gate $C \in \mathcal{C}$ can be decomposed into a sequence of $\mathcal{O}(q^2)$ one- and two-qubit gates (generators of $\mathcal{C}$) in time $\mathcal{O}(q^2)$ [8]. Finally, the number of sequences N needed in the averaging is asymptotically independent of the sequence length m and the number of qubits q, even though the number of possible sequences scales exponentially in both. The scaling of N and sharp bounds on this number needed in case of some finite number m and q is discussed in more detail at the end of this section.

Data: Let $\mathcal{C}_q$ be the Clifford group on a d-dimensional Hilbert space $\mathcal{H}$, with $d = 2^q$ for q qubits. Assume the error model $\tilde{C} = \Lambda \circ C$ for all $C \in \mathcal{C}_q$, where $\Lambda \in \mathcal{S}(\mathcal{H})$.
Input: Fix the integers N, M and K and choose a non-trivial POVM element E.
Output: An estimate of the average gate fidelity $\overline{F}(\Lambda)$.

for $m = 1, \ldots, M$ **do**
  for $i = 1, \ldots, N$ **do**
    Sample a random sequence $C_{i_1}, \ldots, C_{i_m}$ of m gates independently and uniformly drawn from $\mathcal{C}_q$;
    Compose the sequence $S_{\mathbf{i_m}} = \Lambda \circ C_{i_{m+1}} \circ \Lambda \circ C_{i_m} \cdots \circ \Lambda \circ C_{i_1}$, where $C_{i_{m+1}}$ is chosen such that $S_{\mathbf{i_m}} = \mathcal{I}$ is the identity in the error free case ($\Lambda = \mathcal{I}$);
    Prepare q qubits in state ρ, aiming to maximize $\mathrm{Tr}[\rho E]$;
    Measure the survival probability $p_{\mathbf{i_m}} = \mathrm{Tr}[E S_{\mathbf{i_m}}(\rho)]$ to high precision by performing the measurement $\{E, I - E\}$ a total of K times;
  end
  Compute the average sequence fidelity $\overline{p}_m = \frac{1}{N} \sum_{i=1}^{N} p_{\mathbf{i_m}}$;
end
Fit $\overline{p}_m$ to the model $A_0 f^m + B_0$, where A_0 and B_0 are constants and f is related to the average single gate fidelity $\overline{F}(\Lambda) = f + \frac{1-f}{d}$.

Algorithm 1: Outline of the randomized benchmarking protocol.

4.2.1. SUMMARY OF THE PROTOCOL

Here a brief overview of the protocol is given, supplementing the description in Algorithm 1. As stated previously, the protocol description is phrased under the assumption of a gate and time independent error model. This means that $\tilde{C} = C \circ \Lambda$ is the noisy implementation of C, for all $C \in \mathcal{C}$, where $\Lambda \in \mathcal{S}(\mathcal{H})$ is a CPTP map. The goal of the protocol is to obtain an estimate of $\overline{F}(\Lambda)$, the average gate fidelity of Λ to the identity channel. The protocol consists of drawing N sequences of length m of Clifford gates uniformly at random. A final gate is then appended such that the overall sequence is the identity operator in the ideal case. In particular, the noisy implementation of such a sequence

is given by

$$S_{\mathbf{i_m}} = \Lambda \circ C_{i_{m+1}} \circ \Lambda \circ C_{i_m} \circ \cdots \circ \Lambda \circ C_{i_1}, \tag{4.1}$$

where $\mathbf{i_m} = (i_1, ..., i_m)$ an m-tuple of the indices and where $C_{i_{m+1}} = (C_{i_m} \circ \cdots C_{i_1})^\dagger$ is the inverse of the noise-free sequence. The index i runs over the different number of sequences and its subscript denotes the position in the sequence. In the rest of this section, the subscript $\mathbf{i_m}$ is understood to indicate a particular sequence of length m, where the inverse gate $C_{i_{m+1}}$ is uniquely determined by the string. For each string, the survival probability is measured, which is defined as

$$p_{\mathbf{i_m}} = \langle E | S_{\mathbf{i_m}}(\rho) \rangle = \mathrm{Tr}[E S_{\mathbf{i_m}}(\rho)], \tag{4.2}$$

where $\rho \in \mathcal{D}(\mathcal{H})$ is the density operator incorporating state preparation errors and $0 \preceq E \preceq I$ is a POVM element describing the performed measurement including the measurement errors. Which states and measurements should be aimed for is discussed in the next subsection. Sampling N random strings $S_{\mathbf{i_m}}$ and averaging the quantity $p_{\mathbf{i_m}}$ yields an estimate of the average over all possible strings. The empirical average is then computed as

$$\overline{p}_m = \frac{1}{N} \sum_{\mathbf{i_m}} p_{\mathbf{i_m}}, \tag{4.3}$$

where the sum is understood to be over the N drawn sequences here. Finally several values for $\overline{p}_m$ are obtained for various m and fitted to a model of the form

$$A_0 f^m + B_0, \tag{4.4}$$

where A_0 and B_0 are constants that depend on ρ, E and Λ and where $f = f(\Lambda)$ is the RB decay parameter, depending on Λ only. This parameter is directly related to the average gate fidelity by

$$\overline{F}(\Lambda) = f + \frac{1-f}{d}. \tag{4.5}$$

4.2.2. DERIVATION OF THE FIT MODEL

It is not immediately clear from the protocol that this works and delivers the desired result. The reason this protocol works essentially comes down to why the expectation value

$$\mathbb{E}[p_{\mathbf{i_m}}] := \frac{1}{|\mathcal{C}|^m} \sum_{\mathbf{i_m}} p_{\mathbf{i_m}}$$

over all possible sequences $S_{\mathbf{i_m}}$ is of the form of the fit model (4.4). This in turn depends heavily on Theorem 3.8.2, stating that the twirl of the error map Λ over the Clifford group $\mathcal{C}$ yields a depolarizing channel Θ_f, where f depends on Λ. It is then merely a technical task to show that applying random sequences of Clifford gates and averaging over the survival probability (see Algorithm 1) is effectively twirling over the Clifford group, such that the average gate fidelity of the error channel can be computed from the depolarizing parameter of the twirled error channel. All these steps are made precise in the following, based on [8].

First it is shown that the exact averaging over all possible sequences $S_{\mathbf{i_m}}$ of length m is effectively an m-fold composition of twirls over $\mathcal{C}$. In order to do so, the string

$$S_{\mathbf{i_m}} = \Lambda \circ C_{i_{m+1}} \circ \Lambda \circ C_{i_m} \circ \cdots \circ \Lambda \circ C_{i_1}, \tag{4.6}$$

is rewritten in an alternative form. First let $D_{i_1} = C_{i_1}$ and then define for $j = 2, ..., m+1$ the gates D_{i_j} recursively by $C_{i_j} = D_{i_j} \circ D_{i_{j-1}}^\dagger$, explicitly yielding

$$D_{i_j} = C_{i_j} \circ \cdots \circ C_{i_1} = \bigcirc_{s=1}^{j} C_{i_s}, \qquad j = 1, ..., m+1. \tag{4.7}$$

This allows $S_{\mathbf{i_m}}$ to be rewritten in the form

$$\begin{aligned} S_{\mathbf{i_m}} &= \Lambda \circ C_{i_{m+1}} \circ \Lambda \circ C_{i_m} \circ \cdots \circ \Lambda \circ C_{i_1} \\ &= \Lambda \circ D_{i_m}^\dagger \circ \Lambda \circ D_{i_m} \circ D_{i_{m-1}}^\dagger \circ \cdots \circ D_{i_1}^\dagger \Lambda \circ D_{i_1}, \\ &= \Lambda \circ \left(\bigcirc_{s=1}^m \left[D_{i_s}^\dagger \circ \Lambda \circ D_{i_s} \right] \right) \end{aligned} \tag{4.8}$$

using $D_{i_{m+1}} = \bigcirc_{s=1}^{m+1} C_{i_s} = \mathcal{I}$ is the identity by definition of $C_{i_{m+1}}$. Averaging over all possible sequences of length m yields

$$\begin{aligned} S_m &:= \frac{1}{|\mathcal{C}|^m} \sum_{\mathbf{i_m}} S_{\mathbf{i_m}} \\ &= \frac{1}{|\mathcal{C}|^m} \sum_{\mathbf{i_m}} \Lambda \circ \left(\bigcirc_{s=1}^m \left[D_{i_s}^\dagger \circ \Lambda \circ D_{i_s} \right] \right) \\ &= \Lambda \circ \left(\bigcirc_{s=1}^m \frac{1}{|\mathcal{C}|} \sum_{i_s} \left[D_{i_s}^\dagger \circ \Lambda \circ D_{i_s} \right] \right) \\ &= \Lambda \circ \left(\bigcirc_{s=1}^m \Theta_f \right) \\ &= \Lambda \circ \Theta_{f^m}. \end{aligned} \tag{4.9}$$

Note that summing over each i_s runs over every Clifford gate in $\mathcal{C}$ once and only once in D_{i_s}, which is why the second line of the above equation holds. This is so because $\mathcal{C}$ forms a group and therefore for any $C \in \mathcal{C}$ it holds that $C\mathcal{C} := \{CG | G \in \mathcal{C}\} = \mathcal{C}$. Furthermore because each string has the same weight in the averaging (the average is uniform), the summation can be done over each i_s independently, which justifies the third line. The next line is justified by Theorem 3.8.2 and the last equality is due to Lemma 3.7.1.

By linearity of the trace and of each quantum channel, averaging $p_{\mathbf{i_m}}$ over all strings is equivalent to applying the average string S_m. Explicitly,

$$\mathbb{E}[p_{\mathbf{i_m}}] = \frac{1}{|\mathcal{C}|^m} \sum_{\mathbf{i_m}} \mathrm{Tr}[E S_{\mathbf{i_m}}(\rho)] = \mathrm{Tr}[E \frac{1}{|\mathcal{C}|^m} \sum_{\mathbf{i_m}} S_{\mathbf{i_m}}(\rho)] = \mathrm{Tr}[E \left(\frac{1}{|\mathcal{C}|^m} \sum_{\mathbf{i_m}} S_{\mathbf{i_m}} \right)(\rho)] = \mathrm{Tr}[E S_m(\rho)], \tag{4.10}$$

where $\rho \in \mathcal{D}(\mathcal{H})$ describes the state preparation process and POVM element $0 \preceq E \preceq I$ describes the measurement $\{E, I - E\}$. Plugging (4.10) into (4.9) yields

$$\mathbb{E}[p_{\mathbf{i_m}}] = \mathrm{Tr}[E(\Lambda \circ \Theta_{f^m})(\rho)] = \mathrm{Tr}[E\Lambda(\rho)] f^m + (1 - f^m) \mathrm{Tr}\left[E\Lambda\left(\frac{I}{d} \right) \right] = A_0 f^m + B_0, \tag{4.11}$$

where $A_0 = \mathrm{Tr}[E\Lambda(\rho - \frac{I}{d})]$ and $B_0 = \mathrm{Tr}[E\Lambda(\frac{I}{d})]$, using linearity. The state preparation and measurement errors, encoded by ρ and POVM element E, as well as the final error gate Λ accounting for the error in $C_{i_{m+1}}$, are absorbed into the constants A_0 and B_0. In the absence of state preparation and measurement errors one typically has $\rho = E = |\psi\rangle\langle\psi|$ for some pure state ψ. In particular, in order yield the best fit, the experimenter should aim to maximize the constant A_0, therefore preparing a state that maximizes $\mathrm{Tr}[E\Lambda(\rho)]$, which under the assumption that $\overline{F}$ is large (i.e. Λ is close to the identity channel) in practice means just maximizing $\mathrm{Tr}[E\rho]$. However, it should be emphasized that any ρ and any E work in this protocol. This means that the protocol is completely robust against state preparation and measurement errors.

To summarize, averaging the survival probability $p_{\mathbf{i_m}}$ over all possible sequences of length m yields the value expectation value $\mathbb{E}[p_{\mathbf{i_m}}]$, which satisfies the exponential relation $\mathbb{E}[p_{\mathbf{i_m}}] = A_0 f^m + B_0$ as a function of the sequence length m, where A_0 and B_0 are unknown constants (independent of m). Thus with several estimates $\overline{p}_m$ of $\mathbb{E}[p_{\mathbf{i_m}}]$ for different m, a fitting procedure can be used to extract

Table 4.1: The linear relationship between the average gate fidelity $\overline{F}$, infidelity r, randomized benchmarking decay parameter f and χ_{00} of a quantum channel $\mathcal{E} \in \mathcal{S}(\mathcal{H})$ with $d = \mathrm{Dim}(\mathcal{H})$. Source: [45]

	$\overline{F}$	r	f	χ_{00}
$\overline{F} =$	-	$1-r$	$\frac{(d-1)f+1}{d}$	$\frac{d\chi_{00}+1}{d+1}$
$r =$	$1-\overline{F}$	-	$\frac{d-1}{d}(1-f)$	$\frac{d}{d+1}(1-\chi_{00})$
$f =$	$\frac{d\overline{F}-1}{d-1}$	$1-\frac{d}{d-1}r$	-	$\frac{d^2\chi_{00}-1}{d^2-1}$
$\chi_{00} =$	$\frac{(d+1)\overline{F}-1}{d}$	$1-\frac{d+1}{d}r$	$\frac{(d^2-1)f+1}{d^2}$	-

an estimate of the depolarizing parameter f (along with A_0 and B_0), which now fully describes the CPTP channel Θ_f.

The average fidelity of the error channel Λ can then be computed as a function of the depolarizing parameter (also called the RB decay parameter) $f = f(\Lambda)$ by

$$\overline{F}(\Lambda) = \overline{F}(\Lambda_T) = \overline{F}(\Theta_f) = f + \frac{1-f}{d}. \tag{4.12}$$

The first equality follows from Lemma 3.8.1, which states that twirling over the Clifford group leaves the average gate fidelity invariant. The second equality uses the fact that $\Lambda_T = \Theta_f$ (Theorem 3.8.2). The third equality is done by direct computation in Lemma 3.7.2. This shows that $f(\Lambda)$ and $\overline{F}(\Lambda)$ in essence capture the same information, and the quantities can be related by the above linear equation. Sometimes the infidelity $r := 1-\overline{F}$ is used in literature, as well as a quantity χ_{00}, to characterize the channel Λ. χ_{00} is the $(0,0)$-th entry of the χ-matrix representation of a quantum channel, which is a $d^2 \times d^2$ complex matrix that fully specifies the channel $\mathcal{E}$ [23]. All these quantities can be related to each other by linear equations involving only the dimension d. The relations between all these quantities are summarized in Table 4.1.

4.2.3. FIRST ORDER BOUND ON THE NUMBER OF SEQUENCES REQUIRED

This subsection focuses on the parameter N of the protocol, the number of sequences needed to obtain a good estimate $\overline{p}_m$ of $\mathbb{E}[p_{\mathbf{i_m}}]$. This number may possibly depend on m. In view of the scalability of the protocol, it is clearly infeasible to average over all sequences, since the number of sequences scales exponentially as $|\mathcal{C}|^m = 2^{m\mathcal{O}(q^2)}$ (see Theorem 3.5.1). However instead of averaging over all possible sequences of length m, the average is taken over N strings of length m of gates C_{i_s} that are independently and uniformly at random drawn from $\mathcal{C}$. Because of independent and uniform sampling, $S_{\mathbf{i_m}}$ is then uniformly sampled from all possible strings. Therefore $\overline{p}_m$ is an unbiased estimator of $\mathbb{E}[p_{\mathbf{i_m}}]$. So $p_{\mathbf{i_m}}$ can be regarded as an independent and identically distributed random variables with an estimator $\overline{p}_m$ of the expectation value $\mathbb{E}[p_{\mathbf{i_m}}]$. $p_{\mathbf{i_m}}$ is a bounded random variable, with $a \le p_{\mathbf{i_m}} \le b$ for some $a < b$ (here $a = 0$ and $b = 1$, since $0 \preceq E \preceq I$) for all strings $S_{\mathbf{i_m}}$. This allows for the use of a concentration inequality, that quantifies the probability that $\overline{p}_m$ deviates from $\mathbb{E}[p_{\mathbf{i_m}}]$ relative to $b-a$ by by less than $\epsilon > 0$ as a function of N. Hoeffding's first inequality Theorem 3.1.1, which does not require any more information on the distribution of $p_{\mathbf{i_m}}$ except for its boundedness, is such a concentration inequality and it claims that

$$\mathbb{P}\left[\left|\frac{\overline{p}_m - \mathbb{E}[p_{\mathbf{i_m}}]}{b-a}\right| \ge \epsilon\right] \le 2e^{-2N\epsilon^2}. \tag{4.13}$$

Suppose that a priori the relative interval size ϵ is set and the above probability is to be upper bounded by δ for some small $\delta > 0$. Then the number of sequences needed N can be bounded by solving $\delta \geq 2e^{-2N\epsilon^2}$ for N, yielding

$$N \geq \frac{\ln(\frac{2}{\delta})}{2\epsilon^2}, \tag{4.14}$$

a number that is independent of q and m. In principle given a specified confidence interval on $\overline{p}_m$ (which is specified by ϵ and δ, perhaps depending to $b-a$), the number of sequences N needed can be computed using the above procedure.

The confidence interval of the RB decay parameter f ultimately depends on the confidence interval around each $\overline{p}_m$, on the fitting procedure, on the number of data points M and on the value of A_0. As noted earlier, maximizing A_0 yields the easiest fit. This stochastic approach assumes that $p_{\mathbf{i_m}}$ can be measured to arbitrary precision. In practice this is done by performing K single-shot repetitions of preparing ρ, performing the fixed string of gates $S_{\mathbf{i_m}}$ and measuring $\{E, I-E\}$, and counting the number of outcomes K_E associated with E. Then $p_{\mathbf{i_m}} \approx \frac{K_E}{K}$ is estimated according the third postulate of quantum mechanics (subsection 2.4.1). Experimentally it is easy to do a large number K of single shot repetitions, since this does not require any compilation or pre-processing time. A bound on K that is experimentally feasible depends on the physical implementation of the qubits.

This result, as first obtained in [8], looks promising, since it is definitely scalable in both q and m. However, the number of sequences needed for a reasonable confidence interval is still relatively large. For example 99% confidence interval ($\delta = 0.01$) of size $\epsilon = 0.01$ required at a total of $N = 26492$ sequences, which is still a lot experimentally. In an attempt to bring this number down even further for the sake of experimental feasibility, a second order concentration inequality can be used. Theorem 3.1.2 provides a bound that may provide a tighter concentration inequality, provided that one knows the variance $\mathbb{V}[p_{\mathbf{i_m}}]$ of the distribution from which $p_{\mathbf{i_m}}$ is sampled. This is precisely the route that [16] followed, proving a bound on $\mathbb{V}[p_{\mathbf{i_m}}]$ which brings down the number of sequences N. The following subsection explains this in more detail.

4.2.4. VARIANCE ANALYSIS

In this section it is outlined how a better bound on the number of sequences N needed to obtain a certain confidence interval, can be obtained. As discussed above, the desire is to apply Hoeffding's second inequality (Theorem 3.1.2), which requires a bound on the variance $\mathbb{V}[p_{\mathbf{i_m}}]$. This is done in [16]. Here only the $\mathbb{V}[p_{\mathbf{i_m}}]$ is expressed in terms of twirls of Λ and the result of [16] is stated. The derivation is difficult and long and therefore omitted here. The goal of this section is twofold: summarizing current literature on the number of sequences needed and outlining the general idea of why this analysis is performed, since this thesis is about performing the variance analysis for a protocol similar to randomized benchmarking (this protocol is described in section 4.4 and full variance analysis is done in chapter 5).

In order to simplify the analysis and to prepare for the later use of the notation, some of the key equations from the previous sections are restated in Liouville representation. A random sequence of Clifford gates of length m, analogous to (4.8), is written in Liouville representation (see section 3.6 for details) as

$$\begin{aligned} \mathbf{S_{i_m}} &= \prod_{s=1}^{m+1} \mathbf{\Lambda C}_{i_s} = \mathbf{\Lambda C}_{i_{m+1}} \mathbf{\Lambda C}_{i_m} \cdots \mathbf{\Lambda C}_{i_1} \\ &= \mathbf{\Lambda} \prod_{s=1}^{m} \mathbf{D}_{i_s}^\dagger \mathbf{\Lambda D}_{i_s} = \mathbf{\Lambda} (\mathbf{D}_{i_m}^\dagger \mathbf{\Lambda D}_{i_m}) \cdots (\mathbf{D}_{i_1}^\dagger \mathbf{\Lambda D}_{i_1}). \end{aligned} \tag{4.15}$$

Note that the product is defined from right to left in accordance with the composition from right to left. The survival probability of such a sequence is then written as $p_{\mathbf{i_m}} = \langle\langle E|\mathbf{S_{i_m}}|\rho\rangle\rangle$ and its expecta-

tion value (4.11) is written as

$$\mathbb{E}[p_{\mathbf{i_m}}] = \langle\langle E|\mathbf{\Lambda}(T_{\mathcal{C}}(\mathbf{\Lambda}))^m|\rho\rangle\rangle = \langle\langle E|\mathbf{\Lambda}\mathbf{\Theta}_{f^m}|\rho\rangle\rangle = \langle\langle E|\mathbf{\Lambda}|\rho - \frac{I}{d}\rangle\rangle f^m + \langle\langle E|\mathbf{\Lambda}|\frac{I}{d}\rangle\rangle, \tag{4.16}$$

where $T_{\mathcal{C}}(\mathbf{\Lambda}) = \frac{1}{|\mathcal{C}|}\sum_{C\in\mathcal{C}}\mathbf{C}^\dagger\mathbf{\Lambda}\mathbf{C} = \mathbf{\Theta}_f$ by Theorem 3.8.2 written in Liouville representation (see (3.39)). Recall that in the Liouville representation, a depolarizing channel is represented as

$$\mathbf{\Theta}_f = |\sigma_0\rangle\rangle\langle\langle\sigma_0| + f\sum_{\tau\in\mathcal{Q}^*}|\tau\rangle\rangle\langle\langle\tau|. \tag{4.17}$$

Now let us express the variance $\mathbb{V}[p_{\mathbf{i_m}}] = \mathbb{E}[p_{\mathbf{i_m}}^2] - \mathbb{E}[p_{\mathbf{i_m}}]^2$ in this notation. Using the identity

$$\langle\langle E|\boldsymbol{\mathcal{E}}|\rho\rangle\rangle^2 = \langle\langle E^{\otimes 2}|\boldsymbol{\mathcal{E}}^{\otimes 2}|\rho^{\otimes 2}\rangle\rangle$$

for any E, ρ and $\mathcal{E}$ (Lemma 3.6.2), and the mixed-product property of the tensor product, the expectation value of $p_{\mathbf{i_m}}^2$ becomes

$$\mathbb{E}[p_{\mathbf{i_m}}^2] = \frac{1}{|\mathcal{C}|^m}\sum_{\mathbf{i_m}}\langle\langle E^{\otimes 2}|\mathbf{S}_{\mathbf{i_m}}^{\otimes 2}|\rho^{\otimes 2}\rangle\rangle = \langle\langle E^{\otimes 2}|\mathbf{\Lambda}^{\otimes 2}(T_{\mathcal{C}}^{(2)}(\mathbf{\Lambda}^{\otimes 2}))^m|\rho^{\otimes 2}\rangle\rangle, \tag{4.18}$$

where

$$T_{\mathcal{C}}^{(n)}(\boldsymbol{\mathcal{E}}) := \frac{1}{|\mathcal{C}|}\sum_{C\in\mathcal{C}}(\mathbf{C}^\dagger)^{\otimes n}\boldsymbol{\mathcal{E}}\mathbf{C}^{\otimes n}, \quad \forall\, n\in\mathbb{N}, \tag{4.19}$$

under the assumption that the quantum channel $\mathcal{E}$ is of the appropriate dimension such that the definition makes sense. Note that $T_{\mathcal{C}} = T_{\mathcal{C}}^{(1)}$, but

$$\frac{1}{|\mathcal{C}|}\sum_{C\in\mathcal{C}}(\mathbf{C}^\dagger)^{\otimes 2}\boldsymbol{\mathcal{E}}\mathbf{C}^{\otimes 2} = T_{\mathcal{C}}^{(2)}(\boldsymbol{\mathcal{E}}^{\otimes 2}) \neq (T_{\mathcal{C}}(\boldsymbol{\mathcal{E}}))^{\otimes 2} = \left(\frac{1}{|\mathcal{C}|}\sum_{C\in\mathcal{C}}\mathbf{C}^\dagger\boldsymbol{\mathcal{E}}\mathbf{C}\right)^{\otimes 2}.$$

Similarly then

$$\mathbb{E}[p_{\mathbf{i_m}}]^2 = \langle\langle E|\mathbf{\Lambda}(T_{\mathcal{C}}(\mathbf{\Lambda}))^m|\rho\rangle\rangle^2 = \langle\langle E^{\otimes 2}|\mathbf{\Lambda}^{\otimes 2}((T_{\mathcal{C}}(\mathbf{\Lambda}))^{\otimes 2})^m|\rho\rangle\rangle. \tag{4.20}$$

Therefore, the variance can be written as

$$\begin{aligned}\mathbb{V}[p_{\mathbf{i_m}}] &= \langle\langle E^{\otimes 2}|\mathbf{\Lambda}^{\otimes 2}\left([T_{\mathcal{C}}^{(2)}(\mathbf{\Lambda}^{\otimes 2})]^m - [(T_{\mathcal{C}}(\mathbf{\Lambda}))^{\otimes 2}]^m\right)|\rho^{\otimes 2}\rangle\rangle \\ &= \sum_{s=1}^{m}\langle\langle\tilde{E}^{\otimes 2}|[T_{\mathcal{C}}^{(2)}(\mathbf{\Lambda}^{\otimes 2})]^{m-s}\left(T_{\mathcal{C}}^{(2)}(\mathbf{\Lambda}^{\otimes 2}) - T_{\mathcal{C}}(\mathbf{\Lambda})^{\otimes 2}\right)[(T_{\mathcal{C}}(\mathbf{\Lambda}))^{\otimes 2}]^{s-1}|\rho^{\otimes 2}\rangle\rangle,\end{aligned} \tag{4.21}$$

where $|\tilde{E}\rangle\rangle := \mathbf{\Lambda}^\dagger|E\rangle\rangle$ absorbs the final error channel into E as a measurement error and where the telescoping lemma, Lemma 3.2.1, is used in the second line. A single error map can be absorbed in E $\tilde{E}$ remains a valid POVM element, given that E is and that Λ is CPTP. To see that this is the case, note that $\Lambda^\dagger$ is a completely positive and unital channel by Proposition 2.5.2. Therefore $\tilde{E} = \Lambda^\dagger(E) \geq 0$ by the complete positivity of $\Lambda^\dagger$ and the fact that $E \geq 0$. Similarly $I - \tilde{E} = \Lambda^\dagger(I) - \Lambda^\dagger(E) = \Lambda^\dagger(I - E) \geq 0$ by unitality (and CP) of $\Lambda^\dagger$ and the fact that $I - E \geq 0$, showing that $\tilde{E}$ is a POVM element. The application of the telescoping lemma is only for the ease of the analysis of the expression. Note that the variance, just as the expectation value, of $p_{\mathbf{i_m}}$ still depends on m.

In [16], a thorough study of the quantity $\mathbb{V}[p_{\mathbf{i_m}}]$ is done in order to provide sharp bounds for it such that Theorem 3.1.2 can be applied to obtain a sharp bounds on the number N of random sequences needed (as a function of m and other a priori known parameters). The variance $\mathbb{V}[p_{\mathbf{i_m}}]$ and the bound depend on the state preparation and measurement errors as well, and therefore prescribe

some ideal state preparation and measurement that minimizes the variance bound. In the reference, the protocol is formulated to aim for the following state and measurement operator

$$\rho = \frac{1}{d}(I+P) \qquad \text{and} \qquad E = \frac{1}{2}(I+P), \tag{4.22}$$

where $P \in \mathcal{P}^*$ is some non-identity multi-qubit Pauli operator and $d = 2^q$ is the dimension of the system under investigation. Under this assumption, the variance can be bounded in the following way [16]

$$\mathbb{V}[p_{\mathbf{i_m}}] \leq \left(2\frac{d+1}{d-1}\left[\frac{1-u^m}{1-u}\right] + \frac{1}{4}\frac{d^2-2}{(d-1)^2}\left[\frac{1-f^{2m}}{1-f^2}\right]\right)r^2 + \left(\frac{d\hat{\eta}}{d-1}\left[\frac{1-f^m}{1-f}\right] + \frac{d\eta}{d-1}\left[\frac{1-f^{2m}}{1-f^2}\right]\right)r, \tag{4.23}$$

where $r = r(\Lambda)$ is the infidelity of Λ, $f = f(\Lambda)$ is de decay parameter (see Table 4.1 for their respective relations to $\overline{F}(\Lambda)$) and where $u = u(\Lambda)$ is the unitarity of Λ, which is defined as

$$u(\mathcal{E}) := \frac{d}{d-1}\int \mathrm{d}\psi \,\mathrm{Tr}\left[\left(\mathcal{E}\Big(|\psi\rangle\langle\psi| - \frac{I}{d}\Big)\right)^2\right] = \frac{1}{d^2-1}\,\mathrm{Tr}[\boldsymbol{\mathcal{E}}_{\mathrm{u}}\boldsymbol{\mathcal{E}}_{\mathrm{u}}^{\dagger}]. \tag{4.24}$$

See section 4.4 on details of the unitarity. Finally, the terms η and $\hat{\eta}$ are complicated terms (see [16]) that solely depend on the state preparation error and measurement errors. The point is that in case $\eta = \hat{\eta} = 0$, which corresponds to the case of ideal state preparation and measurements, the variance is bounded by a term proportional to r^2 and in case of small SPAM a small term linear in r is added. This ensures that in the limit of small r (that is, good gates) the variance is small, yielding significant improvement in the bound on N.

