A review of optimal cloning of pure quantum states

by

Sam van Poelgeest

to obtain the degree of Bachelor of Science
at the Delft University of Technology

Student number:	4573463	
Project duration:	September, 2018 – July, 2019	
Thesis committee:	Dr. B. Janssens,	TU Delft, supervisor
	Dr. D. Elkouss,	TU Delft, supervisor
	Dr. K. Vuik,	TU Delft
	Dr. M. Blaauboer,	TU Delft

Delft
University of
Technology

Abstract

In this project, quantum cloning machines are analyzed that take in N quantum systems in the same unknown pure state and output M quantum systems with $M > N$, such that the output best resembles the ideal, but impossible output of an M-fold tensor product of the pure input state. The proof of Keyl and Werner is reviewed in which a unique optimal solution is constructed, both in the case where the quality of the cloning is determined by the entire output, and in the case where the quality is determined by measurements on a single clone. Furthermore, it is shown that previous work on qubit cloning machines is a special case of the presented optimal solution.

Contents

1
Introduction

The invention of the digital computer in the 20th century was revolutionary. With its ever-growing processing power and storage capabilities, it enabled the scientific community to construct numerical models of the laws of physics that could be computed to incredible precision; it allowed us to land a man on the moon. However, with the advent of quantum mechanics, two hurdles appeared: firstly, our computer chips have steadily become more powerful whilst not growing in size, by shrinking the size of transistors, but this process has a limit. Once the electronics become small enough, the laws of quantum mechanics and its effects such as electron tunneling become apparent. Secondly, our classical computers are fundamentally ill-equipped to simulate quantum effects: Feynman pointed out in [Fey82] that the amount of processing power and storage capacity to simulate quantum systems grows exponentially with the size of the quantum system, thus rendering it unfeasible for a classical computer to simulate larger quantum systems.

However, the very quantum mechanics that appear to cause fundamental problems in computing technology also offer exciting solutions: the quantum computer, and quantum internet. Feynman first conjectured that a quantum computer might be capable of simulating quantum effects efficiently in [Fey82], and Lloyd proved that this is indeed the case in [Llo96]. Not only is the quantum computer efficient in simulating quantum mechanics, it can be more efficient in certain other tasks than the classical computer. An example of this is Shor's algorithm [Sho99], which allows one to perform prime factorization in polynomial time on a quantum computer, whilst the current fastest algorithm for a classical computer runs in sub-exponential time according to Lee and Venkatesan [LV18]. With recent developments such as IBM's *Q System One* and Google's *Bristlecone* quantum processor, progress is achieved towards commercially viable quantum computers.

Along with the development of quantum computers, the QuTech research centre, a collaboration between the Delft University of Technology and the Dutch Organisation for Applied Scientific Research (TNO), is also researching the possibilities of quantum networks, and has published a roadmap towards quantum internet: see [WEH18]. One of the promising features of such a network is secure communication: due to the unique phenomenon to quantum mechanics called *entanglement*, it is possible to construct communication channels such that eavesdropping becomes impossible – not just incredibly difficult, on which classical encryption is based, but strictly prohibited by the laws of quantum mechanics itself.

The technological effort to implement quantum mechanics rests on the fundamental research into quantum information: the possibilities and impossibilities of manipulating and communicating information using quantum mechanical devices. It is thus of great importance to investigate the laws and consequences of quantum theory. A range of theoretical and impossible tasks in quantum mechanics have been investigated: a teleportation device, cloning device, joint measurement device, and Bell's Telephone. These impossible devices have a hierarchy, in the sense that if one could construct a teleporation device, one could build a cloning device from this, and then a joint measurement device, and finally Bell's Telephone. As Bell's Telephone violates our principle of causality, this chain is reversed in a set of no-go theorems: none of these machines are possible in quantum mechanics, see for example [ABH+03, Chapter 2, page 14].

The cloning machine is a particularly interesting impossible machine. If we were capable of cloning perfectly, surely the scientific landscapes of quantum error correction and quantum encryption would look completely differently. As Bužek and Hillery described it in [BH98]:

> "*The most fundamental difference between classical and quantum information is that while classical information can be copied perfectly, quantum information cannot.*"

It was first proven by Wootters and Zurek that it is impossible to construct such a device that can clone an *arbitrary* qubit perfectly [WZ82]. Given the fact that we cannot clone perfectly, naturally the question arises *how well* we can perform cloning, and whether this cloning capability increases when we restrict ourselves to a smaller set of possible qubits. For example, Bužek and Hillery looked into building a universal quantum copying machine that takes in a qubit and produces two qubits, with the interesting property that the machine has a performance independent of the state of the input qubit [BH96]. On top of that, they looked into copying qubits in the case that the input qubits are all close to a pre-defined state. Extending the problem to N input qubits and M output qubits (with $M > N$), Gisin and Massar looked at optimal cloning devices, where they tested optimality by looking at *one* of the output clones [GM97].

Not much later did Werner publish an article in which he presented an optimal cloning device that takes in N quantum states and produces M quantum states (with $M > N$), where the states were no longer restricted to the qubit case, but instead to states on any finite-dimensional Hilbert space [Wer98]. The measure of optimality looked at the performance of *all* clones, and a year later Keyl and Werner published an article in which the same cloning device was proven to be optimal with respect to the performance of *one* of the output clones [KW99].

In this thesis, the problem of quantum cloning is analysed along the lines of the argument presented in [Wer98] and [KW99]. The aim of this thesis is to review the proof of optimal cloning presented by Keyl and Werner, and to juxtapose the differences between testing for optimality by considering the performance of *all* clones and by considerig the performance of *one* clone. It further describes the underlying symmetries of this problem, which play a powerful role and were already mentioned by Gisin and Massar in their conclusion [GM97]. Lastly, it connects the work of Bužek and Hillery [BH96] on cloning one qubit to two qubits with the work of Werner, indeed showing that the proposed cloning map of Bužek and Hillery is in fact identical to the one first proposed by Werner.

In **Chapter** 2, all necessary mathematical and physical concepts are introduced. Although the reader is invited to read through these tools, it is not necessary to closely study them: whenever the theory from this chapter is necessary, the relevant theory will be referenced in the paper.

In **Chapter** 3, the No-Cloning Theorem is stated and a proof is provided. In this chapter, an intuitive connection to the figures of merit that will be used to test the copying devices is also provided.

In **Chapter** 4, the quantum copying problem is fully specified, and the figures of merit that will determine the performance of a cloning device are introduced. Furthermore, a description of the optimal cloning map is provided.

In **Chapter** 5, the underlying symmetries of the problem are fully analysed.

In **Chapter** 6, the optimal cloning map itself is studied: firstly, it is proven that the cloning map is in fact an admissible quantum operation, secondly the symmetries of Chapter 5 are connected to the cloning device, and thirdly the performance of the cloning map with respect to the figures of merit is calculated.

In **Chapter** 7, the optimality of the proposed cloning map is proven.

In **Chapter** 8, the input system is restricted to one qubit, and the output system restricted to two qubits. The optimal cloning device of Keyl and Werner [KW99] is then compared to a cloning device that copies orthogonal states perfectly (the "Wootters-Zurek quantum-copying machine", as Bužek and Hillery [BH96] call it), and it is proven that the universal quantum copying machine proposed by Bužek and Hillery is indeed a special instance of the optimal cloning device of Keyl and Werner.

Lastly, a conclusion and discussion is provided in the **Conclusion** 9.

2

Description of necessary mathematical tools

Before proceeding in our enquiry into optimal quantum cloning, it is imperative to discuss the mathematical tools and spaces that will be used intensively throughout this paper.

2.1. On quantum mechanics

Let us first build the quantum mechanical framework in which this research takes place. To be complete, we first take a look at *closed* quantum mechanical systems (that is, systems that are perfectly insulated from their environment), and then naturally extend these notions to a more suitable framework for *open* systems.

2.1.1. Quantum mechanics of a closed system

We will consider quantum systems that are modelled by finite-dimensional complex Hilbert spaces. Hence, let us commence from this viewpoint:

Definition 2.1.1 (Hilbert space). [Dri03] A complex Hilbert space is a complex inner product (vector) space $(\mathcal{H}, \langle \cdot, \cdot \rangle)$ such that the Hilbertian norm $\|x\| := \sqrt{\langle x, x \rangle}$ is complete.

A quantum state of a quantum system is modelled by a ray $\mathbb{C}\psi$ in $\mathcal{H}$, which we normalize to unit length. Thus, the vectors $\psi, \psi' \in \mathcal{H}$ with unit length represent the same quantum state if and only if there exists a $\theta \in [0, 2\pi)$ such that $\psi = e^{i\theta}\psi'$. We will often use the Dirac bra-ket notation, in which vectors are denoted by $| \cdot \rangle \in \mathcal{H}$, where $\cdot$ can be any symbol (or string) to label the state. This is convenient notation, as linear functionals (row vectors, if a basis is chosen) can be denoted by $\langle \cdot | \in \mathcal{H}^*$, such that inner products are written as $\langle \cdot | \cdot \rangle$.

In order to manipulate quantum states, we need a notion of the dynamics of a quantum system. Let us introduce:

Definition 2.1.2 (Operator on $\mathcal{H}$). An operator on $\mathcal{H}$ is a linear map $A : \mathcal{H} \to \mathcal{H}$

In the general case of a (not necessarily finite-dimensional) Hilbert space $\mathcal{H}$, operators on $\mathcal{H}$ *may* be unbounded, that is, there may not exist a $c \geq 0$ such that $\|A\psi\| \leq c\|\psi\|$ for all $\psi \in \mathcal{H}$. However, in the finite-dimensional case, *all* operators are bounded (see for example [Lan17, A.6]). Thus, in our finite-dimensional case, the algebra of all operators on $\mathcal{H}$ coincides with the algebra of all *bounded* operators on $\mathcal{H}$, which we will denote by $\mathcal{B}(\mathcal{H})$.

Quantum systems that are closed to (i.e. have no interaction with) the outside world are transformed by unitary operators on $\mathcal{H}$. The *observables* of a quantum system are self-adjoint operators on $\mathcal{H}$:

Definition 2.1.3 (Adjoint operator on $\mathcal{H}$). Let $A \in \mathcal{B}(\mathcal{H})$. The **adjoint** operator A^* is defined by the equation

$$\langle A^*\phi \ , \ \psi \rangle = \langle \phi \ , \ A\psi \rangle \qquad \forall \phi \ , \ \psi \in \mathcal{H} \tag{2.1}$$

In our finite-dimensional case, the matrix representation of A^* can be obtained by choosing a basis of $\mathcal{H}$, and taking the conjugate transpose of the matrix representation of A.

Definition 2.1.4 (Self-adjoint operator on $\mathcal{H}$). An operator A on $\mathcal{H}$ is called **self-adjoint** if $A^* = A$.

Lastly, let us introduce positive operators, which we will need shortly:

Definition 2.1.5 (Positive operators on $\mathcal{H}$). Let $A \in \mathcal{B}(\mathcal{H})$. Then A is said to be positive if $\forall \psi \in \mathcal{H}$: $\langle \psi, A\psi \rangle \geq 0$.

We will sometimes choose to write $A \geq 0$ to indicate that A is a positive operator, and also $A \geq B$ if $A - B \geq 0$, that is, the operator $A - B$ is positive. Note that any positive operator on $\mathcal{H}$ is also self-adjoint, see for example [Fas11, Ch. 2].

So far, we have seen the states ψ of a quantum system $\mathcal{H}$, which are transformed (if the system is closed) by unitary operators U on $\mathcal{H}$, and whose observables are self-adjoint operators on $\mathcal{H}$. However, we have not yet considered interactions between quantum systems (as we have so far considered a *closed* quantum system). We now wish to broaden this picture to include so-called *mixed* states, as opposed to the states that we have defined so far, the so-called *pure* states, and we need to develop methods to consider the coupling of multiple quantum *subsystems* into larger quantum systems. The key to this is the introduction of density matrices.

2.1.2. Quantum mechanics of an open system

Previously, we modelled states (which we will now call *pure* states) as vectors $\psi \in \mathcal{H}$ (up to a phase factor) with $\|\psi\| = 1$. Along with a state comes a linear functional $f_\psi : \mathcal{B}(\mathcal{H}) \to \mathbb{C}$, with $f_\psi(A) = \langle \psi, A\psi \rangle$ for any $A \in \mathcal{B}(\mathcal{H})$. This map assigns to each observable its expectation value and linearly extends to all of $\mathcal{B}(\mathcal{H})$. This is well-defined, because if ψ and ψ' describe the same quantum state, there exists a $\theta \in [0, 2\pi)$ such that $\psi = e^{i\theta}\psi'$, and the complex phase factor drops out such that $\langle \psi, A\psi \rangle = \langle \psi', A\psi' \rangle$. Conversely, according to [Jan10, p.7], if $f_\psi = f_{\psi'}$, then $\psi = c\psi'$ for some $0 \neq c \in \mathbb{C}$, and by our constraint that both have unit length, this means that $\psi = e^{i\theta}\psi'$ for some $\theta \in [0, 2\pi)$, which represent the *same* quantum state. Thus, we could equivalently use these linear functionals to describe pure quantum states.

Note that f_ψ is linear, positive in the sense that $A \geq 0 \implies f_\psi(A) \geq 0$, and normalized in the sense that $f_\psi(\mathrm{Id}_\mathcal{H}) = 1$ as we chose $\|\psi\| = 1$. We can now naturally extend our notion of (pure) states to *any* linear, positive, normalized functional $f : \mathcal{B}(\mathcal{H}) \to \mathbb{C}$. According to [Jan10, p.16], for each such an f we can find a unique positive operator ρ on $\mathcal{H}$ with $\mathrm{Tr}\,[\rho] = 1$ such that

$$f(A) = \mathrm{Tr}\,[\rho A] \qquad \forall A \in \mathcal{B}(\mathcal{H}) \tag{2.2}$$

We call ρ the **density matrix**.

Definition 2.1.6 (Density matrix on $\mathcal{H}$). A positive operator ρ on $\mathcal{H}$ is called a density matrix if it has $\mathrm{Tr}[\rho] = 1$. In the case we have a pure state $|\psi\rangle \in \mathcal{H}$ (up to a phase factor), the density matrix is given by $\rho = |\psi\rangle \langle\psi|$. In the case we have a mixed state,

$$\rho = \sum_i p_i \, |\psi_i\rangle \langle\psi_i| \tag{2.3}$$

where the system has probability p_i to be in state $|\psi_i\rangle$, and thus we have $\sum_i p_i = 1$ and all $p_i \geq 0$.

The space of all density matrices will be denoted by $\mathcal{S}(\mathcal{H}) \subseteq \mathcal{B}(\mathcal{H})$.

Although we now have a more general way to describe both pure and mixed states on $\mathcal{H}$, we have not yet provided a way in which different quantum systems can interact with one another. In order to do so, we first describe how one can bring together multiple quantum systems and view them as *subsystems* of a larger quantum system by using tensor products, and then we will describe operations between quantum systems.

Let us commence with defining tensor products; we offer two equivalent definitions.

Definition 2.1.7 (Tensor product). [Fre12] Let V and W be vector spaces over a field $\mathbb{F}$. Let $F(V,W)$ denote the vector space of all linear combinations of points (v,w) with coefficients in $\mathbb{F}$, i.e. functions $V \times W \to \mathbb{F}$ vanishing at all but finitely many ordered pairs. Let $R(V,W)$ be the subspace spanned by all elements of the form:

$$\lambda(v,w) - (\lambda v, w) \quad ; \quad \lambda(v,w) - (v, \lambda w) \tag{2.4}$$

$$(v, w_1 + w_2) - (v, w_1) - (v, w_2) \quad ; \quad (v_1 + v_2, w) - (v_1, w) - (v_2, w) \tag{2.5}$$

for all $\lambda \in \mathbb{F}$, $v, v_1, v_2 \in V$ and $w, w_1, w_2 \in W$. We define the tensor product space $V \otimes W := F(V,W)/R(V,W)$ as the quotient space, such that we have the structure

$$(\lambda v_1 + v_2) \otimes w = \lambda(v_1 \otimes w) + v_2 \otimes w \quad ; \quad v \otimes (\lambda w_1 + w_2) = \lambda(v \otimes w_1) + v \otimes w_2 \tag{2.6}$$

for all $v_1, v_2, v \in V$, $w_1, w_2, w \in W$ and $\lambda \in \mathbb{F}$.

Definition 2.1.8 (Tensor product). [FH04] The tensor product of two vector spaces V and W over a field is a vector space $V \otimes W$ equipped with a bilinear map $\phi : V \times W \to V \otimes W$, $v \times w \mapsto v \otimes w$, which is **universal**: for any bilinear map $\beta : V \times W \to U$ to a vector space U, there exists a unique linear map $\tilde{\beta} : V \otimes W \to U$ such that $v \otimes w$ is mapped to $\beta(v,w)$.

Thus:

$$\begin{tikzcd} V \times W \arrow[r, "\phi"] \arrow[dr, "\beta"] & V \otimes W \arrow[d, "\tilde{\beta}"] \\ & U \end{tikzcd}$$

As $U \otimes (V \otimes W) \cong (U \otimes V) \otimes W$, we can safely write $U \otimes V \otimes W$ for any three vector space U, V, W. We will often discuss n-times tensor product Hilbert spaces, i.e.

$$\mathcal{H}^{\otimes n} := \underbrace{\mathcal{H} \otimes \mathcal{H} \otimes \cdots \otimes \mathcal{H}}_{n} \tag{2.7}$$

When we bring quantum systems $\mathcal{H}_1$ and $\mathcal{H}_2$ together, and view the new system as $\mathcal{H}_1 \otimes \mathcal{H}_2$, we need to be able to understand how operators work on this new space:

Definition 2.1.9 (Tensor product of operators). Given two vector spaces V and W, and their tensor product $V \otimes W$. Consider an operator A on V and an operator B on W. We define the operator $A \otimes B : V \otimes W \to V \otimes W$ by:

$$(A \otimes B)\left(\sum_i \alpha_i v_i \otimes w_i\right) = \sum_i \alpha_i A(v_i) \otimes B(w_i) \qquad \forall v_i \in V \ , \ \forall w_i \in W \ , \ \forall \alpha_i \in \mathbb{C} \tag{2.8}$$

When we wish to describe a combination of quantum systems through density operators, we can now construct a natural way of discussing the entire quantum system by tensor products of density operators.

In order to do so, note that for Hilbert spaces $(\mathcal{H}_1, \langle \cdot, \cdot \rangle_1)$ and $(\mathcal{H}_2, \langle \cdot, \cdot \rangle_2)$, we can construct $\mathcal{H}_1 \otimes \mathcal{H}_2$, which is again a Hilbert space with respect to the inner product defined by:

$$\left\langle \sum_i \alpha_i v_i \otimes w_i \ , \ \sum_j \beta_j v'_j \otimes w'_j \right\rangle = \sum_i \sum_j \langle \alpha_i v_i \ , \ \beta_j v'_j \rangle_1 \cdot \langle w_i \ , \ w'_j \rangle_2 \tag{2.9}$$

where $v_i, v'_j \in V$, $w_i, w'_j \in W$ and $\alpha_i, \beta_j \in \mathbb{C}$. Note that, as both $\langle \cdot, \cdot \rangle_1$ and $\langle \cdot, \cdot \rangle_2$ are inner products, the distribution of scalars on the right-hand side is arbitrary. We left the scalars inside the inner product on purpose; this makes the definition independent of the choice of which argument has conjugate linearity and which has linearity in the sesquilinear inner products.

Proposition 2.1.10. *Given Hilbert spaces* $(\mathcal{H}_1, \langle\cdot,\cdot\rangle_1)$ *and* $(\mathcal{H}_2, \langle\cdot,\cdot\rangle_2)$ *and density operators* $\rho \in S(\mathcal{H}_1)$ *and* $\sigma \in S(\mathcal{H}_2)$ *. Then* $\sigma \otimes \rho$ *is again a density matrix on the tensor Hilbert space* $\mathcal{H}_1 \otimes \mathcal{H}_2$*.*

Proof. Note that $(\rho \otimes \sigma)^* = \rho^* \otimes \sigma^* = \rho \otimes \sigma$, thus $\rho \otimes \sigma$ is self-adjoint. We prove that $\rho \otimes \sigma$ is positive, and has trace unity. For positivity, note that all eigenvalues of $\rho \otimes \sigma$ are precisely of the form $\lambda_i \mu_j$, where λ_i is an eigenvalue of ρ and μ_j an eigenvalue of σ, see for example [Sch13, p.9]. Because both ρ and σ are positive Hermitian operators, all their eigenvalues are nonnegative. As $\rho \otimes \sigma$ is Hermitian, and all eigenvalues are of the form $\lambda_i \mu_k \geq 0$, we conclude that $\rho \otimes \sigma$ is positive.

For trace unity, we can directly calculate, using the fact that

$$\{e_i \otimes f_j \in \mathcal{H}_1 \otimes \mathcal{H}_2 \quad ; \quad i \in \{1, \dots, d_1\}, j \in \{1, \dots, d_2\}\} \qquad ; \qquad d_i = \dim \mathcal{H}_i \tag{2.10}$$

is a basis for $\mathcal{H}_1 \otimes \mathcal{H}_2$ if $\{e_i\}$ and $\{f_j\}$ are bases for $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Thus:

$$\mathrm{Tr}\,(\rho \otimes \sigma) = \sum_{i=1}^{d_1} \sum_{j=1}^{d_2} \langle e_i \otimes f_j \ , \ (\rho \otimes \sigma)(e_i \otimes f_j)\rangle = \sum_{i=1}^{d_1} \sum_{j=1}^{d_2} \langle e_i \ , \ \rho(e_i)\rangle_1 \cdot \langle f_j \ , \ \sigma(f_j)\rangle_2 = \tag{2.11}$$

$$\sum_{i=1}^{d_1} \langle e_i \ , \ \rho(e_i)\rangle_1 \cdot \sum_{j=1}^{d_2} \langle f_j \ , \ \sigma(f_j)\rangle_2 = \mathrm{Tr}(\rho) \cdot \mathrm{Tr}(\sigma) = 1 \tag{2.12}$$

□

Thus indeed, our descriptions of $\mathcal{H}_1, \mathcal{H}_2$ with density matrices ρ and σ respectively, naturally extends to the description of $\mathcal{H}_1 \otimes \mathcal{H}_2$ by density matrices $\rho \otimes \sigma$.

We have now developed ways to join quantum systems through tensor products, and are capable of operating on these new spaces. The last key element is to build a framework that allows us to describe all possible quantum operations, which should thus include operators on quantum systems, but also bringing quantum systems into contact (through tensor products), and "forgetting" about a part of a system, i.e. never interacting with this subsystem [1]. To develop the framework of quantum operations, we will discuss the formalisms of the so-called **Schrödinger picture** and the **Heisenberg picture**. Roughly speaking, in the Schrödinger picture we will transform states (equivalently, density operators), whilst the observables remain fixed, whilst in the Heisenberg picture we will transform observables while the states remain fixed. Throughout this article, both pictures are used interchangeably, thus it is important to specify both. Both pictures are used in literature, for example Nielsen and Chuang [NC01] prefers the Schrödinger picture, whilst Maassen [Maa04] frequently works with the Heisenberg picture. According to [Maa04, p.35], any quantum operation should be an affine map by the *stochastic equivalence principle*: a system in state σ_1 with probability p_1 and in state σ_2 with probability $p_2 = 1 - p_1$ cannot be distinguished from a system in the state $p_1\sigma_1 + (1 - p_1)\sigma_2$. Any such map can be uniquely extended to a linear map, and thus we assume from now on that any quantum operation must be linear.

In both the Schrödinger and the Heisenberg picture, we are interested in operations that act on bounded operators (be it density matrices in the Schrödinger picture, or observables in the Heisenberg picture), and thus it is useful to first introduce which subsets of *all* bounded operators $\mathcal{B}(\mathcal{H})$ we can look at: these are the unital $*$-algebras.

Definition 2.1.11 (**$*$-algebra**)**.** [Maa04, p.24] A (unital) $*$-algebra of operators on a Hilbert space $\mathcal{H}$ is a subspace $\mathcal{A} \subseteq \mathcal{B}(\mathcal{H})$ such that $\mathrm{Id}_{\mathcal{H}} \in \mathcal{A}$ and

$$A, B \in \mathcal{A} \implies \lambda A \ , \ A + B \ , \ A \cdot B \ , \ A^* \in \mathcal{A} \quad \forall \lambda \in \mathbb{C} \tag{2.13}$$

Before specifying the differences between the Schrödinger and the Heisenberg picture, we can introduce the general concept of positivity and complete positivity.

Definition 2.1.12 (**Positivity of a quantum operation**)**.** Consider a linear map $T : \mathcal{A} \to \mathcal{B}$, where $\mathcal{A} \subseteq \mathcal{B}(\mathcal{H}_1)$ and $\mathcal{B} \subseteq \mathcal{B}(\mathcal{H}_2)$ are $*$-algebras of operators on Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$. Then T is called **positive** if for all *positive* $A \in \mathcal{A}$, $T(A)$ is also positive.

[1] Remarkably, *all* quantum operations can be written as the composition of tensoring on another quantum system, letting a unitary operator act on the product space, and then taking a partial trace ("forgetting" about a subsystem). This is called Stinespring's dilation theorem, see for example [NC01, p.358]

When the system we are interested in is combined with another system, we could consider a transformation on our subsystem as a transformation on the entire system, where it acts as the identity on the other subsystem (i.e. leaves this system unchanged). We wish for our transformation to be positivity-preserving, and this quality must actually hold when we view it our system as a subsystem of a larger quantum system. This is not automatically guaranteed due to quantum entanglement, for an example of a positive, but not completely positive map, see [Maa04, p.36]. We define:

Definition 2.1.13 (Complete positivity). Consider a linear map $T : \mathcal{A} \to \mathcal{B}$, where $\mathcal{A} \subseteq \mathcal{B}(\mathcal{H}_1)$ and $\mathcal{B} \subseteq \mathcal{B}(\mathcal{H}_2)$ are $*$-algebras of operators on Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$. Then T is called **completely positive** if $\forall n \in \mathbb{Z}_{>0}$, the map $\mathrm{Id}_n \otimes T : M_n \otimes \mathcal{A} \to M_n \otimes \mathcal{B}$ is positive, where M_n denotes the unital $*$-algebra of all $n \times n$ matrices with complex entries.

Quantum operations: the Schrödinger picture

In the Schrödinger picture, we look at the transformations of quantum states. See for example [NC01, Section 8.2, p. 356]. The allowed transformations are linear maps that are completely positive and trace preserving, sometimes abbreviated to CPTP maps:

Definition 2.1.14 (Quantum operation (Schrödinger)). A linear map $T_* : \mathcal{A} \to \mathcal{B}$, where $\mathcal{A} \subseteq \mathcal{B}(\mathcal{H}_1)$ and $\mathcal{B} \subseteq \mathcal{B}(\mathcal{H}_2)$ are unital $*$-algebras of operators on Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, is called a quantum operation if it is a completely positive, trace preserving (CPTP) map: that is,

- It is **trace preservering (TP)**: for all $\rho \in \mathcal{A}$ we have $\quad \mathrm{Tr}\left[T_*(\rho)\right] = \mathrm{Tr}\left[\rho\right] \quad$, where both $\mathcal{A}$ and $\mathcal{B}$ inherit the trace functional from $\mathcal{B}(\mathcal{H}_1)$ and $\mathcal{B}(\mathcal{H}_2)$, respectively.
- It is **completely positive (CP)**: for all $n \in \mathbb{Z}_{>0}$, the map $\quad \mathrm{Id}_n \otimes T_* \quad$ is a positive operation.

Note that the requirement on T_* to be (linear and) CPTP precisely means that states (in our case, density matrices) are mapped to states. We will often be sloppy, and write $T_* : \mathcal{S}(\mathcal{H}_1) \to \mathcal{S}(\mathcal{H}_2)$ to signify that we are only interested in what T_* does to *states*, whilst technically $\mathcal{S}(\mathcal{H})$ is not a unital $*$-algebras (for example, the sum of two states has trace 2). However, using the linearity of T_*, and the fact that *any* operator on a Hilbert space $\mathcal{H}$ can be written as the (complex) linear combination of at most 4 states on $\mathcal{H}$, such a map uniquely extends to a map $\mathcal{B}(\mathcal{H}_1) \to \mathcal{B}(\mathcal{H}_2)$ (in Appendix A.6.1, we decompose general operators into the linear combination of four positive operators, and by choosing the right normalization per operator one would indeed find four states. See also [Maa04, p.36]).

Quantum operations: the Heisenberg picture

In the Heisenberg picture, we look at the transformation of observables. See for example [Maa04, Sec. 4.4, p. 36]. The allowed transformations are linear maps that are completely positive and unital:

Definition 2.1.15 (Quantum operation (Heisenberg)). A linear map $T : \mathcal{B} \to \mathcal{A}$, where $\mathcal{A} \subseteq \mathcal{B}(\mathcal{H}_1)$ and $\mathcal{B} \subseteq \mathcal{B}(\mathcal{H}_2)$ are unital $*$-algebras of operators on Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, is called a quantum operation if it is a completely positive, unital map: that is,

- It is **unital**: $\quad T\left(\mathrm{Id}_{\mathcal{B}}\right) = \mathrm{Id}_{\mathcal{A}}$
- It is **completely positive**: for all $n \in \mathbb{Z}_{>0}$, the map $\quad \mathrm{Id}_n \otimes T \quad$ is a positive operation.

Connection between the two pictures

As these two formalisms should describe the same quantum mechanics, these quantum operations must be each other's adjoint, that is: for each quantum operation T in the Heisenberg picture, there is a dual quantum operation T_* in the Schrödinger picture, such that the expectation value of observable A with respect to $T_*(\rho)$ for any density matrix ρ must be the same as the expectation value of observable $T(A)$ with respect to ρ. Thus, we have:

$$\mathrm{Tr}\left[\rho\; T(A)\right] = \mathrm{Tr}\left[T_*(\rho)\; A\right] \tag{2.14}$$

2.2. On group theory, Lie theory and representation theory

Throughout the enquiry into the optimal cloning map, we will need a group theoretic framework to find symmetries in our problem: for example, it will become apparent that an optimal cloning map must be permutation invariant. The set of permutations forms a *group*, and it must act on our quantum systems through a *representation*. To this end, we need to introduce theory with regard to groups, Lie groups and Lie algebras, and representations of groups. Let us start with group theory.

2.2.1. Group theory

A *group* is defined by:

Definition 2.2.1 (Group). A group is a set G together with an **associative** operation $\circ : G \times G \to G$, such that G is closed under the operation, G contains an identity element e such that $g \circ e = e \circ g = g$ for all $g \in G$, and for each $g \in G$, there exists an element $g^{-1} \in G$ such that $g \circ g^{-1} = g^{-1} \circ g = e$.