This bound also depends on the unitarity u, but there are some simplifications that can be made in the single-qubit case. The first is that $d = 2$ and (by definition) $\hat{\eta} = 0$. Furthermore, the dependence on u can be eliminated, yielding [16]

$$\mathbb{V}[p_{\mathbf{i_m}}] \leq \min\left(\frac{13}{2}mr^2 + 2\eta mr, \frac{7}{2}r + \eta\right). \tag{4.25}$$

As an example, [16] states that in the absence of SPAM errors ($\eta = 0$) and in the limit of large m (the minimum above is attained in the m-independent term), with an a priori estimate $r \leq 10^{-4}$ and confidence parameters $\delta = \epsilon = 0.01$, the number of sequences required is $N = 221$. In contract, if a less sharp bound on r is assumed, say $r \leq 10^{-2}$, the same other parameters yield $N = 4035$, but this is still a large improvement over [8] which has the earlier computed $N = 26492$.

4.3. INTERLEAVED RANDOMIZED BENCHMARKING

The interleaved randomized benchmarking protocol is a natural and simple extension of the standard randomized benchmarking protocol discussed in the previous section. It was first proposed by [44]. The goal of this protocol is to benchmark an individual gate in the gate set. Again here the analysis is here restricted to the Clifford group, but any unitary 2-design that is a finite subgroup of the unitary group satisfies. Randomized benchmarking provides a single figure of merit (the average gate fidelity) of the error gate associated with the entire Clifford group. This fixed error map associated with the entire group can also be viewed as the average error gate, averaged over the group. Typically it is assumed that the variation of the error maps over the gates in the group is small. This is the perturbation analysis that was performed in [8] on the original protocol. The interleaved extension intends to quantify how much worse a particular single gate is compared to the average.

First some notation is set. Let $C \in \mathcal{C}$ be an ideal fixed Clifford element, which one wishes to benchmark. The noisy implementation is then $\tilde{C} = \Lambda_C \circ C$. Suppose that each element $C_i \in \mathcal{C}$ has a noisy implementation $\tilde{C}_i = \Lambda_i \circ C_i$ and let $\Lambda = \frac{1}{|\mathcal{C}|}\sum_{i=1}^{|\mathcal{C}|}\Lambda_i$ be the average noise map associated with $\mathcal{C}$.

The interleaved randomized benchmarking protocol provides information on how much the average gate fidelity of Λ_C differs from that of Λ. How this is done is outlined in Algorithm 2. There are basically three main steps involved. In the first step, standard randomized benchmarking is performed. This yields an estimate of $\overline{F}(\Lambda)$. In the second step, perform the interleaved step, a modification of randomized benchmarking. After each randomly drawn channel C_{i_s}, perform the fixed channel C that is under investigation. Then, after m random gates interleaved with m times the gate C, the global inverse gate $C_{i_{m+1}}$ is performed, that is an inverse of the entire previous string. The modification is illustrated in Figure 4.1. This interleaved step is described by lines 2-11 in Algorithm 2. This step effectively yields an estimate of $\overline{F}(C^\dagger \circ \Lambda_C \circ C \circ \Lambda)$. The third and final step is to bound $\overline{F}(\Lambda_C) = \overline{F}(C^\dagger \circ \Lambda_C \circ C)$ based on the obtained estimates of $\overline{F}(C^\dagger \circ \Lambda_C \circ C \circ \Lambda)$ and $\overline{F}(\Lambda)$. This step is an analytical post-processing step.

Data: Let $\mathcal{C}_q$ be the Clifford group on a d-dimensional Hilbert space $\mathcal{H}$, with $d = 2^q$ for q qubits. Assume the error model $\tilde{C} = \Lambda_i \circ C$ for all $C_i \in \mathcal{C}$, where $\Lambda_i \in \mathcal{S}(\mathcal{H})$. Let $\Lambda := \frac{1}{|\mathcal{C}|}\sum_{i=1}^{\|\mathcal{C}\|} \Lambda_i$. Fix a specific $C \in \mathcal{C}$ that is to be benchmarked and denote Λ_C its error map.

Input: Fix the integers N, M and K and choose a non-trivial POVM element E.

Output: An estimate of the average gate fidelity $\overline{F}(\Lambda)$.

1 Perform the standard randomized benchmarking protocol of Algorithm 1 to obtain an estimate of $\overline{F}(\Lambda)$;
2 **for** $m = 1, ..., M$ **do**
3 **for** $i = 1, ..., N$ **do**
4 Sample a random sequence $C_{i_1}, ..., C_{i_m}$ of m gates independently and uniformly drawn from $\mathcal{C}$;
5 Compose $V_{\mathbf{i_m}} = \Lambda_{i_{m+1}} \circ C_{i_{m+1}} \circ \Lambda_C \circ C \circ \Lambda_{i_m} \circ C_{i_m} \circ \cdots \circ \Lambda_C \circ C\Lambda_{i_1} \circ C_{i_1}$, where $C_{i_{m+1}}$ is chosen such that $V_{\mathbf{i_m}} = \mathcal{I}$ is the identity in the error free case;
6 Prepare q qubits in state ρ, aiming to maximize $\mathrm{Tr}[\rho E]$;
7 Measure the survival probability $p_{\mathbf{i_m}} = \mathrm{Tr}[E V_{\mathbf{i_m}}(\rho)]$ to high precision by performing the measurement $\{E, I - E\}$ a total of K times;
8 **end**
9 Compute the average sequence fidelity $P_{m,N} = \frac{1}{N}\sum_{i=1}^{N} p_{\mathbf{i_m}}$;
10 **end**
11 Fit $P_{m,N}$ to the model $A_0 f^m + B_0$, where A_0 and B_0 are constants and $f = f(C^\dagger \circ \Lambda_C \circ C \circ \Lambda)$ is the randomized benchmarking decay parameter associate with the composite map $C^\dagger \circ \Lambda_C \circ C \circ \Lambda$;
12 Use Theorem 4.3.1 to obtain a lower bound on $\overline{F}(\Lambda_C) = \overline{F}(C^\dagger \circ \Lambda_C \circ C)$ using $\overline{F}(\Lambda)$ and $\overline{F}(C^\dagger \circ \Lambda_C \circ C \circ \Lambda)$ from step 1 and 2-11.

Algorithm 2: Outline of the interleaved randomized benchmarking protocol.

It is clear that this is a small modification of the randomized benchmarking protocol. Much of the analysis of that protocol directly carries over here. Only two things need some clarification. First it is shown that the interleaved step indeed provides an estimate of $\overline{F}(C^\dagger \circ \Lambda_C \circ C \circ \Lambda)$, and second a discussion is given on how to do the post-processing step. A random interleaved string of length m can be represented as

$$V_{\mathbf{i_m}} = \Lambda_{i_{m+1}} \circ C_{i_{m+1}} \circ \left(\bigcirc_{s=1}^{m} \left[\Lambda_C \circ C \circ \Lambda_{i_s} \circ C_{i_s}\right]\right). \tag{4.26}$$

This string can be rewritten in a similar way as is done in the analysis of randomized benchmarking by recursively defining $D_{i_1} = C_{i_1}$, $D_{i_j} \circ D_{i_{j-1}}^\dagger \circ C^\dagger = C_{i_j}$. This yields the explicit definition

$$D_{i_j} := C_{i_j} \circ \left(\bigcirc_{s=1}^{j-1} \left[C \circ C_{i_s}\right]\right). \tag{4.27}$$

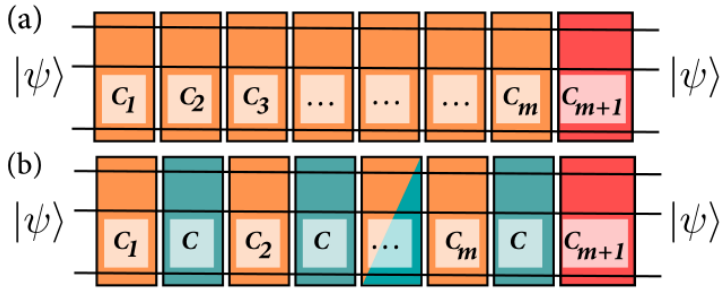

Figure 4.1: Illustration of the modification of randomized benchmarking (a) to interleaved randomized benchmarking (b). The target gate C is interleaved with random gates C_i chosen uniformly at random from $\mathcal{C}$. A final gate C_{m+1} is performed to make the total sequence the identity (in the ideal case). Source: [44].

Note that by definition of $C_{i_{m+1}}$ it follows that $D_{i_{m+1}} = \mathcal{I}$. The interleaved string can then be represented as

$$V_{\mathbf{i_m}} = \Lambda_{i_{m+1}} \circ \left(\bigcirc_{s=1}^{m} \left[D_{i_s}^{\dagger} \circ C^{\dagger} \circ \Lambda_C \circ C \circ \Lambda_{i_s} \circ D_{i_s} \right] \right). \tag{4.28}$$

One can recognize that this is equivalent to the randomized benchmarking string $S_{\mathbf{i_m}}$ of (4.8) with Λ replaced by $C^{\dagger} \circ \Lambda_C \circ C \circ \Lambda_{i_s}$. Therefore averaging over all possible strings $\mathbf{i_m}$ yields

$$V_m := \frac{1}{|\mathcal{C}|^m} \sum_{\mathbf{i_m}} V_{\mathbf{i_m}} = \Lambda_{i_{m+1}} \circ \left(\bigcirc_{s=1}^{m} T_{\mathcal{C}}(C^{\dagger} \circ \Lambda_C \circ C \circ \Lambda) \right), \tag{4.29}$$

neglecting here the deviation of each Λ_{i_s} from the mean error channel Λ (which is assumed to be small) only for the randomly chosen Cliffords C_{i_s} (which may include our special gate C), but not for the interleaved Clifford C. Effectively this means that each Λ_{i_s} was replaced with Λ in the above equation. See [8, 44] for details on how to take into account these deviations. The analysis continues in a one-to-one correspondence as in the standard randomized benchmarking protocol, yielding a depolarizing parameter $f(C^{\dagger} \circ \Lambda_C \circ C \circ \Lambda)$, from which the average gate fidelity can be obtained.

The last step is a problem of estimating $\overline{F}(\Lambda_C)$ in terms of the measured quantities. The original proposal of the protocol [44] provided two separate bounds

$$r(\Lambda_C) \leq \frac{d-1}{d} \left(1 - \frac{f(C^{\dagger} \circ \Lambda_C \circ C \circ \Lambda)}{f(\Lambda)} \right) + \frac{2(d^2-1)(1-f(\Lambda))}{f(\Lambda) d^2} + \frac{4\sqrt{1-f(\Lambda)}\sqrt{d^2-1}}{f(\Lambda)}, \tag{4.30}$$

$$r(\Lambda_C) \leq \frac{d-1}{d} \left(2 - \frac{f(C^{\dagger} \circ \Lambda_C \circ C \circ \Lambda)}{f(\Lambda)} - f(\Lambda) + \left| f(\Lambda) - \frac{f(C^{\dagger} \circ \Lambda_C \circ C \circ \Lambda)}{f(\Lambda)} \right| \right). \tag{4.31}$$

Note that r, f and $\overline{F}$ are all linearly related to each other using the conversion equations of Table 4.1. The first bound (4.30) is generally applicable but very loose, except in the limit $\overline{F}(\Lambda) \to 1$. The second bound (4.31) used the a priori assumption that $\overline{F}(\Lambda_C) \geq 2\overline{F}(\Lambda) - 1$, an assumption that can not be verified. Initially, this reduced the power of the protocol. These problems with the original bounds were also noted by various authors [45, 46], who improved on the result. To do so, the problem has been stated in a slightly more general way. The question is asked how can one bound $\overline{F}(\mathcal{E}_1)$ given $\overline{F}(\mathcal{E}_2)$ and $\overline{F}(\mathcal{E}_1 \circ \mathcal{E}_2)$. Identifying $\mathcal{E}_1 = C^{\dagger} \circ \Lambda_C \circ C$ and $\mathcal{E}_2 = \Lambda$, together with the fact that $\overline{F}(\Lambda_C) = \overline{F}(C^{\dagger} \circ \Lambda_C \circ C)$ by the unitarity invariance of the average gate fidelity (Proposition 2.5.12), the current problem is retrieved. First an improved bound was proved by [46], which stated the same problem in terms of χ_{00}. In a subsequent paper [45] this problem was completely solved, generalizing the result of [46] and proving that the bound saturates for certain channels. This shows the optimality of the

bound. The result is stated below, also in terms of χ_{00}. Note that χ_{00} can always be converted to $\overline{F}$ by using the linear relations of Table 4.1.

Theorem 4.3.1. *Let $\mathcal{E}_1, \mathcal{E}_2 \in \mathcal{S}(\mathcal{H})$ be two quantum channels. Then*

$$\begin{aligned}\left|\chi_{00}(\mathcal{E}_1 \circ \mathcal{E}_2) - \chi_{00}(\mathcal{E}_1)\chi_{00}(\mathcal{E}_2) - (1-\chi_{00}(\mathcal{E}_1))(1-\chi_{00}(\mathcal{E}_2))\right| \\ \leq 2\sqrt{\chi_{00}(\mathcal{E}_1)\chi_{00}(\mathcal{E}_2)(1-\chi_{00}(\mathcal{E}_1))(1-\chi_{00}(\mathcal{E}_2))}. \quad (4.32)\end{aligned}$$

Furthermore, for all even dimensions $d = \mathrm{Dim}(\mathcal{H})$ and all values of $\chi_{00}(\mathcal{E}_1)$ and $\chi_{00}(\mathcal{E}_2)$, there exists $\mathcal{E}_1$ and $\mathcal{E}_2$ that saturate both signs of the above inequality.

Proof. See Theorem 1 of [45]. ■

Returning to interleaved randomized benchmarking, Theorem 4.3.1 can be applied by rearranging the inequalities yields a lower bound on $\chi_{00}(C^\dagger \circ \Lambda_C \circ C)$, which can in turn be converted to a lower bound on $\overline{F}(C^\dagger \circ \Lambda_C \circ C) = \overline{F}(\Lambda_C)$.

Since the interleaved randomized benchmarking protocol is essentially performing standard randomized benchmarking twice, the statistical analysis of the protocol directly carries over from the standard randomized benchmarking protocol. Thus [16] provides a method to robustly determine the number of random sequences one needs to average over to obtain accurate estimates for

$$\overline{F}(C^\dagger \circ \Lambda_C \circ C \circ \Lambda)$$

and $\overline{F}(\Lambda)$. Adding the confidence intervals to Theorem 4.3.1, yields a rigid bound on $\overline{F}(\Lambda_C)$ up to an a priori specified certainty.

4.4. UNITARITY RANDOMIZED BENCHMARKING

In unitarity randomized benchmarking one tries to obtain an estimate of how close the average error map of the Clifford group (or any group that forms a unitary 2-design) is to being unitary. In order to do so, the unitarity [13] was introduced. The unitarity roughly quantifies the output purity of a quantum channel, averaged over pure input states. This quantity is useful to characterize if the dominant error in the system is unitary (i.e. over-/underrotations) or not (i.e. depolarizing, dephasing or relaxation). In quantum error correction codes it can be useful to understand the type of the dominant noise factor.

Under the assumption that the error map is a quantum channel, i.e. is CPTP, the unitarity is defined as follows: [13]

Definition 4.4.1. Let $\mathcal{E}$ be a quantum channel (i.e. a CPTP map). Then the unitarity of the channel is defined as

$$u(\mathcal{E}) = \frac{d}{d-1}\int \mathrm{d}\psi \,\mathrm{Tr}\left[\left(\mathcal{E}\left(|\psi\rangle\langle\psi| - \frac{I}{d}\right)\right)^2\right], \quad (4.33)$$

where d is the dimension of the underlying Hilbert space $\mathcal{H}$, I is the identity on $\mathcal{H}$ and $\mathrm{d}\psi$ is the uniform, normalized Haar measure on the state space. □

This definition can be generalized to include completely positive and trace decreasing channels. In Example 4.4.1 the unitarity of some example channels have been computed. An alternative definition of the unitarity can be given in the Liouville representation as [13]

$$u(\mathcal{E}) = \frac{1}{d^2-1}\mathrm{Tr}[\boldsymbol{\mathcal{E}}_{\mathrm{u}}^\dagger \boldsymbol{\mathcal{E}}_{\mathrm{u}}] = \frac{1}{d^2-1}\mathrm{Tr}[\boldsymbol{\mathcal{E}}_{\mathrm{u}} \boldsymbol{\mathcal{E}}_{\mathrm{u}}^\dagger], \quad (4.34)$$

where $\mathcal{E}_u$ is the unital block of $\mathcal{E}$ as defined by equation (3.22). This definition is often more pleasant to work with. This equation evaluates as

$$\begin{aligned} u(\mathcal{E}) &= \frac{1}{d^2-1}\sum_{\sigma\in\mathcal{Q}^*}\langle\langle\sigma|\mathcal{E}_u\mathcal{E}_u^\dagger|\sigma\rangle\rangle \\ &= \frac{1}{d^2-1}\sum_{\sigma,\tau\in\mathcal{Q}^*}\langle\langle\sigma|\mathcal{E}_u|\tau\rangle\rangle\langle\langle\tau|\mathcal{E}_u^\dagger|\sigma\rangle\rangle \\ &= \frac{1}{d^2-1}\sum_{\sigma,\tau\in\mathcal{Q}^*}\langle\langle\sigma|\mathcal{E}_u|\tau\rangle\rangle\langle\langle\sigma|\mathcal{E}_u|\tau\rangle\rangle^* \\ &= \frac{1}{d^2-1}\sum_{\sigma,\tau\in\mathcal{Q}^*}\langle\langle\sigma|\mathcal{E}_u|\tau\rangle\rangle^2 \end{aligned} \tag{4.35}$$

since $\langle\langle\sigma|\mathcal{E}|\tau\rangle\rangle$ is real by Proposition 3.6.1 due to the positivity of $\mathcal{E}$.

Example 4.4.1 (Unitarity of example channels)**.** Let us consider the two examples of CPTP channels that map $\mathcal{L}(\mathcal{H})$ into itself. The two channels considered here are the depolarizing channel $\mathcal{E}_1$ and a unitary channel $\mathcal{E}_2$, as defined by

$$\begin{aligned} &\mathcal{E}_1(A) := \Theta_f(A) = fA + d^{-1}(1-f)\operatorname{Tr}[A]I, \\ &\mathcal{E}_2(A) := UAU^\dagger. \end{aligned} \tag{4.36}$$

The first example channel has unitarity

$$\begin{aligned} u(\mathcal{E}_1) &= \frac{d}{d-1}\int \mathrm{d}\psi \operatorname{Tr}\left[\mathcal{E}_1\left(|\psi\rangle\langle\psi| - \frac{I}{d}\right)^2\right] \\ &= \frac{d}{d-1}\int \mathrm{d}\psi \operatorname{Tr}\left[\left(f(|\psi\rangle\langle\psi| - \frac{I}{d}) + d^{-1}(1-f)\operatorname{Tr}[|\psi\rangle\langle\psi| - \frac{I}{d}]I\right)^2\right] \\ &= \frac{d}{d-1}\int \mathrm{d}\psi \operatorname{Tr}\left[\left(f(|\psi\rangle\langle\psi| - \frac{I}{d})\right)^2\right] = \frac{df^2}{d-1}\int \mathrm{d}\psi \operatorname{Tr}\left[\left(|\psi\rangle\langle\psi| - \frac{I}{d}\right)^2\right] \\ &= \frac{df^2}{d-1}\int \mathrm{d}\psi \operatorname{Tr}\left[(1-\frac{2}{d})|\psi\rangle\langle\psi| + \frac{I}{d^2}\right] = \frac{df^2}{d-1}\int \mathrm{d}\psi\left(1-\frac{2}{d}+\frac{1}{d}\right) \\ &= f^2\frac{d}{d-1}\left(1-\frac{1}{d}\right) = f^2. \end{aligned} \tag{4.37}$$

The second example is similar, and the unitarity is shown to be 1, since it is a unitary channel:

$$\begin{aligned} u(\mathcal{E}_2) &= \frac{d}{d-1}\int \mathrm{d}\psi \operatorname{Tr}\left[\mathcal{E}_2\left(|\psi\rangle\langle\psi| - \frac{I}{d}\right)^2\right] = \frac{d}{d-1}\int \mathrm{d}\psi \operatorname{Tr}\left[\left(U|\psi\rangle\langle\psi|U^\dagger - \frac{I}{d}\right)^2\right] \\ &= \frac{d}{d-1}\int \mathrm{d}\psi \operatorname{Tr}\left[(1-\frac{2}{d})U|\psi\rangle\langle\psi|U^\dagger + \frac{I}{d^2}\right] \\ &= \frac{d}{d-1}\int\left(\mathrm{d}\psi(1-\frac{2}{d})\operatorname{Tr}\left[U|\psi\rangle\langle\psi|U^\dagger\right] + \frac{1}{d}\operatorname{Tr}\left[\frac{I}{d^2}\right]\right) \\ &= \frac{d}{d-1}\left(\int \mathrm{d}\psi(1-\frac{2}{d}) + \frac{1}{d}\right) = \frac{d}{d-1}\left(1-\frac{1}{d}\right) = 1. \end{aligned}$$

□

Before moving on to the protocol that allows for robust estimation of the unitarity of a channel, some of the properties of the unitarity are stated first. The first relates the unitarity to the non-unitality and the fidelity of the channel.

Proposition 4.4.1 (Relation to non-unitality and fidelity)**.** *Let $\mathcal{E} \in \mathcal{S}(\mathcal{H})$ be a quantum channel with unitarity $u(\Lambda)$, non-unitality vector $\alpha(\Lambda)$ and randomized benchmarking decay parameter $f(\Lambda)$. Then*

$$f(\mathcal{E})^2 \leq u(\mathcal{E}) \leq 1 - \frac{\|\alpha(\mathcal{E})\|^2}{d-1} \leq 1. \tag{4.38}$$

Proof. See Proposition 6 and 8 of [13]. ■

Recall that the average gate fidelity $\overline{F}$ is related to the decay parameter f by $\overline{F}(\mathcal{E}) = \frac{(d-1)f(\mathcal{E})+1}{d}$ (see Table 4.1). The example channels of Example 4.4.1 saturate both sides of the inequality, so these inequalities are actually optimal. The depolarizing channel can be interpreted as the 'least unitary channel', given a certain average gate fidelity to the identity $\overline{F}$ (or equivalently, given a certain f).

The second proposition states that the unitarity behaves as expected, attaining a value 1 if and only if the channel is unitary (the if part is shown in Example 4.4.1). Furthermore it states that the unitarity is unitarily invariant.

Proposition 4.4.2. *Let $\mathcal{E} \in \mathcal{S}(\mathcal{H})$ be a quantum channel and let $U, V \in \mathcal{U}(\mathcal{H})$. Then*

1. $u(\mathcal{E}) = 1 \quad \Leftrightarrow \quad \mathcal{E} \circ \mathcal{E}^\dagger = \mathcal{E}^\dagger \circ \mathcal{E} = \mathcal{I}$,
2. $u(\mathcal{E}) = u(U \circ \mathcal{E} \circ V)$.

Proof. See Proposition 7 of [13]. ■

4.4.1. SUMMARY OF THE PROTOCOL

In this section, the protocol as proposed by [13] is presented. This protocol provides an experimental procedure to estimate the unitarity of the Clifford group, under the assumption of a gate and time independent error model. Explicitly, consider a Clifford gate $C \in \mathcal{C}$. A noisy implementation is then modeled as $C \circ \Lambda$, where $\Lambda \in \mathcal{S}(\mathcal{H})$ is a CPTP map that is independent of gate and time. Here, the error map is placed in front of the ideal operator, which is in agreement with the error model employed by [13]. The protocol inherits its robustness against state preparation and measurement errors from the family of randomized benchmarking protocols, but is not directly scalable (in the number of qubits) as presented in [13]. The authors leave it as an open problem to analyze a scalable implementation. In this section, emphasize will be put on a scalable and non-scalable implementation of the protocol.

Unitarity benchmarking provides a simple protocol to estimate the unitarity of the average error map Λ associated with the Clifford group, acting on a d-dimensional Hilbert space $\mathcal{H}$, with $d = 2^q$ for q qubits. In summary, the protocol consists of drawing N sequences of length m of Clifford elements uniformly at random. Such a particular sequence is then of the form

$$W_{\mathbf{i_m}} = C_{i_m} \circ \Lambda \circ C_{i_{m-1}} \circ \Lambda \circ \cdots \circ C_1 \circ \Lambda. \tag{4.39}$$

The idea is to obtain the expectation value of the following random variable (due to the uniformly at random chosen string $W_{\mathbf{i_m}}$)

$$q_{\mathbf{i_m}} = \mathrm{Tr}[Q W_{\mathbf{i_m}}^{\otimes 2}(\rho)] = \langle\langle Q | \mathbf{W}_{\mathbf{i_m}}^{\otimes 2} | \rho \rangle\rangle, \tag{4.40}$$

where $Q \in \mathrm{Herm}(\mathcal{H} \otimes \mathcal{H})$ and $\rho \in \mathcal{D}(\mathcal{H} \otimes \mathcal{H})$ are a hermitian observable and a density operator over a twofold copy of the system respectively. In order to obtain an estimate of the expectation value

$$\mathbb{E}[q_{\mathbf{i_m}}] = \frac{1}{|\mathcal{C}|^m} \sum_{\mathbf{i_m}} q_{\mathbf{i_m}} = \frac{1}{|\mathcal{C}|^m} \sum_{\mathbf{i_m}} \mathrm{Tr}[Q W_{\mathbf{i_m}}^{\otimes 2}(\rho)]$$

over the random sequences $W_{\mathbf{i_m}}$ of length m, the experimenter samples N random strings $W_{\mathbf{i_m}}$ uniformly at random, and averages the result $q_{\mathbf{i_m}}$ to obtain the empirical average $\overline{q}_m = \frac{1}{N} \sum_{\mathbf{i_m}} q_{\mathbf{i_m}} =$

$\frac{1}{N}\sum_{\mathbf{i_m}} \mathrm{Tr}[QW_{\mathbf{i_m}}^{\otimes 2}(\rho)]$. Obtaining estimates $\overline{q}_m$ for various m and fitting to the model

$$\overline{q}_m = A_0 + B_0 u(\Lambda)^{m-1}, \tag{4.41}$$

yields the unitarity $u(\Lambda)$ of the average error map. The constants A_0 and B_0 absorb the choice of Q and ρ, the respective errors made in preparation and measurement (SPAM) as well as a single residual error map Λ. In subsection 4.4.2 details are given as to why this fit model works.

A slight modification of the protocol is proposed here, yielding certain benefits. Instead of defining $q_{\mathbf{i_m}}$ as above, let us define

$$q_{\mathbf{i_m}} = \langle\langle Q|\mathbf{W}_{\mathbf{i_m}}^{\otimes 2}|\rho - \hat{\rho}\rangle\rangle = \langle\langle Q|\mathbf{W}_{\mathbf{i_m}}^{\otimes 2}|\rho\rangle\rangle - \langle\langle Q|\mathbf{W}_{\mathbf{i_m}}^{\otimes 2}|\hat{\rho}\rangle\rangle, \tag{4.42}$$

where $\rho, \hat{\rho} \in \mathcal{D}(\mathcal{H}\otimes\mathcal{H})$ are two different states. This requires double the resources from the experimenter (in terms of number of single-shot repetitions required), but has the advantage that the input state $\rho - \hat{\rho}$ is traceless (even in the presence of noise). As a first consequence, the fit model can then be reduced to

$$\overline{q}_m = B_0 u(\Lambda)^{m-1}. \tag{4.43}$$

This yields much easier fits, since taking the logarithm gives rise to a linear fitting problem with slope $u(\Lambda)$. Furthermore, this modification allows for smaller number N of random sequences needed, since the variance $\mathbb{V}[q_{\mathbf{i_m}}]$ is reduced. This is analyzed in full detail in chapter 5.