Example 2.2.2. *An important example for us is the unitary group $U(d)$, which is the set of $d \times d$ unitary matrices with matrix multiplication as group operation, and the special unitary group $SU(d) \subset U(d)$ which contains all $d \times d$ unitary matrices with determinant 1.*

Example 2.2.3. *Another example that plays a key role in this paper is the symmetric group $\mathfrak{S}_n$ for some $n \in \mathbb{Z}_{>0}$, which is the set of all bijections $\{1, \ldots, n\} \to \{1, \ldots, n\}$, which are typically called **permutations**, together with the function composition $\circ$ as group operation.*

2.2.2. Lie theory

If the group G is also a smooth manifold, i.e. the product and inverse operations are smooth functions on G, then G is a Lie group. Luckily, we can characterise the Lie groups that are of interest in this paper in another way: these Lie groups are *matrix* Lie groups. Through the closed-subgroup theorem (Cartan's theorem), we can identify these matrix Lie groups, which we will adopt as a definition in this paper:

Definition 2.2.4 (Matrix Lie group). [Hal15, p.4] Any closed subgroup of $\mathrm{GL}(n, \mathbb{R})$ is a matrix Lie group

Now, we are ready to define Lie algebras. First, let us discuss the abstract definition of a Lie algebra, and afterwards we will connect Lie algebras to their respective Lie groups.

Definition 2.2.5 (Lie algebra). [KS09, p.47] A Lie algebra $\mathfrak{a}$ over a field $\mathbb{K}$ is a finite- or infinite-dimensional $\mathbb{K}$-vector space with a $\mathbb{K}$-bilinear, antisymmetric operation $[\cdot, \cdot] : \mathfrak{a} \times \mathfrak{a} \to \mathfrak{a}$ satisfying the Jacobi identity

$$[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0 \qquad \forall X, Y, Z \in \mathfrak{a} \tag{2.15}$$

We call the bilinear operation $[\cdot, \cdot]$ the Lie bracket.

Example 2.2.6. *[KS09, p.48] An important example for us is the vector space of $n \times n$ matrices with coefficients in the field $\mathbb{K}$, with the matrix commutator as the Lie bracket, which is denoted as $\mathfrak{gl}(n, \mathbb{K})$. So:*

$$[X, Y] = XY - YX \in \mathfrak{gl}(n, \mathbb{K}) \qquad \forall X, Y \in \mathfrak{gl}(n, \mathbb{K}) \tag{2.16}$$

Before we can connect the Lie algebra to a Lie group, we need a quick review of the exponential map

Definition 2.2.7 (Exponential map). [KS09, p.51] Let $X \in \mathfrak{gl}(n, \mathbb{K})$. We define

$$\exp X := e^X := \sum_{p=0}^{\infty} \frac{X^p}{p!} \tag{2.17}$$

As we have $\exp(-X) = (\exp X)^{-1}$, for each X, $\exp X$ is invertible, and thus $\exp : \mathfrak{gl}(n, \mathbb{K}) \to \mathrm{GL}(n, \mathbb{K}) \subset \mathfrak{g}(n, \mathbb{K})$. Further note that the map $\mathbb{R} \ni t \mapsto \exp(tX)$ is differentiable and its derivative is equal to $\exp(tX)X$. We can now connect the idea of Lie groups with their respective Lie algebras: a Lie algebra is a vector space that is tangent to the identity element:

Theorem 2.2.8. *[KS09, p.56] Let G be a matrix Lie group, and consider*

$$\mathfrak{g} := \left\{ X = \gamma'(0) \mid \gamma : \mathcal{I} \to G \ , \quad \textit{of class } C^1 \ , \ \gamma(0) = I \right\} \tag{2.18}$$

where $\mathcal{I}$ is an open interval of $\mathbb{R}$ containing 0. We then have

1. *$\mathfrak{g}$ is a vector subspace of $\mathfrak{gl}(n, \mathbb{R})$*

2. $X \in \mathfrak{g} \Longleftrightarrow \forall t \in \mathbb{R} \ : \ \exp(tX) \in G$
3. *If* $X \in \mathfrak{g}$ *and* $g \in G$*, then* $gXg^{-1} \in \mathfrak{g}$
4. $\mathfrak{g}$ *is closed under the matrix commutator*

We call $\mathfrak{g}$ *the* Lie algebra of the Lie group G.

2.2.3. Representation theory

The relevant representation theory for this paper can be divided into two parts: firstly, we will need to consider representations of the symmetric group $\mathfrak{S}_n$, which is a finite group (in fact, it has $n!$ elements). Secondly, we will also need representations of the (special) unitary group $\mathrm{U}(n)$ $(\mathrm{SU}(n))$, which is an infinite but compact group. The following definitions and theorems can be found in [KS09].

Definition 2.2.9 (Representation of a finite group). [KS09, p.9] A representation of a finite group G is a finite-dimensional complex vector space E along with a group morphism $\pi : G \to \mathrm{GL}(E)$. Thus, for every group element $g \in G$, $\pi(g)$ is some invertible linear operator in $\mathrm{GL}(E)$, and π respects group operations:

$$\pi(gg') = \pi(g)\pi(g') \qquad , \qquad \pi(g^{-1}) = (\pi(g))^{-1} \qquad , \qquad \pi(e) = \mathrm{Id}_E \tag{2.19}$$

In a more general case, we can find representations of (infinite) compact groups:

Definition 2.2.10 (Representation of a compact group). [KS09, p.36] Let G be a topological group. A **continuous representation** or simply a representation of G is defined as a Hilbert space E and a group morphism $\pi : G \to \mathrm{GL}(E)$ such that $\forall x \in E$, $G \ni g \mapsto \pi(g)x \in E$ is a continuous mapping.

Definition 2.2.11 (Unitary representation of finite/compact groups). [KS09, p.10] A representation (E, π) is unitary if there is a scalar product $\langle \cdot \ , \ \cdot \rangle$ on E such that

$$\langle \pi(g)x \ , \ \pi(g)y \rangle = \langle x \ , \ y \rangle \qquad \forall g \in G \ , \ \forall x, y \in E \tag{2.20}$$

Theorem 2.2.12. *[KS09, p.39] Every representation of a finite or compact group is unitarizable*

Certain representations can be decomposed into "smaller" representations, i.e. representations on vector subspaces. Let us define:

Definition 2.2.13 (Subrepresentations). Let (E, π) be a representation of a group G. We say that the vector subspace F is **invariant** under π if:

$$\pi(g)f \in F \qquad \forall g \in G \ , \ \forall f \in F \tag{2.21}$$

This is often denoted by $\forall g \in G : \pi(g)F \subset F$. Then, we can restrict the representation π to the vector subspace F, which we will denote by $\pi|_F$. We then say that $(F, \pi|_F)$ is a **subrepresentation** of (E, π).

Definition 2.2.14 (Irreducible representation). [KS09, p.11] A representation (E, π) is called irreducible if $E \neq \{0\}$ and if the only vector subspaces of E that are invariant under π are $\{0\}$ and E itself. Equivalently, we could say that (E, π) has no *proper subrepresentations*

Definition 2.2.15 (Completely reducible representation). [KS09, p.11] A representation (E, π) of a group G is called completely reducible if it is a direct sum of irreducible representations. With a *direct sum* of the representations (E_1, π_1) and (E_2, π_2) of a group G we mean $(E_1 \oplus E_2, \pi_1 \oplus \pi_2)$ where

$$(\pi_1 \oplus \pi_2)(g)(x_1, x_2) = (\pi_1(g)x_1, \pi_2(g)x_2) \qquad \forall g \in G \ , \ x_1 \in E_1 \ , \ x_2 \in E_2 \tag{2.22}$$

In the compact case, we replace the direct sum by the Hilbert direct sum.

Theorem 2.2.16 (Maschke's Theorem). *[KS09, p.12] Every finite-dimensional representation of a finite group or compact group is completely reducible.*

One important concept in this paper is the commutative behaviour of certain maps with representations. In this case, we build towards Schur's lemma. Firstly, we introduce:

Definition 2.2.17 (Intertwining operator). [KS09, p.12] Let (E_1, π_1) and (E_2, π_2) be unitary representations of a group G. We say that a linear map $T : E_1 \to E_2$ intertwines π_1 and π_2 if

$$\pi_2(g) \circ T = T \circ \pi_1(g) \qquad \forall g \in G \tag{2.23}$$

Intertwiners are also called G-morphism, or $T \in \mathrm{Hom}_G(E_1, E_2)$

Definition 2.2.18 (Equivalent representations). [KS09, p.12] Let (E_1, π_1) and (E_2, π_2) be representations of a group G. If there exists an intertwiner $T : E_1 \to E_2$ that is also bijective, then we say that the two representations are equivalent.

Note that, if we choose $E_1 = E_2 = E$ and $\pi_1 = \pi_2 = \pi$, the definition of an intertwiner becomes the definition of a linear map that **commutes** with the representation (E, π). This leads to Schur's lemma, after we state the following helpful lemma:

Lemma 2.2.19. *[KS09, p.13] Given representations (E_1, π_1) and (E_2, π_2) of group G, and an intertwiner T. Then the kernel ker(T) is an invariant subspace under π_1 and the image im(T) is an invariant subspace under π_2.*

Proof. If $x \in \ker(T)$, then $T(x) = 0$. But then

$$T\left(\pi_1(g)x\right) = \pi_2(g)\left(T(x)\right) = 0 \tag{2.24}$$

so $\pi_1(g)x \in \ker(T)$ again for any $g \in G$, thus $\ker(T)$ is an invariant subspace of π_1.

Similarly, if $y \in \mathrm{im}(T)$, then $\exists x \in E_1 : T(x) = y$. But then

$$\pi_2(g)y = \pi_2(g)\left(T(x)\right) = T\left(\pi_1(g)x\right) \in \mathrm{im}(T) \tag{2.25}$$

for any $g \in G$, such that $\mathrm{im}(T)$ is an invariant subspace of π_2. □

Theorem 2.2.20 (Schur's lemma). *[KS09, p.13] Let T be an operator intertwining irreducible the representations (E_1, π_1) and (E_2, π_2) of a group G*

- *If π_1 and π_2 are not equivalent, then $T = 0$.*
- *If $E_1 = E_2 := E$ and $\pi_1 = \pi_2 := \pi$, then T is a scalar multiple of the identity of E*

Proof. We prove both assertions.

- If π_1 and π_2 are not equivalent, then T cannot be bijective. Thus either $\ker(T) \neq \{0\}$ or $\mathrm{im}(T) \neq E_2$. In the first case, as $\ker(T)$ is an invariant subspace and π_1 is irreducible, we must have $\ker(T) = E_1$. But then clearly $T = 0$. In the second case, $\mathrm{im}(T) \neq E_2$. But this is an invariant subspace under π_2 and π_2 is irreducible, so now we must have $\mathrm{im}(T) = \{0\}$. But then evidently $T = 0$.

- Let $\lambda \in \mathbb{C}$ be an eigenvalue of T, which must exist because T is an operator on a vector space over $\mathbb{C}$. Let E_λ be the eigenspace associated with λ. But then, E_λ is an invariant vector subspace of E under π: for any $x \in E_\lambda$ we have

  $$T(\pi(g)x) = \pi(g)\left(T(x)\right) = \pi(g)\left(\lambda x\right) = \lambda\pi(g)x \qquad \forall g \in G \tag{2.26}$$

  i.e. the vector $\pi(g)x$ is again in E_λ (as it has eigenvalue λ), so $\pi(g)E_\lambda \subset E_\lambda$. Now, we have $E_\lambda \neq \{0\}$ as it is an eigenspace. But, π is irreducible. Thus, we must have $E_\lambda = E$. But then, $Tv = \lambda v$ for any $v \in E$, which means that we have $T = \lambda\mathrm{Id}_E$.

□

2.2.4. Representations of Lie algebras and tensor products

Given a representation (E, π) of a Lie group, there is a natural way to consider a representation of its Lie algebra:

Definition 2.2.21 (Differential representations). [KS09, p.63] Given a representation (E, π) of a Lie group G. The differential representation of π is the Lie algebra representation $\partial\pi : \mathfrak{g} \to \mathfrak{gl}(E)$ given by

$$\partial\pi(X) := \frac{\mathrm{d}}{\mathrm{d}t}\pi\left(e^{tX}\right)\Big|_{t=0} \quad , \quad X \in \mathfrak{g} \tag{2.27}$$

So, $\pi(\exp(tX))$ is a one-parameter subgroup of $\mathrm{GL}(E)$, and $\partial\pi(X)$ is called an infinitesimal generator.

When considering tensor products of representations, we define

Definition 2.2.22 (Tensor product of representations). [KS09, p.16] Let (E_1, π_1) and (E_2, π_2) be representations of a group G. We define their tensor product as $(E_1 \otimes E_2, \pi_1 \otimes \pi_2)$ where

$$(\pi_1 \otimes \pi_2)(g) := \pi_1(g) \otimes \pi_2(g) \tag{2.28}$$

We can now combine these definitions to yield:

Definition 2.2.23 (Differential of tensor product representations). [KS09, p.64] Let (E_1, π_1) and (E_2, π_2) be representations of a Lie group G. Then, the differential of the tensor product representation is

$$\partial(\pi_1 \otimes \pi_2) = \partial\pi_1 \otimes \mathrm{Id}_{E_2} + \mathrm{Id}_{E_1} \otimes \partial\pi_2 \tag{2.29}$$

2.2.5. The Lie algebra $\mathfrak{su}(d)$

Recall from Theorem 2.2.8 that, as $\mathrm{SU}(d)$ is a matrix Lie group (as it is a closed subgroup of $\mathrm{GL}(n, \mathbb{R})$), we can construct its Lie algebra:

$$\mathfrak{su}(d) := \left\{X = \gamma'(0) \mid \gamma : \mathcal{I} \to \mathrm{SU}(d) \ , \ \text{ of class } C^1 \ , \ \gamma(0) = I\right\} \tag{2.30}$$

where $\mathcal{I}$ is an open interval in $\mathbb{R}$ that contains 0. In our case, see for example [Sti08, p.101]:

$$\mathfrak{su}(d) = \left\{X \in \mathbb{C}^{d\times d} \mid X + X^* = 0 \text{ and } \mathrm{Tr}[X] = 0\right\} \tag{2.31}$$

so $\mathfrak{su}(d)$ is the the set of all traceless anti-Hermitian $d \times d$ matrices.

Note that $\mathfrak{su}(d)$ is an algebra over the *real* numbers. Analyses of its irreducible representations are easier when we first complexify:

Definition 2.2.24 (Complexification of a vector space). [Hal15, p.65] Let V be a finite dimensional real vector space. The **complexification** of V, denoted $V_{\mathbb{C}}$, is the space of formal linear combinations of the form $v_1 + iv_2$ with $v_1, v_2 \in V$, where we define

$$i(v_1 + iv_2) := -v_2 + iv_1 \tag{2.32}$$

Then $V_{\mathbb{C}}$ is a complex vector space.

The reason this complexification will help us is the following useful theorem, from [KS09, p.51]:

Theorem 2.2.25. *Let $\mathfrak{g}_{\mathbb{C}}$ be the complexification of a real Lie algebra $\mathfrak{g}$. Every representation of $\mathfrak{g}$ can be extended uniquely to a representation of $\mathfrak{g}_{\mathbb{C}}$. There is a bijective correspondence between irreducible representations of $\mathfrak{g}$ and of $\mathfrak{g}_{\mathbb{C}}$*

So, when we wish to study the representations of $\mathfrak{su}(d)$, we can also look at its complexification (see for example [Sti08, p.110]):

Theorem 2.2.26.

$$\mathfrak{sl}(d, \mathbb{C}) = \mathfrak{su}(d) + i\mathfrak{su}(d) \tag{2.33}$$

The Lie algebra $\mathfrak{su}(2)$

In the case of $\mathfrak{su}(2)$, one can show that this is a vector space of dimension 3, and is spanned by the Pauli matrices:

$$\mathfrak{su}(2) = \text{Span}\left\{i\sigma_x, i\sigma_y, i\sigma_z\right\} \tag{2.34}$$

where the Pauli matrices are given by

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.35}$$

Furthermore, we will need to add another mathematical tool to our toolbox: the Casimir element of SU(2). The theory regarding Casimir elements deals with universal enveloping algebras, and as this is quite involved and the Casimir element of SU(2) has an intuitive physical connection, the formal mathematical definitions can be found in the Appendix B. The Casimir element of SU(2) is associated with the "total angular momentum" in Physics: that is, our Casimir element $\widetilde{\mathbf{C}}_2$ is defined as

$$\widetilde{\mathbf{C}}_2 := \sum_{k=1}^{3} X_k^2 \tag{2.36}$$

where we use a basis $\{X_1, X_2, X_3\}$ of $\mathfrak{su}(2)$ with the commutation relations $[X_1, X_2] = X_3$ (and cyclic permutations of the indices): they are scalar multiples of the Pauli matrices that we have already seen above. Namely, we can use $X_1 = -i\sigma_x/2$, $X_2 = -i\sigma_y/2$ and $X_3 = -i\sigma_z/2$.

In literature, we often write L_x, L_y, and L_z for the angular momentum basis, and then we identify $\widetilde{\mathbf{C}}_2$ with the L^2 element. Of special interest is the fact that the Casimir element commutes with all X_i, and returns the eigenvalue $j(j+1)$ if the quantum system is in the state $|j, m\rangle$ for some $m \in \{-j, -j+1, \ldots, j\}$. In our framework, we have $\partial\pi_j(\widetilde{\mathbf{C}}_2) = j(j+1)\text{Id}_j$ if we extend the representation $\partial\pi_j$ of the Lie algebra to its universal enveloping algebra.

2.3. On the symmetric subspace

We have now built the quantum mechanical framework of quantum systems, and the mathematical framework of (Lie) groups and representations. In our problem, we will restrict our input space to the symmetric subspace $\mathcal{H}_+^{\otimes n} \subset \mathcal{H}^{\otimes n}$ for some $n \in \mathbb{Z}_{>0}$, which is the subset of states that are invariant under permutations. We first define permutations before defining $\mathcal{H}_+^{\otimes n}$:

Definition 2.3.1 (Permutation operator). [Aud06] , [Har13] Given a tensor product space $\mathcal{H}^{\otimes n}$ for some $n \in \mathbb{Z}_{>0}$. Consider the symmetric group $\mathfrak{S}_n$, and an element $\pi \in \mathfrak{S}_n$. The permutation π is **represented** by a permutation matrix P_π on $\mathcal{H}^{\otimes n}$, that is, P_π is a square binary matrix with exactly one entry equal to 1 in each row and column (and thus all other entries equal zero) with respect to any orthonormal basis of $\mathcal{H}^{\otimes n}$. Let us choose an orthonormal basis $\{|i\rangle\}_{i=1}^d$ for $\mathcal{H} = \mathbb{C}^d$. Let $[d] := \{1, \ldots, d\}$. We then have the orthonormal basis for $\mathcal{H}^{\otimes n}$

$$\left\{|i_1, \ldots, i_n\rangle := |i_1\rangle \otimes \cdots \otimes |i_n\rangle \in \mathcal{H}^{\otimes n} \;:\; i_1, \ldots, i_n \in [d]\right\} \tag{2.37}$$

Then, according to [Har13], we have:

$$P_\pi = \sum_{i_1, \ldots, i_n \in [d]} |i_{\pi^{-1}(1)}, \ldots, i_{\pi^{-1}(n)}\rangle \langle i_1, \ldots, i_n| \tag{2.38}$$

As an example, consider $|\psi\rangle = |1,2,3\rangle + |1,2,4\rangle \in \mathcal{H}^{\otimes 3}$, with $\mathcal{H} = \mathbb{C}^4$. That is, $|\psi\rangle = |1\rangle \otimes |2\rangle \otimes (|3\rangle + |4\rangle)$, so physically speaking we have three quantum particles, of which the first two are in some orthonormal basis state, and the last particle is in a superposition state. We wish to permute particles 2 and 3: $\pi = (23) \in \mathfrak{S}_3$. Then:

$$P_{(23)}|\psi\rangle = |1,3,2\rangle\langle 1,2,3 \mid \psi\rangle + |1,4,2\rangle\langle 1,2,4 \mid \psi\rangle = |1,3,2\rangle + |1,4,2\rangle = |1\rangle \otimes (|3\rangle + |4\rangle) \otimes |2\rangle \tag{2.39}$$

So indeed, $P_{(23)}$ swaps the second and third particle.

Definition 2.3.2 (Symmetric subspace). [Har13] The symmetric subspace $\mathcal{H}_+^{\otimes n} \subset \mathcal{H}^{\otimes n}$ (in literature sometimes denoted by $\text{Sym}^n(\mathcal{H})$ or $\vee^n(\mathcal{H})$) is defined by

$$\mathcal{H}_+^{\otimes n} := \left\{\psi \in \mathcal{H}^{\otimes n} \;:\; P_\pi\psi = \psi \qquad \forall \pi \in \mathfrak{S}_n\right\} \tag{2.40}$$

Next, we will show a theorem which makes the construction of $\mathcal{H}_+^{\otimes n}$ easier, as it does not rely on the representation theory of the symmetric group directly:

Theorem 2.3.3 (Construction of the symmetric subspace). *The symmetric subspace $\mathcal{H}_+^{\otimes n}$ can also be characterised as:*

$$\mathcal{H}_+^{\otimes n} = Span\left\{\phi \otimes \phi \otimes \cdots \otimes \phi = \phi^{\otimes n} \in \mathcal{H}^{\otimes n} \ : \ \phi \in \mathcal{H}\right\} \tag{2.41}$$

For a proof of this theorem, see for example [Har13]. Note that the proof uses a construction of a basis of $\mathcal{H}_+^{\otimes N}$ similar to the basis we find in Appendix A.1.1 - however, we use this theorem to find this basis and prove the dimensionality of $\mathcal{H}_+^{\otimes N}$.

As we consider the symmetric subspace $\mathcal{H}_+^{\otimes N}$ as the vector space in which our original states live, it is of interest to construct a projector that takes states from $\mathcal{H}^{\otimes N}$ to $\mathcal{H}_+^{\otimes N}$. We prove:

Proposition 2.3.4 (Projection of $\mathcal{H}_+^{\otimes N}$). *There is an orthogonal projection $S_N : \mathcal{H}^{\otimes N} \to \mathcal{H}_+^{\otimes N}$ and it is of the form:*

$$S_N = \frac{1}{N!} \sum_{\sigma \in \mathfrak{S}_N} P_\sigma \tag{2.42}$$

Proof. We need to prove $S_N \mathcal{H}^{\otimes N} = \mathcal{H}_+^{\otimes N}$, $S_N^2 = S_N$, and $S_N^* = S_N$. Linearity is evident from the construction of S_N.

Firstly, we prove $S_N \mathcal{H}^{\otimes N} \subset \mathcal{H}_+^{\otimes N}$. Given any $\pi \in \mathfrak{S}_N$, we will prove that $P_\pi S_N \psi = S_N \psi$ for any $\psi \in \mathcal{H}^{\otimes N}$, thus proving that indeed $S_N \psi$ is a permutation invariant state. We compute:

$$P_\pi S_N \psi = \frac{1}{N!} \sum_{\sigma \in \mathfrak{S}_N} P_\pi P_\sigma \psi = \frac{1}{N!} \sum_{\sigma \in \mathfrak{S}_N} P_{\pi\sigma} \psi = \frac{1}{N!} \sum_{\tau \in \mathfrak{S}_N} P_\tau \psi = S_N \psi \tag{2.43}$$

where we have used that $P_\pi P_\sigma = P_{\pi\sigma}$ where $\pi\sigma$ denotes the group operation, which is the composition of permutations. Furthermore, we are allowed to change the summation variable in this way as the map $\sigma \mapsto \pi\sigma = \tau$ is a bijection.

Secondly, we prove that $\mathcal{H}_+^{\otimes N} \subset S_N \mathcal{H}^{\otimes N}$. Choose any $\psi \in \mathcal{H}_+^{\otimes N} \subset \mathcal{H}^{\otimes N}$. By definition, for all $\pi \in \mathfrak{S}_N$ we have $P_\pi \psi = \psi$, thus also $S_N \psi = \psi$.

Thus, we have $\mathcal{H}_+^{\otimes N} = S_N \mathcal{H}^{\otimes N}$.

Thirdly, we prove that $S_N^2 = S_N$:

$$S_N S_N \psi = \frac{1}{N!} \sum_{\sigma \in \mathfrak{S}_N} P_\sigma \cdot \frac{1}{N!} \sum_{\pi \in \mathfrak{S}_N} P_\pi \psi = \left(\frac{1}{N!}\right)^2 \sum_{\sigma \in \mathfrak{S}_N} \sum_{\pi \in \mathfrak{S}_N} P_{\sigma\pi} \psi \tag{2.44}$$

We can again rewrite the last sum over π to $\sum_{\tau \in \mathfrak{S}_N} P_\tau \psi$. Realising this sum then does not depend on σ, we may write:

$$S_N^2 \psi = \left(\frac{1}{N!}\right)^2 \cdot N! \cdot \sum_{\tau \in \mathfrak{S}_N} P_\tau \psi = S_N \psi \tag{2.45}$$

so indeed $S_N^2 = S_N$.

Lastly, we can directly compute

$$S_N^* = \frac{1}{N!} \sum_{\sigma \in \mathfrak{S}_N} P_\sigma^* = \frac{1}{N!} \sum_{\sigma \in \mathfrak{S}_N} P_{\sigma^{-1}} = \frac{1}{N!} \sum_{\tau \in \mathfrak{S}_N} P_\tau = S_N \tag{2.46}$$

where we have used that $\sigma \mapsto \sigma^{-1} = \tau$ is a bijection. □

3

The No Cloning Theorem

Before we review optimal quantum cloning machines with respect to a specific measure, we review the raison d'être for this enquiry: the No Cloning Theorem. This theorem tells us that we cannot perfectly copy arbitrary quantum states. As we are prohibited from perfectly cloning arbitrary states, we logically turn our attention to the best possible, but imperfect, cloning device. It is thus insightful to start with the No Cloning Theorem itself.

The statement and proof of the No Cloning Theorem are loosely based on multiple sources, see for example [WZ82] (the first to provide a proof for the No Cloning Theorem), or [NC01, page 24]. Both these sources use the Schrödinger picture of quantum mechanics, in which we look at a quantum operation on *states*. We furthermore supply a version of the No-Cloning Theorem in the Heisenberg picture, based on [Maa04, page 44] in which we look at a quantum operation on *observables*. More information about the Schrödinger and Heisenberg pictures can be found in Definitions 2.1.14 and 2.1.15.

3.1. The No-Cloning Theorem in the Schrödinger picture

We would like to investigate whether it is possible to copy an arbitrary quantum system perfectly. We therefore look at a finite-dimensional Hilbert space $\mathcal{H}$ with $1 < d = \dim \mathcal{H} < \infty$, in which our quantum states live, with orthonormal basis $\{|i\rangle\}_{i=0}^{d-1}$. We consider the input of our system: an arbitrary state $|\psi\rangle \in \mathcal{H}$ which needs to be "copied" onto another qubit, initialized into an arbitrary state, say $|0\rangle \in \mathcal{H}$. In quantum mechanics, the transformations of such systems must be linear and preserve inner products: these are unitary transformations. We are thus looking for a unitary transformation $U : \mathcal{H}\otimes\mathcal{H} \to \mathcal{H}\otimes\mathcal{H}$ such that $U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$. This means that the resulting states must be **separable**, all information of $|\psi\rangle$ is **perfectly copied** to the second state, and the **original state is not changed**. Thus we arrive at:

Theorem 3.1.1 (No Cloning Theorem). *Given a Hilbert space $\mathcal{H}$ with $1 < d = \dim \mathcal{H} < \infty$ and an orthonormal basis $\{|i\rangle\}_{i=0}^{d-1}$. There is no unitary transformation $U : \mathcal{H} \otimes \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$ such that $U |\psi\rangle \otimes |0\rangle = |\psi\rangle \otimes |\psi\rangle$ for all $|\psi\rangle \in \mathcal{H}$*

Proof. We prove this theorem by contradiction. Assume there is such a unitary transformation U. As $d > 1$, we can compute for $|0\rangle, |1\rangle \in \mathcal{H}$:

$$U |0\rangle \otimes |0\rangle = |0\rangle \otimes |0\rangle \qquad ; \qquad U |1\rangle \otimes |0\rangle = |1\rangle \otimes |1\rangle \tag{3.1}$$

but now, consider a state $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ for some $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$. Surely then $|\psi\rangle \in \mathcal{H}$, so we can compute, using linearity:

$$U |\psi\rangle \otimes |0\rangle = U (\alpha |0\rangle \otimes |0\rangle + \beta |1\rangle \otimes |1\rangle) = \alpha U |0\rangle \otimes |0\rangle + \beta U |1\rangle \otimes |0\rangle = \alpha |0\rangle \otimes |0\rangle + \beta |1\rangle \otimes |1\rangle \tag{3.2}$$

But surely this cannot be correct, because we can manually compute:

$$|\psi\rangle \otimes |\psi\rangle = (\alpha |0\rangle + \beta |1\rangle) \otimes (\alpha |0\rangle + \beta |1\rangle) = \alpha^2 |0\rangle \otimes |0\rangle + \beta^2 |1\rangle \otimes |1\rangle + \alpha\beta (|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle) \tag{3.3}$$

But then we must have $\alpha\beta = 0$. Thus U can only perfectly copy the orthogonal basis elements, but not linear combinations. This directly contradicts our assumption that U perfectly clones *any* state in $\mathcal{H}$. We conclude that no perfect cloning map exists. □

3.2. The No-Cloning Theorem in the Heisenberg picture

We look at a finite-dimensional Hilbert space $\mathcal{H}$ with $1 < d = \dim \mathcal{H} < \infty$, and its tensor product $\mathcal{H} \otimes \mathcal{H}$. The ideal quantum operation would be $T_* : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H} \otimes \mathcal{H})$ with $T(\sigma) = \sigma \otimes \sigma$ for all $\sigma \in \mathcal{S}(\mathcal{H})$. Then, we also have:

$$\operatorname{Tr}\left[(\mathrm{Id}_{\mathcal{H}} \otimes A)\, T_*(\sigma)\right] = \operatorname{Tr}\left[(A \otimes \mathrm{Id}_{\mathcal{H}})\, T_*(\sigma)\right] = \operatorname{Tr}\left[A\sigma\right] \qquad \forall A \in \mathcal{B}(\mathcal{H}) \tag{3.4}$$

Instead of looking at what T_* does to the states, we now look at what its dual T does to the observables: The traces are equal to $\operatorname{Tr}\left[T\left(\mathrm{Id}_{\mathcal{H}} \otimes A\right)\sigma\right]$ and $\operatorname{Tr}\left[T\left(A \otimes \mathrm{Id}_{\mathcal{H}}\right)\sigma\right]$ according to the duality between T_* and T in Definitions 2.1.2. So, we must have $T(\mathrm{Id}_{\mathcal{H}} \otimes A) = T(A \otimes \mathrm{Id}_{\mathcal{H}}) = A$, and we arrive at:

Theorem 3.2.1 (No-Cloning Theorem). *Given a Hilbert space $\mathcal{H}$, and a $*$-algebra $\mathcal{A} \subseteq \mathcal{B}(\mathcal{H})$. If there exists a $T : \mathcal{A} \otimes \mathcal{A} \to \mathcal{A}$ such that*

$$T\left(Id_{\mathcal{H}} \otimes A\right) = T\left(A \otimes Id_{\mathcal{H}}\right) = A \qquad \forall A \in \mathcal{A} \tag{3.5}$$

then $\mathcal{A}$ is abelian.

The proof is based on the following multiplication lemma, which we will state without proof. Its statement and proof can be found in [Maa04, page 42]:

Lemma 3.2.2. *If $T : \mathcal{A} \to \mathcal{B}$ is an operation, where $\mathcal{A}, \mathcal{B}$ are $*$-algebras, and $T(A^*A) = T(A)^*T(A)$ for some $A \in \mathcal{A}$, then for all $B \in \mathcal{A}$:*

$$T(A^*B) = T(A)^*T(B) \qquad ; \qquad T(B^*A) = T(B)^*T(A) \tag{3.6}$$

Proof of Theorem 3.2.1. Note that we can apply the lemma to our theorem, if we observe that, for all $A \in \mathcal{A}$:

$$T\left((\mathrm{Id}_{\mathcal{H}} \otimes A)^*(\mathrm{Id}_{\mathcal{H}} \otimes A)\right) = T\left(\mathrm{Id}_{\mathcal{H}} \otimes A^*A\right) = A^*A = T\left(\mathrm{Id}_{\mathcal{H}} \otimes A\right)^* T\left(A \otimes \mathrm{Id}_{\mathcal{H}}\right) \tag{3.7}$$

But then for all $A, B \in \mathcal{A}$:

$$AB = T\left(A \otimes \mathrm{Id}_{\mathcal{H}}\right) \cdot T\left(\mathrm{Id}_{\mathcal{H}} \otimes B\right) = T\left((A \otimes \mathrm{Id}_{\mathcal{H}})(\mathrm{Id}_{\mathcal{H}} \otimes B)\right) = \tag{3.8}$$

$$T\left((\mathrm{Id}_{\mathcal{H}} \otimes B)(A \otimes \mathrm{Id}_{\mathcal{H}})\right) = T\left(\mathrm{Id}_{\mathcal{H}} \otimes B\right) \cdot T\left(A \otimes \mathrm{Id}_{\mathcal{H}}\right) = BA \tag{3.9}$$

□

In conclusion, we can only build perfect cloning machines when we consider commuting observables, and thus we cannot build a general cloning machine.

3.3. Connection to optimal cloning: figures of merit

Alternatively to the statement above, we could also express the No-Cloning Theorem in terms of the fidelity of a cloning map, or the performance of a cloning map with respect to the expectation value of observables on a single clone. Those are precisely the two figures of merit that we will use in this paper, and it is therefore useful to intuitively build up to those figures of merit, using the No-Cloning Theorem.

If we let $|\psi\rangle \in \mathcal{H}$, then ideally our cloning map would produce a state corresponding to $|\psi\rangle \otimes |\psi\rangle \in \mathcal{H} \otimes \mathcal{H}$, in the case of density matrices thus the density matrix described by $\sigma \otimes \sigma$ with $\sigma := |\psi\rangle\langle\psi|$. In such a case, the density matrix is a projection onto the one dimensional subspace spanned by $|\psi\rangle \otimes |\psi\rangle$. Thus, we could investigate how much the cloning device overlaps with this projection. We let $T_* : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H} \otimes \mathcal{H})$ denote a cloning map that takes states on $\mathcal{H}$ to states on $\mathcal{H} \otimes \mathcal{H}$. We can then inspect the expectation value of $T_*(\sigma)$ with respect to $|\psi\rangle \otimes |\psi\rangle$. In the ideal case, $T_*(\sigma) = \sigma \otimes \sigma$, and the expectation value evaluates to 1. However, any quantum operation will perform worse by the

No-Cloning Theorem, which will result in a value between 0 and 1. Thus, looking at the overlap of the cloned state with a one-dimensional projection yields a useful figure of merit for cloning maps. We can recast the No-Cloning Theorem in the following inequality:

$$\forall T_* : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H}\otimes\mathcal{H}) \ : \ \exists \left|\psi\right\rangle \in \mathcal{H} \ , \ \sigma = \left|\psi\right\rangle\left\langle\psi\right| \in \mathcal{S}(\mathcal{H}) \ : \ \mathrm{Tr}\left[\sigma^{\otimes 2}\ T_*\left(\sigma\right)\right] < 1 \tag{3.10}$$

This line of thought is the foundation on which we will build the *fidelity* of a cloning map in the next Chapter, in which we generalize the previous expression to arbitrary amounts of input clones and output clones. Taking the infimum over all pure density matrices σ of the trace expression then yields our expression for the fidelity. Stronger than the consequence of the No-Cloning Theorem, we will show that the fidelity is always smaller than a number between 0 and 1 that increases with the amount of input clones available, and decreases with the amount of output clones demanded. In the case of one input state, and two output states, this upper bound is $1/(d+1)$ where $d = \dim\mathcal{H}$, so even in the smallest qubit case, the infimum over all pure states of the trace expression is smaller than $1/3$.

The previous figure of merit depends on the overlap of the entirety of the output states with the ideal output. Alternatively, we could look at the performance of a single output clone: to be more exact, we would like to compare the expectation value of an observable on one output clone with the expectation value of this observable on the input. We let $a \in \mathcal{B}(\mathcal{H})$ be an observable on the original Hilbert space, and $\sigma = \left|\psi\right\rangle\left\langle\psi\right| \in \mathcal{S}(\mathcal{H})$ again a pure state density matrix. We denote with $a_{(1)} := a \otimes \mathrm{Id}_{\mathcal{H}}$ and $a_{(2)} := \mathrm{Id}_{\mathcal{H}} \otimes a$ two observables on $\mathcal{H}\otimes\mathcal{H}$, that only impact the first and the second clone, respectively. We can then look at their expectation value:

$$\mathrm{Tr}\left[a_{(k)} T_*\left(\sigma\right)\right] \quad k = 1,2 \tag{3.11}$$

Ideally, $T_*(\sigma) = \sigma\otimes\sigma$, and then this expectation simply evaluates to $\mathrm{Tr}\left[\sigma a\right]$, i.e. the expectation of a with respect to the input state. So quite naturally, we can look at the difference

$$\left|\mathrm{Tr}\left[a_{(k)} T_*\left(\sigma\right)\right] - \mathrm{Tr}\left[\sigma a\right]\right| \quad k = 1,2 \tag{3.12}$$

Equivalently to looking at what T_* does with states in the Schrödinger picture, we could also look at what a cloning map $T : \mathcal{B}(\mathcal{H}\otimes\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ does to the observables in the Heisenberg picture, where the two views are related by $\mathrm{Tr}\left[\sigma T(A)\right] = \mathrm{Tr}\left[A T_*(\sigma)\right]$ (see Definitions 2.1.15).

Namely, this allows us to rewrite the first trace in the previous equation to $\mathrm{Tr}\left[\sigma T(a_{(k)})\right]$. Then using the fact that $\sigma = \left|\psi\right\rangle\left\langle\psi\right|$ for some $\left|\psi\right\rangle \in \mathcal{H}$, we can rewrite the previous expression, including the No-Cloning Theorem:

$$\forall T \ : \ \exists k \in \{0,1\} \ , \ \exists \left|\psi\right\rangle \in \mathcal{H} \ , \ \exists a \in \mathcal{B}(\mathcal{H}) \ : \ \left|\left\langle\psi \ , \ T\left(a_{(k)}\right) \ \psi\right\rangle - \left\langle\psi \ , \ a \ \psi\right\rangle\right| > 0 \tag{3.13}$$

This is an intuitive expression: it is the distance between the expectation values of $T(a_{(k)})$ and a with respect to the state $\left|\psi\right\rangle$. This line of thought is the foundation of the *one-clone testing* figure of merit which we will introduce in the next Chapter (again generalizing to arbitrary amounts of input states and output clones). We take the supremum over all k, all states $\left|\psi\right\rangle$ with $\left\langle\psi,\psi\right\rangle = 1$ and all observables $0 \leq a \leq \mathrm{Id}_{\mathcal{H}}$. In the case of one input state and two output clones, the lower bound for qubits is $1/6$.

4

Description of problem and result

After looking at the No Cloning Theorem, one can naturally wonder what kind of cloning map can clone quantum states optimally. However, to investigate such a notion, we first need to establish what it precisely means to clone quantum states, and in what way we will test the performance of such a cloning machine. It is thus imperative to first dedicate some thought to a precise formulation of the problem we wish to solve.

4.1. Statement of the problem

To formulate the problem of optimal quantum cloning, one needs to specify three components: firstly, one needs to specify what kind of quantum system is supplied to the quantum cloning machine as input, and what kind of quantum system is expected of the cloning machine. Secondly, one then needs to specify what one sees as an admissible quantum cloning machine, such as to specify all the possible operations that take in the specified input and output a quantum system on the output space. Lastly, one needs to specify how one will determine the performance of a cloning machine: we call those the *figures of merit*. We will specify all three components, respectively.

4.1.1. Description of input and output spaces

We look at quantum states in some finite-dimensional Hilbert space $\mathcal{H}$ with $1 < d = \dim \mathcal{H} < \infty$. We will consider pure states in this research, thus density operators on this Hilbert space will be of the form $\sigma = |\psi\rangle \langle\psi|$ for some $|\psi\rangle \in \mathcal{H}$ and thus $\langle\psi| \in \mathcal{H}^*$.

To be as general as possible, we allow for the preparation of N separate copies of the original state that we would like to copy into M quantum systems with $M > N$. Thus, the input quantum system can be described by density matrices of the form $\sigma^{\otimes N}$ for some $\sigma = |\psi\rangle \langle\psi|$ a pure state. These states are supported by the so-called Bose subspace, denoted by $\mathcal{H}_+^{\otimes N}$:

$$\mathcal{H}_+^{\otimes N} := \operatorname{Span}\left\{\phi \otimes \phi \otimes \cdots \otimes \phi = \phi^{\otimes N} \in \mathcal{H}^{\otimes N} \mid \phi \in \mathcal{H}\right\} \tag{4.1}$$

An alternative definition of $\mathcal{H}_+^{\otimes N}$ based on permutation invariance, and the proof that these two definitions are equivalent, can be found in Theorem 2.3.3. Furthermore, the dimension of this subspace is $\dim \mathcal{H}_+^{\otimes N} = \binom{d+N-1}{N}$, where $d = \dim \mathcal{H}$. The calculations for this expression can be found in the Appendix A.1.1 , where an explicit basis for this subspace is constructed.

This concludes the description of the initial system. Looking at the output system, we would like to make M copies of the quantum systems, so naturally we look at $\mathcal{H}^{\otimes M}$. Note that we do not impose further *a priori* constraints on this output system.

4.1.2. Description of the quantum cloning device

The connection between these two systems must be a cloning map that must be a quantum operation. We can state the problem in two (related) ways: either we look at a cloning map of *states*, or a cloning map of *observables*. These methods correspond to the Schrödinger picture of quantum mechanics and the Heisenberg picture, respectively. See Definitions 2.1.14 and 2.1.15. We state both descriptions for our specific problem:

Schrödinger picture : We look at (linear) completely positive trace preserving (CPTP) cloning maps of the form $T_* : \mathcal{B}(\mathcal{H}_+^{\otimes N}) \to \mathcal{B}(\mathcal{H}^{\otimes M})$ that take in density matrices of the form $\sigma^{\otimes N} \in \mathcal{S}(\mathcal{H}_+^{\otimes N})$ with $\sigma \in \mathcal{S}(\mathcal{H})$ and output some density matrix on $\mathcal{H}^{\otimes M}$. (Note that T_* is fully specified when it is specified for $\mathcal{S}(\mathcal{H}_+^{\otimes N}) \subset \mathcal{B}(\mathcal{H}_+^{\otimes N})$, see the discussion below Definition 2.1.14).

Heisenberg picture : We look at linear, completely positive, unital cloning maps of the form $T : \mathcal{B}(\mathcal{H}^{\otimes M}) \to \mathcal{B}(\mathcal{H}_+^{\otimes N})$ that take in observables $A \in \mathcal{B}(\mathcal{H}^{\otimes M})$ and output some observable on $\mathcal{H}_+^{\otimes N}$.

The defining equation between these two views is:

$$\operatorname{Tr}\left[\rho T(A)\right] = \operatorname{Tr}\left[T_*(\rho) A\right] \qquad \forall \rho \in \mathcal{S}(\mathcal{H}_+^{\otimes N}) \ , \ \forall A \in \mathcal{B}(\mathcal{H}^{\otimes M}) \tag{4.2}$$

We must, however, still specify how we determine whether one cloning map "performs better" than another: i.e., we need to introduce a measure of optimality.

4.1.3. Figures of merit

We introduce two figures of merit, that measure the performance of the cloning device. The motivation for these figures of merit can be found in Section 3.3 : in summary, the *fidelity* represents the expectation value of the quantum state after cloning with respect to the ideal output, whilst the *one-clone test* measures the difference in expectation values of an observable *before* and *after* cloning.

Firstly, we could look at the fidelity:

Definition 4.1.1 (Fidelity of a cloning map). [Wer98] The fidelity of a linear CPTP cloning map T_* in the Schrödinger picture is defined as:

$$\mathcal{F}(T_*) = \inf_{\sigma,\ \text{pure}} \operatorname{Tr}\left[\sigma^{\otimes M} T_*\left(\sigma^{\otimes N}\right)\right] \tag{4.3}$$

Note that the fidelity can at best be 1, and this precisely happens when $T_*(\sigma^{\otimes N}) = \sigma^{\otimes M}$ (although this is prohibited by the No Cloning Theorem). Thus, we wish to find a map that has a fidelity as close to 1 as possible.

Secondly, we propose a measure of merit that takes into account only *one* of the clones:

Definition 4.1.2 (Measure of merit based on one clone). [KW99] A test based on one output clone of a cloning map T can be designed as:

$$\Delta_{\text{one}}(T) := \sup_{a,\psi,k} \left|\langle \psi^{\otimes N} \ , \ T(a_{(k)})\psi^{\otimes N}\rangle - \langle \psi \ , \ a\psi\rangle\right| \tag{4.4}$$

where the supremum is taken over all $\psi \in \mathcal{H}$ with $\|\psi\| = 1$, all operators $a \in \mathcal{B}(\mathcal{H})$ with $0 \leq a \leq \mathrm{Id}_{\mathcal{H}}$ and all integer $1 \leq k \leq M$. Note that we write

$$a_{(k)} := \mathrm{Id}_{\mathcal{H}}^{\otimes(k-1)} \otimes a \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-k)} \qquad a \in \mathcal{B}(\mathcal{H}) \ , \ 1 \leq k \leq M \tag{4.5}$$

i.e. $a_{(k)}$ is an observable on $\mathcal{H}^{\otimes M}$ that acts as the identity on all but the k-th clone, on which it acts as the observable $a \in \mathcal{B}(\mathcal{H})$.

4.2. Statement of the result

Remarkably, we will show that there exists a unique cloning machine that is optimal with respect to both figures of merit:

Theorem 4.2.1 (Optimal cloning map). *There is a unique cloning map $\hat{T}_*$ that is optimal with respect to both figures of merit previously described, and it can be described as:*

$$\hat{T}_*(\rho) = \frac{d[N]}{d[M]}\; S_M \left(\rho \otimes Id_{\mathcal{H}}^{\otimes(M-N)}\right) S_M \tag{4.6}$$

where $\rho \in \mathcal{S}(\mathcal{H}_+^{\otimes N})$, $S_M : \mathcal{H}^{\otimes M} \to \mathcal{H}_+^{\otimes M}$ is the symmetric projection from the output space to its symmetric (permutation invariant) subspace, and for any $n \in \mathbb{Z}_{>0}$ we let $d[n] = \binom{d+n-1}{n}$ denote the dimension of the symmetric subspace $\mathcal{H}_+^{\otimes n}$.

In order to prove that this map is indeed the optimal cloning map, we will prove the following theorems:

Theorem 4.2.2 (Optimality condition for $\Delta_{\mathbf{one}}(T)$). *For any cloning map $T : \mathcal{B}(\mathcal{H}^{\otimes M}) \to \mathcal{B}(\mathcal{H}_+^{\otimes N})$ we have*

$$\Delta_{one}(T) \geq \frac{d-1}{d}\left|1 - \frac{N}{N+d} \cdot \frac{M+d}{M}\right| \tag{4.7}$$

with equality iff $T = \hat{T}$.

Theorem 4.2.3 (Optimality condition for $\mathcal{F}(T_*)$). *For any cloning map $T_* : \mathcal{B}(\mathcal{H}_+^{\otimes N}) \to \mathcal{B}(\mathcal{H}^{\otimes M})$ we have*

$$\mathcal{F}(T_*) \leq \frac{d[N]}{d[M]} \tag{4.8}$$

with equality iff $T = \hat{T}$

Note that, before we start our journey into proving the previous theorems, the optimal cloning map looks remarkably "simple" : it takes in a quantum system of the form $\sigma^{\otimes N}$, prepares all other $(M-N)$ clones in the maximally mixed state $\mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)}$ (up to a normalization constant), tensors on these two quantum systems, and projects the entire system into the symmetric subspace (the output Bose subspace). Thus we already notice two important concept that will play a central role in our proof: firstly, the optimal cloner is **permutation invariant** because it projects its result to the Bose subspace, so interchanging any of the resulting clones does not change the output state. The second statement is perhaps not readily seen from the form of $\hat{T}_*$, but will play a key role nonetheless: our optimal cloner has **unitary covariance**, which means that a unitary transformation *before* cloning (on $\sigma^{\otimes N}$) has the same effect as a unitary transformation *after* cloning (on $\hat{T}_*(\sigma^{\otimes N})$).

5

Symmetries of an optimal cloning device

In this chapter, we will look at a central theme in the search for an optimal cloning device: permutation invariance of the output clones and unitary covariance (the property that applying a unitary transformation *before* cloning has the same effect as applying these transformations *after* cloning). Although we cannot yet guarantee that *all* optimal cloning devices have these properties, we can prove that averaging them over permutation and unitaries will lead to cloning devices that have the invariance properties, and that those cloning devices perform at least as well as the original cloning device. In other words, given any cloning device, making it permutation invariant or unitary covariant cannot worsen its performance. Later on, we will prove that there is a *unique* optimal cloning device (and thus, by necessity, this optimal cloning device must also be permutation invariant and unitary covariant).

Before we can state the permutation and unitary theorems, we need some mathematical framework to handle permutations and unitary transformations on tensor product spaces. This is done through representations of the symmetric group $\mathfrak{S}_n$ and the unitary group $\mathrm{U}(d)$. Some representation theory can be found in Section 2.2.3. All relevant representations will be stated in the following section. After building the mathematical machinery needed, we will state the symmetry theorems and prove them.

5.1. Construction of necessary mathematical tools

The notions of permutations of quantum clones and unitary covariance can be precisely stated once we have developed the techniques of using representations of the permutation group and the unitary group. Furthermore, we show that these two representations commute, and we can state the precise definition of unitary covariance.

5.1.1. The representation of permutations on $\mathcal{H}^{\otimes n}$

Let us first look at permutations. We thus turn our attention to the group $\mathfrak{S}_n$ for some $n \in \mathbb{Z}_{>0}$: precisely, the set of bijections from $\{1, \dots, n\}$ to $\{1, \dots, n\}$, equipped with the group operation $\circ$ of composition of bijections. We would like to let this group act on the quantum states that live in $\mathcal{H}^{\otimes n}$: thus, we need a representation of the group on the vector space $\mathcal{H}^{\otimes n}$. We will write $P_\pi : \mathcal{H}^{\otimes n} \to \mathcal{H}^{\otimes n}$ for $\pi \in \mathfrak{S}_n$ as the permutation operator, as described in Definition 2.3.1, where we also provide a construction for such a permutation operator. It acts on states as follows:

$$P_\pi \left(\psi_1 \otimes \psi_2 \otimes \cdots \otimes \psi_n\right) = \psi_{\pi^{-1}(1)} \otimes \cdots \otimes \psi_{\pi^{-1}(n)} \qquad ; \qquad \psi_1 \otimes \cdots \otimes \psi_n \in \mathcal{H}^{\otimes n} \ , \ \pi \in \mathfrak{S}_n \tag{5.1}$$

This indeed is the mathematical description of the intuitive "swapping" of quantum copies.

5.1.2. The representation of unitary matrices on $\mathcal{H}^{\otimes n}$

Now, let us turn our attention to the group of unitary matrices, $\mathrm{U}(d)$, equipped with the standard matrix product. These elements have a fundamental representation $(\pi_\square, \mathbb{C}^d)$, which is just $\pi_\square(u) = u$ for $u \in \mathrm{U}(d)$, as they can act on vectors living in $\mathcal{H} = \mathbb{C}^d$ by the standard matrix-vector relation.

However, we would also like to describe unitary actions on quantum states that live in tensor product spaces. Luckily, we have a natural way of doing this: we build the representation $(\pi_{\square}^{\otimes n},\mathcal{H}^{\otimes n})$ with $\pi_{\square}^{\otimes n}(u) = u^{\otimes n}$, such that it acts as:

$$\pi_{\square}^{\otimes n}(u)\,(\psi_1 \otimes \cdots \otimes \psi_n) = (u\psi_1) \otimes \cdots \otimes (u\psi_n) \qquad ; \qquad \psi_1 \otimes \cdots \otimes \psi_n \in \mathcal{H}^{\otimes n}\ ,\ u \in \mathrm{U}(d) \tag{5.2}$$

5.1.3. Commuting relationship between these representations

An important concept is the fact that the previous two representations commute: let any $\psi_1 \otimes \cdots \otimes \psi_n \in \mathcal{H}^{\otimes n}$, any $\pi \in \mathfrak{S}_n$ and any $u \in \mathrm{U}(d)$, then we see that:

$$P_\pi \pi_{\square}^{\otimes n}(u)\,(\psi_1 \otimes \cdots \otimes \psi_n) = P_\pi\left((u\psi_1) \otimes \cdots \otimes (u\psi_n)\right) = (u\psi_{\pi^{-1}(1)}) \otimes \cdots \otimes (u\psi_{\pi^{-1}(n)}) = \tag{5.3}$$

$$\pi_{\square}^{\otimes n}(u)\left(\psi_{\pi^{-1}(1)} \otimes \cdots \otimes \psi_{\pi^{-1}(n)}\right) = \pi_{\square}^{\otimes n}(u) P_\pi\,(\psi_1 \otimes \cdots \otimes \psi_n) \tag{5.4}$$

5.1.4. The representation of unitary matrices on $\mathcal{H}_+^{\otimes n}$

If we restrict ourselves to the symmetric subspace $\mathcal{H}_+^{\otimes n} \subset \mathcal{H}^{\otimes n}$, as defined by Definition 2.3.2 (i.e. the space of all states that are invariant under permutations), we can also restrict our representation $\pi_n^+ := \pi_{\square}^{\otimes n} \restriction \mathcal{H}_+^{\otimes n}$. This is well-defined, precisely because the unitary representation and the permutation representation commute: any state in $\mathcal{H}_+^{\otimes n}$ will stay in $\mathcal{H}_+^{\otimes n}$ when acted upon by π_n^+. The representation $(\pi_n^+, \mathcal{H}_+^{\otimes n})$ plays a pivotal role, as it is an irreducible representation.

5.1.5. Definition of unitary covariance

We can now also define precisely what is meant by maps that are $\mathrm{U}(d)$-covariant

Definition 5.1.1 (U(d)-covariance of a cloning map). Given a cloning map $T : \mathcal{B}(\mathcal{H}^{\otimes M}) \to \mathcal{B}(\mathcal{H}_+^{\otimes N})$. This map is called $\mathrm{U}(d)$-covariant, also called unitary covariant, if the following holds:

$$T\left(\pi_{\square}^{\otimes M}(u)\ A\ \pi_{\square}^{\otimes M}(u)^*\right) = \pi_N^+(u)\ T(A)\ \pi_N^+(u)^* \qquad \forall u \in \mathrm{U}(d)\ ,\ \forall A \in \mathcal{B}(\mathcal{H}^{\otimes M}) \tag{5.5}$$

Equivalently for the dual $T_* : \mathcal{B}(\mathcal{H}_+^{\otimes N}) \to \mathcal{B}(\mathcal{H}^{\otimes M})$:

$$T_*\left(\pi_N^+(u)\ \rho\ \pi_N^+(u)^*\right) = \pi_{\square}^{\otimes M}(u)\ T_*(\rho)\ \pi_{\square}^{\otimes M}(u)^* \qquad \forall u \in \mathrm{U}(d)\ ,\ \forall \rho \in \mathcal{S}(\mathcal{H}_+^{\otimes N}) \tag{5.6}$$

That is, applying unitary transformations *prior* to the cloning is equivalent to applying them *after* the cloning.

5.2. Permutation and unitary averaging of a cloning map

As a first step towards proving the main theorems, it is useful to exploit the symmetries that were referenced in the previous section: our optimal map seems to be permutation invariant, and unitarily covariant. In fact, we can prove that given any cloning machine, we can actually improve (or at least not worsen) the figures of merit for this cloning machine by averaging over permutations and unitary transformations - which results in permutation invariant and unitarily covariant maps, thus proving that if one finds an optimal cloning map, we can *also* construct an optimal cloning map with these properties. We make these statements precise in this section.

Theorem 5.2.1 (Permutation average of an optimal cloning device). *Given any quantum operation $T_* : \mathcal{B}(\mathcal{H}_+^{\otimes N}) \to \mathcal{B}(\mathcal{H}^{\otimes M})$. Let the map $\widetilde{T}$ and its dual $\widetilde{T}_*$ be the permutation averages of the cloning map. They are defined by*

$$\widetilde{T}(A) := \frac{1}{M!}\sum_{\pi\in\mathfrak{S}_M} T(P_\pi A P_\pi^*) \qquad ; \qquad \widetilde{T}_*(\rho) := \frac{1}{M!}\sum_{\pi\in\mathfrak{S}_M} P_\pi T_*(\rho) P_\pi^* \tag{5.7}$$

where $A \in \mathcal{B}(\mathcal{H}^{\otimes M})$ and $\rho \in \mathcal{S}(\mathcal{H}_+^{\otimes N})$.

This is again an quantum operation and this map has the property that $\mathcal{F}(\widetilde{T}_*) = \mathcal{F}(T_*)$ and $\Delta_{one}(\widetilde{T}) \leq \Delta_{one}(T)$, i.e. $\widetilde{T}$ performs at least as well as T.

Proof. We first prove that the fidelity is invariant under the permutation averaging. We write out:

$$\mathcal{F}(\widetilde{T}_*) = \inf_{\sigma,\text{ pure}} \frac{1}{M!} \sum_{\pi\in\mathfrak{S}_M} \operatorname{Tr}\left[\sigma^{\otimes M} P_\pi T_*(\sigma^{\otimes N}) P_\pi^*\right] = \inf_{\sigma,\text{ pure}} \frac{1}{M!} \sum_{\pi\in\mathfrak{S}_M} \operatorname{Tr}\left[P_\pi^* \sigma^{\otimes M} P_\pi T_*(\sigma^{\otimes N})\right] \tag{5.8}$$

where we have used the cyclic property of the trace. We claim that $P_\pi^* \sigma^{\otimes M} P_\pi = \sigma^{\otimes M}$ for any $\pi \in \mathfrak{S}_M$. Intuitively, this can be understood because $\sigma^{\otimes M}$ projects a column vector in $\mathcal{H}^{\otimes M}$ onto a one-dimensional space, and this projection is permutation invariant. The claim is further worked out in the Appendix, A.2.1. But then, we directly see that $\mathcal{F}(\widetilde{T}_*) = \mathcal{F}(T)$. This result is quite intuitive, as the fidelity looks at the entire system combined, and thus would not care for rearrangement of the individual quantum clones.

We now prove that $\Delta_{\text{one}}(\widetilde{T}) \leq \Delta_{\text{one}}(T)$.

$$\Delta_{\text{one}}(\widetilde{T}) = \sup_{a,\psi,k} \left| \langle \psi^{\otimes N} \ , \ \left(\frac{1}{M!} \sum_{\pi\in\mathfrak{S}_M} T(P_\pi a_{(k)} P_\pi^*) \right) \psi^{\otimes N} \rangle - \langle \psi \ , \ a\psi \rangle \right| = \tag{5.9}$$

$$\frac{1}{M!} \sup_{a,\psi,k} \left| \sum_{\pi\in\mathfrak{S}_M} \left(\langle \psi^{\otimes N} \ , \ T(P_\pi a_{(k)} P_\pi^*) \ \psi^{\otimes N} \rangle - \langle \psi \ , \ a\psi \rangle \right) \right| \tag{5.10}$$

We claim that $P_\pi a_{(k)} P_\pi^* = a_{(\pi(k))}$. This claim is further worked out in the Appendix A.3.1. Note that this is intuitive: first we apply a permutation to shift the clones, then we apply $a_{(k)}$ (but not on clone k anymore, instead on clone $\pi(k)$), then we shift all clones back to their original position.

Further note that the absolute value of a sum is smaller than the sum of absolute values, so we can estimate:

$$\Delta_{\text{one}}(\widetilde{T}) \leq \frac{1}{M!} \sup_{a,\psi,k} \sum_{\pi\in\mathfrak{S}_M} \left| \langle \psi^{\otimes N} \ , \ T(a_{(\pi(k))}) \ \psi^{\otimes N} \rangle - \langle \psi \ , \ a\psi \rangle \right| \tag{5.11}$$

Furthermore, a supremum over a sum is smaller than the sum over the supremum, so we can estimate:

$$\Delta_{\text{one}}(\widetilde{T}) \leq \frac{1}{M!} \sum_{\pi\in\mathfrak{S}_M} \sup_{a,\psi,k} \left| \langle \psi^{\otimes N} \ , \ T(a_{(\pi(k))}) \ \psi^{\otimes N} \rangle - \langle \psi \ , \ a\psi \rangle \right| \tag{5.12}$$

We can evaluate this supremum - it is exactly $\Delta_{\text{one}}(T)$, as the only difference is $\pi(k)$, but we are free to choose k in the supremum. Thus, we indeed see:

$$\Delta_{\text{one}}(\widetilde{T}) \leq \frac{1}{M!} \sum_{\pi\in\mathfrak{S}_M} \Delta_{\text{one}}(T) = \Delta_{\text{one}}(T) \tag{5.13}$$

□

Note that $\widetilde{T}$ itself, an *average* over permutations, is now *invariant* under permutations: let any $\sigma \in \mathfrak{S}_M$, then

$$\widetilde{T}(P_\sigma A P_\sigma^*) = \frac{1}{M!} \sum_{\pi\in\mathfrak{S}_M} T\left(P_\pi P_\sigma A P_\sigma^* P_\pi^*\right) = \frac{1}{M!} \sum_{\tau\in\mathfrak{S}_M} T(P_\tau A P_\tau^*) = \widetilde{T}(A) \tag{5.14}$$

where we have used $P_\pi P_\sigma = P_{\pi\sigma}$ and $P_\sigma^* P_\pi^* = P_{\sigma^{-1}} P_{\pi^{-1}} = P_{(\pi\sigma)^{-1}} = P_{\pi\sigma}^*$, and changed the summation variable as the map $\pi \mapsto \pi\sigma := \tau$ is bijective. A similar argument holds for $\widetilde{T}_*$.