The definition (4.40) of $q_{\mathbf{i_m}}$ was on purpose made slightly more general here than the definition employed by [13], since it allows for the two-copy, scalable implementation of the protocol. Here the distinction between the non-scalable, single-copy implementation and the scalable two-copy implementation will be outlined. The difference is mostly a matter of experimental choice, but the number N of sequences needed to accurately estimate $\mathbb{E}[q_{\mathbf{i_m}}]$ in the single-qubit case depends (by a constant prefactor) on the choice of single- or two-copy implementation. This will be emphasized in our final result in chapter 5 (see Theorem 5.2.1).

Two-copy implementation. In the two-copy implementation, the experimenter has access to two identical copies of the system under investigation. He can prepare any state ρ on the twofold copy of the system $\mathcal{H}\otimes\mathcal{H}$, including entangled states between the systems. The sequence $W_{\mathbf{i_m}}$ then has to be applied to each copy of the system $\mathcal{H}$ separately (and simultaneously), after which any two-copy system observable Q is measured. The analysis in the next subsection shows why this method is scalable. In Algorithm 3 this procedure is outlined. The clear advantage here is that this procedure scales with the number of qubits q in the system $\mathcal{H}$, but requires double the resources (in numbers of qubits and gates).

Single-copy implementation. Alternatively, if the experimenter has only access to a single copy of the system $\mathcal{H}$, he can only perform measurements $Q_{\mathcal{H}} \in \mathrm{Herm}(\mathcal{H})$ and prepare states $\rho_{\mathcal{H}}, \hat{\rho}_{\mathcal{H}} \in \mathcal{D}(\mathcal{H})$. Then, the experimenter measures the expectation value $\mathrm{Tr}[Q_{\mathcal{H}} W_{\mathbf{i_m}}(\rho_{\mathcal{H}} - \hat{\rho}_{\mathcal{H}})]$, and squares this expectation value. This is then equivalent to letting $Q = Q_{\mathcal{H}}^{\otimes 2}$ and $\rho - \hat{\rho} = (\rho_{\mathcal{H}} - \hat{\rho}_{\mathcal{H}})^{\otimes 2}$ in the expression for $q_{\mathbf{i_m}}$, since

$$q_{\mathbf{i_m}} = \mathrm{Tr}[Q_{\mathcal{H}}^{\otimes 2} W_{\mathbf{i_m}}^{\otimes 2}((\rho_{\mathcal{H}} - \hat{\rho}_{\mathcal{H}})^{\otimes 2})] = \mathrm{Tr}[Q_{\mathcal{H}} W_{\mathbf{i_m}}(\rho_{\mathcal{H}} - \hat{\rho}_{\mathcal{H}})]^2.$$

As an extension, the experimenter can use several pairs of states $(\rho_{\mathcal{H}}^{(a)}, \hat{\rho}_{\mathcal{H}}^{(a)})$, $a = 1, ..., K_1$ and several measurements $Q_{\mathcal{H}}^{(b)}$, $b = 1, ..., K_2$. For each combination a, b the expectation value

$$\mathrm{Tr}[Q_{\mathcal{H}}^{(b)} W_{\mathbf{i_m}}(\rho_{\mathcal{H}}^{(a)} - \hat{\rho}_{\mathcal{H}}^{(a)})]$$

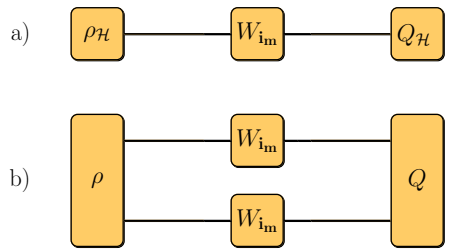

Figure 4.2: Schematic difference between the single-copy implementation (a) and two-copy implementation (b) of the unitarity randomized benchmarking protocol. Each line represents a system on the base Hilbert space $\mathcal{H}$. In the singe-copy implementation (a), the outcome $q_{\mathbf{i_m}} = \mathrm{Tr}[\rho_H c W_{\mathbf{i_m}}(Q_{\mathcal{H}})]^2$ needs to be squared to obtain $q_{\mathbf{i_m}}$, whereas in the two-copy implementation $q_{\mathbf{i_m}} = \mathrm{Tr}[Q W_{\mathbf{i_m}}^{\otimes 2}(\rho)]$ yields the direct outcome.

is measured, the result is then squared and added together for all a, b. That is,

$$q_{\mathbf{i_m}} = \sum_{a=1}^{K_1}\sum_{b=1}^{K_2} \mathrm{Tr}[Q_{\mathcal{H}}^{(b)} W_{\mathbf{i_m}}(\rho_{\mathcal{H}}^{(a)} - \hat{\rho}_{\mathcal{H}}^{(a)})]^2 = \mathrm{Tr}\left[\sum_{b=1}^{K_2} (Q_{\mathcal{H}}^{(b)})^{\otimes 2} W_{\mathbf{i_m}}^{\otimes 2}\left(\sum_{a=1}^{K_1} (\rho_{\mathcal{H}}^{(a)} - \hat{\rho}_{\mathcal{H}}^{(a)})^{\otimes 2}\right)\right], \tag{4.44}$$

yielding effectively

$$\rho - \hat{\rho} = \sum_{a=1}^{K_1} (\rho_{\mathcal{H}}^{(a)} - \hat{\rho}_{\mathcal{H}}^{(a)})^{\otimes 2} \qquad \text{and} \qquad Q = \sum_{b=1}^{K_2} (Q_{\mathcal{H}}^{(b)})^{\otimes 2}. \tag{4.45}$$

This procedure is outlined in Algorithm 4. This implementation is non-scalable in the number of qubits (as will be shown in the next subsection). Intuitively this is because the numbers K_1 and K_2 of different single-copy states and measurements needed scale exponentially with q to keep the constant B_0 in (4.43) high enough to be able to fit. However it has the obvious advantage of only requiring half the amount of resources (in numbers of qubits and gates required) compared to the two-copy implementation. The difference between the two implementations is illustrated in Figure 4.2.

Throughout the rest of this thesis a subscript $\mathcal{H}$ will be used to denote single system states $\rho_{\mathcal{H}}$ and measurements $Q_{\mathcal{H}}$, and ρ, Q will be reserved for the general two-copy operators. It is clear that the single-copy implementation is contained in the general analysis using ρ, Q by letting ρ, Q be of the form (4.45). Therefore, the analysis of chapter 5 will use $\rho - \hat{\rho}$ and Q if there is no distinction between the analysis to be made. Where a difference arises, this is clearly stated by referring to the single-copy and two-copy implementations respectively.

4.4.2. DERIVATION OF THE FIT MODEL

The reason why this protocol works boils down completely to the question why $\mathbb{E}[q_{\mathbf{i_m}}] = B_0 u(\Lambda)^{m-1}$. This section answers this question, following the line of [13], but leaving out some details. First, some notation is introduced, defining the operators

$$\mathbf{C}_{\mathrm{avg}}^{(n)} := \frac{1}{|\mathcal{C}|}\sum_{C\in\mathcal{C}} \mathbf{C}^{\otimes n}, \tag{4.46}$$

$$\boldsymbol{\mathcal{M}} := C_{\mathrm{avg}}^{(2)} \boldsymbol{\Lambda}^{\otimes 2} C_{\mathrm{avg}}^{(2)}. \tag{4.47}$$

Data: Let $\mathcal{C}_q$ be the Clifford group on a d-dimensional Hilbert space $\mathcal{H}$, with $d = 2^q$ for q qubits, with noisy implementation $C \circ \Lambda$ for all $C \in \mathcal{C}_q$, where $\Lambda \in \mathcal{S}(\mathcal{H})$ is a CPTP map.
Input: Fix the integers N, M. Pick states $\rho, \hat{\rho} \in \mathcal{D}(\mathcal{H} \otimes \mathcal{H})$ and observable $Q \in \mathrm{Herm}(\mathcal{H} \otimes \mathcal{H})$
Output: An estimate of the unitarity of the noise map $u(\Lambda)$.

for $m = 1, ..., M$ **do**
  for $i = 1, ..., N$ **do**
    Sample a random sequence $C_{i_1}, ..., C_{i_m}$ of m gates independently and uniformly drawn from $\mathcal{C}_q$;
    Compose the sequence $W_{\mathbf{i_m}} = C_{i_m} \circ \cdots \circ C_{i_1}$;
    Measure the expectation values $\mathrm{Tr}[QW_{\mathbf{i_m}}^{\otimes 2}(\rho)]$, $\mathrm{Tr}[QW_{\mathbf{i_m}}^{\otimes 2}(\hat{\rho})]$ to a desired precision;
    Compute $q_{\mathbf{i_m}} = \mathrm{Tr}[QW_{\mathbf{i_m}}^{\otimes 2}(\rho)] - \mathrm{Tr}[QW_{\mathbf{i_m}}^{\otimes 2}(\hat{\rho})] = \mathrm{Tr}[QW_{\mathbf{i_m}}^{\otimes 2}(\rho - \hat{\rho})]$;
  end
  Compute the empirical average over the sampled strings $\overline{q}_m = \frac{1}{N}\sum_{i=1}^{N} q_{\mathbf{i_m}}$;
end
Fit $\overline{q}_m$ to the model $\overline{q}_m = B_0 u(\Lambda)^{m-1}$, where B_0 is a constant absorbing state preparation and measurement errors, and $u(\Lambda)$ is the unitarity of the average noise map Λ.

Algorithm 3: Outline of the unitarity randomized benchmarking protocol, using the two-copy implementation.

Data: Let $\mathcal{C}_q$ be the Clifford group on a d-dimensional Hilbert space $\mathcal{H}$, with $d = 2^q$ for q qubits, with noisy implementation $C \circ \Lambda$ for all $C \in \mathcal{C}_q$, where $\Lambda \in \mathcal{S}(\mathcal{H})$ is a CPTP map.
Input: Fix the integers N, M. Pick a set of states $\rho_{\mathcal{H}}^{(a)}, \hat{\rho}_{\mathcal{H}}^{(a)} \in \mathcal{D}(\mathcal{H})$ for $a = 1, ..., K_1$ and a set of observables $Q_{\mathcal{H}}^{(b)} \in \mathrm{Herm}(\mathcal{H})$ for $b = 1, ..., K_2$.
Output: An estimate of the unitarity of the noise map $u(\Lambda)$.

for $m = 1, ..., M$ **do**
  for $i = 1, ..., N$ **do**
    Sample a random sequence $C_{i_1}, ..., C_{i_m}$ of m gates independently and uniformly drawn from $\mathcal{C}_q$;
    Compose the sequence $W_{\mathbf{i_m}} = C_{i_m} \circ \cdots \circ C_{i_1}$;
    for $a = 1, ..., K_1$ **do**
      for $b = 1, ..., K_2$ **do**
        Prepare ρ_a and measure $\mathrm{Tr}[Q_{\mathcal{H}}^{(b)} W_{\mathbf{i_m}}(\rho_{\mathcal{H}}^{(a)})]$ to desired precision;
        Prepare $\hat{\rho}_a$ and measure $\mathrm{Tr}[Q_{\mathcal{H}}^{(b)} W_{\mathbf{i_m}}(\hat{\rho}_{\mathcal{H}}^{(a)})]$ to desired precision;
        Compute $q_{\mathbf{i_m}}^{(a,b)} = \mathrm{Tr}[Q_{\mathcal{H}}^{(b)} W_{\mathbf{i_m}}(\rho_{\mathcal{H}}^{(a)})] - \mathrm{Tr}[Q_{\mathcal{H}}^{(b)} W_{\mathbf{i_m}}(\hat{\rho}_{\mathcal{H}}^{(a)})]$;
      end
    end
    Compute $q_{\mathbf{i_m}} = \sum_{a=1}^{K_1}\sum_{b=1}^{K_2} q_{\mathbf{i_m}}^{(a,b)}$;
  end
  Compute the empirical average over the sampled strings $\overline{q}_m = \frac{1}{N}\sum_{i=1}^{N} q_{\mathbf{i_m}}$;
end
Fit $\overline{q}_m$ to the model $\overline{q}_m = B_0 u(\Lambda)^{m-1}$, where B_0 is a constant absorbing state preparation and measurement errors, and $u(\Lambda)$ is the unitarity of the average noise map Λ.

Algorithm 4: Outline of the unitarity randomized benchmarking protocol, using the single-copy implementation.

The expectation value of $q_{\mathbf{i_m}}$ over all sequences of length m is then given by

$$\begin{aligned}\mathbb{E}[q_{\mathbf{i_m}}] &= \frac{1}{|\mathcal{C}|^m}\sum_{\mathbf{i_m}}\langle\langle Q|\mathbf{W}_{\mathbf{i_m}}^{\otimes 2}|\rho-\hat{\rho}\rangle\rangle \\ &= \langle\langle Q|\prod_{s=1}^{m}\frac{1}{|\mathcal{C}|}\sum_{i_s}\mathbf{C}_{\mathbf{i_s}}{}^{\otimes 2}\mathbf{\Lambda}^{\otimes 2}|\rho-\hat{\rho}\rangle\rangle \\ &= \langle\langle Q|\left(\mathbf{C}_{\text{avg}}^{(2)}\mathbf{\Lambda}^{\otimes 2}\right)^m|\rho-\hat{\rho}\rangle\rangle \\ &= \langle\langle Q|\left(\mathbf{C}_{\text{avg}}^{(2)}\mathbf{\Lambda}^{\otimes 2}\mathbf{C}_{\text{avg}}^{(2)}\right)^{m-1}|\Lambda^{\otimes 2}(\rho-\hat{\rho})\rangle\rangle \\ &= \langle\langle Q|\mathcal{M}^{m-1}|\rho-\hat{\rho}\rangle\rangle,\end{aligned} \tag{4.48}$$

where in the first line it is used that the sum can be done over each i_s, $s=1,...,m$ independently, in the second line it is used that $\mathbf{C}_{\text{avg}}^{(n)}$ is an orthogonal projection (onto the trivial subrepresentations of the representation $C\mapsto\mathbf{C}^{\otimes n}$, see Lemma 2.3.5) so that $(\mathbf{C}_{\text{avg}}^{(n)})^2=\mathbf{C}_{\text{avg}}^{(n)}$ for all n, and finally one $\Lambda^{\otimes 2}$ is absorbed into the state preparation error, since up to this point no assumptions about $\rho-\hat{\rho}$ have been made.

Up until now, the expectation value is only rewritten as $\mathbb{E}[q_{\mathbf{i_m}}]=\langle\langle Q|\mathcal{M}^{m-1}|\rho-\hat{\rho}\rangle\rangle$, with $\mathcal{M}$ defined above. To make progress, the matrix $\mathcal{M}$ analyzed. Key fact here is that $\mathbf{C}_{\text{avg}}^{(2)}$ is the orthogonal projection onto the trivial subrepresentations of $C\mapsto\mathbf{C}^{\otimes 2}$ (Lemma 2.3.5). Since $\mathcal{M}=\mathbf{C}_{\text{avg}}^{(2)}\mathbf{\Lambda}^{\otimes 2}\mathbf{C}_{\text{avg}}^{(2)}$, it is clear that $\mathcal{M}$ only has support on the trivial subrepresentations of $C\mapsto\mathbf{C}^{\otimes 2}$. These were found in Proposition 3.6.4, and the result is that there are two trivial subrepresentations present [13], spanned by

$$B_1=\sigma_0\otimes\sigma_0 \quad\text{and}\quad B_2=\frac{1}{\sqrt{d^2-1}}\sum_{\sigma\in\mathcal{Q}^*}\sigma\otimes\sigma. \tag{4.49}$$

Therefore $\mathbf{C}_{\text{avg}}^{(2)}=|B_1\rangle\rangle\langle\langle B_1|+|B_2\rangle\rangle\langle\langle B_2|$ and the only nonzero elements of $\mathcal{M}$ are [13]

$$\begin{aligned}\langle\langle B_1|\mathcal{M}|B_1\rangle\rangle &= \langle\langle\sigma_0|\mathbf{\Lambda}|\sigma_0\rangle\rangle^2=1, \\ \langle\langle B_1|\mathcal{M}|B_2\rangle\rangle &= \frac{1}{\sqrt{d^2-1}}\sum_{\sigma\in\mathcal{Q}^*}\langle\langle\sigma_0|\mathbf{\Lambda}|\sigma\rangle\rangle^2=0, \\ \langle\langle B_2|\mathcal{M}|B_1\rangle\rangle &= \frac{1}{\sqrt{d^2-1}}\sum_{\sigma\in\mathcal{Q}^*}\langle\langle\sigma|\mathbf{\Lambda}|\sigma_0\rangle\rangle^2=\frac{1}{\sqrt{d^2-1}}\|\alpha(\Lambda)\|^2, \\ \langle\langle B_2|\mathcal{M}|B_2\rangle\rangle &= \frac{1}{d^2-1}\sum_{\sigma,\tau\in\mathcal{Q}^*}\langle\langle\sigma|\mathbf{\Lambda}|\tau\rangle\rangle^2=\frac{1}{d^2-1}\text{Tr}[\mathbf{\Lambda}_{\text{u}}^\dagger\mathbf{\Lambda}_{\text{u}}]=u(\mathcal{E}),\end{aligned} \tag{4.50}$$

for any CPTP quantum channel Λ, using the block form of a CPTP map (3.22). In other words, in the basis B_1,B_2, the matrix $\mathcal{M}$ takes the form

$$\mathcal{M}=\begin{bmatrix}1 & 0\\ \frac{\|\alpha(\Lambda)\|^2}{\sqrt{d^2-1}} & u(\Lambda)\end{bmatrix}, \tag{4.51}$$

So that

$$\mathcal{M}^{m-1}=\begin{bmatrix}1 & 0\\ \frac{\|\alpha(\Lambda)\|^2}{\sqrt{d^2-1}}(1+\sum_{j=1}^{m-2}u(\Lambda)^j) & u(\Lambda)^{m-1}\end{bmatrix}=\begin{bmatrix}1 & 0\\ \frac{\|\alpha(\Lambda)\|^2}{\sqrt{d^2-1}}\frac{1-u(\Lambda)^{m-1}}{1-u(\Lambda)} & u(\Lambda)^{m-1}\end{bmatrix}, \tag{4.52}$$

where in the case $u(\Lambda)=1$, the term $\frac{1-u(\Lambda)^{m-1}}{1-u(\Lambda)}$ should be interpreted as the limit, since

$$\lim_{u(\Lambda)\to 1}\frac{1-u(\Lambda)^{m-1}}{1-u(\Lambda)}=m-1=\lim_{u(\Lambda)\to 1}\left(1+\sum_{j=1}^{m-2}u(\Lambda)^j\right).$$

Note that $u(\Lambda) = 1$ implies $\|\alpha(\Lambda)\|^2 = 0$ by Proposition 4.4.1. Now everything is set to evaluate $\mathbb{E}[q_{\mathbf{i_m}}]$ and obtain the fit model

$$\begin{aligned}\mathbb{E}[q_{\mathbf{i_m}}] = \langle\langle Q|\mathcal{M}^{m-1}|\rho - \hat{\rho}\rangle\rangle &= \begin{bmatrix} Q_1 & Q_2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \frac{\|\alpha(\Lambda)\|^2}{\sqrt{d^2-1}} \frac{1-u(\Lambda)^{m-1}}{1-u(\Lambda)} & u(\Lambda)^{m-1} \end{bmatrix} \begin{bmatrix} 0 \\ \rho_2 \end{bmatrix} \\ &= Q_2\rho_2 u^{m-1},\end{aligned} \tag{4.53}$$

where $Q_1 = \langle\langle B_1|Q\rangle\rangle$, $Q_2 = \langle\langle B_2|Q\rangle\rangle$ and $\rho_2 = \langle\langle B_2|\rho - \hat{\rho}\rangle\rangle$. Note that here it is very useful that $\langle\langle B_1|\rho - \hat{\rho}\rangle\rangle = 0$. It can easily be verified here that if this were not used, than a fit model of the form $\mathbb{E}[q_{\mathbf{i_m}}] = A_0 + B_0 u(\Lambda)^{m-1}$ is obtained, by putting $\rho_1 = \langle\langle B_1|\rho\rangle\rangle = \frac{1}{\sqrt{d}}$ in the above expression.

Not only is the form of the fit model derived, also the prefactor is obtained. From this it can be seen that a large component in B_2 is preferred for input states and measurements. This is where the difference between the two implementations of Algorithm 3 and Algorithm 4 becomes clear. In the two-copy, scalable implementation, the aim is to just prepare and measure along B_2 as best as experimentally possible. In the single-copy implementation however, one can not prepare and measure along B_2, since B_2 is not of tensor product form. Instead, the experimenter aims to prepare and measure $\rho_\sigma - \hat{\rho}_\sigma \propto \sigma$ and $Q_\tau \propto \tau$ for all $\sigma, \tau \in \mathcal{Q}^*$ and measures

$$q_{\mathbf{i_m}} = \sum_{\sigma,\tau\in\mathcal{Q}^*} \mathrm{Tr}[Q_\tau W_{\mathbf{i_m}} (\rho_\sigma - \hat{\rho}_\sigma)]^2,$$

such that $q_{\mathbf{i_m}}$ is then computed with the equivalent states and measurements $\rho - \hat{\rho} = \sum_{\sigma\in\mathcal{Q}^*} \rho_\sigma - \hat{\rho}_\sigma$ and $Q = \sum_{\tau\in\mathcal{Q}^*} Q_\tau \otimes Q_\tau$. This yields approximate proportionality to B_2, but is not scalable since the number of non-identity Pauli matrices is $d^2 - 1 = 4^q - 1$.

The key advantage of this protocol, similar to the standard randomized benchmarking protocol, is its robustness against state preparation and measurement errors (SPAM). In fact, no assumptions about Q, ρ and $\hat{\rho}$ have been made so far, so they can incorporate arbitrary SPAM errors. However in order to (efficiently) fit the unitarity, a large component Q_2 and ρ_2 in the basis B_2 is required. Simply scaling Q and $\rho - \hat{\rho}$ does not achieve anything however, since then $q_{\mathbf{i_m}}$ scales accordingly. The state preparation and measurement errors do influence the variance $\mathbb{V}[q_{\mathbf{i_m}}]$, which is discussed in detail in chapter 5.

4.4.3. FIRST ORDER BOUND ON THE NUMBER OF SEQUENCES REQUIRED

Similarly to the randomized benchmarking protocol, it is natural to ask about the statistics of this protocol. In particular, how many strings N (possibly dependent on m) does one need to average over in order to obtain a good estimate for the exact expectation value. Again, it is infeasible to average over all possible sequences of length m, even in the single-qubit case where $|\mathcal{C}_1| = 24$, as the number of different sequences then grows exponentially in m (with base 24). The answer is provided by applying concentration inequalities. Hoeffding's first inequality (Theorem 3.1.1), which states

$$\mathbb{P}\left[\left|\frac{\overline{q}_m}{b-a} - \mathbb{E}[\frac{q_{\mathbf{i_m}}}{b-a}]\right| \geq \epsilon\right] \leq 2e^{-2N\epsilon^2}, \tag{4.54}$$

can be used to provide a first estimate N. Here $q_{\mathbf{i_m}} \in [a, b]$ and ϵ is the distance of the estimate $\overline{q}_m$ to the mean $\mathbb{E}[q_{\mathbf{i_m}}]$ *relative to* the interval size $b - a$. Given a relative interval $\epsilon > 0$ and a desired upper bound of the probability $\delta > 0$, the number of sequences needed is then given (just like for standard randomized benchmarking) by

$$N \geq \frac{\ln(\frac{2}{\delta})}{2\epsilon^2}, \tag{4.55}$$

Following the approach of [16], a bound on $\mathbb{V}[q_{\mathbf{i_m}}]$ is required to provide a sharper bound using Hoeffding's second inequality (Theorem 3.1.1). In chapter 5 this quantity is analyzed for the first time, in order to put a rigorous bound on N that is hopefully much smaller than the above equation.

5

BOUND ON THE NUMBER OF RANDOM SEQUENCES IN UNITARITY RANDOMIZED BENCHMARKING

In this chapter the statistics of the unitarity randomized benchmarking protocol are analyzed in detail. The main question answered in this section is how many random sequences are needed to rigorously perform unitarity randomized benchmarking. All the relevant prerequisite knowledge as well as details of the protocol have been introduced in the previous chapters. Therefore this chapters directly starts with a statement of the main result of our analysis, with a new theorem that gives a reduced number of sequences needed. The result is discussed in detail, with extra emphasis on the different implementations possible and the contributions of state preparation and measurements. Only after this presentation of the result, a detailed proof on the variance bound required to prove our main result is shown. First a treatment of ideal state preparation and measurements is done, after which the result is extended to the general case that allows for non-ideal state preparation and measurements. This chapter concludes with a discussion on a possible extension to the multi-qubit case and a summary of the main implications of our result.

5.1. INTRODUCTION

In this chapter the main results of the thesis are presented. Our result puts a rigorous bound on the number of sequences N needed to perform the unitarity randomized benchmarking protocol and obtain the unitarity of the error map up to a specified degree of certainty. The unitarity randomized benchmarking protocol was discussed in section 4.4 and this chapter continues to build on the contents of this section. A first order concentration inequality was used to bound the number of sequences N in subsection 4.4.3, providing a bound that is independent of sequence length m and number of qubits q comprising the system. This result was valid under the assumption that the error model is gate and time independent. This means that any Clifford gate $C \in \mathcal{C}$ has a noisy implementation that can be modeled by $C \circ \Lambda$, where Λ is a CPTP quantum channel independent of C and of any previous or sequentially applied gates. In this chapter, this result is improved under two additional assumptions. The first additional assumption is that the gate set to be benchmarked is the Clifford group $\mathcal{C}$. Even though the protocol works for any finite subgroup of the unitary group that is also a unitary 2-design, the analysis here is specific to the group being benchmarked. The Clifford group is chosen, because of its importance in quantum information applications and because of the thorough understanding of the relevant representations of this group. The second additional assumption is the restriction to the single-qubit case, because it is considerably more easy to analyze than the multi-qubit case. This is due to several reasons, on which some more comments are provided in section 5.5.

This chapters is structured in a top-down way, starting with the statement of our main result in section 5.2. The purpose of this section is to state in complete detail the result and show precisely how the second order concentration inequality was used to derive a bound on the number of sequences, given a variance bound. It is discussed in detail how the number of sequences N depends on the various parameters involved. The difference between single-copy and two-copy implementation is discussed. Then section 5.3 serves to illustrate the main result using experimental data on the magnitude of the state preparation and measurement errors. Next in section 5.4 a bound on the variance needed to bound the number of sequences is presented. This section contains all the technical parts to completely proof the bound. First a bound is derived for ideal state preparation and measurements. This result is then extended to include state preparation and measurement errors, completing the variance bound. A brief discussion on the result is also given. The chapter continues with section 5.5, which draws a comparison between the single-qubit and multi-qubit case, outlining where specific single-qubit results are used. Finally the chapter concludes with section 5.6, which summarized the main implications of our result and suggests some future research directions.

5.2. THE IMPROVED BOUND ON THE NUMBER OF SEQUENCES REQUIRED

This section starts from the goal of finding a better bound on the number of sequences N than the bound found in subsection 4.4.3 using a first order concentration inequality. In an attempt to improve the bound, a second order concentration inequality (Theorem 3.1.2) can be used. Here 'first order' means that only information on the upper and lower bound of the distribution of the random variable $q_{\mathbf{i_m}}$ is needed, while a 'second order' means that additionally a bound on the variance $\mathbb{V}[q_{\mathbf{i_m}}]$ is required. The main effort of improving the bound on N is finding a tight enough bound on $\mathbb{V}[q_{\mathbf{i_m}}]$, a task to which most of the remainder of this chapter is dedicated. This section however shows how to apply the concentration inequality and summarizes the bound that this yields on N, given the bound on the variance $\mathbb{V}[q_{\mathbf{i_m}}]$ that is derived in a later section in this chapter.

Let us briefly recapture what we have so far. Consider string $W_{\mathbf{i_m}}$ of m independently and uniformly drawn elements from the single-qubit Clifford group. Then

$$q_{\mathbf{i_m}} = \langle\langle Q | \mathbf{W}_{\mathbf{i_m}}^{\otimes 2} | \rho - \hat{\rho} \rangle\rangle \tag{5.1}$$

is the random variable of interest in the protocol, where Q is any two-qubit hermitian observable

and $\rho, \hat{\rho}$ are any two different two-qubit states. The mean of the random variable $q_{\mathbf{i_m}}$ over all strings $W_{\mathbf{i_m}}$ of length m satisfies

$$\mathbb{E}[q_{\mathbf{i_m}}] = \langle Q_{\text{ideal}} | \rho_{\text{ideal}} \rangle \, u^{m-1}, \tag{5.2}$$

where ρ_{ideal} and Q_{ideal} are defined in (5.73) and (5.74) respectively and where $u = u(\Lambda)$ is the unitarity of the error channel. The experimental procedure is clear: obtain an estimate $\overline{q}_m = \frac{1}{N}\sum_{\mathbf{i_m}} q_{\mathbf{i_m}}$ of $\mathbb{E}[q_{\mathbf{i_m}}]$ for various values of m to certain degree of accuracy and fit to a model of the form Ku^{m-1} for some constant K. Since the number of strings $W_{\mathbf{i_m}}$ grows exponentially in m, it is infeasible to obtain an exact average. The natural question then is how many sequences N (possibly dependent on m) are needed to be sure that the estimate $\overline{q}_m$ is close enough to the exact mean $\mathbb{E}[q_{\mathbf{i_m}}]$. A first order concentration inequality (Theorem 3.1.1) yielded

$$N \geq \frac{\ln(\frac{2}{\delta})}{2\epsilon^2}, \tag{5.3}$$

where $\delta > 0$ is an upper bound for the probability that the estimate $\overline{q}_m$ deviates more than $\epsilon > 0$ from the exact mean $\mathbb{E}[q_{\mathbf{i_m}}]$ *relative to* the interval length $b-a$, where $a \leq q_{\mathbf{i_m}} \leq b$. In an effort to improve this bound, a second order concentration inequality is invoked (Theorem 3.1.2):

$$\mathbb{P}\left[\frac{|\overline{q}_m - \mathbb{E}[q_{\mathbf{i_m}}]|}{b-a} \geq \epsilon\right] \leq 2\left(\left(\frac{1}{1-\epsilon}\right)^{\frac{1-\epsilon}{\sigma^2+1}}\left(\frac{\sigma^2}{\sigma^2+\epsilon}\right)^{\frac{\sigma^2+\epsilon}{\sigma^2+1}}\right)^N, \tag{5.4}$$

where $\sigma^2 \geq \mathbb{V}[\frac{q_{\mathbf{i_m}}}{b-a}]$ is an upper bound for the variance of the scaled random variable $\frac{q_{\mathbf{i_m}}}{b-a}$. Bounding this probability by a small number $\delta > 0$ and solving for N provides a method to find the number of sequences needed as a function of σ^2, δ and ϵ:

$$N \geq \frac{\ln\left(\frac{\delta}{2}\right)}{\left(\frac{1-\epsilon}{\sigma^2+1}\right)\ln\left(\frac{1}{1-\epsilon}\right) + \left(\frac{\sigma^2+\epsilon}{\sigma^2+1}\right)\ln\left(\frac{\sigma^2}{\sigma^2+\epsilon}\right)}, \tag{5.5}$$

It is now clear that a sufficiently good bound σ^2 is required in order for this bound to be better than the first order bound of (5.3). Note that this bound also requires knowledge of the interval $b-a$ in which $q_{\mathbf{i_m}}$ is contained.

The resulting main theorem is a bound on N that is stated using bounds a, b on $q_{\mathbf{i_m}}$ (Proposition 5.4.12) and a bound on $\mathbb{V}[q_{\mathbf{i_m}}]$ (Theorem 5.4.9), both of which are formulated in later sections of this chapter. The idea is to first put emphasis on the result and illustrate its practical implications using an example. The theorem provides a procedure for computing N, and the proof is relatively straightforward. It illustrates nicely how the concentration inequality is applied and what the parameters are on which N depends.

Theorem 5.2.1 (Main theorem: Improved bound on number of sequences)**.** *Let $\Lambda \in \mathcal{S}(\mathbb{C}^2)$ be a single-qubit CPTP quantum channel that corresponds to the constant error map associated with each element of the single-qubit Clifford group $\mathcal{C}_1$, with a priori estimate of the unitarity $u(\Lambda) \geq u$. Furthermore let $\rho, \hat{\rho} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ be two density matrices and let $Q \in \text{Herm}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ be a hermitian observable. Define the following basis operators in $\mathcal{L}(\mathcal{H})$:*

$$B_1 = \sigma_0 \otimes \sigma_0 = \frac{I \otimes I}{2} \qquad \textit{and} \qquad B_2 = \frac{1}{3}\sum_{\tau \in \mathcal{Q}_1^*} \tau \otimes \tau = \frac{1}{2\sqrt{3}}(X \otimes X + Y \otimes Y + Z \otimes Z), \tag{5.6}$$

where I, X, Y, Z are the four single-qubit Pauli matrices. Also denote $\tilde{Q} := Q - \langle B_1 | Q \rangle \, B_1$ and define the following two mutually orthogonal components of $\rho - \hat{\rho}$ and $\tilde{Q}$ respectively

$$\rho_{\text{ideal}} := \langle B_2 | \rho - \hat{\rho} \rangle \, B_2, \qquad\qquad \rho_{\text{err}} := \rho - \hat{\rho} - \rho_{\text{ideal}}, \tag{5.7}$$

$$Q_{\text{ideal}} := \langle B_2|Q\rangle\, B_2, \qquad Q_{\text{err}} := \tilde{Q} - Q_{\text{ideal}}. \tag{5.8}$$

Finally let $\delta > 0$ and $0 < \epsilon < 1$. Denote $a \le q_{\mathbf{i_m}} \le b$ upper and lower bounds for $q_{\mathbf{i_m}}$ and let $L = \frac{b-a}{\|\tilde{Q}\|_2\|\rho-\hat{\rho}\|_2}$.

Then the number of sequences N needed to bound

$$\mathbb{P}\left[\left|\frac{\overline{q}_m - \mathbb{E}[q_{\mathbf{i_m}}]}{\|\tilde{Q}\|_2\|\rho-\hat{\rho}\|_2}\right| \ge \epsilon L\right] \le \delta \tag{5.9}$$

by δ is given by

$$N \ge \frac{\ln\frac{\delta}{2}}{\frac{1-\epsilon L}{\sigma^2+1}\ln\left(\frac{1}{1-\epsilon L}\right) + \frac{\sigma^2+\epsilon L}{\sigma^2+1}\ln\left(\frac{\sigma^2}{\sigma^2+\epsilon L}\right)}. \tag{5.10}$$

If the general two-copy implementation is used, then $L = 2\sqrt{2}$ and σ^2 is given by

$$\sigma^2 = \left(\left[\frac{3\sqrt{3}}{2} + \sqrt{2}\right](1-u)^2\frac{1-u^{2(m-1)}}{1-u^2}\frac{\|\rho_{\text{ideal}}\|_2^2}{\|\rho-\hat{\rho}\|_2^2} + \alpha\frac{\|\rho_{\text{err}}\|_2^2}{\|\rho-\hat{\rho}\|_2^2}\right)\left(1 + \frac{\|Q_{\text{err}}\|_2^2}{\|\tilde{Q}\|_2^2}\right), \tag{5.11}$$

where $\alpha = 4$.

However, if $\rho, Q \in \text{Span}\{\mathcal{Q}_1^*\}^{\otimes 2} = \text{Span}\{\frac{X}{\sqrt{2}}, \frac{Y}{\sqrt{2}}, \frac{Z}{\sqrt{2}}\}^{\otimes 2}$, which is the case in the single-copy implementation of Algorithm 4, the bound can be improved to $\alpha = 1$ and $L = 1$ in the above expressions.

Proof. The idea is to apply the variance bound of Theorem 5.4.9 to the concentration inequality of Theorem 3.1.2. In order to do so, one needs a interval $q_{\mathbf{i_m}} \in [a, b]$ in which $q_{\mathbf{i_m}}$ is assumed to lie. This is provided by Proposition 5.4.12. In the general case, one has that

$$L = \frac{b-a}{\|\tilde{Q}\|_2\|\rho-\hat{\rho}\|_2} = 2\sqrt{2}.$$

The variance of $q_{\mathbf{i_m}}$ satisfies (Theorem 5.4.9)

$$\mathbb{V}[q_{\mathbf{i_m}}] \le \left(\left(\frac{3\sqrt{3}}{2} + \sqrt{2}\right)(1-u)^2\frac{1-u^{2(m-1)}}{1-u^2}\|\rho_{\text{ideal}}\|_2^2 + \alpha\|\rho_{\text{err}}\|_2^2\right)\left(\|Q_{\text{ideal}}\|_2^2 + 2\|Q_{\text{err}}\|_2^2\right),$$

with $\alpha = 4$, so that

$$\mathbb{V}\left[\frac{q_{\mathbf{i_m}}}{\|\tilde{Q}\|_2\|\rho-\hat{\rho}\|_2}\right] = \frac{\mathbb{V}[q_{\mathbf{i_m}}]}{\|\tilde{Q}\|_2^2\|\rho-\hat{\rho}\|_2^2} \le \sigma^2$$

by dividing the above inequality by $\|\tilde{Q}\|_2^2\|\rho-\hat{\rho}\|_2^2$. Then the concentration inequality Theorem 3.1.2 claims that

$$\mathbb{P}\left[\left|\frac{\overline{q}_m - \mathbb{E}[q_{\mathbf{i_m}}]}{b-a}\right| \ge \epsilon\right] \le 2\left(\left(\frac{1}{1-\epsilon}\right)^{\frac{1-\epsilon}{\sigma^2+1}}\left(\frac{\sigma^2}{\sigma^2+\epsilon}\right)^{\frac{\sigma^2+\epsilon}{\sigma^2+1}}\right)^N,$$

which is equivalent to

$$\mathbb{P}\left[\left|\frac{\overline{q}_m - \mathbb{E}[q_{\mathbf{i_m}}]}{\|\tilde{Q}\|_2\|\rho-\hat{\rho}\|_2}\right| \ge \epsilon L\right] \le 2\left(\left(\frac{1}{1-\epsilon L}\right)^{\frac{1-\epsilon L}{\sigma^2+1}}\left(\frac{\sigma^2}{\sigma^2+\epsilon L}\right)^{\frac{\sigma^2+\epsilon L}{\sigma^2+1}}\right)^N.$$

Upper bounding this by δ and Solving for N, yields the result.

In case of single-copy implementation, where $\rho, Q \in \text{Span}\{\mathcal{Q}_1^*\}^{\otimes 2}$, Proposition 5.4.12 implies $L = 1$ and Theorem 5.4.9 implies $\alpha = 1$ in the above equations, improving the result. ∎

The form of the bound as presented in Theorem 5.2.1 is aimed at showing clearly the key independent parameters that determine the number N of sequences needed. Of course, if there is a reason to assume a different interval $[a,b]$ than presented in Proposition 5.4.12, the final result changes slightly, but the proof of Theorem 5.2.1 clearly outlines the simple procedure how to apply the variance bound of Theorem 5.4.9. As presented here, N can be computed as a function of

$$N = N\left(u, m, \alpha, \frac{\|\rho_{\text{err}}\|_2^2}{\|\rho-\hat{\rho}\|_2^2}, \frac{\|Q_{\text{err}}\|_2^2}{\|\tilde{Q}\|_2^2}, \epsilon, \delta, L\right). \tag{5.12}$$

This is clear from the theorem by noting that

$$\|Q_{\text{err}}\|_2^2 + \|Q_{\text{ideal}}\|_2^2 = \|\tilde{Q}\|_2^2 \qquad \text{and} \qquad \|\rho_{\text{err}}\|_2^2 + \|\rho_{\text{ideal}}\|_2^2 = \|\rho-\hat{\rho}\|_2^2,$$

due to the orthogonality between the ideal and error components of $\rho-\hat{\rho}$ and $\tilde{Q}$ respectively. This dependence makes sense intuitively. The pair of variables ϵ, δ determine the amount of confidence desired. The quantities

$$0 \leq \frac{\|\rho_{\text{err}}\|_2^2}{\|\rho-\hat{\rho}\|_2^2}, \frac{\|Q_{\text{err}}\|_2^2}{\|\tilde{Q}\|_2^2} \leq 1$$

are interpreted as the magnitude of the error components relative to the total magnitude squared of the state preparation and measurement operator respectively. For simplicity from now on they are referred to as the relative state preparation error and relative measurement error respectively. Together with u, an a priori lower bound on the unitarity of the error channel, m, the length of the sequence, and α, a constant depending on the choice of implementation (single-copy versus two-copy), these relative state preparation and measurement errors influence the bound σ^2 on the variance of the scaled random variable $\mathbb{V}\left[\frac{q_{\mathbf{i_m}}}{\|\tilde{Q}\|_2, \|\rho-\hat{\rho}\|_2}\right]$. The quantity L quantifies the a priori interval length $b-a$ (in units of $\|\tilde{Q}\|_2, \|\rho-\hat{\rho}\|_2$) in which $q_{\mathbf{i_m}}$ is assumed to lie (therefore also providing information about the distribution). Note that L is here computed depending on the choice of implementation.

To get the number N down, it is necessary to get a good bound on L, which was done in Proposition 5.4.12 and used in the above theorem. If there is a reason to refine this bound, this should be done as it decreases N (or alternatively, improves the confidence interval ϵL by bringing this number down). The variable $q_{\mathbf{i_m}}$ was scaled by $\|\tilde{Q}\|_2\|\rho-\hat{\rho}\|_2$ in order to show the independence of the result to scaling the operators. Furthermore it allowed to formulate a bound σ^2 that only depends on u, m and the relative state preparation and measurement errors

$$\frac{\|\rho_{\text{err}}\|_2^2}{\|\rho-\hat{\rho}\|_2^2}, \frac{\|Q_{\text{err}}\|_2^2}{\|\tilde{Q}\|_2^2}.$$

An obvious question that can be raised is how sensitive this result is to state preparation and measurement errors, since they contribute a constant factor (that is, constant with respect to $(1-u)$) to the number of sequences needed. This constant term, independent of m, u is of the form

$$\alpha \frac{\|\rho_{\text{err}}\|_2^2}{\|\rho-\hat{\rho}\|_2^2}\left(1 + \frac{\|Q_{\text{err}}\|_2^2}{\|\tilde{Q}\|_2^2}\right), \tag{5.13}$$

where $\alpha = 4$ or $\alpha = 1$ depending on the choice of two-copy or single-copy implementation. It is clear that the relative error in state preparation contributes more to this term than the relative error in measurement. Therefore reducing the number of sequences needed can best be achieved by increasing the quality of the state preparation. Figure 5.1 shows a contour plot of N as a function of the relative state preparation and measurement errors, holding all other parameters constant. This shows indeed the stronger dependence on the state preparation error than the measurement

error. The relative state preparation and measurement errors are required in the Hilbert-Schmidt norm. This can be experimentally challenging to obtain. The absolute state preparation error may be bounded by the fidelity using the Fuchs–Van de Graaf inequalities (Theorem 2.5.11). However, as these inequalities may be really loose, this can result in a huge overestimation of the required number of sequences N. In the next section, experimental data is used to illustrate realistic numbers for these errors.

Before doing so, it is analyzed how the new bound of Theorem 5.2.1 performs compared to the simple first order concentration inequality bound as a function of u. In Figure 5.2 N is plotted as a function of u in the limit of large m for 'small' and 'large' relative SPAM errors. The justification of these errors is done in the next section, where the role of these errors is examined in more detail. The main conclusions of this figure are the following: the second order inequality outperforms the first order only in the regime of large unitarity, where $u > 0.9$ approximately, even in the absence of SPAM errors. Adding SPAM errors pushes up this regime slightly further, but in the regime of interest (say $u > 0.99$) the reduction of N is significant even in the present of SPAM. It can be seen that the SPAM errors contribute a more or less fixed offset in N (the offset is not constant, since N is a nonlinear function of σ^2).

5.3. ILLUSTRATION OF THE RESULTS

In this section, the result of Theorem 5.2.1 is illustrated using experimental data. The idea is to use realistic values for relative SPAM errors, obtained from experimental data. The data is a complete gate set tomography (GST) dataset[1] for a transmon qubit, obtained in the experiment discussed in [47]. The data that a full GST provides is the Liouville vector of the state that is prepared and the POVM element that constitutes the physical measurement performed, as well as the Liouville matrices for the physical gates that can be implemented. Of course, having such a complete description renders the benchmarking protocol redundant, but the main idea here is just to illustrate realistic values for the relative state preparation and measurement errors.

In this dataset, the pure state $|0\rangle\langle 0|$ is aimed for during state preparation, whereas the measurement aimed for is the projective measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. The noisy state preparation is then denoted ρ_0 and the noisy general POVM is denoted $\{I - E_1, E_1\}$, where E_1 is aimed to be the projection $|1\rangle\langle 1|$. The qubit operations that can be performed are rotations about the X- and Y-axis of the Bloch sphere by $\pi/2$ and π radians. Let them be denoted $X_{\pi/2}, X_\pi, Y_{\pi/2}, Y_\pi$ respectively. These four rotations are in practice sufficient to implement any single-qubit Clifford (since any antipodal pole on the Bloch sphere can be rotated to any other by concatenation of these rotations). The data that describes the noisy state preparation and measurement is summarized in Table 5.1, whereas the noisy gate data is summarized in Table 5.2. The experimental uncertainty in the data is ignored, since this data is only used as an example calculation. To relate this data to experimentally accessible quantities, the state fidelity is computed to be

$$F(\rho_0, |0\rangle\langle 0|) = \sqrt{0.9815} = 0.991. \tag{5.14}$$

An experimental way to quantify the performance of a measurement, is to estimate the probability ϵ_{ij} of incorrectly assigning measurement result j for an input state $|i\rangle$ [48]. In the case here, that means that

$$\epsilon_{01} := \mathrm{Tr}[E_1\rho_0], \tag{5.15}$$

$$\epsilon_{10} := 1 - \mathrm{Tr}[E_1 X_\pi(\rho_0)], \tag{5.16}$$

where the rotation $X_\pi(\rho)$ is used to simulate the state preparation of $|1\rangle\langle 1|$ under noisy circumstances. Computing these quantities for the data set at hand yields $\epsilon_{01} = 0.0471$ and $\epsilon_{10} = 0.0730$.

[1] The data was received via private communication with the authors of [47]

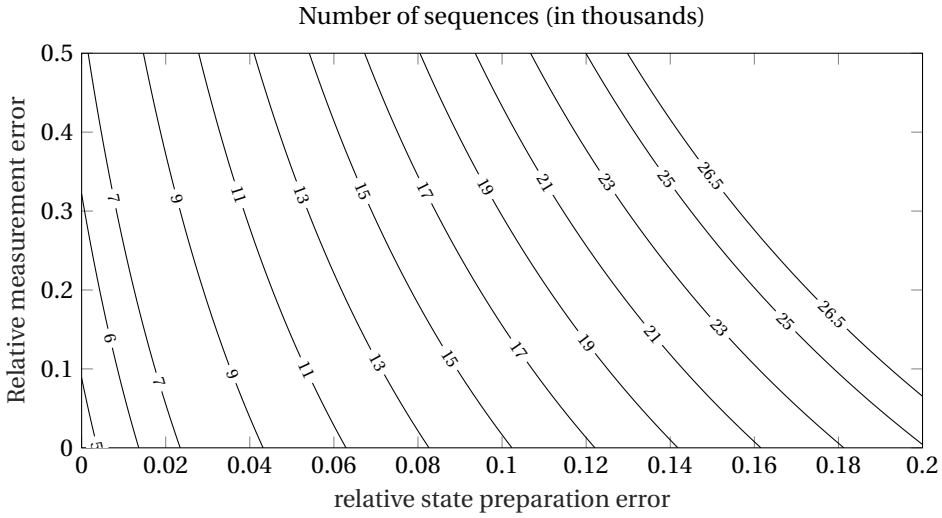

Figure 5.1: Contour plot of the number of sequences needed N (in thousands), as a function of the relative state preparation error $\frac{\|\rho_{\text{error}}\|_2^2}{\|\rho-\hat{\rho}\|_2^2}$ and the relative measurement error $\frac{\|Q_{\text{error}}\|_2^2}{\|\bar{Q}\|_2^2}$, for constant values of $u = 0.98$, $\delta = \epsilon = 0.01$ in the limit of large m, under the assumption of the single-copy implementation ($\alpha = L = 1$). In the region where $N > 26500$, the variance analysis does not provide any more information than can already be obtained from the first order concentration inequality.

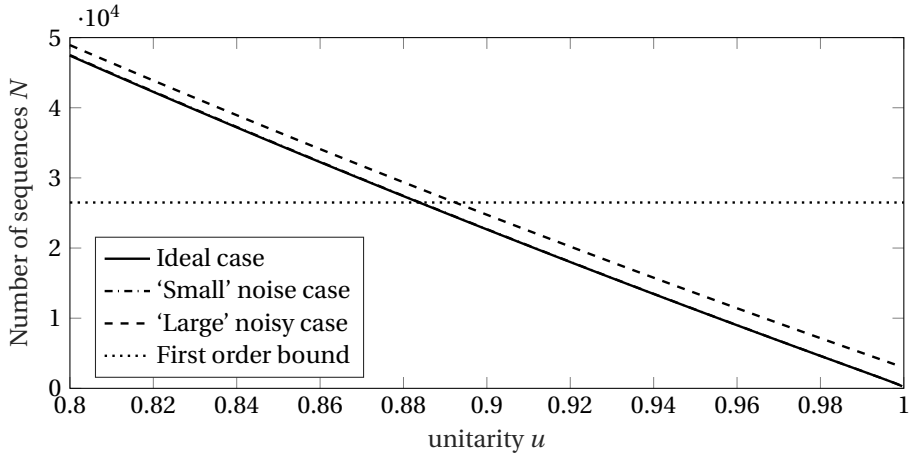

Figure 5.2: Plot of the number of sequences N as a function of the unitarity u in the limit of large m, using $\delta = \epsilon = 0.01$ and $\alpha = L = 1$ (corresponding to the single-copy implementation). Here 'small' noise case corresponds to $\frac{\|\rho_{\text{err}}\|_2^2}{\|\rho-\hat{\rho}\|_2^2} = 3.90 \cdot 10^{-5}$ and $\frac{\|Q_{\text{err}}\|_2^2}{\|\bar{Q}\|_2^2} = 1.63 \cdot 10^{-3}$, whereas 'large' errors correspond to $\frac{\|\rho_{\text{err}}\|_2^2}{\|\rho-\hat{\rho}\|_2^2} = 0.0249$ and $\frac{\|Q_{\text{err}}\|_2^2}{\|\bar{Q}\|_2^2} = 8.43 \cdot 10^{-4}$. See next section for justification of these choices. The dashdotted line of the 'small' noise case is on top of the solid line of the idea case, indicating negligible contribution of the state preparation and measurement errors.

Sometimes ϵ_{10} and ϵ_{01} are combined in a single figure of merit for the performance of a measurement, using the average assignment fidelity of single-shot readout defined as $F_{\text{a}} := 1 - \frac{1}{2}(\epsilon_{01} + \epsilon_{10})$ [48]. The data used here then yields $F_{\text{a}} = 0.940$. The average gate fidelity $\overline{F}$ of all of these gates can be computed to be at least $\overline{F} = 0.999$ for all four gates.

In the simulated protocol, the states $\rho_{\mathcal{H}}^{(\sigma)} = \frac{I+\sigma}{2}$, $\hat{\rho}_{\mathcal{H}}^{(\sigma)} = \frac{I-\sigma}{2}$ are prepared for all three non-identity Pauli's $\sigma \in \mathcal{P}_1^* = \{X, Y, Z\}$, using the available state preparation ρ_0 that is a noisy preparation of $|0\rangle$ followed by an available noisy gate to rotate the qubit to the correct state. The measurement $Q_{\mathcal{H}} = \mathcal{E}_0 - E_1$ is the Z-measurement, and the X and Y measurements are performed by rotating the qubit directly before performing the measurement. All combinations of X, Y, Z states and measurements are performed for a single sequence, and their outcomes squared are added together to form $q_{\mathbf{i_m}}$. In other words, $q_{\mathbf{i_m}}$ is measured as follows

$$q_{\mathbf{i_m}} = \sum_{\sigma,\tau \in \mathcal{P}_1^*} \langle\langle \rho_{\mathcal{H}}^{(\sigma)} - \hat{\rho}_{\mathcal{H}}^{(\sigma)} | \mathbf{W}_{\mathbf{i_m}} | Q_{\mathcal{H}}^{(\tau)} \rangle\rangle^2, \tag{5.17}$$

yielding an effective

$$\rho - \hat{\rho} = \sum_{\sigma \in \mathcal{P}_1^*} \left(\rho_{\mathcal{H}}^{(\sigma)} - \hat{\rho}_{\mathcal{H}}^{(\sigma)} \right)^{\otimes 2} \qquad \text{and} \qquad Q = \sum_{\tau \in \mathcal{P}_1^*} \left(Q_{\mathcal{H}}^{(\tau)} \right)^{\otimes 2}, \tag{5.18}$$

where the simulated $\rho_{\mathcal{H}}^{(\sigma)}$, $\hat{\rho}_{\mathcal{H}}^{(\sigma)}$ and $Q_{\mathcal{H}}^{(\sigma)}$ are defined in Table 5.3. Using this data, it can be computed that

$$\frac{\|\rho_{\text{err}}\|_2^2}{\|\rho - \hat{\rho}\|_2^2} = 3.90 \cdot 10^{-5} \qquad \text{and} \qquad \frac{\|Q_{\text{err}}\|_2^2}{\|\tilde{Q}\|_2^2} = 1.63 \cdot 10^{-3}. \tag{5.19}$$

In Figure 5.3 the number of sequences needed is plotted as a function of the sequence length m for various u (shown in different colors), where these relative errors are plotted in the dashdotted lines. For comparison, the ideal case of zero relative errors has been added in de solid lines, which is nearly on top of the dashdotted lines. It is clear from this picture that these errors are extremely small, contributing very little extra to N. The question is how can such a good error be accomplished when the experimental figures of merit do not seem to be astonishingly good (state preparation fidelity of 99.1% and average assignment fidelity of 94.0% and average gate fidelity of 99.9%). This can be explained by the type of error that dominates the process. The main physical contribution to the processes are thermal excitation/relaxation, which can be seen from the Liouville vectors of ρ_0 and E_1 in Table 5.1 by observing mainly Pauli-Z error components. The error components are the absolute value of the noisy components minus the ideal components. That is

$$|\rho_0 - |0\rangle\langle 0|| = \begin{bmatrix} 0 & 0.0021 & 0.0022 & 0.0261 \end{bmatrix},$$
$$|E_1 - |1\rangle\langle 1|| = \begin{bmatrix} 0.0178 & 0.0071 & 0.0112 & 0.0606 \end{bmatrix},$$

in which it can be seen that the Pauli-Z components are an order of magnitude larger that the X and Y errors. As a result, the amplitude in the ideal direction decreases a bit, but the preparation process has very little leakage of probability amplitude out of the ideal state component B_2. The other antipodal states are also well prepared because of the high average gate fidelity compared to the state preparation and measurement errors.

To illustrate that it is very useful to have information about the noise map Λ, a second simulated example is constructed. The procedure is identical, but the physical state preparation ρ_0' and measurement E_1' are constructed differently. For comparison to the other case, it is assumed that the state preparation fidelity and incorrect measurement assignment probabilities are equal, i.e.

$$F(\rho_0', |0\rangle\langle 0|) = F(\rho_0, |0\rangle\langle 0|), \qquad \epsilon_{01} = \epsilon_{01}' \text{ and } \qquad \epsilon_{10} = \epsilon_{10}'.$$

Table 5.1: Experimental gate set tomography data of SPAM errors for a transmon qubit obtained in [47], which is here used to simulate and compute the relative errors for the unitarity randomized benchmarking protocol. The experimental uncertainty in the data is ignored, since this data is only used as an example calculation.

Operator	Liouville vector (norm. Pauli basis)	Matrix (computational basis)
ρ_0	$\begin{bmatrix} \frac{1}{\sqrt{2}} & 0.0021 & 0.0022 & 0.681 \end{bmatrix}$	$\begin{bmatrix} 0.9815 & 0.0021e^{-i0.8} \\ 0.0021e^{i0.8} & 0.0185 \end{bmatrix}$
E_1	$\begin{bmatrix} 0.6893 & -0.0071 & -0.0112 & -0.6465 \end{bmatrix}$	$\begin{bmatrix} 0.0303 & 0.0094e^{i2.1} \\ 0.0094e^{-i2.1} & 0.9446 \end{bmatrix}$

Table 5.2: Experimental gate set tomography data of SPAM errors for an transmon qubit obtained in [47], which is here used to simulate and compute the relative errors for the unitarity randomized benchmarking protocol. The experimental uncertainty in the data is ignored, since this data is only used as an example calculation.

Gate	Liouville matrix of noisy implementation	Liouville matrix of ideal gate
$X_{\pi/2}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 4\cdot10^{-5} & 0.9992 & 0.0183 & 0.0148 \\ -0.0003 & 0.0136 & 0.0003 & -0.9989 \\ 0.0001 & -0.0180 & 0.9988 & -0.0012 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
X_{π}	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ -0.0001 & 0.9994 & -0.0079 & 0.0016 \\ 0.0002 & -0.0069 & -0.9985 & -0.0023 \\ 0.0002 & 0.0023 & 0.0024 & -0.9986 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
$Y_{\pi/2}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0.0003 & 0.0016 & -0.0132 & 0.9987 \\ 3e-5 & -0.0132 & 0.9991 & 0.0136 \\ 0.0004 & -0.9987 & -0.0126 & 0.0011 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}$
Y_{π}	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ -0.0004 & -0.9985 & 0.0216 & 0.0016 \\ 3e-5 & 0.0224 & 0.9991 & 0.0003 \\ -0.0001 & -0.0013 & -0.0008 & -0.9982 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$

Table 5.3: The model that describes Pauli state preparations and measurements in terms of the available physical operations that can be performed.