Analogously to averaging the cloning map over permutations, it is possible to average over unitary transformations. However, whilst the permutation representation comes from the finite group $\mathfrak{S}_M$, the unitary representation is of the infinite (but compact, see [Hal15, Section 1.3]) group $\mathrm{U}(d)$: it is thus imperative we first state what we precisely mean by averaging over this group. The summation is changed to integration, and we should choose a measure such that the averaged cloning map has the unitary covariance property. This happens when the measure is left-invariant, and this measure is uniquely specified (up to multiplication by a real number) for locally compact groups: this is the Haar measure [KS09, page 34]. For example, in the case we choose the group $\mathbb{R}$ with addition as group operation (which is locally compact), the Lebesgue measure is a Haar measure. In our case, we choose the compact group $\mathrm{U}(d)$, and in the compact case the Haar measure is also right-invariant. In the compact case, we can also normalize the Haar measure. Let us first specify the unitary averaging of a cloning map, and then show unitary covariance of the new cloning map, which will use the invariance-property of the Haar measure.

Theorem 5.2.2 (Unitary average of an optimal cloning device). *Given any quantum operation $T_* : \mathcal{B}(\mathcal{H}_+^{\otimes N}) \to \mathcal{B}(\mathcal{H}^{\otimes M})$. Let the map $\overline{T}$ and its dual $\overline{T}_*$ be the unitary averages of the cloning map. They are defined by*

$$\overline{T}(A) = \int_{U(d)} u^{*\otimes N} T(u^{\otimes M} A u^{*\otimes M}) u^{\otimes N} \ du \tag{5.15}$$

$$\overline{T}_*(\rho) = \int_{U(d)} u^{*\otimes M} T(u^{\otimes N} \rho u^{*\otimes N}) u^{\otimes M} \ du \tag{5.16}$$

where again $A \in \mathcal{B}(\mathcal{H}^{\otimes M})$ and $\rho \in \mathcal{S}(\mathcal{H}_+^{\otimes N})$, and du denotes the normalized Haar measure on $U(d)$.

This is again a quantum operation and this map has the property that $\mathcal{F}(\overline{T}) \geq \mathcal{F}(T)$ and $\Delta_{one}(\overline{T}) \leq \Delta_{one}(T)$, i.e. $\overline{T}$ performs at least as well as T.

Proof. We first prove that the fidelity can only increase due to the unitary averaging. We will denote $\sigma_u := u\sigma u^*$ to shorten our expressions. Note then that $u^{\otimes N}\sigma^{\otimes N}u^{*\otimes N} = \sigma_u^{\otimes N}$. We find:

$$\mathrm{Tr}\left[\sigma^{\otimes M}\overline{T}_*\left(\sigma^{\otimes N}\right)\right] = \mathrm{Tr}\left[\sigma^{\otimes M}\int_{\mathrm{U}(d)} u^{*\otimes M} T_*(\sigma_u^{\otimes N}) u^{\otimes M} \ \mathrm{d}u\right] \tag{5.17}$$

We can swap the trace and the integral as both are linear:

$$\mathrm{Tr}\left[\sigma^{\otimes M}\overline{T}_*\left(\sigma^{\otimes N}\right)\right] = \int_{\mathrm{U}(d)} \mathrm{Tr}\left[\sigma^{\otimes M} u^{*\otimes M} T_*\left(\sigma_u^{\otimes N}\right) u^{\otimes M}\right] \ \mathrm{d}u \tag{5.18}$$

using the cyclic property of the trace, the integrand now becomes $\mathrm{Tr}\left[\sigma_u^{\otimes M} T_*\left(\sigma_u^{\otimes N}\right)\right]$. Note that σ_u is also a pure state, so by definition we have

$$\mathrm{Tr}\left[\sigma_u^{\otimes M} T_*\left(\sigma_u^{\otimes N}\right)\right] \geq \mathcal{F}(T_*) \qquad \forall \sigma \in \mathcal{S}(\mathcal{H}) \ , \ \forall u \in \mathrm{U}(d) \tag{5.19}$$

using this expression in the integral expression yields:

$$\mathrm{Tr}\left[\sigma^{\otimes M}\overline{T}_*\left(\sigma^{\otimes N}\right)\right] \geq \int_{\mathrm{U}(d)} \mathcal{F}(T_*) \ \mathrm{d}u = \mathcal{F}(T_*) \qquad \forall \sigma \in \mathcal{S}(\mathcal{H}) \tag{5.20}$$

But as this expression holds for arbitrary $\sigma \in \mathcal{S}(\mathcal{H})$, we can safely take the infimum over pure σ to find:

$$\mathcal{F}(\overline{T}_*) = \inf_{\sigma,\ \text{pure}} \ \mathrm{Tr}\left[\sigma^{\otimes M}\overline{T}_*\left(\sigma^{\otimes N}\right)\right] \geq \mathcal{F}(T_*) \tag{5.21}$$

Furthermore, we will prove $\Delta_{\text{one}}(\overline{T}) \leq \Delta_{\text{one}}(T)$.

$$\Delta_{\text{one}}(\overline{T}) = \sup_{a,\psi,k} \left| \langle \psi^{\otimes N} \ , \int_{\mathrm{U}(d)} u^{*\otimes N} T(u^{\otimes M} a_{(k)} u^{*\otimes M}) u^{\otimes N} \ \mathrm{d}u \ , \ \psi^{\otimes N} \rangle - \langle \psi, a\psi \rangle \right| \tag{5.22}$$

due to linearity, we can rewrite this to

$$\Delta_{\text{one}}(\overline{T}) = \sup_{a,\psi,k} \left| \int_{\mathrm{U}(d)} \langle \psi^{\otimes N} \ , \ u^{*\otimes N} T(u^{\otimes M} a_{(k)} u^{*\otimes M}) u^{\otimes N} \ , \ \psi^{\otimes N} \rangle - \langle \psi, a\psi \rangle \ \mathrm{d}u \right| \tag{5.23}$$

As the absolute value of an integral is smaller than the integral over the absolute value of its integrand, so we can estimate this by:

$$\Delta_{\text{one}}(\overline{T}) \leq \sup_{a,\psi,k} \int_{\mathrm{U}(d)} \left| \langle \psi^{\otimes N} \ , \ u^{*\otimes N} T(u^{\otimes M} a_{(k)} u^{*\otimes M}) u^{\otimes N} \ , \ \psi^{\otimes N} \rangle - \langle \psi, a\psi \rangle \right| \ \mathrm{d}u \tag{5.24}$$

Furthermore, the supremum over an integral is smaller than the integral over a supremum, so:

$$\Delta_{\text{one}}(\overline{T}) \leq \int_{\mathrm{U}(d)} \sup_{a,\psi,k} \left| \langle \psi^{\otimes N} \ , \ u^{*\otimes N} T(u^{\otimes M} a_{(k)} u^{*\otimes M}) u^{\otimes N} \ , \ \psi^{\otimes N} \rangle - \langle \psi, a\psi \rangle \right| \ \mathrm{d}u \tag{5.25}$$

but now we see an interesting property: $u^{\otimes N} |\psi^{\otimes N}\rangle = |\phi^{\otimes N}\rangle$ is again a pure state, and we take the supremum over all pure states (with unity norm, but unitary transformations preserve length). Furthermore, $u^{\otimes M} a_{(k)} u^{*\otimes M} = (uau^*)_{(k)}$, and uau^* is again an observable. As we take the supremum over all observables (with $0 \leq a \leq \mathrm{Id}_{\mathcal{H}}$, but again unitary transformations do not change eigenvalues and thus do not alter this property), this unitary shift does not matter. Note that we can rewrite the last expectation value as

$$\langle \psi, a\psi \rangle = \langle \psi u^* \ uau^* \ u\psi \rangle \tag{5.26}$$

so indeed we see that the entire expression over which we take the supremum has been shifted by a unitary transformation. As this does not matter for a supremum, we find:

$$\Delta_{\text{one}}(\overline{T}) \leq \int_{\mathrm{U}(d)} \Delta_{\text{one}}(T) \ \mathrm{d}u = \Delta_{\text{one}}(T) \tag{5.27}$$

□

To show that the unitary average cloning map has the unitary covariance property, we can compute, for any unitary transformation $v \in \mathrm{U}(d)$:

$$\overline{T}(v^{\otimes M} A v^{*\otimes M}) = \int_{\mathrm{U}(d)} u^{*\otimes N} T(u^{\otimes M} v^{\otimes M} A v^{*\otimes M} u^{*\otimes M}) u^{\otimes N} \ \mathrm{d}u \tag{5.28}$$

This should equal $v^{\otimes N} \overline{T}(A) v^{*\otimes N}$, and we can compute:

$$v^{\otimes N} \overline{T}(A) v^{*\otimes N} = \int_{\mathrm{U}(d)} v^{\otimes N} u^{*\otimes N} T(u^{\otimes M} A u^{*\otimes M}) u^{\otimes N} v^{*\otimes N} \ \mathrm{d}u \tag{5.29}$$

Let $w := uv^*$ (and thus $w^* = vu^*$), then $u^{\otimes N} v^{*\otimes N} = w^{\otimes N}$, and we see that we can write:

$$v^{\otimes N} \overline{T}(A) v^{*\otimes N} = \int_{\mathrm{U}(d)} w^{*\otimes N} T\left[w^{\otimes M} v^{\otimes M} A v^{*\otimes M} w^{*\otimes M} \right] w^{\otimes N} \ \mathrm{d}u \tag{5.30}$$

Now the useful property of the Haar measure becomes apparent: as w is just a right-multiplication of the integration variable u with some (fixed) group element v^*, the translation-invariance of the Haar measure tells us that this integral has precisely the same result as Equation 5.28. Thus indeed, the averaged cloning map $\overline{T}$ has the unitary covariance property.

6

Description of the optimal cloning device

In this chapter, we will look more in-depth at the proposed optimal cloning device: firstly, we must verify that it is an admissible device (that is, we must verify it is a valid *quantum operation*). Secondly, we check that this optimal cloning device is indeed permutation invariant and has the unitary covariance property, as described in the previous chapter. Lastly, we will calculate its fidelity directly, and also calculate its *Black Cow Factor*, the defining factor for calculating Δ_{one}. For convenience, we restate:

$$\hat{T}_*(\rho) = \frac{d[N]}{d[M]} \, S_M \left(\rho \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)} \right) S_M \tag{6.1}$$

where $\rho \in \mathcal{S}(\mathcal{H}_+^{\otimes N})$, $S_M : \mathcal{H}^{\otimes M} \to \mathcal{H}_+^{\otimes M}$ is the symmetric projection from the output space to its symmetric (permutation invariant) subspace, and for any $n \in \mathbb{Z}_{>0}$ we let $d[n] = \binom{d+n-1}{n}$ denote the dimension of the symmetric subspace $\mathcal{H}_+^{\otimes n}$.

6.1. Proof that the proposed map $\hat{T}_*$ is a quantum operation

Before proceeding in our proof of the optimality of $\hat{T}$, we should prove that $\hat{T}$ itself is an quantum operation. From its construction, it is clear that the map is linear. We must thus prove that $\hat{T}_*$ is completely positive and trace preserving (CPTP), which would make it a quantum operation.

6.1.1. Proof that $\hat{T}_*$ is completely positive

The cloning map $\hat{T}_*$ appears to exist of a composition of two operations: first, tensoring on $(M-N)$ quantum systems in the maximally mixed state (up to normalization), and then projecting this system to the symmetric subspace. If we can prove that both these operations are completely positive, then their composition (and thus $\hat{T}_*$), should also be completely positive. To prove this, we can invoke two Lemmas by [Maa04, page 37]:

Lemma 6.1.1. *If $f : \mathcal{B}(\mathcal{H}_+^{\otimes N}) \to \mathcal{B}(\mathcal{H}^{\otimes M})$ is a $*$-homomorphism, i.e. $f(AB) = f(A)f(B)$ and $f(A^*) = f(A)^*$ for all $A, B \in \mathcal{B}(\mathcal{H}_+^{\otimes N})$, then f is completely positive.*

We apply this lemma to the mapping $\rho \mapsto \rho \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)}$, which is indeed a $*$-homomorphism. Furthermore, we have

Lemma 6.1.2. *If we have a linear map $V : \mathcal{H}^{\otimes M} \to \mathcal{H}^{\otimes M}$, then the map*

$$T : \mathcal{B}(\mathcal{H}^{\otimes M}) \to \mathcal{B}(\mathcal{H}^{\otimes M}) \ : \ A \mapsto V^* A V \tag{6.2}$$

is completely positive

We can apply this lemma to $S_M = V$, and note that $S_M^* = S_M$.

As compositions of completely positive maps stay completely positive, and we see that $\hat{T}_*$ is the composition of $\rho \mapsto \rho \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)}$ and $A \mapsto S_M A S_M$, up to a normalization constant. Thus, indeed, $\hat{T}_*$ must be completely positive.

6.1.2. Proof that $\hat{T}_*$ is trace preserving

This proof follows the argument of [Wer98, Section III]. In short, the proof is as follows: firstly, we rewrite the trace over $\hat{T}_*(\rho)$ to a trace over ρX for some positive operator X on $\mathcal{H}_+^{\otimes N}$. Secondly, we prove that X commutes with the unitary operators of the form $u^{\otimes N}$, and by Schur's Lemma it must thus be a multiple of the identity operator. Lastly, we prove that the multiplication constant must be 1 (i.e. X is precisely the identity operator) by explicitly calculating the trace over $\hat{T}_*(\tau_N)$, where τ_N is the maximally mixed density matrix on $\mathcal{H}_+^{\otimes N}$.

First, we rewrite $\mathrm{Tr}[\hat{T}_*(\rho)]$ to $\mathrm{Tr}\left[\rho X\right]$ for some positive operator $X \in \mathcal{B}(\mathcal{H}_+^{\otimes N})$. We can justify this in the following way: let $\{|i\rangle\}_{i=1}^{d[N]}$ be an orthonormal basis for $\mathcal{H}_+^{\otimes N}$, then we can write $\rho = \sum_i \sum_j \rho_{ij} |i\rangle \langle j|$ and similarly $X = \sum_i \sum_j x_{ij} |i\rangle \langle j|$ for some coefficients $\rho_{ij}, x_{ij} \in \mathbb{C}$. By linearity of the trace operator and by linearity of T we then find:

$$\mathrm{Tr}\left[\hat{T}_*(\rho)\right] = \sum_{i=1}^{d[N]} \sum_{j=1}^{d[N]} \rho_{ij}\, \mathrm{Tr}\left[\hat{T}_*(|i\rangle \langle j|)\right] \quad ; \quad \mathrm{Tr}\left[\rho X\right] = \sum_{i=1}^{d[N]} (\rho X)_{ii} = \sum_{i=1}^{d[N]} \sum_{j=1}^{d[N]} \rho_{ij} x_{ji} \tag{6.3}$$

We see that both expressions equal in the case we choose $x_{ij} = \mathrm{Tr}[\hat{T}_*(|j\rangle \langle i|)]$. Furthermore, X has to be positive. If not, there exists a $|\psi\rangle \in \mathcal{H}_+^{\otimes N}$ such that $\langle \psi \mid X\psi \rangle < 0$. But then we could let $\rho = |\psi\rangle \langle \psi|$ be the pure state associated with $|\psi\rangle$ (up to normalization, but this does not change the negativity of the expectation of X) , and we know certainly that $\hat{T}_*(\rho)$ is positive as we already have proven complete positivity, but then

$$0 \leq \mathrm{Tr}\left[\hat{T}_*(|\psi\rangle \langle \psi|)\right] = \mathrm{Tr}\left[|\psi\rangle \langle \psi| X\right] = \langle \psi \mid X\psi \rangle < 0 \tag{6.4}$$

which is impossible. Thus, X must be a positive operator.

Theorem 6.1.3. *The positive operator X commutes with $u^{\otimes N}$*

Proof. We can compute for arbitrary $A \in \mathcal{B}(\mathcal{H}^{\otimes N})$:

$$\mathrm{Tr}\left[AX\right] = \mathrm{Tr}\left[\hat{T}_*(A)\right] \overset{(1)}{=} \mathrm{Tr}\left[u^{*\otimes M} u^{\otimes M} \hat{T}_*(A)\right] \overset{(2)}{=} \mathrm{Tr}\left[u^{\otimes M} \hat{T}_*(A) u^{*\otimes M}\right] \overset{(3)}{=} \tag{6.5}$$

$$\mathrm{Tr}\left[\hat{T}_*(u^{\otimes N} A u^{*\otimes N})\right] \overset{(4)}{=} \mathrm{Tr}\left[\left(u^{\otimes N} A u^{*\otimes N}\right) X\right] \overset{(5)}{=} \mathrm{Tr}\left[A u^{*\otimes N} X u^{\otimes N}\right] \tag{6.6}$$

where (1) is justified by the fact that $u^{*\otimes M} u^{\otimes M} = \mathrm{Id}_{\mathcal{H}}^{\otimes M}$, (2) by the cyclic property of the trace, (3) by the covariant property of $\hat{T}_*$, (4) by letting X act on the new state $u^{\otimes N} A u^{*\otimes N}$ and (5) by the cyclic property of the trace.

Note that this derivation holds for an arbitrary operator $A \in \mathcal{B}(\mathcal{H}^{\otimes N})$. This can only be the case if $X = u^{*\otimes N} X u^{\otimes N}$, but then $\left[X, u^{\otimes N}\right] = 0$ □

But as $X \in \mathcal{B}(\mathcal{H}_+^{\otimes N})$, and $u^{\otimes N} = \pi_N^+(u)$, X commutes with an irreducible representation. Then, by Schur's Lemma (see Theorem 2.2.20), we must have $X = \lambda \mathrm{Id}_{\mathcal{H}_+^{\otimes N}}$ for some $\lambda \in \mathbb{C}$.

Theorem 6.1.4. $\mathrm{Tr}[\hat{T}_*(\rho)] = \mathrm{Tr}\left[\rho\right]$*, so $X = Id_{\mathcal{H}_+^{\otimes N}}$, i.e. in the previous expression $\lambda = 1$.*

Proof. It suffices to show that the trace of *some* density operator is preserved. Consider $\tau_N := d[N]^{-1} \mathrm{Id}_{\mathcal{H}_+^{\otimes N}}$, i.e. the maximally mixed state on $\mathcal{H}_+^{\otimes N}$. In the larger space $\mathcal{H}^{\otimes N}$ we can write $\tau_N = d[N]^{-1} S_N$, with S_N the projector of $\mathcal{H}^{\otimes N} \to \mathcal{H}_+^{\otimes N}$ (indeed S_N acts as the identity on $\mathcal{H}_+^{\otimes N}$). We can then compute:

$$\hat{T}_*(\tau_N) = \frac{d[N]}{d[M] \cdot d[N]} S_M \left(S_N \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes (M-N)}\right) S_M \tag{6.7}$$

We claim that $S_M(S_N \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes (M-N)}) = S_M$. Intuitively, this can be understood as follows: $S_N \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes (M-N)}$ only makes the first N copies symmetric, whilst leaving the last $(M-N)$ unchanged. If we then make all M copies symmetric with S_M, this is the same as just directly symmetrising all copies through S_M.

Formally, we can argue as follows: for each permutation operator $P'_{\pi'}$ on $\mathcal{H}^{\otimes N}$ (one of the permutations in the average of S_N) with $\pi' \in \mathfrak{S}_N$, we can view $P'_{\pi'} \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes (M-N)}$ as a permutation operator on

$\mathcal{H}^{\otimes M}$: namely, precisely the permutation $\pi \in \mathfrak{S}_M$ that leaves the last $(M-N)$ entries unchanged, and acts the same as π' on the first N entries. As discussed before, we have $S_M P_\pi = S_M$ for any $\pi \in \mathfrak{S}_M$. Thus, in particular, we have $S_M P'_{\pi'} \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)} = S_M$ for $\pi' \in \mathfrak{S}_N$. But then, by linearity this extends to sums of permutation operators of this form, and thus the argument extends to S_N.

We thus have:

$$\hat{T}_*(\tau_N) = \frac{1}{d[M]} S_M^2 = \frac{1}{d[M]} S_M = \tau_M \tag{6.8}$$

where we have $S_M^2 = S_M$ because S_M is a projector. As τ_M indeed is a valid density matrix on $\mathcal{H}^{\otimes M}$ and has unity trace, we now have:

$$1 = \mathrm{Tr}\left[\tau_M\right] = \mathrm{Tr}\left[\hat{T}_*(\tau_N)\right] = \mathrm{Tr}\left[\tau_N X\right] = \mathrm{Tr}\left[\lambda\tau_N\right] = \lambda \tag{6.9}$$

so indeed we have $X = \mathrm{Id}_{\mathcal{H}_+^{\otimes N}}$, and thus we indeed see that $\hat{T}_*$ is trace preserving. □

6.2. Permutation invariance and unitary covariance of $\hat{T}_*$

Now that we have established that $\hat{T}_*$ is indeed a quantum operation, we can check that it is permutation invariant and has the unitary covariance property. Let us first look at permutation invariance:

$$P_\pi \hat{T}_*(\rho) P_\pi^* = \frac{d[N]}{d[M]} P_\pi S_M \left(\rho \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)}\right) S_M P_\pi^* \tag{6.10}$$

and we immediately see that $P_\pi S_M = S_M$ and $S_M P_\pi^* = S_M$ because S_M is an average over all permutations. Thus indeed $P_\pi \hat{T}_*(\rho) P_\pi^* = \hat{T}_*(\rho)$.

Furthermore, the map is unitarily covariant:

$$u^{*\otimes M} \hat{T}_*\left(u^{\otimes N} \rho u^{*\otimes N}\right) u^{\otimes M} = \frac{d[N]}{d[M]} u^{*\otimes M} S_M \left[\left(u^{\otimes N} \rho u^{*\otimes N}\right) \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)}\right] S_M u^{\otimes M} \tag{6.11}$$

We now make two observations: firstly, $u^{\otimes M}$ and S_M commute: this is because $\pi_\square^{\otimes M}$ and V_π commute, and S_M is an average over V_π. Secondly, the expression in square brackets can be expanded into:

$$\left(u^{\otimes N} \rho u^{*\otimes N}\right) \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)} = u^{\otimes M}\left(\rho \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)}\right) u^{*\otimes M} \tag{6.12}$$

as $uu^* = \mathrm{Id}_{\mathcal{H}}$ on the last $M-N$ copies. We can summarize both statements into:

$$u^{*\otimes M} \hat{T}_*\left(u^{\otimes N} \rho u^{*\otimes N}\right) u^{\otimes M} = \frac{d[N]}{d[M]} S_M u^{*\otimes M}\left[u^{\otimes M}\left(\rho \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)}\right) u^{*\otimes M}\right] u^{\otimes M} S_M \tag{6.13}$$

from this expression it becomes apparent, as $u^{*\otimes M} u^{\otimes M} = \mathrm{Id}_{\mathcal{H}}^{\otimes M}$, that

$$u^{*\otimes M} \hat{T}_*\left(u^{\otimes N} \rho u^{*\otimes N}\right) u^{\otimes M} = \hat{T}_*\left(\rho\right) \tag{6.14}$$

So indeed our proposed map $\hat{T}$ cannot be improved by taking permutation averages or unitary averages.

6.3. The Black Cow Factor and fidelity of $\hat{T}_*$

So far, we have proven that $\hat{T}_*$ is indeed a quantum operation, and also has the permutation invariance and unitary covariance properties. We now focus on the performance of this cloning map: we can directly calculate the fidelity $\mathcal{F}(\hat{T}_*)$, and we can do important preliminary work for calculating $\Delta_{\text{one}}(\hat{T})$. We start with the fidelity.

6.3.1. The fidelity of $\hat{T}_*$

We can directly calculate the fidelity:

$$\mathcal{F}(\hat{T}_*) = \inf_{\sigma,\text{ pure}} \frac{d[N]}{d[M]} \operatorname{Tr}\left[\sigma^{\otimes M} S_M \left(\sigma^{\otimes N} \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)}\right) S_M\right] \tag{6.15}$$

We can use the fact that $\sigma^{\otimes M} = S_M \sigma^{\otimes M} = \sigma^{\otimes M} S_M$ as $\sigma^{\otimes M}$ is a smaller projector than S_M. The proof can be found in Appendix A.2.1. By using the cyclic property of the trace, we can thus find for any pure σ:

$$\operatorname{Tr}\left[S_M \sigma^{\otimes M} S_M \left(\sigma^{\otimes N} \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)}\right)\right] = \operatorname{Tr}\left[\sigma^{\otimes M} \left(\sigma^{\otimes N} \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)}\right)\right] = \tag{6.16}$$

$$\operatorname{Tr}\left[\left(\sigma^2\right)^{\otimes N} \otimes \sigma^{\otimes(M-N)}\right] = \operatorname{Tr}\left[\sigma^{\otimes M}\right] = 1 \tag{6.17}$$

where in the second to last equality we have used $\sigma^2 = \sigma$ as σ is a pure state. We see that the trace is even indepent of our choice of σ, and we can thus directly conclude that

$$\mathcal{F}(\hat{T}_*) = \frac{d[N]}{d[M]} \tag{6.18}$$

6.3.2. Calculating Δ_{one}: the Black Cow Factor of $\hat{T}_*$

In the proof of optimality in Chapter 7, we will calculate Δ_{one} of any optimal cloning map. This figure of merit will be rewritten in terms of what [Wer98] describes as the "Black Cow Factor", a factor that only depends on the provided cloning map.

The "Black Cow Factor" has originally been used in the description of the (more specific) problem of cloning qubits: let us thus briefly limit our objective to qubits. In this case, a (possibly mixed) density operator $\rho^{(\text{in})}$ of one qubit can be described as

$$\rho^{(\text{in})} = \frac{1}{2}\left(\mathrm{Id}_{\mathcal{H}} + \vec{s}^{\,(\text{in})} \cdot \vec{\sigma}\right) \tag{6.19}$$

where $\mathcal{H} = \mathbb{C}^2$, $\vec{s}^{\,(\text{in})}$ denotes the Bloch vector, and $\vec{\sigma}$ denotes the three Pauli matrices (which span $\mathfrak{su}(2)$, see Definitions 2.2.5). As the eigenvalues of $\rho^{(\text{in})}$ are $1/2(1 \pm \|\vec{s}^{\,(\text{in})}\|)$, all *pure states* must have $\|\vec{s}^{\,(\text{in})}\| = 1$, and all mixed states have $\|\vec{s}^{\,(\text{in})}\| < 1$. Geometrically, this means that pure states are on the surface of the Bloch sphere, whilst mixed states lie within its volume.

An important argument from [BDE$^+$98, Section II.a] states that, if we look at a quantum cloner with the unitary covariance property, then this cloner needs to treat all input states in the same way. The authors then argue that if we look at the reduced density matrix of *one* of the clones, this must be a rescaled, but *not* rotated, version of the Bloch vector of the original qubit. This is due to the property that a rotation always has two fixed points on the sphere, and the two corresponding states would be transformed in a special way by the cloner, which is not allowed by its unitary covariance property.

This argument from [BDE$^+$98] leads us to write the reduced density matrix of one output clone as (see [BEM98]):

$$\rho^{(\text{out})} = \frac{1}{2}\left(\mathrm{Id}_{\mathcal{H}} + \eta(N,M) \cdot \vec{s}^{\,(\text{in})} \cdot \vec{\sigma}\right) \tag{6.20}$$

where we now clearly see that no rotation takes place, and the Bloch vector is shrunk by a *shrinking factor* $\eta(N,M)$. In this picture, an optimal cloner would produce an $\eta(N,M)$ that is as close to 1 as possible. Also note that the shrinking of the Bloch vector means that the output state is a mixed state.

We now wish to describe a similar factor $\gamma(T)$ that coincides with the definition of $\eta(N,M)$ in the special case of qubits. To introduce this factor, we must first have a way of computing the reduced density matrix of one output clone, that no longer needs to be a qubit. In order to do so, let us first introduce the *one-site restriction* (a partial trace over all but one clone), and then a description that is similar to $\rho^{(\text{out})}$.

Definition 6.3.1 (One-site restriction). Given any density matrix $\rho \in \mathcal{S}(\mathcal{H}^{\otimes n})$ for some $n \in \mathbb{Z}_{\geq 1}$. We define $R : \mathcal{B}(\mathcal{H}^{\otimes n}) \to \mathcal{B}(\mathcal{H})$ as its one-site restriction by

$$\operatorname{Tr}\left[R(\rho)A\right] = \operatorname{Tr}\left[\rho\left(A \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(n-1)}\right)\right] \qquad \forall A \in \mathcal{B}(\mathcal{H}) \tag{6.21}$$

This one-site restriction is the partial trace over all but the first quantum copy.

We wish to find an explicit expression for $R\left(\hat{T}_*(\sigma^{\otimes N})\right)$. We prove for an arbitrary quantum operation T_* that has the unitary covariance property:

Theorem 6.3.2. *Given any quantum operation $T_* : \mathcal{S}(\mathcal{H}_+^{\otimes N}) \to \mathcal{S}(\mathcal{H}^{\otimes M})$ with unitary covariance. There exists a factor $\gamma(T)$ such that, for any pure $\sigma \in \mathcal{S}(\mathcal{H})$:*

$$R\left(T_*\left(\sigma^{\otimes N}\right)\right) = \gamma(T)\sigma + [1 - \gamma(T)]\,(1/d)Id_{\mathcal{H}} \tag{6.22}$$

Proof. Let us denote $R_T(\sigma) := R\left(T_*\left(\sigma^{\otimes N}\right)\right)$ for brevity. Choose any pure $\sigma \in \mathcal{S}(\mathcal{H})$. Define

$$S := \mathrm{Span}\,\{\sigma, \mathrm{Id}_{\mathcal{H}}\} \subset \mathcal{B}(\mathcal{H}) \qquad ; \qquad S' := \{A \in \mathcal{B}(\mathcal{H}) \mid AB = BA \quad \forall B \in S\} \tag{6.23}$$

We call S' the *commutant* (set) of S. We claim that S is a $*$-subalgebra of $\mathcal{B}(\mathcal{H})$. As S is the linear span of two elements of $\mathcal{B}(\mathcal{H})$, it is a vector space. It is also closed under matrix multiplication, as $\sigma^2 = \sigma$ as σ is a pure state, thus S is an algebra. Furthermore, $\sigma^* = \sigma$ as σ is a density matrix, thus S is closed under the involution. Thus, S is a unital $*$-subalgebra of $\mathcal{B}(\mathcal{H})$, and as $\mathcal{H}$ is finite-dimensional, we have a variant of the Von Neumann bicommutant theorem: $S'' := (S')' = S$. See for example [Jon09, page 12]. Note that S' simply consists of all operators that commute with σ, as all operators trivially commute with (multiples of) $\mathrm{Id}_{\mathcal{H}}$.