σ	$\rho_{\mathcal{H}}^{(\sigma)}$	$\hat{\rho}_{\mathcal{H}}^{(\sigma)}$	$Q_{\mathcal{H}}^{(\sigma)}$
X	$Y_{\pi/2}(\rho_0)$	$Y_{\pi}\circ Y_{\pi/2}(\rho_0)$	$Y_{\pi/2}^{\dagger}(I-2E_1)$
Y	$X_{\pi}\circ X_{\pi/2}(\rho_0)$	$X_{\pi/2}(\rho_0)$	$X_{\pi/2}^{\dagger}(I-2E_1)$
Z	ρ_0	$X_{\pi}(\rho_0)$	$I-2E_1$

The pair

$$\rho_0' = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0.1346 & 0.1346 & 0.6810 \end{bmatrix},$$
$$E_1' = \begin{bmatrix} 0.7071 & -0.0930 & -0.0930 & -0.6283 \end{bmatrix},$$

satisfies these constraints. The idea of this construction is clear. The dominating error process here is rotation away from the computational states, instead of thermal excitation/decay. As expected, this should contribute much more leakage of probability out of the ideal component. Indeed, these underlying physical processes yield $\frac{\|\rho_{\text{err}}\|_2^2}{\|\rho-\hat{\rho}\|_2^2} = 0.0249$ and $\frac{\|Q_{\text{err}}\|_2^2}{\|\bar{Q}\|_2^2} = 8.43\cdot 10^{-4}$. The relative state preparation error $\frac{\|\rho_{\text{err}}\|_2^2}{\|\rho-\hat{\rho}\|_2^2}$ is orders of magnitude worse than in the previous example based on the GST data. This yields a significant increase in the number of sequences N needed. This is indicated in Figure 5.3 by the dashed lines.

5

The conclusion of these examples is that having additional information about the dominating process of your errors can help bound the relative errors significantly. The constructed 'bad' case example might not even be the worst possible giving the fidelity constraints. If one only has fidelity numbers, the Fuchs–Van de Graaf inequalities may be too weak to yield good bounds on the relative SPAM errors alone. Therefore it is recommended that effort is put into finding a realistic error model for the state preparation and measurement processes, such that a more rigid estimate of the relative SPAM errors affecting unitarity randomized benchmarking can be computed.

5.4. DERIVATION OF THE VARIANCE BOUND

In this section a bound on the variance $\mathbb{V}[q_{\mathbf{i_m}}]$ is derived. The main result of this section is Theorem 5.4.9, which is the derived bound. This result is the fundamental building block of Theorem 5.2.1 in which an improved bound on the number of sequences was presented. This section is split into two parts. First, a statement is made about the variance under the assumption of ideal state preparation and measurements. This means that first, it is assumed that $\rho = \hat{\rho} = Q = B_2$. This is done to illustrate the techniques and introduce most of the technical propositions before introducing the extra difficulty of SPAM terms. The second part builds directly on the first, extending the result to include any state preparation and measurement errors (SPAM).

In order to analyze the variance, first an expression must be found for it. The variance of $q_{\mathbf{i_m}}$ is computed as

$$\begin{aligned}
\mathbb{V}[q_{\mathbf{i_m}}] &= \mathbb{E}[q_{\mathbf{i_m}}^2] - \mathbb{E}[q_{\mathbf{i_m}}]^2 \\
&= \frac{1}{|\mathcal{C}|^m}\sum_{\mathbf{i_m}} \langle\langle Q|\mathbf{W}_{\mathbf{i_m}}^{\otimes 2}|\rho-\hat{\rho}\rangle\rangle^2 - \left(\frac{1}{|\mathcal{C}|^m}\sum_{\mathbf{i_m}} \langle\langle Q|\mathbf{W}_{\mathbf{i_m}}^{\otimes 2}|\rho-\hat{\rho}\rangle\rangle\right)^2 \\
&= \langle\langle Q^{\otimes 2}|\frac{1}{|\mathcal{C}|^m}\sum_{\mathbf{i_m}} \mathbf{W}_{\mathbf{i_m}}^{\otimes 4}|(\rho-\hat{\rho})^{\otimes 2}\rangle\rangle - \langle\langle Q^{\otimes 2}|\left(\frac{1}{|\mathcal{C}|^m}\sum_{\mathbf{i_m}} \mathbf{W}_{\mathbf{i_m}}^{\otimes 2}\right)^{\otimes 2}|(\rho-\hat{\rho})^{\otimes 2}\rangle\rangle \\
&= \langle\langle Q^{\otimes 2}|(\mathbf{C}_{\text{avg}}^{(4)}\mathbf{\Lambda}^{\otimes 4})^m|(\rho-\hat{\rho})^{\otimes 2}\rangle\rangle - \langle\langle Q^{\otimes 2}|\left((\mathbf{C}_{\text{avg}}^{(2)}\mathbf{\Lambda}^{\otimes 2})^m\right)^{\otimes 2}|(\rho-\hat{\rho})^{\otimes 2}\rangle\rangle \\
&= \langle\langle Q^{\otimes 2}|\boldsymbol{\mathcal{N}}^{m-1}\mathbf{\Lambda}^{\otimes 4}|(\rho-\hat{\rho})^{\otimes 2}\rangle\rangle - \langle\langle Q^{\otimes 2}|(\boldsymbol{\mathcal{M}}^{\otimes 2})^{m-1}\mathbf{\Lambda}^{\otimes 4}|(\rho-\hat{\rho})^{\otimes 2}\rangle\rangle \\
&= \sum_{j=1}^{m-1} \langle\langle Q^{\otimes 2}|\boldsymbol{\mathcal{N}}^{m-j-1}\left[\boldsymbol{\mathcal{N}}-\boldsymbol{\mathcal{M}}^{\otimes 2}\right](\boldsymbol{\mathcal{M}}^{\otimes 2})^{j-1}|(\rho-\hat{\rho})^{\otimes 2}\rangle\rangle,
\end{aligned} \tag{5.20}$$

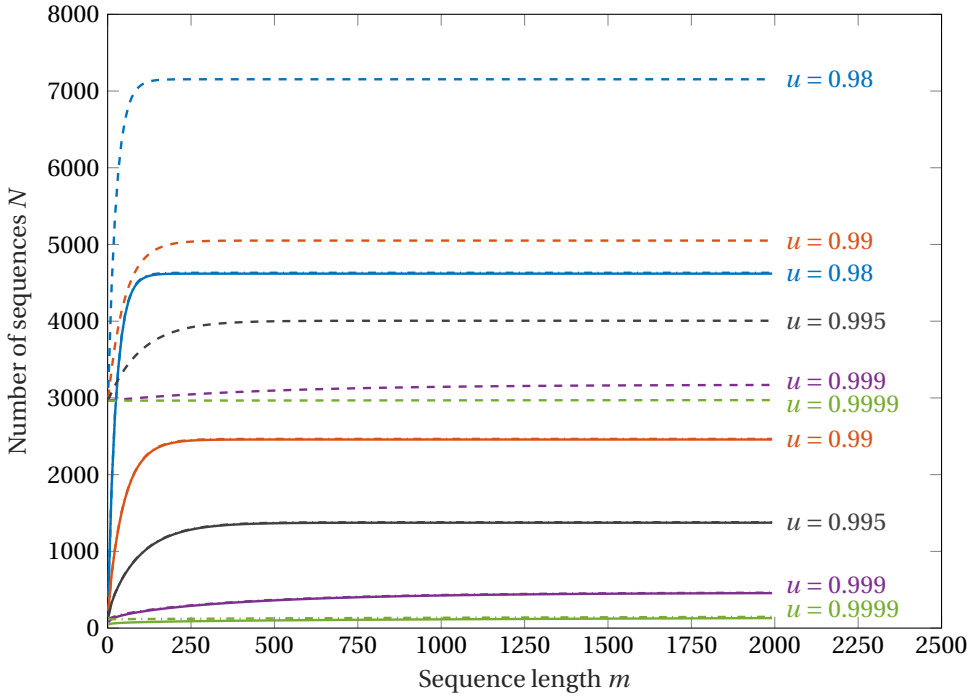

Figure 5.3: The number of sequences N needed as a function of m for various unitarity u and relative errors, using $\epsilon = \delta = 0.01$ and $\alpha = L = 1$ for the single-copy implementation. The unitarity is indicated by color, as indicated next to the lines drawn. The solid lines correspond to the ideal case of $\frac{\|\rho_{\text{err}}\|_2^2}{\|\rho-\hat{\rho}\|_2^2} = \frac{\|Q_{\text{err}}\|_2^2}{\|\bar{Q}\|_2^2} = 0$, the dashdotted lines correspond to $\frac{\|\rho_{\text{err}}\|_2^2}{\|\rho-\hat{\rho}\|_2^2} = 3.90 \cdot 10^{-5}$ and $\frac{\|Q_{\text{err}}\|_2^2}{\|\bar{Q}\|_2^2} = 1.63 \cdot 10^{-3}$, and the dashed lines correspond to $\frac{\|\rho_{\text{err}}\|_2^2}{\|\rho-\hat{\rho}\|_2^2} = 0.0249$ and $\frac{\|Q_{\text{err}}\|_2^2}{\|\bar{Q}\|_2^2} = 8.43 \cdot 10^{-4}$. The dashdotted line is on top of the solid line and therefore not visible. The small error does not significantly contribute to the number of sequences needed. The choice of state preparation and measurement errors arose from two different examples where the underlying physical state preparation and measurement processes were performed with equal fidelities. This shows that the particular form of these noisy processes influences N significantly. See main text for details.

where the definitions

$$\begin{aligned} \mathbf{C}_{\text{avg}}^{(n)} &:= \frac{1}{|\mathcal{C}|}\sum_{C\in\mathcal{C}} \mathbf{C}^{\otimes n}, \\ \mathcal{M} &:= C_{\text{avg}}^{(2)} \mathbf{\Lambda}^{\otimes 2} C_{\text{avg}}^{(2)} \\ \mathcal{N} &:= \mathbf{C}_{\text{avg}}^{(4)} \mathbf{\Lambda}^{\otimes 4} \mathbf{C}_{\text{avg}}^{(4)} \end{aligned} \tag{5.21}$$

are used. In the fourth line it was used that the sum over each i_s, $s = 1,...,m$ can be done independently and in the fifth line it is used that $\mathbf{C}_{\text{avg}}^{(n)}$ is an orthogonal projection (Lemma 2.3.5) so that $\mathbf{C}_{\text{avg}}^{(n)} = (\mathbf{C}_{\text{avg}}^{(n)})^2$ for all $n \in \mathbb{N}$. In the last line the telescoping series (Lemma 3.2.1) is used and a single error map $\Lambda^{\otimes 4}$ has been absorbed into the state as preparation error.

In order to make progress with this expression, the structure of the matrix $\mathcal{N}$ is analyzed. The size of the matrix $\mathcal{N}$ is already large for a single-qubit system, having dimension $2^8 \times 2^8 = 256 \times 256$. However, since $\mathbf{C}_{\text{avg}}^{(4)}$ is the projector onto the trivial subrepresentations of $C \mapsto \mathbf{C}^{\otimes 4}$, the matrix $\mathcal{N}$ has only support on this subspace. For a single qubit, this subspace is of dimension 15 by Lemma 3.6.5 and Lemma 2.3.8.

5

5.4.1. IDEAL STATE PREPARATION AND MEASUREMENTS

This subsection is devoted to proving a new bound on the variance of the random variable $q_{\mathbf{i_m}} = \langle\langle Q|\mathbf{W}_{\mathbf{i_m}}^{\otimes 2}|\rho\rangle\rangle$ over the unitarity randomized benchmarking sequences $W_{\mathbf{i_m}}$ in the absence of state preparation and measurement errors. The complete proof is rather long and technical, and for clarity it is split into several lemma's and propositions. Below, first the main result is presented, and the main steps of the proof are given. Technical details are delegated to separate lemma's and propositions, which are presented below the main theorem. The following theorem states the obtained result, bounding the variance of the unitarity randomized benchmarking protocol in the following way.

Theorem 5.4.1 (Noiseless single-qubit variance bound)**.** *Let $\Lambda \in \mathcal{S}(\mathbb{C}^2)$ be a CPTP quantum channel that corresponds to the error map associated with the single-qubit Clifford group $\mathcal{C}_1$, with unitarity $u(\Lambda) = u$. Furthermore, let $\rho, \hat{\rho} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ be two density operators and $Q \in \text{Herm}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ be a hermitian observable, such that $\rho - \hat{\rho} = Q = B_2$, where B_2 is defined in (4.49).*

Then the variance $\mathbb{V}[q_{\mathbf{i_m}}]$ of the survival probability $q_{\mathbf{i_m}} = \langle\langle Q|\mathbf{W}_{\mathbf{i_m}}^{\otimes 2}|\rho - \hat{\rho}\rangle\rangle$ over the unitary randomized benchmarking sequences $W_{\mathbf{i_m}}$ (as defined by (4.39)) satisfies

$$\mathbb{V}[q_{\mathbf{i_m}}] \leq \left(\frac{3\sqrt{3}}{2} + \sqrt{2}\right)(1-u)^2 \frac{1-u^{2(m-1)}}{1-u^2}. \tag{5.22}$$

Corollary. *In the limit of large sequence length m (that is, when $u^{2m-2} \ll 1$), the variance is independent of m, and satisfies*

$$\mathbb{V}[q_{\mathbf{i_m}}] \leq \left(\frac{3\sqrt{3}}{2} + \sqrt{2}\right)\frac{(1-u)^2}{1-u^2}. \tag{5.23}$$

This bound is valid for all m, but is only close to the original bound in the appropriate limit.

Proof. The proof consists of multiple steps and each different step is delegated to a separated lemma or proposition, in order not to obscure the bigger picture of this proof. The point of departure is (5.20). Under the assumptions that $\rho - \hat{\rho} = Q = B_2$ the variance satisfies

$$\mathbb{V}[q_{\mathbf{i_m}}] = \sum_{j=1}^{m-1} \langle\langle B_2 \otimes B_2 | \mathcal{N}^{m-j-1}\left[\mathcal{N} - \mathcal{M}^{\otimes 2}\right](\mathcal{M}^{\otimes 2})^{j-1}|B_2 \otimes B_2\rangle\rangle. \tag{5.24}$$

First of all, $\mathcal{M}$ only has support on B_1 and B_2, and (4.50) has shown that

$$\langle\langle B_1|\mathcal{M}|B_2\rangle\rangle = 0 \quad \text{and} \quad \langle\langle B_2|\mathcal{M}|B_2\rangle\rangle = u. \tag{5.25}$$

That is, B_2 is an eigenvector of $\mathcal{M}$ with eigenvalue u, i.e. $\mathcal{M}\,|B_2\rangle\rangle = u\,|B_2\rangle\rangle$. Therefore

$$(\mathcal{M}^{\otimes 2})^{j-1}\,|B_2\otimes B_2\rangle\rangle = u^{2(j-1)}\,|B_2\otimes B_2\rangle\rangle.$$

In order to make further progress, an analysis of the projector $\mathbf{C}^{(4)}_{\text{avg}}$ is needed, the projector onto the trivial subrepresentations of $C \mapsto \mathbf{C}^{\otimes 4}$ on the single-qubit Clifford group $\mathcal{C}_1$. This is so because $\mathcal{N} = \mathbf{C}^{(4)}_{\text{avg}}\mathbf{\Lambda}^{\otimes 4}\mathbf{C}^{(4)}_{\text{avg}}$ only has support on the subspace $\text{Rge}(\mathbf{C}^{(4)}_{\text{avg}})$. Lemma 5.4.2 provides a basis $\{A_i : i = 1,\ldots,15\}$ for this subspace. Note that $A_2 = B_2 \otimes B_2$. Now the matrix entries of $\mathcal{N}$ can be analyzed with respect to this basis. This is done in Proposition 5.4.3. The main result is that

$$\left[\mathcal{N} - \mathcal{M}^{\otimes 2}\right]|B_2\otimes B_2\rangle\rangle = \left[\mathcal{N} - \mathcal{M}^{\otimes 2}\right]|A_2\rangle\rangle = a_{14}\,|A_{14}\rangle\rangle + a_{15}\,|A_{15}\rangle\rangle, \tag{5.26}$$

where $a_{14} = \langle\langle A_{14}|\mathcal{N}|A_2\rangle\rangle$ and $a_{15} = \langle\langle A_{15}|\mathcal{N}|A_2\rangle\rangle$ are defined in (5.37). Collecting our results so far yields

$$\mathbb{V}[q_{\mathbf{i_m}}] = \sum_{j=1}^{m-1} u^{2(j-1)}\left(a_{14}\langle\langle A_2|\mathcal{N}^{m-j-1}|A_{14}\rangle\rangle + a_{15}\langle\langle A_2|\mathcal{N}^{m-j-1}|A_{15}\rangle\rangle\right). \tag{5.27}$$

So far, our analysis is exact. It is only at this point that terms are upper bounded. In Proposition 5.4.5 and Proposition 5.4.6 the quantities a_{14} and a_{15} are analyzed. They claim that both quantities have lower bounds zero, i.e. $a_{14}, a_{15} \geq 0$. From Proposition 5.4.7 it follows that

$$\begin{aligned}\langle\langle A_2|\mathcal{N}^n|A_{14}\rangle\rangle &\leq 1,\\ \langle\langle A_2|\mathcal{N}^n|A_{15}\rangle\rangle &\leq 1,\end{aligned} \tag{5.28}$$

since $A_2, A_{14}, A_{15} \in \text{Span}\{Q_1^*\}^{\otimes 4}$ by their definition (see Lemma 5.4.2) are all three hermitian operators with Hilbert-Schmidt norm one. Using these inequalities yields

$$\mathbb{V}[q_{\mathbf{i_m}}] \leq (a_{14}+a_{15})\sum_{j=1}^{m-1} u^{2(j-1)} = (a_{14}+a_{15})\frac{1-u^{2(m-1)}}{1-u^2}, \tag{5.29}$$

where the case $u = 1$ is understood as the limit $u \to 1$ in the closed form expression of the geometric series. Now the main result of Proposition 5.4.5 and Proposition 5.4.6, which is

$$a_{14} \leq \frac{3\sqrt{3}}{2}(1-u)^2 \qquad \text{and} \qquad a_{15} \leq \sqrt{2}(1-u)^2, \tag{5.30}$$

is plugged into the last expression to yield the final result. ■

Throughout the rest of this section, the notation is slightly simplified by omitting the tensor symbol $\otimes$ to avoid cluttering. Therefore AB is understood to mean $A\otimes B$. The matrix product is then indicated by a dot, i.e. $(A\cdot B)$. All lemma's and propositions can then be proven in slightly more clean notation. The proof of Theorem 5.4.1 refers to several propositions and lemma's that contain the technical parts of the proof. The first step of the proof, is identifying the subspace $\text{Rge}(\mathbf{C}^{(4)}_{\text{avg}})$, since the matrix $\mathcal{N}$ has only support on this subspace. This can be done since $\mathbf{C}^{(4)}_{\text{avg}}$ is the orthogonal projection onto the trivial subrepresentations of $C \mapsto \mathbf{C}^{\otimes 4}$ by Lemma 2.3.5. The following lemma finds all of these trivial subrepresentations, giving an explicit basis for each of them.

Lemma 5.4.2 (Trivial subrepresentations of the single-qubit Liouville representation)**.** *Let $R : \mathcal{C} \to \mathcal{L}(V)$ defined by $C \mapsto \mathbf{C}$ be the Liouville representation on the single-qubit Clifford group $\mathcal{C}_1$, where*

$V := \{|\sigma\rangle\rangle \in \mathcal{Q}_1\}$. Then there are 15 copies of the trivial representation present in the decomposition of the tensor-4 Liouville representation $R^{\otimes 4} : C \mapsto \mathbf{C}^{\otimes 4}$ and each of them is spanned by one of the following vectors

$$A_1 = \sigma_0\sigma_0\sigma_0\sigma_0 = B_1B_1, \qquad A_2 = \frac{1}{3}\sum_{\sigma,\tau\in\mathcal{Q}_1^*} \sigma\sigma\tau\tau = B_2B_2,$$

$$A_3 = \frac{1}{\sqrt{3}}\sum_{\tau\in\mathcal{Q}_1^*} \sigma_0\sigma_0\tau\tau = B_1B_2, \qquad A_4 = \frac{1}{\sqrt{3}}\sum_{\tau\in\mathcal{Q}_1^*} \tau\tau\sigma_0\sigma_0 = B_2B_1,$$

$$A_5 = \frac{1}{\sqrt{3}}\sum_{\tau\in\mathcal{Q}_1^*} \sigma_0\tau\sigma_0\tau, \qquad A_6 = \frac{1}{\sqrt{3}}\sum_{\tau\in\mathcal{Q}_1^*} \tau\sigma_0\tau\sigma_0,$$

$$A_7 = \frac{1}{2\sqrt{3}}\sum_{\substack{\sigma,\tau\in\mathcal{Q}_1^*\\ \sigma\neq\tau}} \sigma\tau\sigma\tau - \sigma\tau\tau\sigma, \qquad A_8 = \frac{1}{\sqrt{3}}\sum_{\tau\in\mathcal{Q}_1^*} \sigma_0\tau\tau\sigma_0,$$

$$A_9 = \frac{1}{\sqrt{3}}\sum_{\tau\in\mathcal{Q}_1^*} \tau\sigma_0\sigma_0\tau, \qquad A_{10} = \frac{i}{\sqrt{3}}\sum_{\substack{\sigma,\tau\in\mathcal{Q}_1^*\\ \sigma\neq\tau}} \sigma_0(\tau\cdot\sigma)\sigma\tau,$$

$$A_{11} = \frac{i}{\sqrt{3}}\sum_{\substack{\sigma,\tau\in\mathcal{Q}_1^*\\ \sigma\neq\tau}} (\tau\cdot\sigma)\sigma_0\sigma\tau, \qquad A_{12} = \frac{i}{\sqrt{3}}\sum_{\substack{\sigma,\tau\in\mathcal{Q}_1^*\\ \sigma\neq\tau}} \sigma\tau\sigma_0(\tau\cdot\sigma),$$

$$A_{13} = \frac{i}{\sqrt{3}}\sum_{\substack{\sigma,\tau\in\mathcal{Q}_1^*\\ \sigma\neq\tau}} \sigma\tau(\tau\cdot\sigma)\sigma_0, \qquad A_{14} = \frac{1}{2\sqrt{3}}\sum_{\substack{\sigma,\tau\in\mathcal{Q}_1^*\\ \sigma\neq\tau}} \sigma\tau\sigma\tau + \sigma\tau\tau\sigma,$$

$$A_{15} = -\frac{1}{3\sqrt{2}}\sum_{\sigma,\tau\in\mathcal{Q}_1^*} (-2)^{\langle\langle\sigma|\tau\rangle\rangle}\sigma\sigma\tau\tau,$$

respectively. Note that these vectors satisfy $\langle\langle A_i|A_j\rangle\rangle = \delta_{ij}$, i.e. they are normalized and span orthogonal subspaces (as must be the case by Maschke's theorem). These vectors therefore are an orthonormal basis of $\mathrm{Rge}(\mathbf{C}^{(4)}_{\mathrm{avg}})$.

Proof. The number of trivial subrepresentations of is given by $\langle\chi_{R^{\otimes 4}}, \chi_1\rangle = \langle\chi_{R^{\otimes 2}}, \chi_{R^{\otimes 2}}\rangle = 15$, by Lemma 2.3.8 and Lemma 3.6.5 using that $q = 1$ in the single-qubit case. The idea is to use these irreducible subrepresentations (together with the isomorphisms connecting the ones that are equivalent) and apply Lemma 2.3.8 to find the trivial subrepresentations of $R^{\otimes 4}$ (in complete analogy of the corollary to Proposition 3.6.4).

The full decomposition of the representation $R^{\otimes 2} : C \to \mathbf{C}^{\otimes 2}$ on $V \otimes V$ for the single-qubit case $q = 1$ as reported in [41] is summarized in Table 5.4. The equivalent subrepresentation present can be related to each other by the following isomorphisms of representations:

$$\begin{aligned}
&\theta_0 : V_{\mathrm{id}} \to V_0 : && B_1 \mapsto B_2, && \\
&\theta_1 : V_r \to V_l : && \sigma_0\tau \mapsto \tau\sigma_0, && \tau \in \mathcal{Q}_1^* \\
&\theta_2 : V_{\{A\}} \to V_r : && \frac{\tau\sigma - \sigma\tau}{\sqrt{2}} \mapsto -i\sqrt{2}\sigma_0(\tau\cdot\sigma), && \sigma \neq \tau \in \mathcal{Q}_1^* \\
&\theta_3 : V_{\{A\}} \to V_l : && \theta_1 \circ \theta_2, &&
\end{aligned} \tag{5.31}$$

The spaces V_{id} and V_0 are trivially isomorphic. The representations on the spaces V_r and V_l are canonically isomorphic by θ_1. The isomorphism θ_2 sends the basis vector $\frac{\tau\sigma-\sigma\tau}{\sqrt{2}}$ of $V_{\{A\}}$ to the basis vector $\sigma_0\nu$ of V_r, where $\nu = -i\sqrt{2}(\tau\cdot\sigma)$ is the third normalized non-identity Paul matrix (i.e. $\nu \in \mathcal{Q}_1^* : \nu \neq \sigma, \nu \neq \tau$). Note that an equivalent definition of θ_2 is

$$\sigma\tau \mapsto i(\tau\cdot\sigma), \tag{5.32}$$

Table 5.4: The decomposition of the Liouville representation of the single-qubit Clifford group [41].

Space	Definition	Dimension	Equivalent to
V_{id}	$\mathrm{Span}\{B_1\} = \mathrm{Span}\{\sigma_0\sigma_0\}$	1	V_0
V_0	$\mathrm{Span}\{B_2\} = \mathrm{Span}\left\{\frac{1}{\sqrt{3}}\sum_{\sigma\in\mathcal{Q}_1^*}\sigma\sigma\right\}$	1	V_{id}
V_r	$\mathrm{Span}\{\sigma_0\tau : \tau \in \mathcal{Q}_1^*\}$	3	$V_l, V_{\{A\}}$
V_l	$\mathrm{Span}\{\tau\sigma_0 : \tau \in \mathcal{Q}_1^*\}$	3	$V_r, V_{\{A\}}$
$V_{\{A\}}$	$\mathrm{Span}\left\{\frac{\tau\sigma-\sigma\tau}{\sqrt{2}} : \sigma,\tau \in \mathcal{Q}_1^*, \sigma\neq\tau\right\}$	3	V_r, V_l
$V_{\{S\}}$	$\mathrm{Span}\left\{\frac{\tau\sigma+\sigma\tau}{\sqrt{2}} : \sigma,\tau \in \mathcal{Q}_1^*, \sigma\neq\tau\right\}$	3	-
V_1	$\mathrm{Span}\left\{\sigma\sigma : \sigma \in \mathcal{Q}_1^*\right\} \setminus V_0$	2	-

since this implies that $\tau\sigma \mapsto i(\sigma\cdot\tau) = -i(\tau\cdot\sigma)$. Combining the two then results in $\tau\sigma-\sigma\tau \mapsto -2i(\tau\cdot\sigma)$, which shows the equivalence.

In order to apply Lemma 2.3.8, one needs to choose an orthonormal basis for each space listed in Table 5.4. The result is independent of this choice. In fact, all spaces except for V_1 already have a basis, since they are defined by the span of an orthonormal basis. Giving V_1 the following choice of basis, it can be written as

$$V_1 = \mathrm{Span}\left\{\frac{\sigma_X\sigma_X - \sigma_Y\sigma_Y}{\sqrt{2}}, \frac{\sigma_X\sigma_X + \sigma_Y\sigma_Y - 2\sigma_Z\sigma_Z}{\sqrt{6}}\right\}, \tag{5.33}$$

where $\sigma_X, \sigma_Y, \sigma_Z \in \mathcal{Q}_1^*$ denote the normalized Pauli matrices corresponding to Pauli X, Y and Z respectively. The trivial subrepresentations $A_1, ..., A_{15}$ are then found by application of Lemma 2.3.8 to

1. $V_{id} \otimes V_{id}$,
2. $V_0 \otimes V_0$,
3. $V_{id} \otimes V_0$,
4. $V_0 \otimes V_{id}$,
5. $V_r \otimes V_r$,
6. $V_l \otimes V_l$,
7. $V_{\{A\}} \otimes V_{\{A\}}$,
8. $V_r \otimes V_l$,
9. $V_l \otimes V_r$,
10. $V_r \otimes V_{\{A\}}$,
11. $V_l \otimes V_{\{A\}}$,
12. $V_{\{A\}} \otimes V_r$,
13. $V_{\{A\}} \otimes V_l$,
14. $V_{\{S\}} \otimes V_{\{S\}}$,
15. $V_1 \otimes V_1$,

respectively, using the isomorphisms θ_i, $i = 0,1,2,3$ connecting the isomorphic representations. To illustrate this, A_{12} is for example found found as

$$\begin{aligned} A_{12} &= \frac{1}{2\sqrt{3}} \sum_{\substack{\sigma,\tau\in\mathcal{Q}_1^* \\ \sigma\neq\tau}} \left(\frac{\tau\sigma-\sigma\tau}{\sqrt{2}}\right)\theta_2\left(\frac{\tau\sigma-\sigma\tau}{\sqrt{2}}\right) \\ &= \frac{1}{2\sqrt{3}} \sum_{\substack{\sigma,\tau\in\mathcal{Q}_1^* \\ \sigma\neq\tau}} -i\,(\tau\sigma-\sigma\tau)\,\sigma_0(\tau\cdot\sigma) \\ &= \frac{i}{2\sqrt{3}} \sum_{\substack{\sigma,\tau\in\mathcal{Q}_1^* \\ \sigma\neq\tau}} \tau\sigma\sigma_0(\sigma\cdot\tau) + \sigma\tau\sigma_0(\tau\cdot\sigma) \\ &= \frac{i}{\sqrt{3}} \sum_{\substack{\sigma,\tau\in\mathcal{Q}_1^* \\ \sigma\neq\tau}} \sigma\tau\sigma_0(\tau\cdot\sigma), \end{aligned} \tag{5.34}$$

noting that the sum runs over each basis vector twice, which is taken care of by the normalization factor $\frac{1}{2\sqrt{3}}$, and the fact that σ and τ anti-commute to absorb all minus signs. ■

Now it is known onto which subspace the matrix $\mathcal{N} = \mathbf{C}_{\text{avg}}^{(4)} \mathbf{\Lambda}^{\otimes 4} \mathbf{C}_{\text{avg}}^{(4)}$ has support, since the previous lemma showed that $\mathbf{C}_{\text{avg}}^{(4)} = \sum_{i=1}^{15} |A_i\rangle\rangle\langle\langle A_i|$. Furthermore note that $A_2 = B_2 B_2$. The next step in the proof is then to evaluate

$$\mathcal{N}|A_2\rangle\rangle = \sum_{i=1}^{15} \langle\langle A_i|\mathcal{N}|A_2\rangle\rangle |A_i\rangle\rangle. \tag{5.35}$$

The next proposition precisely shows this.

Proposition 5.4.3 (Computation of $\mathcal{N}|A_2\rangle\rangle$)**.** *Let $\mathcal{N}$ and $|A_i\rangle\rangle$ for $i = 1,\ldots,15$ be defined as above and denote $u = u(\Lambda)$. Then*

$$\mathcal{N}|A_2\rangle\rangle = a_2|A_2\rangle\rangle + a_{14}|A_{14}\rangle\rangle + a_{15}|A_{15}\rangle\rangle, \tag{5.36}$$

where

$$\begin{aligned} a_2 &= \langle\langle A_2|\mathcal{N}|A_2\rangle\rangle = u^2, \\ a_{14} &= \langle\langle A_{14}|\mathcal{N}|A_2\rangle\rangle = \frac{1}{3\sqrt{3}} \sum_{\substack{\sigma,\tau\in\mathcal{Q}_1^* \\ \sigma\neq\tau}} \langle\langle \sigma|\mathbf{\Lambda}_{\text{u}}\mathbf{\Lambda}_{\text{u}}^\dagger|\tau\rangle\rangle^2, \\ a_{15} &= \langle\langle A_{15}|\mathcal{N}|A_2\rangle\rangle = -\frac{1}{\sqrt{2}}u(\Lambda)^2 + \frac{1}{3\sqrt{2}} \sum_{\sigma\in\mathcal{Q}_1^*} \langle\langle \sigma|\mathbf{\Lambda}_{\text{u}}\mathbf{\Lambda}_{\text{u}}^\dagger|\sigma\rangle\rangle^2. \end{aligned} \tag{5.37}$$

Proof. The proof is by direct computation, (repeated) application of Lemma 3.6.2 and linearity of the inner product. In general the vector A_k is of the form

$$A_k = \sum_{j=1}^{K_k} c_j^{(k)} \sigma_{1,j}^{(k)} \sigma_{2,j}^{(k)} \sigma_{3,j}^{(k)} \sigma_{4,j}^{(k)}, \tag{5.38}$$

where each $\sigma_{i,j}^{(k)} \in \mathcal{Q}_1$ and $0 \neq c_j^{(k)} \in \mathbb{R}$. The sum over j runs over all K_k nonzero term in the definition of A_k, where $c_j^{(k)}$ is the coefficient of this term and where $\sigma_{i,j}^{(k)}$ is the i-th tensor position in the j-th term in the summation of the vector A_k. Therefore in general, a_k is computed as

$$\begin{aligned} a_k &= \langle\langle A_k|\mathcal{N}|A_2\rangle\rangle \\ &= \frac{1}{3}\sum_j c_j^{(k)} \sum_{\tau,\hat{\tau}\in\mathcal{Q}_1^*} \langle\langle \sigma_{1,j}^{(k)}\sigma_{2,j}^{(k)}\sigma_{3,j}^{(k)}\sigma_{4,j}^{(k)}|\mathbf{\Lambda}^{\otimes 4}|\tau\tau\hat{\tau}\hat{\tau}\rangle\rangle \\ &= \frac{1}{3}\sum_j c_j^{(k)} \sum_{\tau,\hat{\tau}\in\mathcal{Q}_1^*} \langle\langle \sigma_{1,j}^{(k)}|\mathbf{\Lambda}|\tau\rangle\rangle \langle\langle \sigma_{2,j}^{(k)}|\mathbf{\Lambda}|\tau\rangle\rangle \langle\langle \sigma_{3,j}^{(k)}|\mathbf{\Lambda}|\hat{\tau}\rangle\rangle \langle\langle \sigma_{4,j}^{(k)}|\mathbf{\Lambda}|\hat{\tau}\rangle\rangle. \end{aligned} \tag{5.39}$$

So if for all $j = 1,\ldots,K_k$ there is a position $i \in \{1,2,3,4\}$ such that $\sigma_{i,j}^{(k)} = \sigma_0$, then $a_k = 0$ since then $\langle\langle \sigma_{i,j}^{(k)}|\Lambda|\tau\rangle\rangle = \langle\langle \sigma_0|\Lambda|\tau\rangle\rangle = 0$ for all $\tau \in \mathcal{Q}_1^*$ by the trace preserving property of Λ and the fact that all non-identity Pauli's in $\mathcal{Q}_1^*$ are traceless. It can easily be verified that this condition is satisfied for $k = 1,3,4,5,6,8,9,10,11,12,13$.

For all other k ($k = 2,7,14,15$), there is nothing else to do then to evaluate (5.39) directly. Denote $P_{\text{u}} = \sum_{\sigma\in\mathcal{Q}_1^*} |\tau\rangle\rangle\langle\langle\tau|$ the projection onto the traceless subspace. Then the rest of the terms are computed as

$$a_2 = \frac{1}{9} \sum_{\sigma,\hat{\sigma},\tau,\hat{\tau}\in\mathcal{Q}_1^*} \langle\langle \sigma|\mathbf{\Lambda}|\tau\rangle\rangle^2 \langle\langle \hat{\sigma}|\mathbf{\Lambda}|\hat{\tau}\rangle\rangle^2 = \left(\frac{1}{3}\sum_{\sigma,\tau\in\mathcal{Q}_1^*} \langle\langle \sigma|\mathbf{\Lambda}|\tau\rangle\rangle^2\right)^2 = u^2,$$

$$a_7 = \frac{1}{6\sqrt{3}} \sum_{\substack{\sigma,\hat{\sigma},\tau,\hat{\tau}\in\mathcal{Q}_1^* \\ \sigma\neq\hat{\sigma}}} \left(\langle\langle \sigma\hat{\sigma}|\mathbf{\Lambda}^{\otimes 2}|\tau\tau\rangle\rangle \langle\langle \sigma\hat{\sigma}|\mathbf{\Lambda}^{\otimes 2}|\hat{\tau}\hat{\tau}\rangle\rangle - \langle\langle \sigma\hat{\sigma}|\mathbf{\Lambda}^{\otimes 2}|\tau\tau\rangle\rangle \langle\langle \sigma\hat{\sigma}|\mathbf{\Lambda}^{\otimes 2}|\hat{\tau}\hat{\tau}\rangle\rangle \right) = 0,$$

$$\begin{aligned}
a_{14} &= \frac{1}{6\sqrt{3}} \sum_{\substack{\sigma,\hat{\sigma},\tau,\hat{\tau}\in\mathcal{Q}_1^* \\ \sigma\neq\hat{\sigma}}} 2\langle\langle \sigma|\mathbf{\Lambda}|\tau\rangle\rangle \langle\langle \hat{\sigma}|\mathbf{\Lambda}|\tau\rangle\rangle \langle\langle \sigma|\mathbf{\Lambda}|\hat{\tau}\rangle\rangle \langle\langle \hat{\sigma}|\mathbf{\Lambda}|\hat{\tau}\rangle\rangle \\
&= \frac{1}{3\sqrt{3}} \sum_{\substack{\sigma,\hat{\sigma}\in\mathcal{Q}_1^* \\ \sigma\neq\hat{\sigma}}} \left(\sum_{\tau\in\mathcal{Q}_1^*} \langle\langle \sigma|\mathbf{\Lambda}|\tau\rangle\rangle \langle\langle \hat{\sigma}|\mathbf{\Lambda}|\tau\rangle\rangle \right)^2 \\
&= \frac{1}{3\sqrt{3}} \sum_{\substack{\sigma,\hat{\sigma}\in\mathcal{Q}_1^* \\ \sigma\neq\hat{\sigma}}} \langle\langle \sigma|\mathbf{\Lambda} P_{\mathrm{u}} \mathbf{\Lambda}^\dagger|\hat{\sigma}\rangle\rangle^2 \\
&= \frac{1}{3\sqrt{3}} \sum_{\substack{\sigma,\hat{\sigma}\in\mathcal{Q}_1^* \\ \sigma\neq\hat{\sigma}}} \langle\langle \sigma|\mathbf{\Lambda}_{\mathrm{u}} \mathbf{\Lambda}_{\mathrm{u}}^\dagger|\hat{\sigma}\rangle\rangle^2 \\
a_{15} &= -\frac{1}{9\sqrt{2}} \sum_{\sigma,\hat{\sigma},\tau,\hat{\tau}\in\mathcal{Q}_1^*} (-2)^{\langle\langle \sigma|\hat{\sigma}\rangle\rangle} \langle\langle \sigma|\mathbf{\Lambda}|\tau\rangle\rangle^2 \langle\langle \hat{\sigma}|\mathbf{\Lambda}|\hat{\tau}\rangle\rangle^2 \\
&= -\frac{1}{9\sqrt{2}} \sum_{\sigma,\hat{\sigma},\tau,\hat{\tau}\in\mathcal{Q}_1^*} \langle\langle \sigma|\mathbf{\Lambda}|\tau\rangle\rangle^2 \langle\langle \hat{\sigma}|\mathbf{\Lambda}|\hat{\tau}\rangle\rangle^2 + \frac{1}{9\sqrt{2}} \sum_{\sigma,\tau,\hat{\tau}\in\mathcal{Q}_1^*} 3\langle\langle \sigma|\mathbf{\Lambda}|\tau\rangle\rangle^2 \langle\langle \hat{\sigma}|\mathbf{\Lambda}|\hat{\tau}\rangle\rangle^2 \\
&= -\frac{u^2}{\sqrt{2}} + \frac{1}{3\sqrt{2}} \sum_{\sigma\in\mathcal{Q}_1^*} \left(\sum_{\tau\in\mathcal{Q}_1^*} \langle\langle \sigma|\mathbf{\Lambda}|\tau\rangle\rangle^2 \right)^2 \\
&= -\frac{u^2}{\sqrt{2}} + \frac{1}{3\sqrt{2}} \sum_{\sigma\in\mathcal{Q}_1^*} \langle\langle \sigma|\mathbf{\Lambda}_{\mathrm{u}} \mathbf{\Lambda}_{\mathrm{u}}^\dagger|\sigma\rangle\rangle^2
\end{aligned}$$

■

In the last step of the proof, an upper bound is put on the terms

$$a_{14}\langle\langle A_2|\mathcal{N}^{m-j-1}|A_{14}\rangle\rangle \qquad \text{and} \qquad a_{15}\langle\langle A_2|\mathcal{N}^{m-j-1}|A_{15}\rangle\rangle.$$

The idea used in the proof is that if $a_{14}, a_{15} \geq 0$ and $\langle\langle A_2|\mathcal{N}^{m-j-1}|A_{14}\rangle\rangle, \langle\langle A_2|\mathcal{N}^{m-j-1}|A_{15}\rangle\rangle \leq 1$, then the above terms are bounded as

$$a_{14}\langle\langle A_2|\mathcal{N}^{m-j-1}|A_{14}\rangle\rangle \leq a_{14} \qquad \text{and} \qquad a_{15}\langle\langle A_2|\mathcal{N}^{m-j-1}|A_{15}\rangle\rangle \leq a_{15}. \tag{5.40}$$

Then the upper bounds for a_{14} and a_{15} respectively complete the proof. So, in order to complete the proof, the terms a_{14}, a_{15} need to be bounded, as well as terms of the form $\langle\langle A_2|\mathcal{N}^{m-j-1}|A_i\rangle\rangle$. The bounds on a_{14} and a_{15} are treated first. In order to bound these quantities, the following lemma is used [15, 49, 50].

Lemma 5.4.4 (Single-qubit Liouville representation)**.** *Let $\mathcal{H} = \mathbb{C}^2$ be the Hilbert space of a single qubit and let $\mathcal{E} \in \mathcal{T}(\mathcal{H})$ be a trace preserving superoperator. The Liouville representation of such any trace preserving operator is (see* (3.22)*)*

$$\boldsymbol{\mathcal{E}} = \begin{bmatrix} 1 & 0 \\ \alpha(\mathcal{E}) & \boldsymbol{\mathcal{E}}_{\mathrm{u}} \end{bmatrix}. \tag{5.41}$$

If (in addition to being trace preserving) $\mathcal{E}$ is positive, then $\boldsymbol{\mathcal{E}}$ is real and admits the decomposition

$$\boldsymbol{\mathcal{E}} = \begin{bmatrix} 1 & 0 \\ 0 & U \end{bmatrix} \begin{bmatrix} 1 & 0 \\ t & W \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & V \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ Ut & UWV \end{bmatrix}, \tag{5.42}$$

5

where

$$U, V \in SO(\mathbb{R}^3) = \left\{A \in \mathbb{R}^{3\times 3} : AA^T = A^T A = I, \mathrm{Det}(A) = 1\right\},$$

$t = U^\dagger \alpha(\Lambda) \in \mathbb{R}^3$ *and* $W = \mathrm{diag}([w_1\ w_2\ w_3]) \in \mathbb{R}^{3\times 3}$*, satisfying* $|t_i| + |w_i| \leq 1$ *for each* $i = 1,2,3$*. Note that* $\boldsymbol{\mathcal{E}}_\mathrm{u} = UWV$*. If furthermore* $\mathcal{E}$ *is completely positive (and trace preserving), then in addition to the above (recalling that complete positivity implies positivity) the conditions* $(w_i \pm w_j)^2 \leq (1 \pm w_k)^2$ *also hold, for each permutation* $\{i, j, k\}$ *of* $\{1,2,3\}$*.*

Proof. See [49, 50]. ■

Note that UWV is not quite the singular value decomposition of $\boldsymbol{\mathcal{E}}_\mathrm{u}$, since U and V are in $SO(3)$ and not just in $O(3) = \left\{A \in \mathbb{R}^{3\times 3} : AA^T = A^T A = I\right\}$. A slight modification of the singular value decomposition can force $U, V \in SO(3)$ at the cost of giving up the condition that the singular values are positive. So w_i can be negative. However $|w_i|$ are the singular values of $\boldsymbol{\mathcal{E}}_\mathrm{u}$. Now let us relate the unitarity of $\mathcal{E}$ to the decomposition of the above lemma. From (4.34) it follows that

$$u(\mathcal{E}) = \frac{1}{3}\mathrm{Tr}[\boldsymbol{\mathcal{E}}_\mathrm{u}\boldsymbol{\mathcal{E}}_\mathrm{u}^\dagger] = \frac{1}{3}\mathrm{Tr}[UWVV^\dagger WU^\dagger] = \frac{1}{3}\mathrm{Tr}[W^2] = \frac{1}{3}\sum_i w_i^2. \tag{5.43}$$

The above lemma can now be applied to find a bound on a_{14}.

Proposition 5.4.5 (Bound on a_{14})**.** *Let* a_{14} *be the quantity defined in Proposition 5.4.3,*

$$a_{14} = \frac{1}{3\sqrt{3}} \sum_{\substack{\sigma,\tau\in\mathcal{Q}_1^* \\ \sigma\neq\tau}} \langle\langle \sigma|\boldsymbol{\Lambda}_\mathrm{u}\boldsymbol{\Lambda}_\mathrm{u}^\dagger|\tau\rangle\rangle^2, \tag{5.44}$$

and let $u = u(\Lambda)$ *be the unitarity of* Λ*. Then* $0 \leq a_{14} \leq \frac{3\sqrt{3}}{2}(1-u)^2$*.*

Proof. As $\boldsymbol{\Lambda}$ is real by Proposition 3.6.1, so is $\boldsymbol{\Lambda}_\mathrm{u}\boldsymbol{\Lambda}_\mathrm{u}^\dagger$ and therefore $\langle\langle \sigma|\boldsymbol{\Lambda}_\mathrm{u}\boldsymbol{\Lambda}_\mathrm{u}^\dagger|\tau\rangle\rangle^2 \geq 0$. This implies $a_{14} \geq 0$. Application of Lemma 5.4.4 to $\boldsymbol{\Lambda}$ yields

$$\boldsymbol{\Lambda}_\mathrm{u}\boldsymbol{\Lambda}_\mathrm{u}^\dagger = UW^2U^\dagger. \tag{5.45}$$

In the Liouville representation, a vector $|\sigma\rangle\rangle$ is represented by the canonical unit vectors e_i for $i = 1,2,3$ (e_0 is identified with σ_0). Then $\langle\langle \sigma|\boldsymbol{\Lambda}\boldsymbol{\Lambda}^\dagger|\tau\rangle\rangle$ can be represented in index notation by

$$\langle\langle \sigma|\boldsymbol{\Lambda}_\mathrm{u}\boldsymbol{\Lambda}_\mathrm{u}^\dagger|\tau\rangle\rangle = e_i^\dagger UW^2U^\dagger e_j = \sum_{k=1}^3 U_{i,k}w_k^2U_{j,k}. \tag{5.46}$$

Therefore

$$a_{14} = \frac{1}{3\sqrt{3}} \sum_{\substack{i,j=1 \\ i\neq j}}^3 \left(\sum_{k=1}^3 U_{i,k}w_k^2U_{j,k}\right)^2. \tag{5.47}$$

In order to put a bound on a_{14}, a bound on the term in (5.46) is found by applying Lemma 5.4.4. Since $UU^T = I$, one has that $\sum_{k=1}^3 U_{i,k}U_{j,k} = \delta_{ij}$. Assume without loss of generality that $|w_1| \leq |w_2| \leq |w_3|$, as this can be achieved by permutation of the basis. Then progress on a bound can be made in the

following way. For $i \neq j$,

$$\begin{aligned}\left|\sum_{k=1}^{3} U_{i,k} w_k^2 U_{j,k}\right| &= \left|\sum_{k=1}^{3} U_{i,k} w_k^2 U_{j,k} - w_1^2 \sum_{k=1}^{3} U_{i,k} U_{j,k}\right| \\ &= \left|\sum_{k=1}^{3} U_{i,k}(w_k^2 - w_1^2) U_{j,k}\right| \\ &\leq \sum_{k=1}^{3} |U_{i,k} U_{j,k}||w_k^2 - w_1^2| \\ &\leq |w_3^2 - w_1^2| \sum_{k=1}^{3} |U_{i,k} U_{j,k}| \\ &\leq \left(\sqrt{\sum_{k=1}^{3} U_{i,k}^2}\sqrt{\sum_{k=1}^{3} U_{j,k}^2}\right)|w_3^2 - w_1^2| \\ &= w_3^2 - w_1^2,\end{aligned} \tag{5.48}$$

where in the last line Hölder's inequality (Theorem 2.1.10) was used and the fact that the rows of a unitary matrix have 2-norm equal to unity (Proposition 2.1.3). So therefore

$$a_{14} \leq \frac{1}{3\sqrt{3}} \sum_{\substack{i,j=1 \\ i\neq j}}^{3} (w_3^2 - w_1^2)^2 = \frac{2}{\sqrt{3}}(w_3^2 - w_1^2)^2. \tag{5.49}$$

Putting a bound on $(w_3^2 - w_1^2)^2$ is also done by invoking Lemma 5.4.4. Under the assumption that Λ is CPTP, Lemma 5.4.4 claims that $(w_i \pm w_j)^2 \leq (1 \pm w_k)^2$ for each permutation $\{i, j, k\}$ of $\{1, 2, 3\}$. Adding the equalities of opposite sign yields

$$2w_i^2 + 2w_j^2 = (w_i + w_j)^2 + (w_i - w_j)^2 \leq (1 + w_k)^2 + (1 - w_k)^2 = 2 + 2w_k^2, \tag{5.50}$$

which is equivalent to $w_i^2 + w_j^2 - w_k^2 \leq 1$. In particular, this means

$$w_3^2 + w_1^2 - w_2^2 \leq 1, \tag{5.51}$$

$$w_2^2 + w_3^2 - w_1^2 \leq 1. \tag{5.52}$$

Then multiplying (5.52) by 2 and adding to (5.51) yields $-w_1^2 + w_2^2 + 3w_3^2 \leq 3$ or equivalently

$$2(w_3^2 - w_1^2) \leq 3 - (w_1^2 + w_2^2 + w_3^2) = 3(1 - u). \tag{5.53}$$

Plugging this into (5.49) yields

$$a_{14} \leq \frac{2}{\sqrt{3}}\left(\frac{3}{2}(1 - u)\right)^2 = \frac{3\sqrt{3}}{2}(1 - u)^2, \tag{5.54}$$

proving the proposition. ■

Next, a bound on a_{15} is given. Again Lemma 5.4.4 is invoked to give a bound.

Proposition 5.4.6 (Bound on a_{15})**.** *Let a_{15} be the quantity defined in Proposition 5.4.3,*

$$-\frac{1}{\sqrt{2}} u(\Lambda)^2 + \frac{1}{3\sqrt{2}} \sum_{\sigma \in \mathcal{Q}_1^*} \langle\langle \sigma | \mathbf{\Lambda}_u \mathbf{\Lambda}_u^\dagger | \sigma \rangle\rangle^2, \tag{5.55}$$

and let $u = u(\Lambda)$ be the unitarity of Λ. Then $0 \leq a_{15} \leq \sqrt{2}(1 - u)^2$.

Proof. Again, application of Lemma 5.4.4 to $\mathbf{\Lambda}$ yields

$$\mathbf{\Lambda}_u \mathbf{\Lambda}_u^\dagger = UW^2U^\dagger. \tag{5.56}$$

In the Liouville representation, a vector $|\sigma\rangle\rangle$ is represented by the canonical unit vectors e_i for $i = 1,2,3$ (e_0 is identified with σ_0). Then $\langle\langle\sigma|\mathbf{\Lambda}\mathbf{\Lambda}^\dagger|\sigma\rangle\rangle$ can be represented in index notation by

$$\langle\langle\sigma|\mathbf{\Lambda}_u\mathbf{\Lambda}_u^\dagger|\sigma\rangle\rangle = e_i^\dagger UW^2U^\dagger e_i =: x_i \tag{5.57}$$

where x_i is just a shorthand notation with $i = 1,2,3$ associated with each $\sigma \in \mathcal{Q}_1^*$. Using $u = \frac{1}{3}\sum_{i=1}^3 x_i$ it follows that

$$\begin{aligned}
\sqrt{2}a_{15} &= -u^2 + \frac{1}{3}\sum_{\sigma\in\mathcal{Q}_1^*}\langle\langle\sigma|\mathbf{\Lambda}_u\mathbf{\Lambda}_u^\dagger|\sigma\rangle\rangle^2 \\
&= \left(\frac{1}{3}\sum_{j=1}^3 x_j^2\right) - \left(\frac{1}{3}\sum_{i=1}^3 x_i\right)^2 \\
&= \left(\frac{1}{3}\sum_{j=1}^3 x_j^2\right) - 2\left(\frac{1}{3}\sum_{i=1}^3 x_i\right)\left(\frac{1}{3}\sum_{k=1}^3 x_k\right) + \left(\frac{1}{3}\sum_{k=1}^3 x_k\right)^2 \\
&= \frac{1}{3}\sum_{j=1}^3\left(x_j^2 - 2x_j\left(\frac{1}{3}\sum_{k=1}^3 x_k\right) + \left(\frac{1}{3}\sum_{k=1}^3 x_k\right)^2\right) \\
&= \frac{1}{3}\sum_{j=1}^3\left(x_j - \left(\frac{1}{3}\sum_{k=1}^3 x_k\right)\right)^2 \\
&= \frac{1}{3}\sum_{j=1}^3 (x_j - u)^2.
\end{aligned} \tag{5.58}$$

From this it is clear that $a_{15} \geq 0$. An upper bound is found by posing it as an optimization problem. In order to do so, lower and upper limits for x_i are needed. So it is established that $0 \leq x_i = \langle\langle\sigma|\mathbf{\Lambda}_u\mathbf{\Lambda}_u^\dagger|\sigma\rangle\rangle \leq 1$. This is done by application of Lemma 5.4.4, yielding

$$0 \leq x_i = \langle\langle\sigma|\mathbf{\Lambda}_u\mathbf{\Lambda}_u^\dagger|\sigma\rangle\rangle = e_i^\dagger UW^2U^\dagger e_i = \sum_{k=1}^3 U_{i,k}w_k^2U_{k,i}^\dagger = \sum_{k=1}^3 U_{i,k}^2 w_k^2 \leq \sum_{k=1}^3 U_{i,k}^2 = 1, \tag{5.59}$$

The upper bound follows from the fact that $w_k^2 \leq 1$ and $U_{i,k}^2 \geq 0$, together with $\sum_{k=1}^3 U_{i,k}^2 = 1$ since the 2-norm of a row of a unitary matrix is one (Proposition 2.1.3). Clearly, as $U_{i,k}^2, w_k^2 \geq 0$, also $x_i = \langle\langle\sigma|\mathbf{\Lambda}_u\mathbf{\Lambda}_u^\dagger|\sigma\rangle\rangle \geq 0$. An upper bound for a_{15} is then the solution to the maximization problem

$$\begin{aligned}
\max_{x_1,x_2,x_3} \quad & a_{15} = \frac{1}{3\sqrt{2}}\sum_{j=1}^3 (x_j - u)^2 \\
\text{s.t.} \quad & 0 \leq x_j \leq 1, \quad j = 1,2,3, \\
& \frac{1}{3}\sum_{j=1}^3 x_j = u,
\end{aligned} \tag{5.60}$$

where $0 \leq u \leq 1$ is a free parameter of the problem. The key is to note that this is a maximization problem of a convex function over a convex domain, and therefore it attains its maxima at the extreme points of the domain [51]. The extreme points are the points where two of the six given inequalities (that bound the domain) are saturated. The third equality follows from the single equality constraint. The extreme points are unique up to permutation of variables, which yields the same solution since the objective function is invariant under permutation of variables. Table 5.5 lists the extreme points

in which the objective function attains its maximum and the corresponding value of the objective function depending on the value of u. The column 'bound' indicates an upper bound for the solution of the problem, valid in the corresponding region of u. In conclusion, a_{15} is less or equal to the solution of (5.60), which in turn is less or equal to $\sqrt{2}(1-u)^2$.

Table 5.5: Solution to the optimization problem (5.60) up to permutation of the variables x_1, x_2, x_3, which due to the symmetry of the problem yields the same solution. The last column is an upper bound of the solution, valid in the appropriate regime of the parameter u.

case	x_1	x_2	x_3	solution to (5.60)	bound
$\frac{2}{3} \leq u \leq 1$	1	1	$3u-2$	$\sqrt{2}(1-u)^2$	$\sqrt{2}(1-u)^2$
$\frac{1}{3} < u < \frac{2}{3}$	1	$3u-1$	0	$\frac{1}{3\sqrt{2}}\left((1-u)^2+(2u-1)^2+u^2\right)$	$\sqrt{2}(1-u)^2$
$0 \leq u \leq \frac{1}{3}$	$3u$	0	0	$\sqrt{2}u^2$	$\sqrt{2}(1-u)^2$

■

This final proposition used in the proof of Theorem 5.4.1 allows us to conclude that

$$\langle\langle A_2|\boldsymbol{\mathcal{N}}^{m-j-1}|A_{14}\rangle\rangle, \langle\langle A_2|\boldsymbol{\mathcal{N}}^{m-j-1}|A_{15}\rangle\rangle \leq 1.$$

The proposition is stated in a slightly more general form, for later reuse. In the main proof it is illustrated how the conclusion follows from the proposition. The proof of this proposition here makes use of another lemma, that is taken from literature. This lemma is stated after the this proposition.