We now claim that $R_T(\sigma) \in S''$. As $S'' = S$, it then directly follows that $R_T(\sigma)$ is a linear combination of σ and $\mathrm{Id}_{\mathcal{H}}$, which we would like to prove.

We first show that, by unitary covariance of T_*, we must have that $R_T(\sigma)$ commutes with all *unitaries* that commute with σ (that is, all unitary operators in S'). Using the covariance of T_*, we directly see that, for any unitary operator u:

$$\mathrm{Tr}\left[R_T(u\sigma u^*)A\right] = \mathrm{Tr}\left[u^{\otimes M} T_*\left(\sigma^{\otimes N}\right) u^{*\otimes M}\left(A \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(N-1)}\right)\right] \tag{6.24}$$

Using the cyclic property of the trace, we can let the unitaries first act on the observable A (tensored on by the identity), and we find

$$\mathrm{Tr}\left[R_T(u\sigma u^*)A\right] = \mathrm{Tr}\left[T_*\left(\sigma^{\otimes N}\right)\left((u^*Au) \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(N-1)}\right)\right] = \mathrm{Tr}\left[R_T(\sigma)u^*Au\right] \tag{6.25}$$

using the cyclic property of the trace again, and using the fact that this derivation holds for arbitrary observable A, we see that $R_T(u\sigma u^*) = uR_T(\sigma)u^*$. And thus indeed, if the unitary u commutes with σ, on the left-hand side we simply have $R_T(\sigma)$, and we thus find:

$$u \in S' \implies [u, \sigma] = 0 \implies [R_T(\sigma), u] = 0 \tag{6.26}$$

As a last part in our proof, we need to prove the notion that if $R_T(\sigma)$ commutes with all unitary operators in S' (which we have already proven), this implies that $R_T(\sigma)$ actually commutes with *all* operators in S'. We leave this technical proof to Appendix A.4.1.

Thus, we have that $R_T(\sigma) \in S'' = S$. Thus, we must have

$$R_T(\sigma) = \alpha\sigma + \beta\mathrm{Id}_{\mathcal{H}} \tag{6.27}$$

as $R_T(\sigma) \in \mathcal{S}(\mathcal{H})$, it must have unity trace. The trace of σ is unity, the trace of $\mathrm{Id}_{\mathcal{H}}$ is d, thus we see that $\alpha + d\beta = 1$. We call $\alpha := \gamma(T, \sigma)$ and we find:

$$R_T(\sigma) = \gamma(T,\sigma)\sigma + \frac{1 - \gamma(T,\sigma)}{d}\mathrm{Id}_{\mathcal{H}} \tag{6.28}$$

We only need to prove that the factor $\gamma(T, \sigma)$ is actually independent of our choice of σ. Note that for any two pure density matrices σ and ρ, we can always find a unitary such that $u\sigma u^* = \rho$, thus we only need to prove that $\gamma(T, \sigma) = \gamma(T, u\sigma u^*)$ for arbitrary σ and u. We can use the covariance property of T_* to reach this goal:

$$R_T(u\sigma u^*) = \gamma(T, u\sigma u^*)u\sigma u^* + \frac{1 - \gamma(T, u\sigma u^*)}{d}\mathrm{Id}_{\mathcal{H}} \tag{6.29}$$

We have already shown that this must equal $uR_T(\sigma)u^*$, and we have:

$$uR_T(\sigma)u^* = u\left(\gamma(T,\sigma)\sigma + \frac{1-\gamma(T,\sigma)}{d}\mathrm{Id}_{\mathcal{H}}\right)u^* = \gamma(T,\sigma)u\sigma u^* + \frac{1-\gamma(T,\sigma)}{d}\mathrm{Id}_{\mathcal{H}} \tag{6.30}$$

Equating both expressions, and taking both identity operators to one side, we find:

$$\left[\gamma(T,u\sigma u^*) - \gamma(T,\sigma)\right]u\sigma u^* = \frac{1}{d}\left[\gamma(T,u\sigma u^*) - \gamma(T,\sigma)\right]\mathrm{Id}_{\mathcal{H}} \tag{6.31}$$

so either $u\sigma u^* = \frac{1}{d}\mathrm{Id}_{\mathcal{H}} \implies \sigma = \frac{1}{d}\mathrm{Id}_{\mathcal{H}}$, in which trivially $\gamma(T,u\sigma u^*) = \gamma(T,\sigma)$, or indeed $\gamma(T,u\sigma u^*) = \gamma(T,\sigma)$. So in either case, we have $\gamma(T,u\sigma u^*) = \gamma(T,\sigma)$, and we can thus conclude that γ is only dependent on T, not on σ. □

We now have the tools to connect the shrinking factor $\eta(N,M)$ from the beginning of this subsection to the *Black Cow Factor* $\gamma(T)$, by the following observation:

Corollary 6.3.3 (Black Cow Factor and shrinking factor). *The Black Cow Factor $\gamma(T)$ equals $\eta(N,M)$ in the qubit case $d=2$*

Proof. Firstly, let us rewrite the qubit case, where we assume the input qubit to be in a pure state $|\psi\rangle\langle\psi|$ [BDE+98, Section I]:

$$\rho^{(\text{out})} = \eta\,|\psi\rangle\langle\psi| + (1-\eta)\cdot(1/2)\mathrm{Id}_{\mathcal{H}} \quad \text{where} \quad |\psi\rangle\langle\psi| := \frac{1}{2}\left(\mathrm{Id}_{\mathcal{H}} + \vec{s}^{\,(\text{in})}\cdot\vec{\sigma}\right) \tag{6.32}$$

If we compare this with the one-site restriction, where $\sigma = |\psi\rangle\langle\psi|$:

$$R\left(T_*\left(\sigma^{\otimes N}\right)\right) = \gamma(T)\,|\psi\rangle\langle\psi| + (1-\gamma(T))\cdot(1/d)\mathrm{Id}_{\mathcal{H}} \tag{6.33}$$

then we directly see that indeed these expressions overlap in the case $d=2$, and more generally seem to describe the same phenomenon: the shrinking factor and Black Cow Factor give a measure to the amount of information lost by cloning if we look at an individual clone: in the perfect (impossible) case, we would lose no information and thus $\gamma(T)=1$, and in the worst case, we would lose all information and $\gamma(T)=0$, resulting in a reduced density matrix equal to the maximally mixed state. □

From this construction of the one-site restriction of $\hat{T}_*$, we can now actually calculate $\gamma(\hat{T}_*)$.

Theorem 6.3.4. *We have $\gamma(\hat{T}) = \frac{N}{N+d}\cdot\frac{M+d}{M}$*

Proof. This proof follows the argument of [Wer98]. In order to calculate $\gamma(\hat{T})$, we calculate $\mathrm{Tr}\left[\sigma R_T(\sigma)\right]$ in two ways. First, note that

$$\mathrm{Tr}\left[\sigma R\left(\hat{T}_*\left(\sigma^{\otimes N}\right)\right)\right] = \mathrm{Tr}\left[\gamma(\hat{T})\sigma^2 + \frac{1-\gamma(\hat{T})}{d}\sigma\right] = \gamma(\hat{T}) + \frac{1-\gamma(\hat{T})}{d} \tag{6.34}$$

On the other hand, we can also manually compute:

$$\mathrm{Tr}\left[\sigma R\left(\hat{T}_*\left(\sigma^{\otimes N}\right)\right)\right] = \mathrm{Tr}\left[\hat{T}_*\left(\sigma^{\otimes N}\right)\left(\sigma\otimes\mathrm{Id}_{\mathcal{H}}^{\otimes(M-1)}\right)\right] \tag{6.35}$$

by definition of R. Note that $\hat{T}_*$ outputs systems in $\mathcal{H}_+^{\otimes M}$, thus it does not matter which clone we test in the trace. We can express this as:

$$\mathrm{Tr}\left[\hat{T}_*\left(\sigma^{\otimes N}\right)\left(\sigma\otimes\mathrm{Id}_{\mathcal{H}}^{\otimes(M-1)}\right)\right] = \frac{1}{M}\,\mathrm{Tr}\left[\sum_{k=1}^{M}\sigma_{(k)}\hat{T}_*\left(\sigma^{\otimes N}\right)\right] \tag{6.36}$$

where, per usual, $\sigma_{(k)} := \mathrm{Id}_{\mathcal{H}}^{\otimes(k-1)}\otimes\sigma\otimes\mathrm{Id}_{\mathcal{H}}^{\otimes(M-k)}$.

This is a useful expression when we substitute in the expression for $\hat{T}_*$:

$$\frac{1}{M}\,\mathrm{Tr}\left[\sum_{k=1}^{M}\sigma_{(k)}\hat{T}_*\left(\sigma^{\otimes N}\right)\right] = \frac{d[N]}{d[M]\cdot M}\,\mathrm{Tr}\left[\sum_{k=1}^{M}\sigma_{(k)}S_M\left(\sigma^{\otimes N}\otimes\mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)}\right)S_M\right] \tag{6.37}$$

Namely, $\sum_{k=1}^{M}\sigma_{(k)}$ commutes with permutations, and by linearity commutes with S_M. We thus look at traces of the form

$$\mathrm{Tr}\left[S_M\sigma_{(k)}\left(\sigma^{\otimes N}\otimes\mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)}\right)S_M\right] \tag{6.38}$$

In the case $1 \leq k \leq N$, we simply apply σ to σ in the k-th index, and as $\sigma^2 = \sigma$ as it is a pure state, for all these cases applying $\sigma_{(k)}$ changes nothing. Thus for these first N cases we have

$$\operatorname{Tr}\left[S_M\left(\sigma^{\otimes N} \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)}\right) S_M\right] = \frac{d[M]}{d[N]} \operatorname{Tr}\left[\hat{T}_*\left(\sigma^{\otimes N}\right)\right] = \frac{d[M]}{d[N]} \tag{6.39}$$

In the case $N < k \leq M$, we apply σ to the identity operator, and thus end with a tensor product in which σ is present on $N+1$ places. Note that the *order* in which the tensor product state is presented to S_M does not actually matter; only the amount of places in which σ is present affects the outcome. Namely, for any $N < k \leq M$, take the permutation $\pi \in \mathfrak{S}_M$ that transposes the entries $N+1$ and k. Then applying V_π results in $\sigma^{\otimes(N+1)} \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-N-1)}$. But we have already argued that $S_M V_\pi = S_M$ for any V_π, thus we can simply write:

$$S_M\left[\sigma_{(k)}\left(\sigma^{\otimes N} \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)}\right)\right] S_M = S_M\left(\sigma^{\otimes(N+1)} \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-N-1)}\right) S_M \tag{6.40}$$

Identifying this with the cloning map $\hat{T}_*$ if it would take in $N+1$ clones, we follow the same argument as the previous case to determine that the trace must equal

$$\operatorname{Tr}\left[S_M \sigma_{(k)}\left(\sigma^{\otimes N} \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)}\right) S_M\right] = \frac{d[M]}{d[N+1]} \tag{6.41}$$

We can then combine these cases to find:

$$\frac{1}{M} \operatorname{Tr}\left[\sum_{k=1}^{M} \sigma_{(k)} \hat{T}_*\left(\sigma^{\otimes N}\right)\right] = \frac{d[N]}{d[M] \cdot M}\left(N \frac{d[M]}{d[N]} + (M-N) \frac{d[M]}{d[N+1]}\right) \tag{6.42}$$

By equating the expression for $\gamma(\hat{T})$ and the expression above, we can find (for a tedious derivation, see Appendix A.5.1)

$$\gamma(\hat{T}) = \frac{N}{N+d} \cdot \frac{M+d}{M} \tag{6.43}$$

□

In the most atomic situation of copying one qubit to two qubits, the resulting Black Cow Factor equals $(1/3) \cdot (4/2) = 2/3$, which is equal to the optimal value of the shrinking factor η found by for example [BDE+98].

7

Proof of optimality

Thus far, we have seen certain characteristics of the proposed cloning map, such as its fidelity and its permutation covariance. We now have enough mathematical tools and have laid the foundations for the main purpose of this paper: to prove that the proposed map is indeed optimal with respect to the figures of merit. In this chapter, we will prove these assertions.

7.1. Proof of optimality with respect to fidelity

Theorem 7.1.1. *[Wer98] Given any quantum operation $T_* : \mathcal{S}(\mathcal{H}_+^{\otimes N}) \to \mathcal{S}(\mathcal{H}^{\otimes M})$. This quantum operation has*

$$\mathcal{F}(T) := \inf_{\sigma\ ,\ pure} \operatorname{Tr}\left[\sigma^{\otimes M} T_*(\sigma^{\otimes N})\right] \leq \frac{d[N]}{d[M]} \tag{7.1}$$

with equality iff $T = \hat{T}$

Let us first discuss an outline of the proof. Note that the proposed optimal cloning map $\hat{T}_*$ outputs quantum states on $\mathcal{H}_+^{\otimes M}$, so it would be natural to look for a way to assert that *any* optimal cloning map must have this property. In order to do so, we can split $\mathcal{H}^{\otimes M}$ in the direct sum of $\mathcal{H}_+^{\otimes M}$ and its orthogonal complement. By choosing the maximally mixed state on $\mathcal{H}_+^{\otimes N}$ as input and using Schur's lemma, we can prove that the part of the output state supported by $\mathcal{H}_+^{\otimes M}$ must be a scalar multiple of the identity operator. Further note that $\sigma^{\otimes M}$ is a state on $\mathcal{H}_+^{\otimes M}$ (and thus orthogonal to any state on its orthogonal complement), so in calculating the fidelity, the part of the output state supported by the orthogonal complement of $\mathcal{H}_+^{\otimes M}$ does not contribute anything. Thus, for a cloning map to be optimal, a maximally mixed input state should be mapped to the maximally mixed state on $\mathcal{H}_+^{\otimes M}$. From this observation, the fidelity inequality will follow, and we can also show that this constraint is powerful enough to completely fix the behaviour of the cloning map, proving that there is a unique quantum operation with optimal fidelity.

Proof of the fidelity inequality. Assume T_* is optimal with respect to $\mathcal{F}$. Such a cloning map exists by Appendix A.6.1. We will first show that we must have $\overline{T}_*(\tau_N) = \tau_M$, i.e. the maximally mixed state $\tau_N := d[N]^{-1}S_N$ is imaged on $\tau_M := d[M]^{-1}S_M$, thus also directly showing that the output state is supported by $\mathcal{H}_+^{\otimes M}$ (which is *not* an a priori requirement). From this it will follow that indeed the fidelity is bounded from above by $d[N]/d[M]$.

Let us consider τ_N on $\mathcal{H}_+^{\otimes N}$. We have already seen that S_N (and thus τ_N) commutes with all unitaries $u^{\otimes N}$, and by covariance of $\overline{T}_*$ we have:

$$\overline{T}_*(\tau_N) = \overline{T}_*\left(u^{\otimes N}\tau_N u^{*\otimes N}\right) = u^{\otimes M}\overline{T}_*\left(\tau_N\right)u^{*\otimes M} \qquad \Longleftrightarrow \left[\overline{T}_*(\tau_N), u^{\otimes M}\right] = 0 \quad \forall u \in \mathrm{U}(d) \tag{7.2}$$

We know that $\overline{T}(\tau_N)$ must produce a density matrix on $\mathcal{H}^{\otimes M}$. We can split this output space into $\mathcal{H}_+^{\otimes M}$ and its orthogonal complement. But we have seen that $\left(\pi_M^+, \mathcal{H}_+^{\otimes M}\right)$ is an irreducible representation, and as the output needs to commute with $\pi_M^+(u)$ for all $u \in \mathrm{U}(d)$, the output on this subspace thus needs to be a multiple of the identity on $\mathcal{H}_+^{\otimes M}$ by Schur's Lemma (see Definitions 2.2.20). We can thus write:

$$\overline{T}_*(\tau_N) = \frac{\lambda}{d[M]} S_M + (1-\lambda)\chi \tag{7.3}$$

where $S_M = \mathrm{Id}_{\mathcal{H}_+^{\otimes M}}$, and χ is a density matrix on the orthogonal complement of $\mathcal{H}_+^{\otimes M}$, and $0 \leq \lambda \leq 1$.

We can now use the useful fact that if we trace over this quantity with $\sigma^{\otimes M}$, the χ-term will cancel as χ is orthogonal to all density matrices on $\mathcal{H}_+^{\otimes M}$.

Furthermore, we change to argument of $\overline{T}_*$ to $S_N - \sigma^{\otimes N}$. We know this must a positive operator, as $\sigma^{\otimes N}$ is a projection whose range is contained in the range of projection S_N. We thus find:

$$0 \leq \operatorname{Tr}\left[\sigma^{\otimes M}\overline{T}_*\left(S_N - \sigma^{\otimes N}\right)\right] = d[N]\operatorname{Tr}\left[\sigma^{\otimes M}\overline{T}_*(\tau_N)\right] - \operatorname{Tr}\left[\sigma^{\otimes M}\overline{T}_*\left(\sigma^{\otimes N}\right)\right] \tag{7.4}$$

The first trace evaluates to $\lambda d[N]/d[M]\operatorname{Tr}\left[\sigma^{\otimes M}S_M\right]$, and as we know $\sigma^{\otimes M}S_M = \sigma^{\otimes M}$, this just leaves us with the constant factor.

The second trace has a familiar form: its infimum over σ is precisely $\mathcal{F}(\overline{T})$. An important observation is the following: for all pure states σ and ρ on $\mathcal{H}$, we can find a unitary transformation u such that $u\sigma u^* = \rho$. Let us denote $\sigma_u := u\sigma u^*$. We can then compute:

$$\operatorname{Tr}\left[\sigma^{\otimes M}\overline{T}_*\left(\sigma^{\otimes N}\right)\right] = \int_{\mathrm{U}(d)} \operatorname{Tr}\left[\sigma_u^{\otimes M}T_*\left(\sigma_u^{\otimes N}\right)\right]\,\mathrm{d}u = \tag{7.5}$$

$$\int_{\mathrm{U}(d)} \operatorname{Tr}\left[\rho_u^{\otimes M}T_*\left(\rho_u^{\otimes N}\right)\right]\,\mathrm{d}u = \operatorname{Tr}\left[\rho^{\otimes M}\overline{T}_*\left(\rho^{\otimes N}\right)\right] \tag{7.6}$$

Thus we see that this trace is actually independent of our choice of σ. Thus, we can substitute $\mathcal{F}(\overline{T}) = \hat{\mathcal{F}}$ in place of the second trace. We then find:

$$0 \leq \lambda\frac{d[N]}{d[M]} - \hat{\mathcal{F}} \qquad \Longrightarrow \hat{\mathcal{F}} \leq \lambda\frac{d[N]}{d[M]} \leq \frac{d[N]}{d[M]} \tag{7.7}$$

with equality for the last part for $\lambda = 1$. Thus indeed, $\overline{T}_*(\tau_N) = \tau_M$ in the optimal case, and $\hat{\mathcal{F}} \leq d[N]/d[M]$. □

Proof of the fidelity equality. We are left with proving that *if* a cloner has the optimal fidelity, it must be the optimal cloning map $\hat{T}$ that we have already found.

From the previous proof, we must have $\lambda = 1$ in the case of optimality. But then, for any $\sigma^{\otimes N}$ input state, $\overline{T}_*$ must output a state on $\mathcal{H}_+^{\otimes M}$. As permutations and unitary operations commute, the same argument holds for T_*, as $\overline{T}_*$ is just an average over all unitarily rotated copies of T_*. Looking at the last inequality with $\lambda = 1$, we see that

$$\operatorname{Tr}\left[\sigma^{\otimes M}\overline{T}_*\left(S_N - \sigma^{\otimes N}\right)\right] = 0 \qquad \Longrightarrow \qquad \int_{\mathrm{U}(d)} \operatorname{Tr}\left[\sigma_u^{\otimes M}T_*\left(S_N - \sigma_u^{\otimes N}\right)\right]\,\mathrm{d}u = 0 \tag{7.8}$$

where we have used that $u^{\otimes N}S_N u^{*\otimes N} = S_N$, as they commute. The integrand is nonnegative as $T_*(S_N - \sigma_u^{\otimes N})$ is a positive operator for any σ_u, so we must have

$$\operatorname{Tr}\left[\sigma^{\otimes M}T_*\left(S_N - \sigma^{\otimes N}\right)\right] = 0 \qquad \forall\sigma \in \mathcal{S}(\mathcal{H}) \tag{7.9}$$

We can now employ Stinespring's dilation theorem (see for example [Jan10, page 18]) to write

$$T_*(\rho) = \hat{\mathcal{F}}\cdot V^*\left(\rho \otimes \mathrm{Id}_{\mathcal{K}}\right)V \qquad , \qquad \rho \in \mathcal{S}(\mathcal{H}_+^{\otimes N}) \tag{7.10}$$

for $V : \mathcal{H}_+^{\otimes M} \to \mathcal{H}_+^{\otimes N} \otimes \mathcal{K}$ and some auxiliary Hilbert space $\mathcal{K}$. Here we used the factor $\hat{\mathcal{F}}$ so that for an optimal cloner we have $V^*V = \mathrm{Id}_{\mathcal{H}_+^{\otimes M}}$. Then we can rewrite our optimality condition as:

$$\left\langle \psi^{\otimes M}\ ,\ V^*\left[\left(S_N - \sigma^{\otimes N}\right)\otimes \mathrm{Id}_{\mathcal{K}}\right]V\ ,\ \psi^{\otimes M}\right\rangle = 0 \qquad \forall\sigma = \left|\psi\right\rangle\left\langle\psi\right| \in \mathcal{S}(\mathcal{H}) \tag{7.11}$$

We wish to rewrite this to $\left\|\left[\left(S_N - \sigma^{\otimes N}\right)\otimes \mathrm{Id}_{\mathcal{K}}\right]V\psi^{\otimes M}\right\|^2 = 0$.

First note the following:

$$\left[\left(S_N-\sigma^{\otimes N}\right)\otimes \mathrm{Id}_{\mathcal{K}}\right]^2=\left(S_N^2-S_N\sigma^{\otimes N}-\sigma^{\otimes N}+\left(\sigma^2\right)^{\otimes N}\right)\otimes \mathrm{Id}_{\mathcal{K}}=\left(S_N-\sigma^{\otimes N}\right)\otimes \mathrm{Id}_{\mathcal{K}} \tag{7.12}$$

where we have used $S_N^2=S_N$ (as S_N is a projector), and $\sigma^{\otimes N}=S_N\sigma^{\otimes N}=\sigma^{\otimes N}S_N$. Intuitively, this works out as both $S_N-\sigma^{\otimes N}$ and $\mathrm{Id}_{\mathcal{K}}$ are projectors. Further note that we have $\left[\left(S_N-\sigma^{\otimes N}\right)\otimes \mathrm{Id}_{\mathcal{K}}\right]^*=\left[\left(S_N-\sigma^{\otimes N}\right)\otimes \mathrm{Id}_{\mathcal{K}}\right]$.

Thus, we can rewrite the previous statement into:

$$\langle\psi^{\otimes M}V^*\left[\left(S_N-\sigma^{\otimes N}\right)\otimes \mathrm{Id}_{\mathcal{K}}\right]^*,\left[\left(S_N-\sigma^{\otimes N}\right)\otimes \mathrm{Id}_{\mathcal{K}}\right]V\psi^{\otimes M}\rangle=\left\|\left[\left(S_N-\sigma^{\otimes N}\right)\otimes \mathrm{Id}_{\mathcal{K}}\right]V\psi^{\otimes M}\right\|^2 \tag{7.13}$$

thus the optimality condition can be expressed as $\left[\left(S_N-\sigma^{\otimes N}\right)\otimes \mathrm{Id}_{\mathcal{K}}\right]V\psi^{\otimes M}=0$. This in turn means that $V\psi^{\otimes M}$ must be in the subspace $\psi^{\otimes N}\otimes\mathcal{K}$. So $V\psi^{\otimes M}=\psi^{\otimes N}\otimes\xi(\psi)$, with some vector $\xi(\psi)\in\mathcal{K}$. Although we cannot explicitly calculated $\xi(\psi)$, we can calculate inner products:

$$\langle\phi,\psi\rangle^M=\langle\phi^{\otimes M},\psi^{\otimes M}\rangle=\langle V\phi^{\otimes M},V\psi^{\otimes M}\rangle=\langle\phi^{\otimes N}\otimes\xi(\phi)\ ,\ \psi^{\otimes N}\otimes\xi(\psi)\rangle=\langle\phi,\psi\rangle^N\langle\xi(\phi),\xi(\psi)\rangle_{\mathcal{K}} \tag{7.14}$$

Thus we have

$$\langle\xi(\phi),\xi(\psi)\rangle_{\mathcal{K}}=\langle\phi,\psi\rangle^{M-N} \tag{7.15}$$

That this derivation also holds in the case $\langle\phi,\psi\rangle=0$ is further proven in the Appendix: globally speaking, we prove that ξ depends continuously on ϕ, and thus we can take limits (see Appendix A.7.1).

Now we have all information to compute the matrix elements of the optimal cloning map. But then, the map is uniquely determined. As we have already proven that $\hat{T}$ has optimal fidelity, it must be the uniquely determined optimal cloning map with respect to the fidelity. □

Remark 7.1.2. We can also write out the matrix elements to actually check that our optimal cloning map indeed has these matrix elements:

Let T be any optimal cloning map, and take any kind of basis $\left\{|\psi_i^{\otimes M}\rangle\right\}_i$ of $\mathcal{H}_+^{\otimes M}$. Furthermore, we will consider any kind of input $|\phi^{\otimes N}\rangle\langle\phi^{\otimes N}|$. We then find:

$$\begin{aligned}\langle\psi_i^{\otimes M}|\ T_*\left(|\phi^{\otimes N}\rangle\langle\phi^{\otimes N}|\right)\ |\psi_j^{\otimes M}\rangle=\hat{\mathcal{F}}\cdot\langle\psi_i^{\otimes M}|\ V^*\left[|\phi^{\otimes N}\rangle\langle\phi^{\otimes N}|\otimes\mathrm{Id}_{\mathcal{K}}\right]V\ |\psi_j^{\otimes M}\rangle= \quad (7.16)\\ \hat{\mathcal{F}}\cdot\langle\psi_i|^{\otimes N}\otimes\langle\xi(\psi_i)|_{\mathcal{K}}\ \left[|\phi^{\otimes N}\rangle\langle\phi^{\otimes N}|\otimes\mathrm{Id}_{\mathcal{K}}\right]\ |\psi_j\rangle^{\otimes N}\otimes|\xi(\psi_j)\rangle_{\mathcal{K}}= \quad (7.17)\\ \hat{\mathcal{F}}\cdot\langle\psi_i\mid\phi\rangle^N\cdot\langle\phi\mid\psi_j\rangle^N\cdot\langle\xi(\psi_i)\mid\xi(\psi_j)\rangle_{\mathcal{K}}=\hat{\mathcal{F}}\,\langle\psi_i\mid\phi\rangle^N\cdot\langle\phi\mid\psi_j\rangle^N\cdot\langle\psi_i\mid\psi_j\rangle^{M-N} \quad (7.18)\end{aligned}$$

where, in the second equality, we have used the description of $V|\psi^{\otimes M}\rangle$.

We can now compare this with the matrix element for our optimal map $\hat{T}$:

$$\begin{aligned}\langle\psi_i^{\otimes M}|\ \hat{T}_*\left(|\phi^{\otimes N}\rangle\langle\phi^{\otimes N}|\right)\ |\psi_j^{\otimes M}\rangle=\hat{\mathcal{F}}\cdot\langle\psi_i^{\otimes M}|\ S_M\left(|\phi^{\otimes M}\rangle\langle\phi^{\otimes M}|\otimes\mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)}\right)S_M\ |\psi_j^{\otimes M}\rangle= \quad (7.19)\\ \hat{\mathcal{F}}\cdot\langle\psi_i^{\otimes M}|\ \left(|\phi^{\otimes N}\rangle\langle\phi^{\otimes N}|\otimes\mathrm{Id}_{\mathcal{H}}^{\otimes(M-N)}\right)\ |\psi_j^{\otimes M}\rangle=\hat{\mathcal{F}}\cdot\langle\psi_i\mid\phi\rangle^N\cdot\langle\psi_i\mid\psi_j\rangle^{(M-N)}\cdot\langle\phi\mid\psi_j\rangle^N \quad (7.20)\end{aligned}$$

Where in the second equality, we have used the fact that $S_M|\psi\rangle^{\otimes M}=|\psi\rangle^{\otimes M}$, as this vector is already symmetric.

By comparing the results, we indeed see that the two maps are equivalent. Thus, the only possible optimal map is indeed $\hat{T}$.

7.2. Proof of optimality with respect to single clone test

Theorem 7.2.1. *[KW99] Given any quantum operation $T:\mathcal{B}(\mathcal{H}^{\otimes M})\to\mathcal{B}(\mathcal{H}_+^{\otimes N})$. We have*

$$\Delta_{one}(T):=\sup_{a,\psi,k}\left|\langle\psi^{\otimes N}\ ,\ T\left(a_{(k)}\right)\psi^{\otimes N}\rangle-\langle\psi\ ,\ a\psi\rangle\right|\geq\frac{d-1}{d}\left|1-\frac{N}{N+d}\cdot\frac{M+d}{M}\right| \tag{7.21}$$

with equality iff $T=\hat{T}$.

To prove this theorem, we will need considerably more heavy mathematical machinery. We will develop a proof for any general Hilbert space $\mathcal{H} = \mathbb{C}^d$, but in the end we will solely focus on the qubit case $d = 2$ to optimize the cloning map. Note that we assume T to be permutation invariant and unitary covariant: if not, by Chapter 5 we can construct an average map that performs at least as well.

Let us first discuss an outline of the proof below. Our goal is to construct a way to explicitly calculate $T(a_{(k)})$, such that we can calculate Δ_{one}. We first show that this is determined by a factor $\omega(T)$ that is very closely related to the *Black Cow Factor* $\gamma(T)$ that was introduced and calculated for the proposed optimal cloning map in Section 6.3.2. The Lie group and representation theory necessary for this argument is presented in Section 7.2.1, and the calculations for $T(a_{(k)})$ in terms of $\omega(T)$ (and $\gamma(T)$) can be found in Sections 7.2.2 and 7.2.3. We can then rewrite Δ_{one} in terms of $\gamma(T)$ in Section 7.2.4. We can then shift our attention to optimizing $\gamma(T)$ (or equivalently, $\omega(T)$). To find an explicit expression for $\omega(T)$, we decompose our output space $\mathcal{H}^{\otimes M}$ into smaller (irreducible) representations, and on each of these subspaces we further decompose our cloning map using a covariant version of Stinespring's dilation theorem in Section 7.2.5. We then turn our attention to the qubit case, and with the use of total angular momentum (the Casimir element), we can find an explicit expression for $\omega(T)$ in Section 7.2.6. We are then left with optimizing this expression in Section 7.2.7, which will conclude the proof.