Proposition 5.4.7 (Bound on $\boldsymbol{\mathcal{N}}^n$ terms)**.** *Let $\mathcal{N} = C^{(4)}_{\text{avg}} \circ \Lambda^{\otimes 4} \circ C^{(4)}_{\text{avg}}$, where*

$$C^{(4)}_{\text{avg}} = \frac{1}{|\mathcal{C}_1|} \sum_{C \in \mathcal{C}_1} C^{\otimes 4}$$

is the abstract superoperator corresponding to its Liouville representation $\boldsymbol{\mathcal{N}}$ (as defined in (5.21)) and where $\Lambda \in \mathcal{S}(\mathbb{C}^2)$ is any single-qubit quantum channel. Denote $V = \text{Span}\{\mathcal{Q}_1^{\otimes 4}\}$ the Hilbert space (equipped with the Hilbert-Schmidt inner product) on which $\mathcal{N}^n$ acts.

Now let $A, B \in V$. Then

$$|\langle\langle A|\boldsymbol{\mathcal{N}}^n|B\rangle\rangle| \leq 4\|A\|_2\|B\|_2. \tag{5.61}$$

If in addition $B \in \text{Span}\{(\mathcal{Q}_1^*)^{\otimes 4}\} \subset V$ and $B = B^\dagger$, then this can be improved to

$$|\langle\langle A|\boldsymbol{\mathcal{N}}^n|B\rangle\rangle| \leq \|A\|_2\|B\|_2. \tag{5.62}$$

Proof. The first step is to use the Cauchy-Schwarz inequality (Theorem 2.1.1) to get

$$\left|\langle\langle A|\boldsymbol{\mathcal{N}}^n|B\rangle\rangle\right| \leq \|A\|_2\|\mathcal{N}^n(B)\|_2. \tag{5.63}$$

Under no assumptions on B, it just follows then that

$$\left|\langle\langle A|\boldsymbol{\mathcal{N}}^n|B\rangle\rangle\right| \leq \|A\|_2\|\mathcal{N}^n(B)\|_2 \leq \|A\|_2\|\mathcal{N}^n\|_\infty\|B\|_2 \leq 4\|A\|_2\|B\|_2, \tag{5.64}$$

by using Cauchy-Schwarz (Theorem 2.1.1) and Lemma 5.4.8 since $\mathcal{N}^n$ is a CPTP map (see Proposition 2.5.1 and Proposition 2.5.6), proving the first claim.

If $B \in V_0 := \{B \in \mathrm{Span}\{(\mathcal{Q}_1^*)^{\otimes 4}\} : B = B^\dagger\}$, then $\mathcal{N}^n$ can be restricted to the subspace V_0 (which can be viewed as a vector space over $\mathbb{R}$). Thus,

$$\left|\langle\langle A|\boldsymbol{\mathcal{N}}^n|B\rangle\rangle\right| \leq \|A\|_2 \|(\mathcal{N}^n)\big|_{V_0}\|_\infty \|B\|_2 \leq \|A\|_2 \left(\|(C_{\mathrm{avg}}^{(4)})\big|_{V_0}\|_\infty \|(\Lambda^{\otimes 4})\big|_{V_0}\|_\infty \|(C_{\mathrm{avg}}^{(4)})\big|_{V_0}\|_\infty\right)^n \|B\|_2, \quad (5.65)$$

using Cauchy-Schwarz (Theorem 2.1.1) and the submultiplicativity of the ∞-norm (Proposition 2.1.11). Since $\mathbf{C}_{\mathrm{avg}}^{(4)}$ is an orthogonal projection, it follows that

$$\|\mathbf{C}_{\mathrm{avg}}^{(4)}\big|_{V_0}\|_\infty \leq \|\mathbf{C}_{\mathrm{avg}}^{(4)}\|_\infty = 1.$$

Furthermore,

$$(\Lambda^{\otimes 4})\big|_{V_0} = \left(\Lambda\big|_{W_0}\right)^{\otimes 4}, \quad (5.66)$$

where $W_0 = \{B \in \mathrm{Span}\{\mathcal{Q}_1^*\} : B = B^\dagger\}$ since $V_0 = W_0^{\otimes 4}$ if V_0 and W_0 are viewed as Hilbert spaces over $\mathbb{R}$. So (5.65) reduces to

$$\left|\langle\langle A|\boldsymbol{\mathcal{N}}^n|B\rangle\rangle\right| \leq \|A\|_2 \left(\|\left(\Lambda\big|_{W_0}\right)^{\otimes 4}\|_\infty\right)^n \|B\|_2 \quad (5.67)$$

To make progress it is used that $\|A^{\otimes n}\|_\infty = \|A\|_\infty^n$ for any linear operator $A \in \mathcal{L}(\mathcal{H})$ on a Hilbert space. This follows from the singular value theorem (Theorem 2.1.9). Let $A = USW^\dagger$ be its singular value decomposition, with U, W unitary and S a diagonal matrix with the singular values $s_1 \geq s_2 \geq \ldots \geq s_d \geq 0$ on the diagonal. Then $A^{\otimes n} = (USW^\dagger)^{\otimes n} = U^{\otimes n} S^{\otimes n} (W^{\otimes n})^\dagger$, which is precisely the singular value decomposition of $A^{\otimes n}$ since $U^{\otimes n}$ and $W^{\otimes n}$ are unitary and $S^{\otimes n}$ is diagonal with positive elements. Moreover, the largest singular value in $S^{\otimes n}$ is precisely s_1^n. Therefore $\|A\|_\infty^n = s_1^n = \|A^{\otimes n}\|_\infty$. Using this in our inequality yields

$$\left|\langle\langle A|\boldsymbol{\mathcal{N}}^n|B\rangle\rangle\right| \leq \|A\|_2 \left(\|\left(\Lambda\big|_{W_0}\right)\|_\infty\right)^{4n} \|B\|_2 \leq \|A\|_2 \|B\|_2, \quad (5.68)$$

where the last inequality follows from Lemma 5.4.8, which claims that

$$\|\Lambda\big|_{W_0}\|_\infty^{4n} \leq 1^{4n} = 1. \quad (5.69)$$

■

Lemma 5.4.8 (Operator norm bound for superoperators)**.** *Let $\mathcal{E} \in \mathcal{S}(\mathcal{H})$ be a CPTP map on a d-dimensional Hilbert space $\mathcal{H}$, with $d = 2^q$ for a q-qubit system. Then*

$$\|\mathcal{E}\|_\infty = \max_{A \in \mathcal{L}(\mathcal{H})} \{\|\mathcal{E}(A)\|_2 : \|A\|_2 = 1\} \leq \sqrt{d} \quad (5.70)$$

and

$$\|\mathcal{E}\|_\infty^H := \max_{A \in \mathcal{L}(\mathcal{H})} \left\{\|\mathcal{E}(A)\|_2 : \|A\|_2 = 1, \mathrm{Tr}[A] = 0, A = A^\dagger\right\} \leq \sqrt{\frac{d}{2}}. \quad (5.71)$$

Proof. See Theorem 2.1 and 3.1 of [30]. ■

The norm $\|\cdot\|_\infty^H$ is the operator norm when the map $\mathcal{E}$ is restricted to the real vector space of traceless, hermitian operators in $\mathcal{L}(\mathcal{H})$ (in which $\rho - \hat{\rho}$ is contained for two density matrices ρ and $\hat{\rho}$).

This concludes our proof of the variance bound in the case of ideal state preparation and measurement errors. The next subsection continues with the proof for the general case including SPAM.

5.4.2. INCLUDING SPAM

This section expands on the previous result of Theorem 5.4.1 by including state preparation and measurement errors (SPAM). This is of significant importance, since in practice there will always be SPAM present in any experimental setup. Furthermore, one of the strengths of benchmarking type protocols is that they allow for the benchmarking of a gate set independent of SPAM. That is, for the unitarity benchmarking protocol, the fitting procedure yields the unitarity of the average error channel independent of the SPAM. However, as follows from the theorem below, the variance $\mathbb{V}[q_{\mathbf{i_m}}]$ (and therefore also the number of sequences N needed in the protocol to obtain a result with a specific a priori determined confidence interval) depends on SPAM.

In the theorem below the general variance bound is presented. Most of the technique is similar to the ideal case, which is why this was done first. The proof only makes use of two new propositions, which are presented below the theorem.

Theorem 5.4.9 (Noisy variance bound)**.** *Let $\Lambda \in \mathcal{S}(\mathbb{C}^2)$ be a single-qubit CPTP quantum channel that corresponds to the average error map associated with the Clifford group $\mathcal{C}_1$, with unitarity $u(\Lambda) = u$. Furthermore let $\rho, \hat{\rho} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ be two density matrices and let $Q \in \mathrm{Herm}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ be a hermitian observable.*

Then the variance $\mathbb{V}[q_{\mathbf{i_m}}]$ of the survival probability $q_{\mathbf{i_m}} = \langle\langle Q|\mathbf{W}_{\mathbf{i_m}}^{\otimes 2}|\rho - \hat{\rho}\rangle\rangle$ over the unitary randomized benchmarking sequences $W_{\mathbf{i_m}}$ (as defined by (4.39)) satisfies

$$\mathbb{V}[q_{\mathbf{i_m}}] \leq \left(\|\rho_{\text{ideal}}\|_2^2 \left(\frac{3\sqrt{3}}{2} + \sqrt{2} \right) (1-u)^2 \frac{1-u^{2(m-1)}}{1-u^2} + 4\|\rho_{\text{err}}\|_2^2 \right) \left(\|Q_{\text{ideal}}\|_2^2 + 2\|Q_{\text{err}}\|_2^2 \right). \tag{5.72}$$

where

$$\rho_{\text{ideal}} := \langle B_2|\rho - \hat{\rho}\rangle B_2, \qquad \rho_{\text{err}} := \rho - \hat{\rho} - \rho_{\text{ideal}}, \tag{5.73}$$

$$Q_{\text{ideal}} := \langle B_2|Q\rangle B_2, \qquad Q_{\text{err}} := Q - \langle B_1|Q\rangle B_1 - Q_{\text{ideal}}, \tag{5.74}$$

with B_1, B_2 defined in (4.49).

If $\rho - \hat{\rho} \in \mathrm{Span}\{\mathcal{Q}_1^*\}^{\otimes 2}$ (as is the case in the single-copy implementation of the protocol, since then $\rho - \hat{\rho} = (\rho_{\mathcal{H}} - \hat{\rho}_{\mathcal{H}})^{\otimes 2}$ with $\rho_{\mathcal{H}} - \hat{\rho}_{\mathcal{H}} \in \mathrm{Span}\{\mathcal{Q}_1^*\}$), where $\mathcal{Q}_1^*$ is defined as in Definition 3.6.1, then this bound can be improved to

$$\mathbb{V}[q_{\mathbf{i_m}}] \leq \left(\|\rho_{\text{ideal}}\|_2^2 \left(\frac{3\sqrt{3}}{2} + \sqrt{2} \right) (1-u)^2 \frac{1-u^{2(m-1)}}{1-u^2} + \|\rho_{\text{err}}\|_2^2 \right) \left(\|Q_{\text{ideal}}\|_2^2 + 2\|Q_{\text{err}}\|_2^2 \right). \tag{5.75}$$

Corollary. *An m-independent bound can be obtained by noting that*

$$(1-u)^2 \frac{1-u^{2(m-1)}}{1-u^2} \leq \frac{(1-u)^2}{1-u^2}, \tag{5.76}$$

which is a good bound in the limit of large m (when $u^{2(m-1)} \ll 1$).

Proof. The proof utilizes the fact that the basis of the space $\mathcal{L}(\mathcal{H} \otimes \mathcal{H})$ is free to be chosen, except for B_1 and B_2. The idea is to define two hermitian, orthonormal vectors B_3 and B_4 such that both $\rho - \hat{\rho}$ and Q can be expressed in these four basis vectors (by letting B_3 and B_4 depend on $\rho - \hat{\rho}$ and Q). Let throughout the proof $Q_i := \langle B_i|Q\rangle$ and $\rho_i := \langle B_i|\rho - \hat{\rho}\rangle$ for $i = 1, ..., 4$. It is also (implicitly) used that $\rho_i, Q_i \in \mathbb{R}$ since $\rho - \hat{\rho}, Q$ are hermitian.

Since $\rho - \hat{\rho}$ is traceless, it follows that $\rho_1 = 0$. The idea is to chose B_3 orthogonal to B_1 and B_2, in the direction of the remaining component of $\rho - \hat{\rho}$ after subtracting the B_2 component. Therefore define

$$B_3 := \frac{\rho - \hat{\rho} - \rho_2 B_2}{\|\rho - \hat{\rho} - \rho_2 B_2\|_2} \tag{5.77}$$

so that $\rho - \hat{\rho} = \rho_2 B_2 + \rho_3 B_3$. In similar fashion, B_4 is defined as the remaining component of Q that is orthogonal to B_1, B_2, B_3. That is,

$$B_4 := \frac{Q - \sum_{i=1}^{3} \langle B_i | Q \rangle B_i}{\| Q - \sum_{i=1}^{3} \langle B_i | Q \rangle B_i \|_2}, \tag{5.78}$$

allowing us to write $Q = \sum_{i=1}^{4} Q_i B_i$. Plugging these expansions into (5.20), it follows that

$$\begin{aligned} \mathbb{V}[q_{\mathbf{i_m}}] &= \langle\langle Q^{\otimes 2} | \mathcal{N}^{m-1} - (\mathcal{M}^{\otimes 2})^{m-1} | (\rho - \hat{\rho})^{\otimes 2} \rangle\rangle \\ &= \sum_{i,s=2}^{3} \sum_{k,l=1}^{4} \rho_i \rho_s Q_k Q_l \langle\langle B_k \otimes B_l | \mathcal{N}^{m-1} - (\mathcal{M}^{\otimes 2})^{m-1} | B_i \otimes B_s \rangle\rangle, \end{aligned} \tag{5.79}$$

noting that $Q_k \in \mathbb{R}$ for all k, since Q is hermitian. Furthermore, since $\mathcal{M}$ has only support on B_1 and B_2, and $\langle\langle B_3 | B_2 \rangle\rangle = \langle\langle B_3 | B_1 \rangle\rangle = 0$, it follows that $\mathcal{M}^{\otimes 2} | B_i \otimes B_s \rangle\rangle = 0$, unless $i = s = 2$ in the above summation. The variance is therefore split into two terms

$$\mathbb{V}[q_{\mathbf{i_m}}] = \rho_2^2 \sum_{k,l=1}^{4} Q_k Q_l \langle\langle B_k \otimes B_l | \mathcal{N}^{m-1} - (\mathcal{M}^{\otimes 2})^{m-1} | B_2 \otimes B_2 \rangle\rangle \tag{5.80}$$

$$+ \sum_{\substack{i,s=2 \\ i \neq 2 \wedge s \neq 2}}^{3} \sum_{k,l=1}^{4} \rho_i \rho_s Q_k Q_l \langle\langle B_k \otimes B_l | \mathcal{N}^{m-1} | B_i \otimes B_s \rangle\rangle \tag{5.81}$$

Each term in the equation is bounded separately. There are two new propositions, Proposition 5.4.10 and Proposition 5.4.11, which are used to throw away as many zero terms. These propositions are proven below.

The bound on the first term (5.80) mimics the proof of Theorem 5.4.1. Using again the telescoping series (Lemma 3.2.1), (5.80) is written as

$$\begin{aligned} (5.80) &= \rho_2^2 \sum_{j=1}^{m-1} \sum_{k,l=1}^{4} Q_k Q_l \langle\langle B_k \otimes B_l | \mathcal{N}^{m-j-1} \left[\mathcal{N} - \mathcal{M}^{\otimes 2} \right] (\mathcal{M}^{\otimes 2})^{j-1} | B_2 \otimes B_2 \rangle\rangle \\ &= \rho_2^2 \sum_{j=1}^{m-1} u^{2j-2} \sum_{k,l=1}^{4} Q_k Q_l \langle\langle B_k \otimes B_l | \mathcal{N}^{m-j-1} \left[\mathcal{N} - \mathcal{M}^{\otimes 2} \right] | B_2 \otimes B_2 \rangle\rangle \\ &= \rho_2^2 \sum_{j=1}^{m-1} u^{2j-2} \sum_{k,l=1}^{4} Q_k Q_l \Big(a_{14} \langle\langle B_k \otimes B_l | \mathcal{N}^{m-j-1} | A_{14} \rangle\rangle + a_{15} \langle\langle B_k \otimes B_l | \mathcal{N}^{m-j-1} | A_{15} \rangle\rangle \Big). \end{aligned}$$

In the second line it was used that $\mathcal{M} | B_2 \rangle\rangle = u | B_2 \rangle\rangle$, according to (4.50). In the third line, Proposition 5.4.3 was used, noting that $A_2 = B_2 \otimes B_2$. Before applying the bounds as in the error free case, two propositions are used to eliminate some zero terms in this expression. By Proposition 5.4.10 it follows that

$$\langle\langle B_k \otimes B_l | \mathbf{C}_{\text{avg}}^{(4)} = (\mathbf{C}_{\text{avg}}^{(4)} | B_k \otimes B_l \rangle\rangle)^{\dagger} = 0,$$

for all $(k,l) \in \{(1,3),(1,4),(2,3),(2,4),(3,1),(3,2),(4,1),(4,2)\}$, eliminating half of the terms immediately. The terms $(k,l) \in \{(1,1),(1,2),(2,1)\}$ are eliminated by Proposition 5.4.11, since A_{14}, $A_{15} \in \text{Span}\{(Q_2^*)\}^{\otimes 2}$, by Proposition 5.4.10. Therefore (5.80) is reduced to

$$(5.80) = \rho_2^2 \sum_{j=1}^{m-1} u^{2j-2} \sum_{(k,l) \in K} Q_k Q_l \Big(a_{14} \langle\langle B_k \otimes B_l | \mathcal{N}^{m-j-1} | A_{14} \rangle\rangle + a_{15} \langle\langle B_k \otimes B_l | \mathcal{N}^{m-j-1} | A_{15} \rangle\rangle \Big),$$

where the index set $K := \{(2,2),(3,3),(3,4),(4,3),(4,4)\}$. Since $Q_k Q_l$ may be negative, it is necessary here to take the absolute value and use the triangle inequality in order to bound this quantity. Then the quantities a_{14} and a_{15} (which arose from Proposition 5.4.3) can be bounded using

Proposition 5.4.5 and Proposition 5.4.6, whereas the remaining inner products are bounded using Proposition 5.4.7. The results of these three propositions are summarized as follows

$$\begin{aligned} |a_{14}| &\leq \frac{3\sqrt{3}}{2}(1-u)^2, \\ |a_{15}| &\leq \sqrt{2}(1-u)^2, \\ |\langle\langle B_k \otimes B_l | \mathcal{N}^{m-j-1} | A_{14} \rangle\rangle| &\leq 1, \qquad \forall k,l = 1,...,4, \\ |\langle\langle B_k \otimes B_l | \mathcal{N}^{m-j-1} | A_{15} \rangle\rangle| &\leq 1, \qquad \forall k,l = 1,...,4, \end{aligned}$$

since A_{14}, A_{15} and $B_k \otimes B_l$ for all $k,l = 1,...,4$ are hermitian operators with Hilbert-Schmidt norm 1 and $A_{14}, A_{15} \in \text{Span}\{\mathcal{Q}_1\}^{\otimes 4}$ by their definition (see Lemma 5.4.2). Putting this all together yields a bound on (5.80):

$$\begin{aligned} (5.80) &\leq \rho_2^2 \sum_{j=1}^{m-1} u^{2j-2} \sum_{(k,l)\in K} |Q_k Q_l| \Big(|a_{14}| |\langle\langle B_k \otimes B_l | \mathcal{N}^{m-j-1} | A_{14} \rangle\rangle| \\ &\qquad + |a_{15}| |\langle\langle B_k \otimes B_l | \mathcal{N}^{m-j-1} | A_{15} \rangle\rangle| \Big) \\ &\leq \rho_2^2 \sum_{j=1}^{m-1} u^{2j-2} \sum_{(k,l)\in K} |Q_k Q_l| \left(\frac{3\sqrt{3}}{2} + \sqrt{2} \right) (1-u)^2 \\ &= \sum_{(k,l)\in K} |Q_k Q_l| \left[\rho_2^2 \left(\frac{3\sqrt{3}}{2} + \sqrt{2} \right) (1-u)^2 \frac{1-u^{2(m-1)}}{1-u^2} \right]. \end{aligned} \tag{5.82}$$

Next a bound is given for the term of (5.81). This term is also analyzed using Proposition 5.4.10 to throw away some zero terms. First, the proposition claims that $\mathbf{C}_{\text{avg}}^{(4)} | B_i \otimes B_s \rangle\rangle = 0$ for $(i,s) \in \{(2,3),(3,2)\}$. Hence only terms with $i = s = 3$ remain. Furthermore, analogous to the above

$$\langle\langle B_k \otimes B_l | \mathbf{C}_{\text{avg}}^{(4)} = (\mathbf{C}_{\text{avg}}^{(4)} | B_k \otimes B_l \rangle\rangle)^\dagger = 0,$$

for all $(k,l) \in \{(1,3),(1,4),(2,3),(2,4),(3,1),(3,2),(4,1),(4,2)\}$. Next Proposition 5.4.11 is applied, from which it directly follows that

$$\langle\langle B_k \otimes B_l | \mathcal{N}^{m-1} | B_3 \otimes B_3 \rangle\rangle = 0, \qquad (k,l) \in \{(1,1),(1,2),(2,1)\}.$$

Therefore (5.81) is reduced to

$$(5.81) = \rho_3^2 \sum_{(k,l)\in K} Q_k Q_l \langle\langle B_k \otimes B_l | \mathcal{N}^{m-1} | B_3 \otimes B_3 \rangle\rangle, \tag{5.83}$$

where $K = \{(2,2),(3,3),(3,4),(4,3),(4,4)\}$ is the same index set as above. Now to bound this, the absolute value is taken, the triangle inequality is used and finally Proposition 5.4.7 is applied to obtain

$$(5.81) \leq \rho_3^2 \sum_{(k,l)\in K} |Q_k Q_l| |\langle\langle B_k \otimes B_l | \mathcal{N}^{m-1} | B_3 \otimes B_3 \rangle\rangle| \leq 4\rho_3^2 \sum_{(k,l)\in K} |Q_k Q_l|, \tag{5.84}$$

since $B_k \otimes B_l$ for $(k,l) \in K$ are all traceless, hermitian operators with Hilbert-Schmidt norm one. Under the assumption that $\rho - \hat{\rho} \in \text{Span}\{\mathcal{Q}_1^*\}^{\otimes 2}$, the better bound of Proposition 5.4.7 can be used, yielding

$$(5.81) \leq \rho_3^2 \sum_{(k,l)\in K} |Q_k Q_l| |\langle\langle B_k \otimes B_l | \mathcal{N}^{m-1} | B_3 \otimes B_3 \rangle\rangle| \leq \rho_3^2 \sum_{(k,l)\in K} |Q_k Q_l|, \tag{5.85}$$

Putting everything together, yields the bound

$$\mathbb{V}[q_{\mathbf{i_m}}] \leq \left[4\rho_3^2 + \rho_2^2 \left(\frac{3\sqrt{3}}{2} + \sqrt{2} \right) (1-u)^2 \frac{1-u^{2(m-1)}}{1-u^2} \right] \sum_{(k,l)\in K} |Q_k Q_l|. \tag{5.86}$$

Now the goal is to write this bound in a form that is independent from the (arbitrarily chosen) basis vectors B_3 and B_4. The most important thing is to write the term $\sum_{(k,l)\in K}|Q_kQ_l|$ differently by using Hölder's inequality (Theorem 2.1.10) on

$$\sum_{k,l=3}^{4}|Q_kQ_l| = \left(\sum_{k=3}^{4}|Q_k|\right)^2 = \left(\sum_{k=3}^{4}|Q_k||1|\right)^2 \leq \left(\sqrt{\sum_{k=3}^{4}Q_k^2}\sqrt{\sum_{k=3}^{4}1^2}\right)^2 = 2\sum_{k=3}^{4}Q_k^2. \tag{5.87}$$

This leads to

$$\mathbb{V}[q_{\mathbf{i_m}}] \leq \left[4\rho_3^2+\rho_2^2\left(\frac{3\sqrt{3}}{2}+\sqrt{2}\right)(1-u)^2\frac{1-u^{2(m-1)}}{1-u^2}\right]\left(Q_2^2+2[Q_3^2+Q_4^2]\right). \tag{5.88}$$

Now writing the ρ_i^2 and Q_i^2 in terms of norms, yields the result of the theorem since

$$\|\rho_{\text{ideal}}\|_2^2 = \rho_2^2, \qquad \|\rho_{\text{err}}\|_2^2 = \rho_3^2,$$
$$\|Q_{\text{ideal}}\|_2^2 = Q_2^2, \qquad \|Q_{\text{err}}\|_2^2 = Q_3^2+Q_4^2,$$

by their respective definitions (5.73) and (5.74). The factor of 4 can be dropped under the assumption that $\rho-\hat{\rho}\in\text{Span}\{Q_1^*\}^{\otimes 2}$ and the analysis remains the same, yielding the improved result. Note that the statement is now made with respect to the Schatten 2-norm on the operators, which is independent of choice of basis. This justifies the freedom to choose B_3 and B_4 freely, as they are only used as intermediate tools. ■

The above proof made use of two new propositions, which were used to throw away as many zero terms as possible in the variance bound. This first proposition is used to claim that

$$\mathbf{C}_{\text{avg}}^{(4)}|B_i\otimes B_j\rangle\rangle = \mathbf{C}_{\text{avg}}^{(4)}|B_j\otimes B_i\rangle\rangle = 0, \tag{5.89}$$

whenever $i=1,2$ and $j=3,...,16$. This is shown in the proposition below.

Proposition 5.4.10. *Let* $\mathbf{C}_{\text{avg}}^{(4)}$ *be defined as in* (4.46) *and let* $A_i = 1,...,15$ *be defined as in Lemma 5.4.2, such that* $\mathbf{C}_{\text{avg}}^{(4)} = \sum_{i=1}^{15}|A_i\rangle\rangle\langle\langle A_i|$. *Let* $\mathcal{B}=\{B_i : i=1,...,2^4\}$ *be an orthonormal basis of* $\text{Span}\{\mathcal{Q}_1^{\otimes 2}\}$, *such that* B_1 *and* B_2 *satisfy the definition* (4.49). *Denote* $W=\text{Span}\{B_i : i=3,4,...,16\}$.

Then $\mathbf{C}_{\text{avg}}^{(4)}|B_i\otimes w\rangle\rangle = \mathbf{C}_{\text{avg}}^{(4)}|w\otimes B_i\rangle\rangle = 0$ *for* $i=1,2$ *and for all* $w\in W$. *Furthermore* $A_i\in W\otimes W$ *for* $i=5,...,15$.

Proof. To see this, consider the Liouville tensor-2 representation $(V\otimes V, R^{\otimes 2})$, where $V=\text{Span}\{|\sigma\rangle\rangle : \sigma\in\mathcal{Q}_1\}$. In Proposition 3.6.4 the trivial subrepresentations were found to be spanned by B_1 and B_2 respectively. By Machke's theorem (Theorem 2.3.3), there is a decomposition

$$V\otimes V = \text{Span}\{B_1\}\oplus\text{Span}\{B_2\}\oplus W, \tag{5.90}$$

where W is a subrepresentation of $V\otimes V$. Note that by Proposition 3.6.4, W can not contain any trivial subrepresentations (but can certainly be decomposed further). In this decomposition then

$$V^{\otimes 4} = \left(\bigoplus_{i,j=1}^{2}\text{Span}\{B_i\otimes B_j\}\right)\oplus\left(\bigoplus_{i=1}^{2}(\text{Span}\{B_i\}\otimes W)\oplus(W\otimes\text{Span}\{B_i\})\right)\oplus(W\otimes W). \tag{5.91}$$

The spaces $\text{Span}\{B_i\}\otimes W$ and $W\otimes\text{Span}\{B_i\}$ for $i=1,2$ are all four isomorphic to W via the identification $x\mapsto B_i\otimes x$ and $x\mapsto x\otimes B_i$ respectively ($x\in W$). Therefore, these spaces can not contain trivial subrepresentations, since W contains no trivial subrepresentations. Note that $B_i\otimes w\in\text{Span}\{B_i\}\otimes W$ and $w\otimes B_i\in W\otimes\text{Span}\{B_i\}$ for $i=1,2$. Since these spaces do not contain trivial subrepresentations of

$V^{\otimes 4}$ and $\mathbf{C}^{(4)}_{\text{avg}}$ projects onto the trivial subrepresentations of $(V^{\otimes 4}, R^{\otimes 4})$ it follows that $\mathbf{C}^{(4)}_{\text{avg}}|B_i \otimes w\rangle\rangle = \mathbf{C}^{(4)}_{\text{avg}}|w \otimes B_i\rangle\rangle = 0$ for $i = 1,2$ as claimed.