We start with a general observation: We have already discussed that our optimal cloning map is permutation invariant, so we know that

$$T(a_{(k)}) = \frac{1}{M} T\left(\sum_{k=1}^{M} a_{(k)}\right) \tag{7.22}$$

The right-hand side is useful, because T is applied to a generator of the Lie algebra $\mathfrak{su}(d)$. Thus, we first turn our attention to this Lie algebra:

7.2.1. The Lie algebra $\mathfrak{su}(d)$

Recall from the Definitions Chapter that the Lie algebra $\mathfrak{su}(d)$ carries a differential representation (see Definition 2.2.21) for any representation on SU(d). We are interested in the Lie algebra and its representation because of the following identification:

Theorem 7.2.2. *For any $a \in \mathcal{B}(\mathcal{H})$ with* $\operatorname{Tr}[a] = 0$ *we have*

$$\partial\pi_{\square}^{\otimes M}(a) = \sum_{k=1}^{M} a_{(k)} \tag{7.23}$$

Proof. First note that we can apply $\pi_{\square}^{\otimes M}$ to a (whilst it is not necessarily anti-Hermitian) if we uniquely extend the representation $\pi_{\square}^{\otimes M}(a)$ (and thus also $\partial\pi_{\square}^{\otimes M}(a)$) by complexification from $\mathfrak{su}(d)$ to $\mathfrak{sl}(d, \mathbb{C})$ (see Definitions 2.2.25). Furthermore, we can calculate:

$$\partial\pi_{\square}^{\otimes M}(a) := \frac{\mathrm{d}}{\mathrm{d}t}\left(e^{ta}\right)^{\otimes M}\Big|_{t=0} = \tag{7.24}$$

$$\left(\frac{\mathrm{d}}{\mathrm{d}t}e^{ta}\right) \otimes e^{ta} \otimes \cdots\Big|_{t=0} + e^{ta} \otimes \left(\frac{\mathrm{d}}{\mathrm{d}t}e^{ta}\right) \otimes e^{ta} \otimes \cdots\Big|_{t=0} + \cdots = \tag{7.25}$$

$$(a \otimes \mathrm{Id}_{\mathcal{H}} \otimes \cdots) + (\mathrm{Id}_{\mathcal{H}} \otimes a \otimes \mathrm{Id}_{\mathcal{H}} \otimes \cdots) + \cdots = \sum_{k=1}^{M} a_{(k)} \tag{7.26}$$

□

Thus, in this context we see that to calculate $T(a_{(k)})$, we can instead look at the behaviour of T on generator elements of the Lie algebra representation. We wish to connect this to the special property of the cloning map: unitary covariance. We arrive at:

Definition 7.2.3. [KW99, Section III.B] Let $\pi : G \to \mathcal{B}(\mathcal{H}_\pi)$ be a finite dimensional unitary representation of a Lie group G with Lie algebra $\mathfrak{g}$. Then $\mathfrak{g}$ is **nondenegerate** in $\mathcal{B}(\mathcal{H}_\pi)$ with respect to π if any linear operator $L : \mathfrak{g} \to \mathcal{B}(\mathcal{H}_\pi)$ with the covariance property $\pi(g)L(X)\pi(g)^* = L(gXg^{-1})$ is of the form $L(X) = \lambda \cdot \partial\pi(X)$ for some $\lambda \in \mathbb{C}$.

Remark 7.2.4. Note that this is closely related to Schur's Lemma (i.e. intertwiners between representations). One can see this as follows:

Let us first define the **adjoint representation** of a Lie group G. This is quite a special representation, because the vector space of this representation is the Lie algebra $\mathfrak{g}$ itself. Hence, it is a mapping $\mathrm{Ad} : G \to \mathrm{GL}(\mathfrak{g})$ such that it respects the group operation. The representation is given by

$$\text{Adjoint representation :} \quad (\mathrm{Ad}, \mathfrak{g}) \quad ; \quad \mathrm{Ad}(g) = g(\cdot)g^{-1} \tag{7.27}$$

where we mean that $\forall X \in \mathfrak{g}$ we have $\mathrm{Ad}(g)(X) = gXg^{-1}$. We thus see that the right hand side of the covariance property in the definition is actually the composition $L \circ \mathrm{Ad}(g)$.

Similarly, we discuss the left-hand side of the covariance property. The map $g \mapsto \pi(g)(\cdot)\pi(g)^*$ can actually be understood as the representation $\pi \otimes \pi^*$ in the following sense: L maps elements of $\mathfrak{g}$ to $\mathcal{B}(\mathcal{H}_\pi)$, and $\mathcal{B}(\mathcal{H}_\pi) \cong \mathcal{H}_\pi \otimes \mathcal{H}_\pi^*$, on which the representation $\pi \otimes \pi^*$ works. Thus, the left-hand side of the covariance property is the composition $\pi \otimes \pi^* \circ L$.

We now see that indeed the covariance property can be understood as being an intertwiner between the tensor product representation $\pi \otimes \pi^*$ and the adjoint representation Ad.

Theorem 7.2.5. *$\mathfrak{su}(d)$ is nondegenerate in $\mathcal{B}(\mathcal{H}_+^{\otimes N})$ with respect to π_N^+.*

Proof. We only sketch the proof for $d \geq 3$, and explicitly give a proof for the case $d = 2$. In the previous remark we have already done quite some work: if one can prove that the representation Ad is contained exactly once in the decomposition in irreducibles of $\pi \otimes \pi^*$, then by Schur's Lemma the theorem follows. In general this is true for $\mathfrak{su}(d)$ for any $d \geq 2$ with respect to the irreducible representation π_N^+. See [KW99, Appendix A.4]. In the following proof we will only focus on the case $d = 2$, because all irreducible representations of $\mathrm{SU}(2)$ are well-known and its tensor powers are easily decomposed into irreducibles.

In the case of $d = 2$, all possible irreducible representations can be labelled by one half-integer index, called the **total angular momentum** number $j \in \frac{1}{2}\mathbb{Z}_{\geq 0}$. Let (π_j, D_j) be those irreducible representations, where $\dim D_j = 2j+1$. We then have that π_N^+ is isomorphic to π_{2j}, which we can deduce simply by looking at dimensions, as all irreducible representations of $\mathfrak{su}(2)$ have a unique dimension:

$$\dim \mathcal{H}_+^{\otimes N} = \binom{2+N-1}{N} = N + 1 = \dim D_j \quad \text{if } N = 2j \tag{7.28}$$

Note that, as discussed in Definitions 2.2.5, $\mathfrak{su}(2)$ is spanned by the three Pauli matrices, and has thus $\dim \mathfrak{su}(2) = 3$. But, there is a unique irreducible representation with dimension 3: D_1. Thus, we must have $D_1 \cong \mathfrak{su}(2)$ if we picture both as representations, with $\mathfrak{su}(2)$ the adjoint representation.

Furthermore, because we work in finite dimensional spaces and the representations are unitary, we can identify $\mathcal{H}_\pi^* \cong \mathcal{H}_\pi$. Thus, we look at maps

$$L : \mathfrak{su}(2) \cong D_1 \to \mathcal{B}(\mathcal{H}_+^{\otimes N}) = \mathcal{B}(D_j) \cong D_j \otimes D_j^* \cong D_j \otimes D_j \qquad \text{for } j = N/2 \tag{7.29}$$

There is a beautiful decomposition of tensor products of irreducible representations in the case of $\mathfrak{su}(2)$, which is (see, for example, [FH04, page 151]):

$$D_j \otimes D_k \cong D_{|j-k|} \oplus D_{|j-k|+1} \oplus \cdots \oplus D_{j+k} \tag{7.30}$$

But then, in our case, we have:

$$D_1 \xrightarrow{L} D_0 \oplus D_1 \oplus D_2 \oplus D_3 \oplus \cdots \oplus D_{2j} \tag{7.31}$$

But, this is a mapping from an irreducible representation to the direct sum of irreducible representations. By Schur's lemma, the mapping to all spaces D_j with $j \neq 1$ must be the trivial zero map, and the mapping to the space D_1 must be a multiple of the identity. Thus, the space of admissible L is one-dimensional.

To find an expression for $L : \mathfrak{su}(2) \to \mathcal{B}(\mathcal{H}_\pi)$, we can look at the linear map $\partial\pi_N^+$, as this satisfies

$$\pi_N^+(u)\partial\pi_N^+(X)\pi_N^+(u)^* = \partial\pi_N^+\left(uXu^{-1}\right) \tag{7.32}$$

and thus we immediately see that we must have $L(X) = \lambda \cdot \partial\pi_N^+(X)$ for some $\lambda \in \mathbb{C}$. □

Corollary 7.2.6. *Let $\pi : SU(d) \to \mathcal{B}(\mathcal{H}_\pi)$ be a unitary representation, and let $T : \mathcal{B}(\mathcal{H}_\pi) \to \mathcal{B}(\mathcal{H}_+^{\otimes N})$ be a CPTP and $SU(d)$-covariant map, i.e.*

$$T(\pi(u)A\pi(u)^*) = \pi_N^+(u)T(A)\pi_N^+(u)^* \tag{7.33}$$

Then there exists a number $\omega(T)$ such that

$$T\left(\partial\pi(a)\right) = \omega(T)\sum_{k=1}^{N} a_{(k)} \tag{7.34}$$

for every $a \in \mathcal{B}(\mathcal{H})$ with $\mathrm{Tr}(a) = 0$.

Proof. We know that $\mathfrak{su}(d)$ is nondegenerate in $\mathcal{B}(\mathcal{H}_+^{\otimes N})$ with respect to π_N^+. We have the linear map

$$(T\circ\partial\pi) : \mathfrak{su}(d) \to \mathcal{B}(\mathcal{H}_+^{\otimes N}) \qquad ; \qquad \partial\pi : \mathfrak{su}(d) \to \mathcal{B}(\mathcal{H}_\pi) \tag{7.35}$$

where $\partial\pi$ is the representation of the Lie algebra $\mathfrak{su}(d)$ induced by the representation π of $\mathrm{SU}(d)$. We can check the covariance:

$$\pi_N^+(u)\left(T\circ\partial\pi\right)(X)\pi_N^+(u)^* = T\left(\pi(u)\partial\pi(X)\pi(u)^*\right) = T\left(\partial\pi(uXu^{-1})\right) \tag{7.36}$$

Thus, by the definition of nondegenerate Lie algebras, we now have:

$$T\left(\partial\pi(a)\right) = \omega(T)\partial\pi_N^+(a) \tag{7.37}$$

for some factor $\omega(T) \in \mathbb{C}$ that only depends on T. We have already seen that $\pi_N^+(a) = \sum_{k=1}^N a_{(k)}$. □

7.2.2. Explicit expression for $T(a_{(k)})$

Starting out from our wish to find a way to calculate $T(a_{(k)})$, we are now capable of calculating $T(\partial\pi_\square^{\otimes M}(a))$ by Corollary 7.2.6, and we have already seen by Theorem 7.2.2 that $\partial\pi_\square^{\otimes M}(a)$ is actually a sum over operators of the form $a_{(k)}$. Thus, we now turn our focus to expressing $T(a_{(k)})$ in terms of $\omega(T)$, such that we can express $\Delta_{\mathrm{one}}(T)$ in terms of $\omega(T)$ as well in the next sections. We follow the argument of [KW99, Section III.B]. First, for any operator $a \in \mathcal{B}(\mathcal{H})$, we find a traceless operator a' such that:

$$a = \frac{\mathrm{Tr}\,[a]}{d}\mathrm{Id}_{\mathcal{H}} + a' := \alpha\cdot\mathrm{Id}_{\mathcal{H}} + a' \quad \text{ and thus } \quad a_{(k)} = \alpha\mathrm{Id}_{\mathcal{H}}^{\otimes M} + a'_{(k)} \tag{7.38}$$

We can then calculate:

$$T\left(a_{(k)}\right) = T\left(\alpha\cdot\mathrm{Id}_{\mathcal{H}} + a'_{(k)}\right) = \alpha\mathrm{Id}_{\mathcal{H}_+^{\otimes N}} + T(a'_{(k)}) = \alpha\mathrm{Id}_{\mathcal{H}_+^{\otimes N}} + \frac{1}{M}T\left(\sum_{l=1}^{M} a'_{(l)}\right) \tag{7.39}$$

$$= \alpha\mathrm{Id}_{\mathcal{H}_+^{\otimes N}} + \frac{1}{M}T\left(\partial\pi_\square^{\otimes M}(a')\right) = \alpha\mathrm{Id}_{\mathcal{H}_+^{\otimes N}} + \frac{\omega(T)}{M}\sum_{l=1}^{N} a'_{(l)} \tag{7.40}$$

We now substitute $\alpha = \frac{\mathrm{Tr}(a)}{d}$, and we use $a' = a - \alpha\mathrm{Id}_{\mathcal{H}}$,we find:

$$T\left(a_{(k)}\right) = \frac{\mathrm{Tr}(a)}{d}\mathrm{Id}_{\mathcal{H}_+^{\otimes N}} + \frac{\omega(T)}{M}\left(\sum_{l=1}^{N} a_{(l)}\right) - \frac{N}{M}\omega(T)\frac{\mathrm{Tr}(a)}{d}\mathrm{Id}_{\mathcal{H}_+^{\otimes N}} = \tag{7.41}$$

$$\frac{\mathrm{Tr}(a)}{d}\left(1 - \frac{N\omega(T)}{M}\right)\mathrm{Id}_{\mathcal{H}_+^{\otimes N}} + \frac{\omega(T)}{M}\left(\sum_{l=1}^{N} a_{(l)}\right) \tag{7.42}$$

7.2.3. Connection between γ and ω

Before we proceed, we can point out a very specific connection between the factors $\omega(T)$ and $\gamma(T)$ for any quantum operation $T_* : \mathcal{S}(\mathcal{H}_+^{\otimes N}) \to \mathcal{S}(\mathcal{H}^{\otimes M})$ with the unitary covariance property:

Theorem 7.2.7. *We have*

$$\gamma(T) = \frac{N}{M}\omega(T) \tag{7.43}$$

Proof. The defining equation for the Black Cow Factor $\gamma(T)$ was given in Theorem 6.3.2:

$$R\left(T_*\left(\sigma^{\otimes N}\right)\right) = \gamma(T)\sigma + \frac{1-\gamma(T)}{d}\mathrm{Id}_{\mathcal{H}} \tag{7.44}$$

We can thus connect them, for any $\sigma \in \mathcal{S}(\mathcal{H})$ and any operator $a \in \mathcal{B}(\mathcal{H})$:

$$\mathrm{Tr}\left[R\left(T_*\left(\sigma^{\otimes N}\right)\right)a\right] = \mathrm{Tr}\left[\gamma(T)\sigma a + \frac{1-\gamma(T)}{d}a\right] = \gamma(T)\,\mathrm{Tr}\left[\sigma a\right] + \frac{1-\gamma(T)}{d}\,\mathrm{Tr}\left[a\right] \tag{7.45}$$

On the other hand, by definition that R is the partial trace over all clones except the first one, we have that this must also equal:

$$\mathrm{Tr}\left[T_*\left(\sigma^{\otimes N}\right)\left(a \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes(M-1)}\right)\right] = \mathrm{Tr}\left[T_*\left(\sigma^{\otimes N}\right)a_{(1)}\right] = \mathrm{Tr}\left[\sigma^{\otimes N}T\left(a_{(1)}\right)\right] \tag{7.46}$$

With the explicit expression for $T(a_{(k)})$ found above, we can calculate:

$$\mathrm{Tr}\left[\sigma^{\otimes N}T\left(a_{(1)}\right)\right] = \frac{\mathrm{Tr}(a)}{d}\left(1 - \frac{N}{M}\omega(T)\right)\mathrm{Tr}\left[\sigma^{\otimes N}\mathrm{Id}_{\mathcal{H}_+^{\otimes N}}\right] + \frac{\omega(T)}{M}\sum_{l=1}^{N}\mathrm{Tr}\left[\sigma^{\otimes N}a_{(l)}\right] \tag{7.47}$$

First note that the notation $\sigma^{\otimes N}\mathrm{Id}_{\mathcal{H}_+^{\otimes N}}$ is harmless, because $\sigma^{\otimes N} \in \mathcal{B}(\mathcal{H}_+^{\otimes N})$. If one wishes to, we could rewrite $I_{\mathcal{H}_+^{\otimes N}}$ to S_N (if we were discussing the larger space $\mathcal{H}^{\otimes N} \supset \mathcal{H}_+^{\otimes N}$) and note that $\sigma^{\otimes N}S_N = \sigma^{\otimes N}$, so the first trace simply evaluates to 1. Furthermore, for any l, we have in the last trace:

$$\mathrm{Tr}\left[\sigma^{\otimes N}a_{(l)}\right] = \mathrm{Tr}\left[\sigma \otimes \cdots \otimes \sigma \otimes (\sigma a) \otimes \sigma \otimes \cdots \otimes \sigma\right] = \mathrm{Tr}\left[\sigma a\right] \tag{7.48}$$

So we find

$$\mathrm{Tr}\left[\sigma^{\otimes N}T\left(a_{(1)}\right)\right] = \frac{N}{M}\omega(T)\,\mathrm{Tr}\left[\sigma a\right] + \frac{1-(N/M)\omega(T)}{d}\,\mathrm{Tr}\left[a\right] \tag{7.49}$$

and thus indeed by comparison we see that $(N/M)\omega(T) = \gamma(T)$. □

7.2.4. Calculation of $\Delta_{\text{one}}(T)$

So far, we have expressed $T(a_{(k)})$ in terms of $\omega(T)$, and we have linked $\omega(T)$ to $\gamma(T)$. It is now possible to express $\Delta_{\text{one}}(T)$ in terms of $\gamma(T)$, such that the task of optimizing Δ_{one} translates to the task of optimizing $\gamma(T)$.

Let us start with the expectation of $T(a_{(k)})$ with regards to $\psi^{\otimes N}$, the first expectation we encounter in the definition of Δ_{one}. We now use $\gamma(T) = \frac{N}{M}\omega(T)$, and we can calculate for any $\psi \in \mathcal{H}$:

$$\langle \psi^{\otimes N} \ , \ T(a_{(k)})\psi^{\otimes N}\rangle = \frac{\mathrm{Tr}(a)}{d}\left(1-\gamma(T)\right)\langle\psi,\psi\rangle^N + \frac{\gamma(T)}{N}\sum_{l=1}^{N}\langle\psi^{\otimes N} \ , \ a_{(l)}\ \psi^{\otimes N}\rangle \tag{7.50}$$

Now we can calculate the individual summands. Each evaluate to:

$$\langle\psi^{\otimes N} \ , \ a_{(l)}\ \psi^{\otimes N}\rangle = \langle\psi \ , \ \psi\rangle^{N-1}\cdot\langle\psi \ , \ a\ \psi\rangle \tag{7.51}$$

Now using $\langle\psi \ , \ \psi\rangle = 1$, we finally find:

$$\langle\psi^{\otimes N} \ , \ T(a_{(k)})\psi^{\otimes N}\rangle = \frac{\mathrm{Tr}(a)}{d}\left(1-\gamma(T)\right) + \frac{\gamma(T)}{N}\cdot N\,\langle\psi \ , \ a\ \psi\rangle \tag{7.52}$$

We thus find:

$$\langle \psi\ ,\ a\ \psi\rangle\ -\ \langle \psi^{\otimes N}\ ,\ T(a_{(k)})\psi^{\otimes N}\rangle = -\frac{\mathrm{Tr}(a)}{d}\left(1-\gamma(T)\right) + \left(1-\gamma(T)\right)\langle \psi\ ,\ a\ \psi\rangle = \tag{7.53}$$

$$\left(1-\gamma(T)\right)\left(\langle \psi\ ,\ a\ \psi\rangle - \frac{\mathrm{Tr}(a)}{d}\right) \tag{7.54}$$

In order to evaluate $\Delta_{\text{one}}(T)$, we must thus find the supremum of the previous expression for $\|\psi\| = 1$ and $0 \leq a \leq \mathrm{Id}_{\mathcal{H}}$.

Theorem 7.2.8. *We have*

$$\sup_{\psi,a}\left(\langle \psi\ ,\ a\ \psi\rangle - \frac{\mathrm{Tr}(a)}{d}\right) = \frac{d-1}{d} \tag{7.55}$$

where $0 \leq a \leq Id_{\mathcal{H}}$ *and* $\|\psi\| = 1$.

Proof. We know that a is Hermitian (as it is a positive operator, and all positive operators are self-adjoint, see for example [Fas11]), thus it must have a set of eigenvalues $\{\lambda_i\}_{i=1}^{d}$ with a corresponding set of eigenvectors $\{v_i\}_{i=1}^{d}$ which is an orthonormal basis for $\mathbb{C}^d$. As this is an orthonormal basis, we can express ψ as $\psi = \sum_{i=1}^{d}\psi_i v_i$ with $\psi_i \in \mathbb{C}$. We can then calculate:

$$\langle \psi\ ,\ a\ \psi\rangle = \langle \psi\ ,\ \sum_{i=1}^{d}\psi_i\lambda_i v_i\rangle = \sum_{i=1}^{d}\lambda_i|\psi_i|^2 \tag{7.56}$$

Further using $\mathrm{Tr}(a) = \sum_{i=1}^{d}\lambda_i$, we can rewrite our supremum to

$$\sup_{\{|\psi_i|^2\},\{\lambda_i\}}\left(\sum_i \lambda_i|\psi_i|^2 - \frac{\sum_i\lambda_i}{d}\right) = \sup_{\{|\psi_i|^2\},\{\lambda_i\}}\left(\sum_i \lambda_i\frac{d|\psi_i|^2-1}{d}\right) = \frac{1}{d}\sup_{\{|\psi_i|^2\},\{\lambda_i\}}\sum_i\lambda_i\left(d|\psi_i|^2-1\right) \tag{7.57}$$

and we can rewrite our constraints to $0 \leq \lambda_i \leq 1$ (for $0 \leq a \leq \mathrm{Id}_{\mathcal{H}}$, and note that $\lambda_i \in \mathbb{R}$ as a is Hermitian) and $\sum_i|\psi_i|^2 = 1$ (as the set of eigenvectors is orthonormal). We thus have an optimalisation problem, writing $\beta_i := |\psi_i|^2$ and omitting the prefactor $\frac{1}{d}$ for now:

$$\max \sum_{i=1}^{d}\lambda_i\left(d\beta_i - 1\right) \tag{7.58}$$

$$\text{s.t.} \quad 0 \leq \lambda_i \leq 1 \qquad \forall i \in \{1,\dots,d\} \tag{7.59}$$

$$\beta_i \geq 0 \qquad \forall i \in \{1,\dots,d\} \tag{7.60}$$

$$\sum_{i=1}^{d}\beta_i = 1 \tag{7.61}$$

Intuitively, whenever $(d\beta_i - 1)$ is positive, we would set $\lambda_i = 1$, and otherwise $\lambda_i = 0$. Then, the problem looks linear in β_i, and thus the distribution of values over β_i is unimportant, except that we would like to have as little $\lambda_i > 0$ as possible, as each time we have the constant factor -1 that lowers the total result. Thus, we have the following:

Proposition 7.2.9. *An optimal solution to this optimalisation problem is* $\hat{\lambda_1} = 1$, $\hat{\beta_1} = 1$, *and* $\hat{\lambda_i} = \hat{\beta_i} = 0$ *for all* $i \in \{2,\dots,d\}$, *which yields a value of* $d-1$.

For a formal proof, see Appendix A.8.1. So we have the optimal solution $\lambda_1 = 1$, $|\psi_1|^2 = 1$, and all other $\lambda_i = 0$ and $|\psi_i|^2 = 0$. We then indeed find that $\langle\psi \mid a\psi\rangle = 1$, thus our supremum evaluates to $(d-1)/d$, as proposed. □

We thus have:

$$\Delta_{\text{one}}(T) = |1-\gamma(T)|\sup_{a,\psi}\left(\langle\psi,\ a\psi\rangle - \frac{\mathrm{Tr}(a)}{d}\right) = \frac{d-1}{d}|1-\gamma(T)| \tag{7.62}$$

which tells us we need to optimize $|1-\gamma(T)|$. Anticipating that $\gamma(T) < 1$, we optimize $\gamma(T)$ and we show in the process that we must have $\gamma(T) < 1$.

7.2.5. Explicit expression for $\omega(T)$: decomposition of the cloning map

Thus far, we have expressed the figure of merit $\Delta_{\mathrm{one}}(T)$ in terms of $\gamma(T)$, which allows us to focus on optimizing $\gamma(T)$. In order to find $\gamma(T)$ (or, equivalently, $\omega(T)$), we first have to decompose our cloning map. Note that $(\pi_\square^{\otimes M}, \mathcal{H}^{\otimes M})$ is completely reducible, thus a logical first step would be to decompose this into a direct sum of irreducible representations, and see how T performs on each of these representations. We will show that we can write T as a convex sum of quantum operations that take operators on these smaller representations to operators on $\mathcal{H}_+^{\otimes N}$, thus reducing our problem to finding the irreducible subrepresentation on which the quantum copying works best. Ultimately (with the proposed *unique* optimal cloning map in mind), the best irreducible subrepresentation should be $(\pi_M^+, \mathcal{H}_+^{\otimes M})$. To show this, we need to decompose each quantum cloner even further, using a covariant version of Stinespring's dilation theorem. We then specialise to the qubit case, as the irreducible representations are well-known in this case, and the Casimir element has the physical interpretation of total angular momentum. We can then explicitly calculate and optimize ω, which concludes the proof in the qubit case.

Decomposition of T by reducibility of $\pi_\square^{\otimes M}$

An important duality exists between the representations $\pi_\square^{\otimes M}$ of $\mathrm{SU}(d)$ and V_π of $\mathfrak{S}_M$: they act dually on $\mathcal{H}^{\otimes M}$, meaning that their commutant algebras are precisely linear combinations of the other representation. In other words, any operator that commutes with $\pi_\square^{\otimes M}$ must be a linear combination of permutation operators, and vice versa. See for example [Sim95, Thm. IX.11.5]. This proves useful when we combine this with the covariance of the cloning map T and the irreducibility of π_N^+ to get to Schur's Lemma.

First note that $\pi_\square^{\otimes M}$ is a finite-dimensional, unitary representation of the compact group $\mathrm{SU}(d)$, and is completely reducible, so we can decompose it into a direct sum of irreducibles. Thus, we can write

$$\mathcal{H}^{\otimes M} \cong \bigoplus_\alpha \mathcal{H}_\alpha \tag{7.63}$$

where each $(\pi_\alpha, \mathcal{H}_\alpha)$ is an irreducible representation, with the restriction $\pi_\alpha = \pi_\square^{\otimes M} \restriction \mathcal{H}_\alpha$. We wish to study T on each irreducible representation individually. In order to do this, first note that this decomposition comes equipped with the orthogonal projection $E_\alpha : \mathcal{H}^{\otimes M} \to \mathcal{H}_\alpha$. These E_α need to be linear combinations of permutations by our previous observations, as they commute with the representation $\pi_\square^{\otimes M}$. Let us investigate this shortly: for any $\psi \in \mathcal{H}^{\otimes M}$ we have $\psi = \sum_{\alpha'} \psi_{\alpha'}$ with $\psi_{\alpha'} \in \mathcal{H}_{\alpha'}$, and then $E_\alpha \psi = \psi_\alpha$, and $\pi_\square^{\otimes M}(u)\psi = \sum_{\alpha'} \pi_{\alpha'}(u)\psi_{\alpha'}$. Thus, first letting E_α act on ψ, and then letting π_α act on ψ_α has the same result as first applying $\pi_\square^{\otimes M}$ to ψ and then applying E_α, and thus E_α en $\pi_\square^{\otimes M}$ commute. By the duality theorem in the previous paragraph, E_α must be a linear combination of permutation operators.

As T is permutation invariant, we can see:

$$T\left(P_\pi A' P_\pi^*\right) = T(A') \overset{A'=AP_\pi}{\Longrightarrow} T\left(P_\pi A\right) = T\left(AP_\pi\right) \quad \forall A \in \mathcal{B}(\mathcal{H}^{\otimes M}) \ , \ \forall \pi \in \mathfrak{S}_M \tag{7.64}$$

By using $E_\alpha^2 = E_\alpha$ as it is a projector, we now find:

$$T(A'E_\alpha) = T(E_\alpha A') \overset{A'=AE_\alpha}{\Longrightarrow} T(AE_\alpha) = T(E_\alpha A E_\alpha) \quad \forall A \in \mathcal{B}(\mathcal{H}^{\otimes M}) \tag{7.65}$$

This expression becomes useful when one realises that $T(E_\alpha A E_\alpha)$ can be interpreted as a cloning machine, with the added benefit that we can restrict ourselves to bounded operators on $\mathcal{H}_\alpha$. Although this map is again completely positive by the same argument we used to demonstrate that $\hat{T}$ is completely positive, we need to renormalize to make it unital again. We can use the irreducibility of $\mathcal{H}_\alpha$: namely, the E_α need to commute with the representation $\pi_\square^{\otimes M}$. But then, we have by the covariance property of T:

$$\pi_N^+(u) T(E_\alpha) \pi_N^+(u)^* = T\left(\pi_\square^{\otimes M}(u) E_\alpha \pi_\square^{\otimes M}(u)^*\right) = T\left(E_\alpha\right) \tag{7.66}$$

Thus $T(E_\alpha)$ commute with π_N^+, but π_N^+ is irreducible, so by Schur's lemma we must have $T(E_\alpha) = r_\alpha \mathrm{Id}_{\mathcal{H}_+^{\otimes N}}$, for some $r_\alpha \in \mathbb{C}$.

So we can look at the map $T_\alpha(A) := r_\alpha^{-1} T(E_\alpha A E_\alpha)$, which is again a cloning map and we can restrict the input to $\mathcal{B}(\mathcal{H}_\alpha)$. Using the fact that $\sum_\alpha E_\alpha = \mathrm{Id}_{\mathcal{H}^{\otimes M}}$, we have the convex decomposition:

$$T(A) = T\left(A \sum_\alpha E_\alpha\right) = \sum_\alpha T(AE_\alpha) = \sum_\alpha T(E_\alpha A E_\alpha) = \sum_\alpha r_\alpha T_\alpha(A) \tag{7.67}$$

As ω is an affine functional, we now find

$$\omega(T) = \sum_\alpha r_\alpha \omega(T_\alpha) \tag{7.68}$$

and as this is a convex decomposition, we now try to find whichever $T_\alpha : \mathcal{B}(\mathcal{H}_\alpha) \to \mathcal{B}(\mathcal{H}_+^{\otimes N})$ yields the highest $\omega(T_\alpha)$ and use this as our optimal cloning map. However, to find this, we further need to decompose each map T_α by using Stinespring's dilation theorem.

Decomposition of T_α by Stinespring's dilation theorem

We wish to decompose each T_α according to the covariant Stinespring dilation theorem, first stated by [Scu79, Th.1].

Let us first note that $T_\alpha(A) = r_\alpha^{-1} T(E_\alpha A E_\alpha)$ is a linear, completely positive map that we can interpret as a map from $\mathcal{B}(\mathcal{H}_\alpha)$ to $\mathcal{B}(\mathcal{H}_+^{\otimes N})$. Also, T_α has the unitary covariance property, as T has the unitary covariance property, and each E_α is a linear combination of permutations, each of which commute with $\pi_\square^{\otimes M}$. According to [KW99, Appendix B], a completely positive map with the unitary covariance property, together with the fact that π_α and π_N^+ are finite-dimensional unitary representations, is sufficient that the following covariant version of Stinespring holds:

$$T_\alpha = V^*(A \otimes I_\mathcal{K})V \tag{7.69}$$

where $V : \mathcal{H}_+^{\otimes N} \to \mathcal{H}_\alpha \otimes \mathcal{K}$ is an isometry that intertwines the respective representations, and $\mathcal{K}$ is an auxiliary Hilbert space carrying a unitary representation $\widetilde{\pi} : U(d) \to \mathcal{B}(\mathcal{K})$. We thus have:

$$V\pi_N^+(u) = (\pi_\alpha(u) \otimes \widetilde{\pi}(u))\, V \qquad ; \qquad \pi_N^+(u)V^* = V^*\,(\pi_\alpha(u) \otimes \widetilde{\pi}(u)) \tag{7.70}$$

We can again study the irreducible subrepresentations: π_α is already irreducible, but $\widetilde{\pi}$ is not necessarily irreducible. We thus again decompose this into irreducible subrepresentations $\pi_\beta := \widetilde{\pi} \restriction \mathcal{K}_\beta$ where we define $\mathcal{K}_\beta := F_\beta \mathcal{K}$ and where F_β is a minimal orthogonal projection on $\mathcal{K}$. Note that F_β commutes with $\widetilde{\pi}$, thus we can claim: $A \mapsto V^*\,(A \otimes F_\beta)\, V$ is a covariant map. Indeed:

$$\pi_\alpha(u) A \pi_\alpha(u)^* \mapsto V^*\left[(\pi_\alpha(u) A \pi_\alpha(u)^*) \otimes F_\beta\right] V = V^*\left[(\pi_\alpha(u) A \pi_\alpha(u)^*) \otimes (\widetilde{\pi}(u) F_\beta \widetilde{\pi}(u)^*)\right] V = \tag{7.71}$$

$$V^*\left[(\pi_\alpha(u) \otimes \widetilde{\pi}(u))\,(A \otimes F_\beta)\,(\pi_\alpha(u)^* \otimes \widetilde{\pi}(u)^*)\right] V = \pi_N^+(u) V^*\,(A \otimes F_\beta)\, V \pi_N^+(u)^* \tag{7.72}$$

Furthermore, $V^*\,(\mathrm{Id}_\alpha \otimes F_\beta)\, V$ commutes with the irreducible representation π_N^+:

$$V^*\,(\mathrm{Id}_\alpha \otimes F_\beta)\, V \pi_N^+(u) = V^*\,(\mathrm{Id}_\alpha \otimes F_\beta)\,(\pi_\alpha(u) \otimes \widetilde{\pi}(u))\, V = V^*\,(\pi_\alpha(u) \otimes F_\beta \widetilde{\pi}(u))\, V = \tag{7.73}$$

$$V^*\,(\pi_\alpha(u) \otimes \widetilde{\pi}(u) F_\beta)\, V = V^*\,(\pi_\alpha(u) \otimes \widetilde{\pi}(u))\,(\mathrm{Id}_\alpha \otimes F_\beta)\, V = \pi_N^+(u) V^*\,(\mathrm{Id}_\alpha \otimes F_\beta)\, V \tag{7.74}$$

So again by Schur's Lemma, we have $V^*\,(\mathrm{Id}_\alpha \otimes F_\beta)\, V = r_\beta \mathrm{Id}_{\mathcal{H}_+^{\otimes N}}$ for some $r_\beta \in \mathbb{C}$. Thus

$$T_\alpha = \sum_\beta r_\beta T_{\alpha\beta} \qquad ; \qquad T_{\alpha\beta}(A) = r_\beta^{-1} V^*(A \otimes F_\beta)V \tag{7.75}$$

where each $T_{\alpha\beta}$ is again a quantum operation $\mathcal{B}(\mathcal{H}_\alpha) \to \mathcal{B}(\mathcal{H}_+^{\otimes N})$.

We must thus now find a way to explicitly calculate $\omega(T_{\alpha\beta})$, and then optimize this with respect to α and β. We will provide the calculations for the qubit case ($d = 2$) along the arguments of [KW99, Section III.E]. The general case starts similarly, but needs some heavy machinery that is not further discussed in this thesis.

7.2.6. Explicit expression for $\omega(T)$: the qubit case

Thus far, we have shown that we can optimize $\Delta_{\text{one}}(T)$ by optimizing $\omega(T)$, and then sought to calculate $\omega(T)$ by decomposing the cloning map into a convex sum of $T_{\alpha\beta}$. These $T_{\alpha\beta}(A)$ for $A \in \mathcal{B}(\mathcal{H}_\alpha)$ are operators on $\mathcal{H}_+^{\otimes N}$ that act in the following way: firstly, they take states on $\mathcal{H}_+^{\otimes N}$ to the product space $\mathcal{H}_\alpha \otimes \mathcal{K}$, then apply $A \otimes F_\beta$ there for some minimal orthogonal projection F_β on auxiliary Hilbert space $\mathcal{K}$, and then take the resulting state back to $\mathcal{H}_+^{\otimes N}$. We now seek to explicitly calculate $\omega(T_{\alpha\beta})$.

In the qubit case, $d = 2$, we know the irreducible representations very well, as discussed before in Section 7.2.1: each irreducible representation could be identified by the total angular momentum $j \in \frac{1}{2}\mathbb{Z}_{\geq 0}$, and we had $\pi_j \cong \pi_N^+$ for $N = 2j$.

Furthermore, the Lie algebra $\mathfrak{su}(2)$ is spanned by the three Pauli matrices. It is well known that the sum of the squares of the angular momentum operators commutes with those operators, and if measured, returns a value of $j(j+1)$. We call this operator the Casimir invariant operator, see for more information Definitions 2.36 or for more background information see Appendix B. We can express this operator as:

$$\widetilde{\mathbf{C}}_2 := \sum_{k=1}^{3} X_k^2 \qquad ; \qquad \{X_1, X_2, X_3\} \text{ basis of } \mathfrak{su}(2) \text{ with } [X_1, X_2] = X_3 \tag{7.76}$$

This means that $\partial\pi_j(\widetilde{\mathbf{C}}_2) = j(j+1)\text{Id}_{D_j}$.

From our previous discussion, see Corollary 7.2.6, we had learned that for any covariant cloning map T,

$$T(\partial\pi(a)) = \omega(T)\partial\pi_N^+(a) \tag{7.77}$$

for some factor $\omega(T) \in \mathbb{C}$, some operator $a \in \mathcal{B}(\mathcal{H})$ with $\text{Tr}(a) = 0$, and some differential representation $\partial\pi : \mathfrak{su}(2) \to \mathcal{B}(\mathcal{H}^{\otimes M})$ (which was uniquely extended to a representation on $\mathfrak{sl}(2)$).

Choose any $\alpha, \beta \in \frac{1}{2}\mathbb{Z}_{\geq 0}$, we then find for our cloning map $T_{\alpha\beta}$:

$$\omega(T_{\alpha\beta})\partial\pi_N^+(X_k) = V^* \left(\partial\pi_\alpha(X_k) \otimes \text{Id}_\beta\right) V \tag{7.78}$$

We can now use that V is an intertwining isometry between π_N^+ and $\pi_\alpha \otimes \pi_\beta$: its equivalent in the Lie algebra representations then becomes (see Definitions 2.2.23 for the Lie algebra representation of $\pi_\alpha \otimes \pi_\beta$):

$$V\partial\pi_N^+(X) = \left(\partial\pi_\alpha(X) \otimes \text{Id}_\beta + \text{Id}_\alpha \otimes \partial\pi_\beta(X)\right) V \tag{7.79}$$

We can multiply the previous expression for $\omega(T_{\alpha\beta})$ by $\partial\pi_N^+(X_k)$ to find:

$$\omega(T_{\alpha\beta})\left(\partial\pi_N^+(X_k)\right)^2 = V^* \left(\partial\pi_\alpha(X_k) \otimes \text{Id}_\beta\right) V\partial\pi_N^+(X_k) \tag{7.80}$$

By expanding $V\partial\pi_N^+(X_k)$ on the right-hand side, we find:

$$\omega(T_{\alpha\beta})\partial\pi_N^+(X_k^2) = V^* \left(\partial\pi_\alpha(X_k) \otimes \text{Id}_\beta\right) \left(\partial\pi_\alpha(X_k) \otimes \text{Id}_\beta + \text{Id}_\alpha \otimes \partial\pi_\beta(X_k)\right) V \tag{7.81}$$

We can now sum of all k and work out the brackets on the right-hand side to find

$$\omega(T_{\alpha\beta})\partial\pi_N^+(\widetilde{\mathbf{C}}_2) = V^* \left(\partial\pi_\alpha(\widetilde{\mathbf{C}}_2) \otimes \text{Id}_\beta\right) V + \sum_{k=1}^{3} V^* \left(\partial\pi_\alpha(X_k) \otimes \partial\pi_\beta(X_k)\right) V \tag{7.82}$$

We wish to rewrite the sum. Note that we have

$$\frac{1}{2}\sum_{k=1}^{3} \left(\partial\pi_\alpha(X_k) \otimes I_\beta + I_\alpha \otimes \partial\pi_\beta(X_k)\right)^2 = \tag{7.83}$$

$$\frac{1}{2}\sum_{k=1}^{3} \left(\partial\pi_\alpha(X_k^2) \otimes I_\beta + I_\alpha \otimes \partial\pi_\beta(X_k^2) + 2\partial\pi_\alpha(X_k) \otimes \partial\pi_\beta(X_k)\right) = \tag{7.84}$$

$$\frac{1}{2}\partial\pi_\alpha(\widetilde{\mathbf{C}}_2) \otimes I_\beta + \frac{1}{2}I_\alpha \otimes \pi_\beta(\widetilde{\mathbf{C}}_2) + \sum_{k=1}^{3} \left(\partial\pi_\alpha(X_k) \otimes \partial\pi_\beta(X_k)\right) \tag{7.85}$$

Thus we can rewrite the sum in our previous expression:

$$\sum_{k=1}^{3}(\partial\pi_\alpha(X_k)\otimes\partial\pi_\beta(X_k)) = \frac{1}{2}\sum_{k=1}^{3}(\partial\pi_\alpha(X_k)\otimes I_\beta + I_\alpha\otimes\partial\pi_\beta(X_k))^2 - \frac{1}{2}\partial\pi_\alpha(\widetilde{\mathbf{C}}_2)\otimes I_\beta - \frac{1}{2}I_\alpha\otimes\pi_\beta(\widetilde{\mathbf{C}}_2) \tag{7.86}$$

This is useful, because now we can again use the intertwining property of V:

$$\sum_{k=1}^{3}(\partial\pi_\alpha(X_k)\otimes I_\beta + I_\alpha\otimes\partial\pi_\beta(X_k))^2 V = \sum_{k=1}^{3} V\partial\pi_N^+(X_k^2) = V\partial\pi_N^+(\widetilde{\mathbf{C}}_2) \tag{7.87}$$

Combining these equations into the equation for ω yields:

$$\omega(T_{\alpha\beta})\partial\pi_N^+(\widetilde{\mathbf{C}}_2) = V^*\left(\partial\pi_\alpha(\widetilde{\mathbf{C}}_2)\otimes\mathrm{Id}_\beta\right)V + \frac{1}{2}V^*V\partial\pi_N^+(\widetilde{\mathbf{C}}_2) - \frac{1}{2}V^*\left(\partial\pi_\alpha(\widetilde{\mathbf{C}}_2)\otimes I_\beta + I_\alpha\otimes\pi_\beta(\widetilde{\mathbf{C}}_2)\right)V \tag{7.88}$$

We can now reap the benefit of our hard work: each operator is a multiple of the identity (and V^*V is the identity as well), thus this simplifies to

$$\omega(T_{\alpha\beta})(N/2)(N/2+1) = \alpha(\alpha+1) + \frac{1}{2}(N/2)(N/2+1) - \frac{1}{2}\left(\alpha(\alpha+1)+\beta(\beta+1)\right) \tag{7.89}$$

This simplifies to

$$\omega(T_{\alpha\beta}) = \frac{1}{2} + \frac{1}{2}\cdot\frac{\alpha(\alpha+1)-\beta(\beta+1)}{N/2(N/2+1)} \tag{7.90}$$

7.2.7. Optimisation of $\omega(T)$: the qubit case

To optimize $\omega(T_{\alpha\beta})$, we need to figure out the constraints to α and β in the previous expression.

Lemma 7.2.10. *We have $\alpha \leq M/2$.*

Proof. Firstly, note that π_α needs to be an irreducible subrepresentation of $\pi_\square^{\otimes M} = \pi_{j=1/2}^{\otimes M}$ with vector space $D_{1/2}^{\otimes M}$. But, again using the decomposition theory, we can actually compute

$$D_{1/2}\otimes D_{1/2} = D_0 \oplus D_1 \tag{7.91}$$

Tensoring on another two $D_{1/2}$ then leads to

$$D_{1/2}^{\otimes 3} = \left(D_0\otimes D_{1/2}\right)\oplus\left(D_1\otimes D_{1/2}\right) = D_{1/2}\oplus D_{1/2}\oplus D_{3/2} \tag{7.92}$$

$$D_{1/2}^{\otimes 4} = D_0\oplus D_1\oplus D_0\oplus D_1\oplus D_1\oplus D_2 \tag{7.93}$$

it becomes evident that each time, the last summand D_s is split into $D_{s-1/2}\oplus D_{s+1/2}$, and this is the largest space: thus, by induction, by M times tensoring $D_{1/2}$, the largest summand becomes $D_{M/2}$. As (π_α, D_α) is an irreducible subrepresentation of $\pi_{j=1/2}^{\otimes M}$, it must be in this direct sum, and thus we directly find that $\alpha \leq M/2$. □

Furthermore, a constraint for β can be found by the restriction that a nonzero intertwiner V must exist between π_N^+ and $\pi_\alpha\otimes\pi_\beta$.

Lemma 7.2.11. *We have $|\alpha - N/2| \leq \beta \leq \alpha + N/2$*

Proof. As both π_α and π_β are irreducible, we can again use the Clebsch-Gordan decomposition of tensor products of irreducible representations of $\mathfrak{su}(2)$, and we see that

$$D_{N/2}\xrightarrow{V} D_\alpha\otimes D_\beta \cong D_{|\alpha-\beta|}\oplus D_{|\alpha-\beta|+1}\oplus\cdots\oplus D_{\alpha+\beta} \tag{7.94}$$

For V to be a nonzero intertwining isometry, by Schur's Lemma, the space $D_{N/2}$ must appear on the right-hand side, thus we must thus have that

$$|\alpha-\beta| \leq N/2 \leq \alpha+\beta \tag{7.95}$$

We can rewrite this constraint to (for a derivation, see Appendix A.9.1)

$$|\alpha - N/2| \leq \beta \leq \alpha + N/2 \tag{7.96}$$

□

Visually, this gives us the following admissible region:

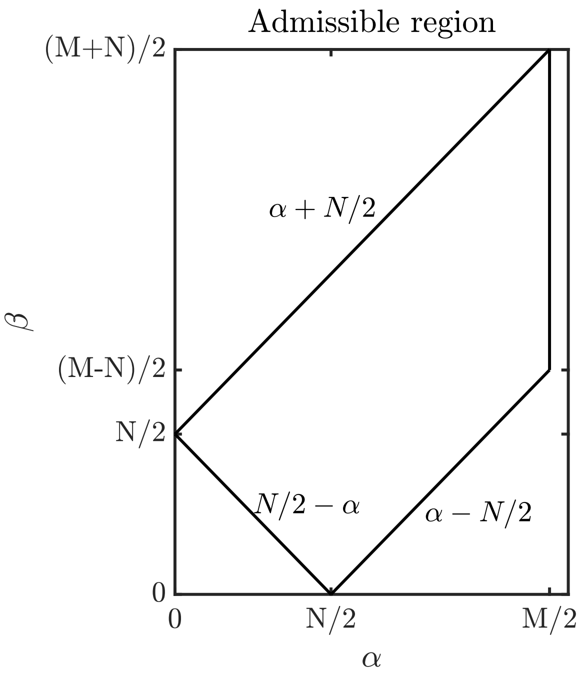

Figure 7.1: The admissible region of possible combinations of α and β. The admissible region is the convex bounded shape. The four constraints are also added to the figure.

We can now optimize $\omega(T_{\alpha\beta})$, so we need to maximize $\alpha(\alpha+1) - \beta(\beta+1)$. Note that, given any choice of α, we would like to choose β as small as possible. The smallest value of β for any α is $|\alpha - N/2|$. We thus wish to maximize

$$\alpha(\alpha+1) - |\alpha - N/2|\,(|\alpha - N/2| + 1) \qquad ; \quad 0 \leq \alpha \leq M/2 \tag{7.97}$$

We work out the brackets to find

$$\alpha^2 + \alpha - \alpha^2 - (N/2)^2 + 2\alpha(N/2) - |\alpha - (N/2)| = 2\alpha(N/2) - (N/2)^2 + \alpha - |\alpha - (N/2)| \tag{7.98}$$

We have

$$\alpha - |\alpha - (N/2)| = \begin{cases} (N/2) & \alpha > N/2 \\ 2\alpha - (N/2) & \alpha \leq N/2 \end{cases} \tag{7.99}$$

which is an increasing function of α, as clearly $\alpha \mapsto 2\alpha - (N/2)$ is increasing, and at $\alpha = N/2$ achieves exactly the value $N/2$. But then, in order to maximimze our expression we must choose α as large as possible, i.e. $\alpha = M/2$. We find (for a tedious derivation, see Appendix A.10.1)

$$\alpha = M/2\ ,\ \beta = (M-N)/2 \implies \max \omega(T_{\alpha\beta}) = \frac{M+2}{N+2} \tag{7.100}$$

In the general case of $\mathcal{H} = \mathbb{C}^d$, we state the solution found in [KW99]:

$$\max \omega(T_{\alpha\beta}) = \frac{M+d}{N+d} \tag{7.101}$$

The careful reader might have already noticed that this expression is similar to $\omega(\hat{T})$:

$$\omega(\hat{T}) = \frac{M}{N}\gamma(\hat{T}) = \frac{M}{N}\frac{N}{N+d}\frac{M+d}{M} = \frac{M+d}{N+d} = \max \omega(T_{\alpha\beta}) \tag{7.102}$$

so indeed, our $\hat{T}$ achieves the highest possible $\omega(\hat{T})$ (equivalently, the highest possible $\gamma(\hat{T})$), and thus is optimal with respect to Δ_{one}. For uniqueness, [KW99] note that there exists a unique unitary covariant cloning map, and with a minor adaptation of the argument used to prove optimal fidelity, one can prove that in this case there is also a unique optimal cloning map, see [KW99, Section F]. This proves Theorem 7.2.1.

8

Example of qubit copying

In order to investigate the optimal cloning map, we can compare it to some other cloning maps found in literature. Most literature focusses on the qubit case (the case where $\mathcal{H} = \mathbb{C}^2$), and thus we will restrict our focus to this case as well. Let us consider the smallest example: cloning one qubit to two qubits, i.e. the case $d = 2$, $N = 1$ and $M = 2$ in our previous discussions.

In this smallest cloning example, we consider the input Hilbert space $\mathcal{H} = \mathbb{C}^2$, and the output Hilbert space $\mathcal{H}^{\otimes 2} = \mathcal{H} \otimes \mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$. Furthermore, consider the canonical orthonormal basis $|0\rangle, |1\rangle$ of $\mathcal{H}$. We use the following basis for $\mathcal{H} \otimes \mathcal{H}$: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ where we abbreviate using the usual convention: $|ij\rangle := |i\rangle \otimes |j\rangle$. We can now concretely describe our optimal cloning device. After doing so, we will compare this cloning device to the cloning device of Wootters-Zurek, which clones orthonormal states perfectly. We look at different figures of merit that are described in the paper by [BH96].

8.1. Description of the optimal cloning device

Recall that the definition of the optimal cloning device was

$$\hat{T}_*(\rho) = \frac{d[N]}{d[M]} S_M \left(\rho \otimes \mathrm{Id}_{\mathcal{H}}^{\otimes (M-N)} \right) S_M \qquad , \qquad \rho \in \mathcal{S}(\mathcal{H}_+^{\otimes N}) \tag{8.1}$$

In this case we have $d[N] = d[1] = \binom{2+1-1}{1} = 2$ and $d[M] = d[2] = \binom{2+2-1}{2} = 3$. Furthermore, we can actually construct the symmetric projector S_2:

$$S_2 = \frac{1}{2} \sum_{\pi \in \mathfrak{S}_2} P_\pi = \frac{1}{2} P_{(1)} + \frac{1}{2} P_{(12)} \tag{8.2}$$

where the subscript (1) denotes the identity element of the $\mathfrak{S}_2$ group, and (12) the transposition that swaps element 1 and 2.

It is convenient to look at the matrix representation of these operators, where we can use the Kronecker product for the tensor product:

$$P_{(1)} = \mathrm{Id}_{\mathcal{H}} \otimes \mathrm{Id}_{\mathcal{H}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad ; \quad P_{(12)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{8.3}$$

where indeed we see for example that $\alpha |01\rangle + \beta |10\rangle$, which is represented by the vector $(0, \alpha, \beta, 0)^T$ is permuted by $P_{(12)}$ to $(0, \beta, \alpha, 0)^T$ which is $\alpha |10\rangle + \beta |01\rangle$, precisely as required. Also, $|00\rangle$ and $|11\rangle$ are left unchanged. We thus find

$$S_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1/2 & 1/2 & 0 \\ 0 & 1/2 & 1/2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{8.4}$$

The input state in this case is some pure state $\sigma \in \mathcal{S}(\mathcal{H})$ (as $N = 1$). Most generally, this is the state associated with the vector $\alpha |0\rangle + \beta |1\rangle$, with $|\alpha|^2 + |\beta|^2 = 1$. Thus, using the Kronecker product to calculate the tensor product, we find:

$$\sigma \otimes \mathrm{Id}_{\mathcal{H}} = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} |\alpha|^2 & 0 & \alpha\beta^* & 0 \\ 0 & |\alpha|^2 & 0 & \alpha\beta^* \\ \alpha^*\beta & 0 & |\beta|^2 & 0 \\ 0 & \alpha^*\beta & 0 & |\beta|^2 \end{pmatrix} \tag{8.5}$$

We can now calculate $S_2 \left(\sigma \otimes \mathrm{Id}_{\mathcal{H}}\right) S_2$, and with the prefactor $2/3$ we find $\hat{T}_*(\sigma)$:

$$\hat{T}_*(\sigma) = \frac{2}{3} S_2 \left(\sigma \otimes \mathrm{Id}_{\mathcal{H}}\right) S_2 = \frac{2}{3} \cdot \frac{1}{4} \begin{pmatrix} 4|\alpha|^2 & 2\alpha\beta^* & 2\alpha\beta^* & 0 \\ 2\alpha^*\beta & 1 & 1 & 2\alpha\beta^* \\ 2\alpha^*\beta & 1 & 1 & 2\alpha\beta^* \\ 0 & 2\alpha^*\beta & 2\alpha^*\beta & 4|\beta|^2 \end{pmatrix} \tag{8.6}$$

8.2. Description of the Wootters-Zurek cloning machine

We recall from the No Cloning Theorem in Chapter 3 that Wootters-Zurek first proved this by looking at a machine that perfectly clones the orthogonal states $|0\rangle$ and $|1\rangle$, and then fails to perfectly clone linear combinations. Thus, any state $\alpha |0\rangle + \beta |1\rangle$ is sent to $\alpha |00\rangle + \beta |11\rangle$.

We can improve the cloner slightly, by also taking into account the Hilbert space in which the cloning machine itself lives as an ancilla space [BH96]. By this, we mean that we have $|0\rangle \mapsto |0\rangle \otimes |0\rangle \otimes |Q_0\rangle_x$ and $|1\rangle \mapsto |1\rangle \otimes |1\rangle \otimes |Q_1\rangle_x$, where $|Q_i\rangle_x$ denotes the state of the quantum cloner (and we thus see our quantum cloner itself as a *subsystem*). Choosing an orthonormal basis for the quantum cloner, we then have

$$\alpha |0\rangle + \beta |1\rangle \mapsto \alpha |00\rangle |Q_0\rangle_x + \beta |11\rangle |Q_1\rangle_x \tag{8.7}$$

We are then free to choose $\langle Q_0, Q_1\rangle_x = 0$. The output density matrix can then be described as the partial trace over the ancilla space, and we denote this cloning map as T_*^{WZ}:

$$T_*^{\mathrm{WZ}}(\sigma) = \begin{pmatrix} |\alpha|^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & |\beta|^2 \end{pmatrix} \quad , \quad \sigma = |\psi\rangle \langle\psi| \quad , \quad |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \tag{8.8}$$

8.3. Performance of the cloning machines

To look at the performance of these cloning maps, we can follow an approach that can for example be found in [BH96], where we look at several norms. All the norms are based on the Hilbert-Schmidt norm

Definition 8.3.1 (Hilbert-Schmidt). Given an operator $A \in \mathcal{B}(\mathcal{H})$ for some Hilbert space $\mathcal{H}$, we can define the Hilbert-Schmidt norm as

$$\|A\|_2 := \sqrt{\mathrm{Tr}\left[A^* A\right]} \tag{8.9}$$

To keep track of the different distances, we first adopt the notation that [BH96] follow: Let us define our systems as system a and b with Hilbert space $\mathcal{H}_a$ and $\mathcal{H}_b$, in both cases identified with $\mathbb{C}^2$. The output system is thus $\mathcal{H}_a \otimes \mathcal{H}_b$. We define density matrices living in $\mathcal{H}_a$ as ρ_a, and ρ_b similarly for $\mathcal{H}_b$. We denote the superscript "(out)" as the output density matrix of a cloning map, "(in)" as the input density matrix, and "(id)" as the ideal output. Thus, in general, the input of a cloning map is $\rho_{\mathrm{a}}^{(\mathrm{in})}$, the output $\rho_{\mathrm{ab}}^{(\mathrm{out})}$, and if we perform the partial trace over this output with respect to system b we find $\rho_{\mathrm{a}}^{(\mathrm{out})}$, and similarly a partial trace over system a yields $\rho_{\mathrm{b}}^{(\mathrm{out})}$. Ideally, the output state on system a is unchanged, i.e. $\rho_{\mathrm{a}}^{(\mathrm{id})} = \rho_{\mathrm{a}}^{(\mathrm{in})}$, and the output state has been copied onto system b, i.e. $\rho_{\mathrm{b}}^{(\mathrm{id})} = \rho_{\mathrm{a}}^{(\mathrm{in})}$. From the No-Cloning Theorem, we know that is impossible to have the total output $\rho_{\mathrm{ab}}^{(\mathrm{id})} = \rho_{\mathrm{a}}^{(\mathrm{id})} \otimes \rho_{\mathrm{b}}^{(\mathrm{id})} = \rho_{\mathrm{a}}^{(\mathrm{in})} \otimes \rho_{\mathrm{a}}^{(\mathrm{in})}$ (with ideal reduced density matrices $\rho_{\mathrm{a}}^{(\mathrm{id})} = \rho_{\mathrm{a}}^{(\mathrm{in})}$ and $\rho_{\mathrm{b}}^{(\mathrm{id})} = \rho_{\mathrm{a}}^{(\mathrm{in})}$).

To look at our density matrices, we look at the following distances:

Definition 8.3.2 (Distances between states). We define four distances:

- We define the distance between the ideal and achieved output for **one subsystem**:

$$D_a := \mathrm{Tr}\left[\left(\rho_{\mathrm{a}}^{(\mathrm{id})} - \rho_{\mathrm{a}}^{(\mathrm{out})}\right)^2\right] \tag{8.10}$$

- We define the distance between the achieved output and the tensor product of the partially traced outputs, which measures the **degree of entanglement**:

$$D_{\mathrm{ab}}^{(1)} := \mathrm{Tr}\left[\left(\rho_{\mathrm{ab}}^{(\mathrm{out})} - \rho_{\mathrm{a}}^{(\mathrm{out})} \otimes \rho_{\mathrm{b}}^{(\mathrm{out})}\right)^2\right] \tag{8.11}$$

- We define the distance between the **entire** ideal and achieved output:

$$D_{\mathrm{ab}}^{(2)} := \mathrm{Tr}\left[\left(\rho_{\mathrm{ab}}^{(\mathrm{out})} - \rho_{\mathrm{ab}}^{(\mathrm{id})}\right)^2\right] \tag{8.12}$$

- We define the distance between the ideal output and the **tensor product** of the partially traced outputs:

$$D_{\mathrm{ab}}^{(3)} := \mathrm{Tr}\left[\left(\rho_{\mathrm{ab}}^{(\mathrm{id})} - \rho_{\mathrm{a}}^{(\mathrm{out})} \otimes \rho_{\mathrm{b}}^{(\mathrm{out})}\right)^2\right] \tag{8.13}$$

We can calculate all the ideal cases, for $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$:

$$\rho_{\mathrm{a}}^{(\mathrm{id})} = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix} \quad , \quad \rho_{\mathrm{ab}}^{(\mathrm{id})} = \rho_{\mathrm{a}}^{(\mathrm{id})} \otimes \rho_{\mathrm{a}}^{(\mathrm{id})} = \begin{pmatrix} |\alpha|^4 & |\alpha|^2\alpha\beta^* & |\alpha|^2\alpha\beta^* & \alpha^2\beta^{*2} \\ |\alpha|^2\alpha^*\beta & |\alpha|^2|\beta|^2 & |\alpha|^2|\beta|^2 & |\beta|^2\alpha\beta^* \\ |\alpha|^2\alpha^*\beta & |\alpha|^2|\beta|^2 & |\alpha|^2|\beta|^2 & |\beta|^2\alpha\beta^* \\ \alpha^{*2}\beta^2 & |\beta|^2\alpha^*\beta & |\beta|^2\alpha^*\beta & |\beta|^4 \end{pmatrix} \tag{8.14}$$

Armed with this knowledge, we can compare the two cloning machines.