The four spaces $\text{Span}\{B_i \otimes B_j\}$, $i, j = 1,2$ are trivial subrepresentations and correspond to the spaces $\text{Span}\{A_i\}$, $i = 1,...,4$ by their direct definition. In Lemma 5.4.2 all other trivial subspaces were found, which must thus be contained in $W \otimes W$, since the spaces isomorphic to W can not contain them. Hence $A_i \in W \otimes W$ for $i = 5,...,15$ as claimed. ■

The second new proposition that was used in the proof of Theorem 5.4.9 to throw away some other terms in variance bound by utilizing the trace-preserving property of Λ. It is argued that

$$\langle\langle B_k \otimes B_l|\mathcal{N}^n|w\rangle\rangle = 0, \tag{5.92}$$

if $k = 1$ and/or $l = 1$ (meaning that either B_k or B_l or both are the identity B_1) and if w can be expanded in the tensor basis $B_i \otimes B_j$ without using the identity B_1. This is made precise in the proposition below.

Proposition 5.4.11 (Invariant space of $\mathcal{N}$)**.** *Let $\mathcal{N}$ be defined as in* (5.21)*. Let $\mathcal{B} = \{B_i : i = 1,...,2^4\}$ be an orthonormal basis of* $\text{Span}\{\mathcal{Q}_1^{\otimes 2}\}$*, such that B_1 and B_2 satisfy their definition of* (4.49)*. Denote $W' = \text{Span}\{B_i : i = 2,3,...,2^4\} = \text{Span}\{Q_2^*\}$. Then*

$$\langle\langle B_k \otimes B_l|\mathcal{N}^n|w\rangle\rangle = 0 \tag{5.93}$$

for all $n \in \mathbb{N}$ and all $w \in W' \otimes W'$, whenever $k = 1$ and/or $l = 1$.

Proof. To show the claim of the proposition it is argued that both $\mathbf{C}^{(4)}_{\text{avg}}$ and $\Lambda^{\otimes 4}$ leave $W' \otimes W'$ invariant. For $\Lambda^{\otimes 4}$ one finds that

$$\langle\langle B_k \otimes B_l|\mathbf{\Lambda}^{\otimes 4}|B_i \otimes B_j\rangle\rangle = \langle\langle B_k|\mathbf{\Lambda}^{\otimes 2}|B_i\rangle\rangle\langle\langle B_l|\mathbf{\Lambda}^{\otimes 2}|B_j\rangle\rangle = 0, \tag{5.94}$$

for all $i, j = 2,3,...,2^4$ if $k = 1$ and/or $l = 1$ by the trace-preserving property of $\Lambda^{\otimes 2}$. So, for any $w \in W$ it follows that $\mathbf{\Lambda}^{\otimes 4}|w\rangle\rangle \in W' \otimes W'$ as claimed. Now $\mathbf{C}^{(4)}_{\text{avg}}$, restricted to $W' \otimes W'$, can be written as

$$\mathbf{C}^{(4)}_{\text{avg}}\Big|_{W' \otimes W'} = |A_2\rangle\rangle\langle\langle A_2| + P,$$

where $A_2 = B_2 \otimes B_2$ and $P = \sum_{i=5}^{15} |A_i\rangle\rangle\langle\langle A_i|$ is an orthogonal projection onto a subspace of $W \otimes W$, where $W = \text{Span}\{B_i : i = 3,...,2^4\}$. This follows Lemma 5.4.2 and Proposition 5.4.10. By noting that $W \subset W'$, it is clear that $\mathbf{C}^{(4)}_{\text{avg}}|w\rangle\rangle \in W' \otimes W'$.

Therefore $\mathcal{N}^n|w\rangle\rangle = (\mathbf{C}^{(4)}_{\text{avg}}\mathbf{\Lambda}^{\otimes 4}\mathbf{C}^{(4)}_{\text{avg}})^n|w\rangle\rangle \in W' \otimes W'$. Since $B_k \otimes B_l \in (W' \otimes W')^{\perp}$ if $k = 1$ and/or $l = 1$, the claim follows. ■

This completes the proof of the variance bound in the presence of state preparation and measurement errors. Next section will provide a discussion on the obtained result.

5.4.3. DISCUSSION OF THE NOISY VARIANCE BOUND

In this section a discussion of the variance bound including state preparation and measurement errors is given. As a first sanity check, it is good to verify that Theorem 5.4.9 is indeed an extension of Theorem 5.4.1. This can be done by applying Theorem 5.4.9 to the ideal input states $\rho - \hat{\rho} = Q = B_2$. This implies that the ideal components are one and the error components are zero, i.e. $\rho_{\text{ideal}} = Q_{\text{ideal}} = B_2$ and $\rho_{\text{err}} = Q_{\text{err}} = 0$. This then indeed reduces the variance bound of Theorem 5.4.9 to the one of Theorem 5.4.1.

The bound in the presence of state preparation and measurement errors of Theorem 5.4.9 has a constant term, independent of the variable $1-u$, whereas the bound scales as $(1-u)^2$ in the ideal case (Theorem 5.4.1). In particular, this means that if $u \to 1$, then $\mathbb{V}[q_{\mathbf{i_m}}] \to 0$ if and only if there is zero SPAM (that is iff $\rho_{\text{err}} = Q_{\text{err}} = 0$). In Example 5.4.1 it is argued that $\mathcal{O}(1)$ with respect to $(1-u)$ is the best achievable. In particular, it is shown that for $\Lambda = \mathcal{I}$ and certain choices of $\rho - \hat{\rho}$ and Q, the variance does not vanish (as is the case in the ideal scenario of perfect state preparation). Since $u(\mathcal{I}) = 1$, it is clear that there does not exists a constant M such that $\mathbb{V} \leq M(1-u)$ for this case. Thus $\mathcal{O}(1)$ is the best that can be done for a variance bound that is independent of Λ, ρ and Q.

Example 5.4.1. Let us consider the case where $\Lambda = \mathcal{I}$, i.e. gates are performed perfectly, but where measurements and state preparation is far from ideal. Suppose that

$$\rho - \hat{\rho} = \frac{X \otimes X}{4} \qquad \text{and} \qquad Q = X \otimes X, \tag{5.95}$$

where $X \in \mathcal{P}_1$ is the Pauli-X matrix over $\mathbb{C}^2$ and the tensor product is omitted between them. Note that $\rho, Q \in \mathcal{L}(\mathcal{H} \otimes \mathcal{H})$, where $\mathcal{H} = \mathbb{C}^2$ is the single-qubit Hilbert space. Since $\Lambda = \mathcal{I}$, the string $W_{\mathbf{i_m}}$ of m independently and uniformly distributed Cliffords reduces to a single Clifford element uniformly drawn from $\mathcal{C}_1$. There are 24 elements of $\mathcal{C}_1$, 8 of which map $X \mapsto \pm X$. The sign is irrelevant, since if C maps $X \mapsto -X$, then CC maps $XX \mapsto XX$. The other 16 Cliffords send $X \mapsto \pm Y$ or $X \mapsto \pm Z$, where again the sign is irrelevant. Since $\langle\langle XX|\frac{XX}{4}\rangle\rangle = 1$ and $\langle\langle XX|\frac{YY}{4}\rangle\rangle = \langle\langle XX|\frac{ZZ}{4}\rangle\rangle = 0$, the following probability distribution on $q_{\mathbf{i_m}}$ is obtained:

$$\mathbb{P}[q_{\mathbf{i_m}} = 1] = \frac{8}{24} = \frac{1}{3} \qquad \text{and} \qquad \mathbb{P}[q_{\mathbf{i_m}} = 0] = \frac{16}{24} = \frac{2}{3}. \tag{5.96}$$

Clearly then $\mathbb{E}[q_{\mathbf{i_m}}] = \frac{1}{3}$ and $\mathbb{V}[q_{\mathbf{i_m}}] = \mathbb{E}[q_{\mathbf{i_m}}^2] - \mathbb{E}[q_{\mathbf{i_m}}]^2 = \frac{1}{3} - \frac{1}{9} = \frac{2}{9}$ is nonzero. This example shows that $\mathbb{V}[q_{\mathbf{i_m}}] \neq 0$ as $(1-u) \to 0$. □

5.4.4. BOUND ON $q_{\mathbf{i_m}}$

The main result of this chapter, Theorem 5.2.1, which puts a bound on the number of sequences N needed to rigorously perform unitarity randomized benchmarking, also requires an interval in which the random variable $q_{\mathbf{i_m}}$ is contained. This is precisely the goal of this proposition. It is presented here because the proof technique uses Lemma 5.4.8, which was only introduced in this section.

Proposition 5.4.12 (Bound on $q_{\mathbf{i_m}}$)**.** *Let $Q \in \text{Herm}(\mathcal{H} \otimes \mathcal{H})$, $\rho, \hat{\rho} \in \mathcal{D}(\mathcal{H} \otimes \mathcal{H})$ and let the unitarity randomized benchmarking $q_{\mathbf{i_m}}$ be defined as in* (5.1)*. Denote $\tilde{Q} = Q - \langle B_1|Q\rangle B_1$. Then*

$$|q_{\mathbf{i_m}}| \leq \sqrt{2}\|\tilde{Q}\|_2 \|\rho - \hat{\rho}\|_2. \tag{5.97}$$

If in addition $Q = Q_{\mathcal{H}}^{\otimes 2}$ and $\rho - \hat{\rho} = (\rho_{\mathcal{H}} - \hat{\rho}_{\mathcal{H}})^{\otimes 2}$ are of tensor form (as in the single-copy implementation), then this can be improved to

$$0 \leq q_{\mathbf{i_m}} \leq \|\tilde{Q}\|_2 \|\rho - \hat{\rho}\|_2. \tag{5.98}$$

Proof. Since

$$q_{\mathbf{i_m}} = \langle\langle Q|\mathbf{W}_{\mathbf{i_m}}^{\otimes 2}|\rho - \hat{\rho}\rangle\rangle = \langle\langle Q|B_1\rangle\rangle\langle\langle B_1|\mathbf{W}_{\mathbf{i_m}}^{\otimes 2}|\rho - \hat{\rho}\rangle\rangle + \langle\langle \tilde{Q}|\mathbf{W}_{\mathbf{i_m}}^{\otimes 2}|\rho - \hat{\rho}\rangle\rangle = \langle\langle \tilde{Q}|\mathbf{W}_{\mathbf{i_m}}^{\otimes 2}|\rho - \hat{\rho}\rangle\rangle,$$

due to the fact that $\langle\langle B_1|\mathbf{W}_{\mathbf{i_m}}^{\otimes 2}|\rho - \hat{\rho}\rangle\rangle = 0$ by the trace-preserving property of $W_{\mathbf{i_m}}$ and $\text{Tr}[\rho - \hat{\rho}] = 0$, Q can be replaced with $\tilde{Q}$. So

$$|q_{\mathbf{i_m}}| \leq \|\tilde{Q}\|_2 \|\rho - \hat{\rho}\|_2 \|W_{\mathbf{i_m}}^{\otimes 2}\|_\infty \leq \sqrt{2}\|\tilde{Q}\|_2 \|\rho - \hat{\rho}\|_2, \tag{5.99}$$

where the first inequality is Cauchy-Swartz and the second inequality is due to Lemma 5.4.8. In the case that $Q = Q_{\mathcal{H}}^{\otimes 2}$ and $\rho - \hat{\rho} = (\rho_{\mathcal{H}} - \hat{\rho}_{\mathcal{H}})^{\otimes 2}$, one has

$$q_{\mathbf{i_m}} = \langle\langle Q_{\mathcal{H}}^{\otimes 2}|\mathbf{W}_{\mathbf{i_m}}^{\otimes 2}|(\rho_{\mathcal{H}} - \hat{\rho}_{\mathcal{H}})^{\otimes 2}\rangle\rangle = \langle\langle Q_{\mathcal{H}}|\mathbf{W}_{\mathbf{i_m}}|\rho_{\mathcal{H}} - \hat{\rho}_{\mathcal{H}}\rangle\rangle^2 \geq 0, \tag{5.100}$$

and

$$\begin{aligned} q_{\mathbf{i_m}} &= \langle\langle \tilde{Q} | \mathbf{W}_{\mathbf{i_m}}^{\otimes 2} | (\rho_{\mathcal{H}} - \hat{\rho}_{\mathcal{H}})^{\otimes 2} \rangle\rangle \\ &\leq \|\tilde{Q}\|_2 \| W_{\mathbf{i_m}}^{\otimes 2} \left((\rho_{\mathcal{H}} - \hat{\rho}_{\mathcal{H}})^{\otimes 2} \right) \|_2 \\ &= \|\tilde{Q}\|_2 \| W_{\mathbf{i_m}} \left(\rho_{\mathcal{H}} - \hat{\rho}_{\mathcal{H}} \right) \|_2^2 \\ &\leq \|\tilde{Q}\|_2 \|\rho_{\mathcal{H}} - \hat{\rho}_{\mathcal{H}}\|_2^2 (\| W_{\mathbf{i_m}} \|_\infty^H)^2 \\ &\leq \|\tilde{Q}\|_2 \|\rho_{\mathcal{H}} - \hat{\rho}_{\mathcal{H}}\|_2^2 \\ &= \|\tilde{Q}\|_2 \|\rho - \hat{\rho}\|_2, \end{aligned} \tag{5.101}$$

where in the third inequality Lemma 5.4.8 was used. ■

5.5. OUTLOOK ON MULTI-QUBIT CASE

In this section it is outlined what steps in the proofs of this chapter are going to be different when a bound for $\mathbb{V}[q_{\mathbf{i_m}}]$ is tried to be found for unitarity randomized benchmarking of the multi-qubit Clifford group. First, there are more trivial subrepresentations of the Liouville tensor-4 representation of the Clifford group $\mathcal{C}_q$ for $q > 1$. This follows from Lemma 3.6.5 and Lemma 2.3.8. In the two-qubit case $q = 2$ there are 29 trivial subrepresentations and in all other cases $q \geq 3$ there are 30. This means that $\mathbf{C}_{\text{avg}}^{(4)}$ projects onto a larger subspace, spanned by $A_i : i = 1, ..., 30$ (or 29). Fortunately, these subspaces can be found by the same technique as employed in Lemma 5.4.2, since [41] also provides a full decomposition of the tensor-2 Liouville representation of $\mathcal{C}_q$ for all $q > 1$. Thus, going to multi-qubit systems would merely make the task of finding all trivial subrepresentations more cumbersome. As a consequence, computing $\mathcal{N}|A_2\rangle\rangle$ would also be more cumbersome.

The actual bounding of terms in the proof basically uses two main results from literature. The first is Lemma 5.4.4, which is a purely single-qubit result that has no known analogue for multi-qubit systems. This lemma essentially allows to use the fact that Λ is completely positive, a property that is used only in this lemma. Proving a bound without using the condition that Λ is completely positive seems hopeless. It is unclear how to use the complete positivity of the error map Λ in the multi-qubit case. The second result used from literature is Lemma 5.4.8. This result can also be applied to multi-qubit systems, but this would introduce a proportionality factor of d^2 in the multi-qubit case. As a result, the variance bound will scale as $d^2 = 4^q$, increasing quadratically as the system size increases. Intuitively, a variance bound that is (at least asymptotically) independent of d should be possible, because $q_{\mathbf{i_m}}$ is still a discrete random variable on a bounded interval that does not depend on d. Therefore the variance can be bounded by a function that is asymptotically independent on the dimension d. This means that other techniques should be found to bound the nonzero constants a_i and the inner products involving higher powers of $\boldsymbol{\mathcal{N}}$, in order to proof a variance bound that is sharp enough to improve the bound on N beyond the first order bound.

5.6. CONCLUSION

The main goal of this chapter was to improve on the existing bound on the number of sequences needed in unitarity randomized benchmarking. This was achieved by using a second order concentration inequality, instead of the previously used first order inequality. In order to apply this second order concentration inequality, a sufficiently sharp bound on the variance of the unitarity randomized benchmarking random variable $q_{\mathbf{i_m}}$ was needed. This variance bound was derived in section 5.4, which lead to the main result of this chapter bounding the number of sequences in Theorem 5.2.1. A distinction was made between the single-copy implementation and two-copy implementation, yielding slightly different bounds. This was quantified by the parameters α and L in the main theorem. The difference between the two implementations are basically due to the difference in the operator bound of Lemma 5.4.8 for single-qubit systems and two-qubit systems. As a result, the bound on the number of sequences N differs slightly due to the constant factors α and L.

The most important conclusion of our result is that the variance bound goes to zero as the unitarity goes to one in the absence of state preparation and measurements. This means that if the a priori estimate of the unitarity u is already good and the state preparation and measurements are also good, that the number of sequences can be made very small. In this experimental limit, the unitarity randomized benchmarking protocol can be performed very efficiently. State preparation and measurement errors contribute a constant factor to the variance, effectively leading to a constant contribution to the number of sequences needed. An argument was presented that a constant contribution to the variance is the best achievable, since it was shown by example that even for perfect gates there is randomness present (leading to nonzero variance) in the presence of state preparation and measurement errors. An important question is how much state preparations and measurement errors contribute to the total number of sequences needed. This was illustrated by examples derived from experimental data on the quality of state preparation and measurement procedures in a particular qubit experiment. It showed that realistic errors still allowed the use of our result to reduce the number of sequences N significantly. It was argued that information on the description of the dominant error process in state preparation and measurement procedures help to obtain a more tight bound on the Hilbert-Schmidt norm of the relative state preparation and measurement errors that quantify those errors in our main result.

Altogether our work provides a method for unitarity randomized benchmarking protocol to be performed with more statistical rigor, in the case of benchmarking the single-qubit Clifford group assuming a gate and time independent error model. The number of sequences needed can in the regime of good control (i.e. good gates and good state preparation/measurements) can be significantly smaller than previously known results, bringing rigorous unitarity randomized benchmarking a step closer to experimental feasibility. Interesting follow up research could investigate if and how much the assumption of gate independent errors can be relaxed and how this affects the statistics of the protocol. Furthermore it is interesting to see if this result can be generalized to multi-qubit systems. As discussed in section 5.5, this requires a different approach than the one taken here, due to the explicit single-qubit character of the lemma's used in this proof.

REFERENCES

[1] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A* **52** no. 4, (1995) 2493–2496, arXiv:quant-ph/0506097.

[2] A. Y. Kitaev, "Quantum computations: algorithms and error correction," *Russ. Math. Surv.* **52** no. 6, (1997) 1191–1249.

[3] E. Knill, "Resilient Quantum Computation," *Science (80-.).* **279** no. 5349, (1998) 342–345, arXiv:quant-ph/9702058.

[4] D. Aharonov and M. Ben-Or, "Fault-Tolerant Quantum Computation With Constant Error Rate," *SIAM J. Comput.* **38** no. 4, (1999) 1207–1282, arXiv:quant-ph/9906129.

[5] J. Emerson, R. Alicki, and K. Zyczkowski, "Scalable noise estimation with random unitary operators," *J. Opt. B* **7** (2005) 347–352.

[6] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, "Randomized benchmarking of quantum gates," *Phys. Rev. A* **77** no. 1, (2008) 012307, arXiv:0707.0963.

[7] E. Magesan, J. M. Gambetta, and J. Emerson, "Scalable and robust randomized benchmarking of quantum processes," *Phys. Rev. Lett.* **106** no. 18, (2011) 180504, arXiv:1009.3639.

[8] E. Magesan, J. M. Gambetta, and J. Emerson, "Characterizing quantum gates via randomized benchmarking," *Phys. Rev. A* **85** no. 4, (2012) 042311, arXiv:1109.6887.

[9] R. Kueng, D. M. Long, A. C. Doherty, and S. T. Flammia, "Comparing Experiments to the Fault-Tolerance Threshold," *Phys. Rev. Lett.* **117** no. 17, (2016) 1–6, arXiv:1510.05653.

[10] T. Xia, M. Lichtman, K. Maller, A. W. Carr, M. J. Piotrowicz, L. Isenhower, and M. Saffman, "Randomized benchmarking of single-qubit gates in a 2D array of neutral-atom qubits," *Phys. Rev. Lett.* **114** no. 10, (2015) 1–5, arXiv:1501.02041.

[11] Y. R. Sanders, J. J. Wallman, and B. C. Sanders, "Bounding quantum gate error rate based on reported average fidelity," *New J. Phys.* **18** no. 1, (2016) 1–22, arXiv:1501.04932v2.

[12] J. J. Wallman, "Error rates in quantum circuits," *ArXiv e-prints* (2016) 1–11, arXiv:1511.00727v2.

[13] J. Wallman, C. Granade, R. Harper, and S. T. Flammia, "Estimating the coherence of noise," *New J. Phys.* **17** no. 11, (2015) 1–10, arXiv:1503.0786.

[14] S. Sheldon, L. S. Bishop, E. Magesan, S. Filipp, J. M. Chow, and J. M. Gambetta, "Characterizing errors on qubit operations via iterative randomized benchmarking," *Phys. Rev. A* **93** no. 1, (2016) 1–6, arXiv:1504.06597.

[15] J. J. Wallman and S. T. Flammia, "Randomized benchmarking with confidence," *New J. Phys.* **16** (2014) 1–31, arXiv:1404.6025.

[16] J. Helsen, J. J. Wallman, S. T. Flammia, and S. Wehner, "Multi-qubit Randomized Benchmarking Using Few Samples," *ArXiv e-prints* (2017) 1–39, arXiv:1701.04299.

[17] J. M. Farinholt, "An ideal characterization of the Clifford operators," *J. Phys. A* **47** no. 30, (2014) 305303, arXiv:1307.5087.

[18] M. Ozols, "Clifford Group," 2008. http://tinyurl.com/mzd3zh4.

[19] W. Hoeffding, "Probability Inequalities for Sums of Bounded Random Variables," *J. Am. Stat. Assoc.* **58** no. 301, (1963) 13–30.

[20] O. Burkinshaw and C. D. Aliprantis, *Principles of Real Analysis*. Academic Press, 3rd ed., 1998.

[21] J. Watrous, *The Theory of Quantum Information*. To be published by Cambridge University Press, 2017. http://tinyurl.com/mdmb66f.

[22] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge University Press, 2nd ed., 2013.

[23] M. A. Nielsen, "A simple formula for the average gate fidelity of a quantum dynamical operation," *Phys. Lett. Sect. A* **303** no. 4, (2002) 249–252, arXiv:quant-ph/0205035.

[24] D. S. Dummit and R. M. Foote, *Abstract Algebra*. John Wiley & Sons, 3rd ed., 2004.

[25] W. Fulton and J. Harris, *Representation Theory*. Springer, 2004.

[26] P. Etingof, O. Golberg, S. Hensel, T. Liu, A. Schwendner, D. Vaintrob, and E. Yudovina, *Introduction to Representation Theory*. American Mathematical Society, 2011.

[27] D. J. Griffiths, *Introduction to Quantum Mechanics*. Pearson Education, 2nd ed., 2005.

[28] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge University Press, 10th anniv ed., 2010.

[29] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics*. Cambridge University Press, 2nd ed., 2004.

[30] D. Pérez-García, M. M. Wolf, D. Petz, and M. B. Ruskai, "Contractivity of positive and trace-preserving maps under L P norms," *J. Math. Phys.* **47** no. 8, (2006) 083506, arXiv:math-ph/0601063.

[31] J. M. Gambetta, A. D. Córcoles, S. T. Merkel, B. R. Johnson, J. A. Smolin, J. M. Chow, C. A. Ryan, C. Rigetti, S. Poletto, T. A. Ohki, M. B. Ketchen, and M. Steffen, "Characterization of addressability by simultaneous randomized benchmarking," *Phys. Rev. Lett.* **109** no. 24, (2012) 240504, arXiv:1204.6308.

[32] M. Tinkham and G. Mckay, *Group Theory and Quantum Mechanics*. McGraw-Hill, 1964.

[33] D. Gottesman, "A Theory of Fault-Tolerant Quantum Computation," *Phys. Rev. A* **57** no. 1, (1997) 127–137, arXiv:quant-ph/9702029.

[34] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," in *Proc. IEEE Int. Symp. Inf. Theory*. 1997. arXiv:quant-ph/9608006.

[35] D. Gottesman, "The Heisenberg Representation of Quantum Computers," in *Proc. XXII Int. Colloq. Gr. Theor. Methods Phys.*, S. P. Corney, R. Delbourgo, and P. D. Jarvis, eds., pp. 32–43. International Press, Cambridge, MA, 1999. arXiv:quant-ph/9807006.

[36] J. Dehaene and B. De Moor, "Clifford group, stabilizer states, and linear and quadratic operations over GF(2)," *Phys. Rev. A* **68** no. 4, (2003) 042318, arXiv:quant-ph/0304125.

[37] C. M. Dawson and M. A. Nielsen, "The Solovay-Kitaev algorithm," *ArXiv e-prints* (2005) 1–15, arXiv:quant-ph/0505030.

[38] G. Nebe, E. M. Rains, and N. J. A. Sloane, "The Invariants of the Clifford Groups," *Des. Codes, Cryptogr.* **24** no. 1, (2001) 99–122, arXiv:math/0001038.

[39] H. Zhu, "Multiqubit Clifford groups are unitary 3-designs," *ArXiv e-prints* (2015) 1–6, arXiv:1510.02619.

[40] H. Zhu, R. Kueng, M. Grassl, and D. Gross, "The Clifford group fails gracefully to be a unitary 4-design," *ArXiv e-prints* (2016) 1–49, arXiv:1609.08172. http://arxiv.org/abs/1609.08172.

[41] J. Helsen, J. J. Wallman, and S. Wehner, "Representations of the multi-qubit Clifford group," *ArXiv e-prints* (2016) 1–14, arXiv:1609.08188.

[42] D. Gross, K. Audenaert, and J. Eisert, "Evenly distributed unitaries: On the structure of unitary designs," *J. Math. Phys.* **48** no. 5, (2007) 052104, arXiv:quant-ph/0611002.

[43] C. Dankert, R. Cleve, J. Emerson, and E. Livine, "Exact and approximate unitary 2-designs and their application to fidelity estimation," *Phys. Rev. A* **80** no. 1, (2009) 012304, arXiv:quant-ph/0606161.

[44] E. Magesan, J. M. Gambetta, B. R. Johnson, C. A. Ryan, J. M. Chow, S. T. Merkel, M. P. Da Silva, G. A. Keefe, M. B. Rothwell, T. A. Ohki, M. B. Ketchen, and M. Steffen, "Efficient measurement of quantum gate error by interleaved randomized benchmarking," *Phys. Rev. Lett.* **109** no. 8, (2012) 080505, arXiv:1203.4550.

[45] A. Carignan-Dugas, J. J. Wallman, and J. Emerson, "Efficiently characterizing the total error in quantum circuits," *ArXiv e-prints* (2016) 1–8, arXiv:1610.05296.

[46] S. Kimmel, M. P. da Silva, C. A. Ryan, B. R. Johnson, and T. Ohki, "Robust extraction of tomographic information via randomized benchmarking," *Phys. Rev. X* **4** no. 1, (2014) 011050, arXiv:1306.2348.

[47] M. A. Rol, C. C. Bultink, T. E. O'Brien, S. R. D. Jong, L. S. Theis, X. Fu, F. Luthi, R. F. L. Vermeulen, J. C. D. Sterke, A. Bruno, D. Deurloo, R. N. Schouten, F. K. Wilhelm, and L. Dicarlo, "Restless Tuneup of High-Fidelity Qubit Gates," *Phys. Rev. Appl.* **7** no. 4, (2017) 041001, arXiv:1611.04815.

[48] C. C. Bultink, M. A. Rol, T. E. O'Brien, X. Fu, B. C. S. Dikken, C. Dickel, R. F. L. Vermeulen, J. C. D. Sterke, A. Bruno, R. N. Schouten, and L. Dicarlo, "Active resonator reset in the nonlinear dispersive regime of circuit QED," *Phys. Rev. Appl.* **6** no. 3, (2016) 034008, arXiv:1604.00916.

[49] M. B. Ruskai, S. Szarek, and E. Werner, "An analysis of completely positive trace-preserving maps on M 2," *Linear Algebra Appl.* **347** (2002) 159–187, arXiv:quant-ph/0101003.

[50] C. King and M. B. Ruskai, "Minimal Entropy of States Emerging from Noisy Quantum Channels," *IEEE Trans. Inf. Theory* **47** no. 1, (2001) 192–209, arXiv:quant-ph/9911079.

[51] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

ACKNOWLEDGMENTS

This work would not have been possible without the excellent supervision of my direct mentor Jonas Helsen. The collaboration was very close and there were frequent discussions during each step of the way. The idea of analyzing unitarity randomized benchmarking was inspired by the analysis that he carried out for standard randomized benchmarking. The collaboration with my supervisors Stephanie Wehner and Wolter Groenevelt were also of critical importance to the success of this project. They always had time to discuss the progress of the research and give feedback on the next steps to be taken to continue to endeavor. In fact, all people in the Wehner group at QuTech provided a fruitful environment to develop this work, always being open to a discussion or a question. My thanks goes out to everyone with whom I had fruitful conversations over the last year.