8.3.1. Performance with respect to D_{A}

- For the optimal cloning map, we compute

$$\rho_{\mathrm{a}}^{(\mathrm{out})} = \mathrm{Tr}_b\left[\rho_{\mathrm{ab}}^{(\mathrm{out})}\right] = \mathrm{Tr}_b\left[\hat{T}_*\left(\rho_{\mathrm{a}}^{(\mathrm{in})}\right)\right] = \frac{1}{6}\begin{pmatrix} 5|\alpha|^2 + |\beta|^2 & 4\alpha\beta^* \\ 4\alpha^*\beta & |\alpha|^2 + 5|\beta|^2 \end{pmatrix} \tag{8.15}$$

From which one can calculate

$$D_{\mathrm{a}}(\hat{T}_*) = \frac{\left(|\alpha|^2 + |\beta|^2\right)^2}{18} = \frac{1}{18} \tag{8.16}$$

- For the Wootters-Zurek cloning map T_*^{WZ}, the reduced output density matrix is:

$$\rho_{\mathrm{a}}^{(\mathrm{out})} = \begin{pmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{pmatrix} \tag{8.17}$$

From which one can calculate

$$D_{\mathrm{a}}(T_*^{\mathrm{WZ}}) = 2|\alpha|^2|\beta|^2 = 2|\alpha|^2\left(1 - |\alpha|^2\right) \tag{8.18}$$

Again we see that our optimal cloning map does not have a preferred direction, which expresses itself in a distance measure D_{a} that is independent of our input state. In contrast, the WZ cloner performs extremely well near $|\alpha| = 1$ and $|\beta| = 1$, but much worse in the area in between.

8.3.2. Performance with respect to $D_{\mathrm{AB}}^{(1)}$

- For the optimal cloning map, the partial trace over system a yields the same result as the partial trace over system b. We can thus immediately compute

$$D_{\mathrm{ab}}^{(1)}(\hat{T}_*) = \frac{19}{324} \tag{8.19}$$

- For the Wootters-Zurek cloning map, the partial trace over a is also equal to the partial trace over b. Thus we find

$$D_{\mathrm{ab}}^{(1)}(T_*^{\mathrm{WZ}}) = 4|\alpha|^8 - 8|\alpha|^6 + 4|\alpha|^4 = D_{\mathrm{a}}(T_*^{\mathrm{WZ}}) \cdot D_{\mathrm{a}}(T_*^{\mathrm{WZ}}) \tag{8.20}$$

8.3.3. Performance with respect to $D_{\mathrm{AB}}^{(2)}$

- For the optimal cloning map, we have

$$D_{\mathrm{ab}}^{(2)}(\hat{T}_*) = \frac{2}{9} \tag{8.21}$$

- For the Wootters-Zurek cloning map, we find

$$D_{\mathrm{ab}}^{(2)}(T_*^{\mathrm{WZ}}) = 2 \cdot 2|\alpha|^2\left(1-|\alpha|^2\right) = 2D_{\mathrm{a}}(T_*^{\mathrm{WZ}}) \tag{8.22}$$

8.3.4. Performance with respect to $D_{\mathrm{AB}}^{(3)}$

- For the optimal cloning map, we have

$$D_{\mathrm{ab}}^{(3)}(\hat{T}_*) = \frac{43}{324} \tag{8.23}$$

- For the Wootters-Zurek cloning map, we find:

$$D_{\mathrm{ab}}^{(3)}(T_*^{\mathrm{WZ}}) = -4|\alpha|^8 + 8|\alpha|^6 - 8|\alpha|^4 + 4|\alpha|^2 = 2D_{\mathrm{a}}(T_*^{\mathrm{WZ}}) - D_{\mathrm{ab}}^{(1)}(T_*^{\mathrm{WZ}}) \tag{8.24}$$

8.3.5. Comparison between performances

Graphically, this looks like:

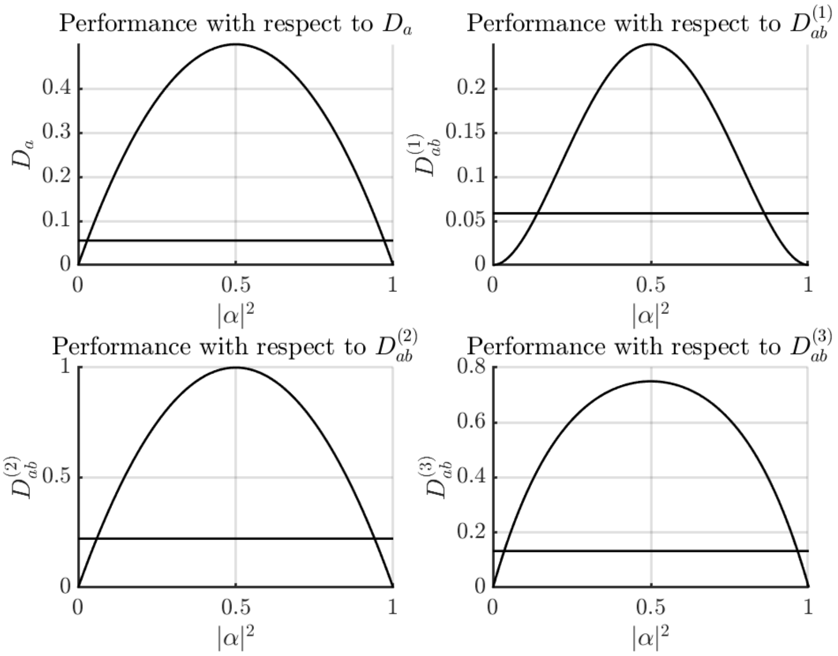

Figure 8.1: All distance measures for $|\alpha|^2 \in [0,1]$. The horizontal lines are the constant values of the distance measures of $\hat{T}_*$, the curved lines belong to T_*^{WZ}.

As expected, the Wootters-Zurek cloning map performs considerably worse than the optimal cloning map, and more specifically, is always perfectly line-symmetric around $|\alpha|^2 = 1/2$, which means that the cloning machine performs worse the more the input state move away from the two orthonormal basis elements (which are captured at $|\alpha|^2 = 0$ and $|\alpha|^2 = 1$ and are copied perfectly).

8.4. Equivalence with optimal cloning device of Bužek-Hillery

In the paper [BH96], the authors optimize a "universal quantum cloning machine" (UQCM), which means it should perform equally well for any input state, and should perform optimally with regards to the figures of merit in the previous section. Interestingly, their UQCM is familiar to us: it is in fact *exactly* $\hat{T}_*$ for the case $d = 2$, $N = 1$ and $M = 2$. In their paper, Bužek and Hillery propose a cloning machine that not only takes into account the Hilbert space of the input qubit, but also the Hilbert space of the quantum cloning machine itself (thus allowing themselves more degrees of freedom). They start from the defining equations that are a generalization of the Wootters-Zurek cloning machine described previously [BH96, Section III]:

$$|0\rangle_a |Q\rangle_x \to |00\rangle_{ab} |Q_0\rangle_x + |+\rangle_{ab} |Y_0\rangle_x \tag{8.25}$$

$$|1\rangle_a |Q\rangle_x \to |11\rangle_{ab} |Q_1\rangle_x + |+\rangle_{ab} |Y_1\rangle_x \tag{8.26}$$

where we define $|+\rangle := \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, and where $|Q_i\rangle_x$ and $|Y_i\rangle_x$ denotes the state of the quantum copying machine (system "x"), and all the states $|Q_i\rangle_x$ and $|Y_i\rangle_x$ are free parameters in their model. Note that this generalizes the Wootters-Zurek cloning machine by adding the $|+\rangle_{ab}$ term. After optimization the authors find the following expression for the resulting density matrix $\rho_{\text{ab}}^{(\text{out})}$, where it is assumed that $\alpha, \beta \in \mathbb{R}$:

$$\rho_{\text{ab}}^{(\text{out})} = \frac{2\alpha^2}{3} |00\rangle \langle 00| + \frac{\sqrt{2}\alpha\beta}{3} |00\rangle \langle +| + \frac{\sqrt{2}\alpha\beta}{3} |+\rangle \langle 00| + \frac{2(\alpha^2+\beta^2)}{6} |+\rangle \langle +| \tag{8.27}$$

$$+\frac{\sqrt{2}\alpha\beta}{3} |+\rangle \langle 11| + \frac{\sqrt{2}\alpha\beta}{3} |11\rangle \langle +| + \frac{2\beta^2}{3} |11\rangle \langle 11| \tag{8.28}$$

When we rewrite this into the matrix notation that we have adopted for the description of $\hat{T}_*$, we find:

$$\rho_{\text{ab}}^{(\text{out})} = \begin{pmatrix} 2\alpha^2/3 & \alpha\beta/3 & \alpha\beta/3 & 0 \\ \alpha\beta/3 & (\alpha^2+\beta^2)/6 & (\alpha^2+\beta^2)/6 & \alpha\beta/3 \\ \alpha\beta/3 & (\alpha^2+\beta^2)/6 & (\alpha^2+\beta^2)/6 & \alpha\beta/3 \\ 0 & \alpha\beta/3 & \alpha\beta/3 & 2\beta^2/3 \end{pmatrix} \tag{8.29}$$

which is exactly $\hat{T}_*(\sigma)$ for $\sigma = |\psi\rangle \langle\psi|$ with $\psi = \alpha |0\rangle + \beta |1\rangle$ if we assume $\alpha, \beta \in \mathbb{R}$.

In their conclusion, Bužek and Hillery write that they have only explored some of the possibilities, and thus do not know what the best input-state independent quantum-copying machine is. This question has now been answered in an even more general setting: such a cloning machine exists, namely $\hat{T}_*$, is unique, and coincides with the work that Bužek and Hillery have performed for the case $d = 2$, $N = 1$ and $M = 2$.

9 Conclusion

In this paper, the problem of quantum copying, limited by the No-Cloning Theorem, was studied by reviewing the work of [Wer98] and [KW99]. The problem of producing M clones from N provided copies (with $M > N$) revealed underlying symmetries that played a pivotal role in the proof of the existence and uniqueness of an optimal cloning device: these symmetries were the permutation invariance of the output clones, and the unitary covariance of the cloning device. Given the output system, permuting any number of clones should not affect the quantum state at all. Furthermore, rotating the quantum state by a unitary transformation *prior* to cloning should be identical to cloning and *a posteriori* rotating the output state by a unitary transformation. It was shown that the optimal cloning map has these properties, and that these two symmetries essentially prescribe the entire action of a cloning map, thus proving uniqueness of the optimal cloning map.

Remarkably, the (unique) proposed cloning map is optimal with regards to two different figures of merit: the first figure of merit considers the expectation value of the quantum state after cloning with respect to the ideal output, whilst the second figure of merit measures the difference in expectation values of an observable on *one* of the clones before and after cloning. As the first figure of merit considers the entire output quantum system, it allows for an easier symmetry argument to prove optimality and uniqueness of the proposed cloning map. To prove optimality and uniqueness with respect to the second figure of merit takes considerably more work, and requires more involved mathematical arguments.

Furthermore, this optimal cloning device has a remarkably "simple" form: it takes in a quantum system of size N, initializes all $M - N$ new copies in a maximally mixed state, considers the product of these states, and makes this quantum system of size M permutation invariant by a projection (that is, making sure that swapping two clones of the output does not change the output quantum system).

On top of that, this optimal cloning device has been compared to other literature: in the qubit case, its performance with respect to a single output clone has been compared to literature using a *shrinking factor* of the Bloch vector. In the even more specific case of copying one qubit to two qubits, the cloning device was compared to the universal quantum copying device proposed by [BH96]. It was discovered that the device of Bužek and Hillery is a specific instance of the optimal cloning device of Keyl and Werner, in the case of 1 input qubit and 2 output qubits.

The research into optimal quantum cloning is not merely of theoretical interest; quantum copiers can be used for eavesdropping [GH97] , or information retrieval in quantum computers [BH98]. With the advent of quantum computers and quantum networks, research into the theoretical limitations of quantum information theory is necessary to support the technological innovations.

Acknowledgments

I would like to thank both my supervisors Dr. B. Janssens and Dr. D. Elkouss for their guidance and supervision.

Appendices

A

Additional proofs

A.1. Dimensionality and basis of the Bose subspace $\mathcal{H}_+^{\otimes N}$

We wish to establish a basis of $\mathcal{H}_+^{\otimes N}$ and calculate $d[N] := \dim \mathcal{H}_+^{\otimes N}$. An important theorem to help is us Theorem 2.3.3, which tells us that $\mathcal{H}_+^{\otimes N}$ is precisely the span of vectors of the form $\phi^{\otimes N} \in \mathcal{H}^{\otimes N}$ (which is easier to work with than the definition depending on permutations). We thus show that tensors of that form can be written as a linear combination of a basis that is known in literature as the *occupation number basis*, and the proposition that this is indeed a basis for $\mathcal{H}_+^{\otimes N}$ then directly follows from linearity. Thus we must prove:

Theorem A.1.1. *Any vector $\phi^{\otimes N} \in \mathcal{H}_+^{\otimes N}$ can be written as*

$$\phi^{\otimes N} = \sqrt{N!} \sum_{n_1,\dots,n_d} \prod_{\kappa=1}^{d} \frac{\phi_k^{n_\kappa}}{\sqrt{n_\kappa!}} |n_1, \dots, n_d\rangle \tag{A.1}$$

where we use the occupation number basis with $\sum_\kappa n_\kappa = N$. This basis is orthonormal.

Furthermore, we have

$$d[N] := \dim \mathcal{H}_+^{\otimes N} = \binom{d+N-1}{N} \tag{A.2}$$

Proof. To prove this, consider any orthonormal basis $\{e_i\}$ for $\mathcal{H}$, and we construct:

$$\phi = \sum_{i=1}^{d} \phi_i e_i \qquad ; \qquad \phi^{\otimes N} = \left(\sum_{i_1=1}^{d} \phi_{i_1} e_{i_1} \right) \otimes \cdots \otimes \left(\sum_{i_1}^{d} \phi_{i_N} e_{i_N} \right) \tag{A.3}$$

Now we can rewrite this to:

$$\phi^{\otimes N} = \sum_{i_1=1}^{d} \sum_{i_2=1}^{d} \cdots \sum_{i_N=1}^{d} \phi_{i_1}\phi_{i_2}\cdots\phi_{i_N} \; e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_N} \tag{A.4}$$

We now see the motivation for this change of basis: many of the summands have the same coefficient $\phi_{i_1}\cdots\phi_{i_N}$, as this only depends on *how many times* a certain index appears, not *where* it appears. Given any setting $(i_1, \dots, i_N)$, let n_κ be the number of elements in this setting that are equal to the index κ, where $1 \le \kappa \le d$. We can then rewrite $\phi_{i_1}\cdots\phi_{i_N} = \phi_1^{n_1}\cdots\phi_d^{n_d}$.

Each of the d^N summands can be characterised by a setting $(i_1, \dots, i_N)$. Each of these settings has an associated configuration $(n_1, \dots, n_d)$ as specified above. Let

$$J := \left\{ (n_1, \dots, n_d) \;\middle|\; \forall \kappa \in \{1, \dots, d\} : n_\kappa \ge 0 \quad \text{and} \quad \sum_{\kappa=1}^{d} n_\kappa = N \right\} \tag{A.5}$$

be the set of all possible configurations. To each configuration, we can assign the set of all possible settings:

$$I(n_1,\ldots,n_d) := \left\{ (i_1,\ldots,i_N) \;\middle|\; \forall \kappa \in \{1,\ldots,d\} : [\text{nr. of indices in } (i_1,\ldots,i_d) \text{ equal to } \kappa] = n_\kappa \right\} \tag{A.6}$$

We can then rewrite the expression for $\phi^{\otimes N}$ as:

$$\phi^{\otimes N} = \sum_{(n_1,\ldots,n_d)\in J} \phi_1^{n_1}\cdots\phi_d^{n_d} \cdot \sum_{(i_1,\ldots,i_N)\in I(n_1,\ldots,n_d)} e_{i_1}\otimes\cdots\otimes e_{i_N} \tag{A.7}$$

We define the sum over $I(n_1,\ldots,n_d)$ as the basis element $|n_1,\ldots,n_d\rangle$, up to normalization.

To calculate the normalization constant, we take the inner product of the sum with itself. To shorten notation, we fix $n_1,\ldots,n_d$, so we can neglect the summation set $I(n_1,\ldots,n_d)$ in the summation sign.

$$\left\langle \sum_{i_1,\ldots,i_N} e_{i_1}\otimes\cdots\otimes e_{i_N} \;,\; \sum_{j_1,\ldots,j_N} e_{j_1}\otimes\cdots\otimes e_{j_N} \right\rangle = \sum_{i_1,\ldots,i_N}\sum_{j_1,\ldots,j_N} \langle e_{i_1}\otimes\cdots\otimes e_{i_N} \;,\; e_{j_1}\otimes\cdots\otimes e_{j_N}\rangle \tag{A.8}$$

Now the inner products on the right hand side equal either 1 when all $e_{i_k} = e_{j_k}$ for $k = 1$ to $k = N$, otherwise they equal 0. Thus, this simplifies to:

$$\sum_{i_1,\ldots,i_N}\sum_{j_1,\ldots,j_N} \langle e_{i_1}\otimes\cdots\otimes e_{i_N} \;,\; e_{j_1}\otimes\cdots\otimes e_{j_N}\rangle = \sum_{i_1,\ldots,i_N} 1 = \#I(n_1,\ldots,n_d) \tag{A.9}$$

The number of elements of I has a nice combinatoric interpretation, and we can calculate:

$$\#I(n_1,\ldots,n_d) = \frac{N!}{\prod_{i=1}^d n_i!} \tag{A.10}$$

If we define $|n_1,\ldots,n_d\rangle$ to have length one, we must thus compensate for this length, and we find:

$$\phi^{\otimes N} = \sum_{(n_1,\ldots,n_d)\in J} \phi_1^{n_1}\cdots\phi_d^{n_d} \frac{\sqrt{N!}}{\sqrt{\prod_{i=1}^d n_i!}} |n_1,\ldots,n_d\rangle \tag{A.11}$$

With some rewriting, this is equivalent to the statement we wished to prove.

Note that we can immediately see that $\{|n_1,\ldots,n_d\rangle\}$ is an orthonormal basis: for any two non-identical elements, at least one n_κ must differ for some $1 \le \kappa \le d$. In the inner product, we then see that all summands must equal zero, as all e_{i_k} must equal e_{j_k} for the inner product to not vanish, but this is impossible if a different amount of indices must be equal to κ for both elements. So indeed, the basis is orthonormal.

We can now also calculate the dimension of this symmetric subspace: $\#J$. This problem has a combinatoric interpretation, and is known as the *stars and bars* problem, and we can compute:

$$d[N] := \dim \mathcal{H}_+^{\otimes N} = \#J = \binom{d+N-1}{N} \tag{A.12}$$

□

A.2. Proof that $\sigma^{\otimes M}$ is a small projector onto $\mathcal{H}_+^{\otimes M}$

We prove our assertion first made in the proof 5.2:

Theorem A.2.1. *Consider a pure density matrix $\sigma \in \mathcal{S}(\mathcal{H})$, and its tensor power $\sigma^{\otimes M}$. Further, consider the permutation operator $P_\pi : \mathcal{H}^{\otimes M} \to \mathcal{H}^{\otimes M}$ for any $\pi \in \mathfrak{S}_M$. We then have*

$$\sigma^{\otimes M} P_\pi = P_\pi \sigma^{\otimes M} = \sigma^{\otimes M} \tag{A.13}$$

Proof. First, note that $\sigma = |\psi\rangle\langle\psi|$ for some $|\psi\rangle \in \mathcal{H}$. We can now look at the action of $\sigma^{\otimes M}$ on any state of the form $|\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_M\rangle \in \mathcal{H}^{\otimes M}$:

$$\sigma^{\otimes M}\left(|\phi_1\rangle \otimes \cdots \otimes |\phi_M\rangle\right) = \left(|\psi\rangle\langle\psi|\phi_1\rangle\right)\otimes\cdots\otimes\left(|\psi\rangle\langle\psi|\phi_M\rangle\right) = \left(\prod_{i=1}^{M}\langle\psi|\phi_i\rangle\right)|\psi\rangle\otimes|\psi\rangle\otimes\cdots\otimes|\psi\rangle \quad (A.14)$$

The resulting state is clearly permutation invariant, and thus in $\mathcal{H}_+^{\otimes M}$. By linearity, $\sigma^{\otimes M}$ acting on any linear combination of these kind of basis vectors also results in a state in $\mathcal{H}_+^{\otimes M}$. This also directly tells us that $P_\pi \sigma^{\otimes M} = \sigma^{\otimes M}$, as any permutation operator leaves permutation invariant states unchanged.

To prove $\sigma^{\otimes M} P_\pi = \sigma^{\otimes M}$, we can manually compute, again for an state of the form $|\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_M\rangle \in \mathcal{H}^{\otimes M}$:

$$\sigma^{\otimes M} P_\pi\left(|\phi_1\rangle \otimes \cdots \otimes |\phi_M\rangle\right) = \sigma^{\otimes M}\left(|\phi_{\pi^{-1}(1)}\rangle \otimes \cdots \otimes |\phi_{\pi^{-1}(M)}\rangle\right) \quad (A.15)$$

Using the previous expression, we know that this must evaluate to:

$$\left(\prod_{i=1}^{M}\langle\psi|\phi_{\pi^{-1}(i)}\rangle\right)|\psi\rangle\otimes\cdots\otimes|\psi\rangle \quad (A.16)$$

Note that the product in brackets is independent of which $\pi \in \mathfrak{S}_M$ is chosen. Thus, this evaluates nicely to

$$\left(\prod_{i=1}^{M}\langle\psi|\phi_i\rangle\right)|\psi\rangle\otimes|\psi\rangle\otimes\cdots\otimes|\psi\rangle = \sigma^{\otimes M}\left(|\phi_1\rangle \otimes \cdots \otimes |\phi_M\rangle\right) \quad (A.17)$$

Thus indeed $\sigma^{\otimes M} = \sigma^{\otimes M} P_\pi = P_\pi \sigma^{\otimes M}$. As a corollary, we immediately see that $\sigma^{\otimes M} = \sigma^{\otimes M} S_M = S_M \sigma^{\otimes M}$, as S_M is an average over permutation operators. □

A.3. PROOF THAT $P_\pi a_{(k)} P_\pi^* = a_{(\pi(k))}$

Theorem A.3.1. *Given a permutation $\pi \in \mathfrak{S}_M$, an observable $a_{(k)} \in \mathcal{B}(\mathcal{H}^{\otimes M})$ with an index $1 \leq k \leq M$. We can then prove that*

$$P_\pi a_{(k)} P_\pi^* = a_{(\pi(k))} \quad (A.18)$$

Proof. We can show this by computing what happens to an arbitrary $\psi_1 \otimes \cdots \otimes \psi_M \in \mathcal{H}^{\otimes M}$. Note first, that

$$P_\pi^* P_\pi = \mathrm{Id}_{\mathcal{H}}^{\otimes M} \implies P_\pi^* = P_\pi^{-1} = P_{\pi^{-1}} \quad (A.19)$$

Then we can compute:

$$a_{(k)}\ P_{\pi^{-1}}\ \left(\psi_1 \otimes \cdots \otimes \psi_M\right) = a_{(k)}\ \left(\psi_{\pi(1)} \otimes \cdots \otimes \psi_{\pi(M)}\right) = \quad (A.20)$$

$$\psi_{\pi(1)} \otimes \cdots \otimes \psi_{\pi(k-1)} \otimes \left(a\psi_{\pi(k)}\right) \otimes \psi_{\pi(k+1)} \otimes \cdots \otimes \psi_{\pi(M)} \quad (A.21)$$

Then applying P_π shall put all elements back in the right order. Thus, whilst $a_{(k)}$ acts on *place* k, the current element there is $\psi_{\pi(k)}$ (as the first permutation is π^{-1}). This element needs to be shifted back to its original position by the permutation π, but takes the action of a with it. Thus, $a_{(k)}$ acts on $\psi_{\pi(k)}$, and thus we can write $P_\pi a_{(k)} P_\pi^* = a_{(\pi(k))}$. □

A.4. PROOF THAT $R_T(\sigma)$ COMMUTES WITH ALL ELEMENTS OF S'

Theorem A.4.1. *Given any density operator $\sigma \in \mathcal{S}(\mathcal{H})$. Let*

$$S := Span\{\sigma, Id_{\mathcal{H}}\} \qquad ; \qquad S' := \{A \in \mathcal{B}(\mathcal{H})\ :\ AB = BA \quad \forall B \in S\} \quad (A.22)$$

Recall that $R_T(\sigma) := R\left(T\left(\sigma^{\otimes N}\right)\right)$ is the partial trace over all but the first quantum copy (i.e. partial trace over $M-1$ dimensions). We have: $R_T(\sigma) \in S'' := (S')'$.

Proof. Recall that we have already proven that for any unitary $u \in S' \implies [R_T(\sigma), u] = 0$. We need to extend this argument to any operator in S'. We prove that any $A \in S'$ can be written as a linear combination of unitary operators in S', which directly implies that $R_T(\sigma)$ commutes with A.

Thus, take any $A \in S'$. If A is unitary, we are done. Otherwise, let us look at the eigenspaces of σ: as σ is an Hermitian matrix, we have

$$\mathcal{H} = \bigoplus_{\lambda} E_\lambda \tag{A.23}$$

where the direct sum ranges over all eigenvalues λ of σ, and E_λ the associated eigenspaces. Thus, there exists a basis for $\mathcal{H}$ in which σ is a diagonal matrix:

$$\sigma = \left(\begin{array}{cc|ccc|c} \lambda_1 & & & & & \\ & \lambda_1 & & & & \\ \hline & & \lambda_2 & & & \\ & & & \lambda_2 & & \\ & & & & \lambda_2 & \\ \hline & & & & & \ddots \end{array}\right) = \mathrm{diag}(\lambda_1, \lambda_1, \lambda_2, \lambda_2, \lambda_2, \ldots, \lambda_n) \tag{A.24}$$

where λ_i denote the eigenvalues of σ, and n the amount of distinct eigenvalues. In this basis, any operator that commutes with σ can be written as

$$A = \left(\begin{array}{c|c|c} A_1 & & \\ \hline & A_2 & \\ \hline & & \ddots \end{array}\right) \tag{A.25}$$

where A_i is a matrix with dimensions equal to the amount of times λ_i appears in the expression for σ.

We would like to decompose each A_i into a linear combination of unitaries. This is actually possible for any complex matrix, see for example [Wu94]. Thus, we can write for $1 \leq i \leq n$: $A_i = \sum_j c^i_j u^i_j$ for some $c^i_j \in \mathbb{C}$ and unitaries u^i_j. We can then rewrite:

$$A = \begin{pmatrix} \sum_j c^1_j u^1_j & & & \\ & \sum_j c^2_j u^2_j & & \\ & & \sum_j c^3_j u^3_j & \\ & & & \ddots \end{pmatrix} \tag{A.26}$$

However, it is not clear from this decomposition that this is actually a linear combination of unitaries in S', as these unitaries act on the *entire* Hilbert space $\mathcal{H}$, whilst each u^i_j here only acts on a part. We must thus rewrite:

$$A = \sum_j c^1_j \begin{pmatrix} u^1_j & & & \\ & I_2 & & \\ & & I_3 & \\ & & & \ddots \end{pmatrix} + \sum_j c^2_j \begin{pmatrix} I_1 & & & \\ & u^2_j & & \\ & & I_3 & \\ & & & \ddots \end{pmatrix} + \sum_j c^3_j \begin{pmatrix} I_1 & & & \\ & I_2 & & \\ & & u^3_j & \\ & & & \ddots \end{pmatrix} + \tag{A.27}$$

$$\ldots \quad - \begin{pmatrix} I_1 \sum_{i\neq 1} \sum_j c^i_j & & & \\ & I_2 \sum_{i\neq 2} \sum_j c^i_j & & \\ & & I_3 \sum_{i\neq 3} \sum_j c^i_j & \\ & & & \ddots \end{pmatrix} \tag{A.28}$$

Each of the diagonal block matrices on the right hand side are unitary because each u^i_j is unitary. We only need to check the last matrix. We can again write this matrix as a linear combination of unitary block-matrices. Let us first rewrite the last matrix in the expression for A, by using for $1 \leq i \leq n$:

$\alpha_i := \sum_{k\neq i} \sum_j c_j^k$, as:

$$\begin{pmatrix} I_1 \sum_{i\neq 1} \sum_j c_j^i & & & \\ & I_2 \sum_{i\neq 2} \sum_j c_j^i & & \\ & & I_3 \sum_{i\neq 3} \sum_j c_j^i & \\ & & & \ddots \end{pmatrix} := \Gamma := \mathrm{diag}(\alpha_1 I_1, \dots, \alpha_n I_n) \tag{A.29}$$

We then see that any matrix of the form $\mathrm{diag}(q_1 I_1, \dots, q_n I_n)$ is unitary if for all q_i we choose $|q_i| = 1$. We can definitely write Γ as a linear combination of the $\mathrm{diag}(q_1 I_1, \dots, q_n I_n)$ matrices. To prove this, note that any of these matrices can be identified one-on-one by the numbers $\{q_i\}_{i=1}^n$, thus there is a bijection between the set of all these matrices and the set

$$Q \equiv \left\{ \begin{pmatrix} q_1 \\ \vdots \\ q_n \end{pmatrix} \;\middle|\; |q_i| = 1 \;\forall i = 1, \dots, n \right\} \tag{A.30}$$

Identifying the vector $(\alpha_1, \dots, \alpha_n)^T \in \mathbb{C}^n$ with our matrix Γ, we need to show that $\mathrm{Span}\{Q\} = \mathbb{C}^n$, because if this assertion holds, then surely $(\alpha_1, \dots, \alpha_n)^T$ can be written as a linear combination of elements from Q, thus solving our original problem. But this definitely is the case. Let us formally prove this assertion by writing, for any canonical basis element e_i:

$$e_i = \frac{1}{2}(1, \dots, 1)^T - \frac{1}{2}(1, \dots, 1, -1, 1, \dots, 1)^T \in \mathrm{Span}\{Q\} \tag{A.31}$$

where -1 of the second vector is placed at the i-th entry. Thus we must be able to write Γ as a linear combination of block-unitaries. This concludes the proof that any operator A can be written as a linear combination of block unitaries that commute with σ. □

A.5. Proof that $\gamma(\hat{T}) = \frac{N}{N+d} \cdot \frac{M+d}{M}$

Theorem A.5.1. *We have* $\gamma(\hat{T}) = \frac{N}{N+d} \cdot \frac{M+d}{M}$

Proof. We have already found

$$\gamma(\hat{T}) + \frac{1-\gamma(\hat{T})}{d} = \frac{d[N]}{d[M]\cdot M}\left(N\frac{d[M]}{d[N]} + (M-N)\frac{d[M]}{d[N+1]}\right) \tag{A.32}$$

Note that

$$\frac{d[N]}{d[N+1]} = \frac{\binom{d+N-1}{N}}{\binom{d+N}{N+1}} = \frac{(d+N-1)!}{N!\cdot(d-1)!}\cdot\frac{(N+1)!\cdot(d-1)!}{(d+N)!} = \frac{N+1}{d+N} \tag{A.33}$$

such that we can rewrite the expression to

$$\gamma(\hat{T}) + \frac{1-\gamma(\hat{T})}{d} = \frac{N}{M} + \frac{M-N}{M}\cdot\frac{N+1}{N+d} \tag{A.34}$$

We start with:

$$\gamma + \frac{1-\gamma}{d} = \frac{N}{M} + \frac{M-N}{M}\cdot\frac{N+1}{d+N} = \frac{N(d+N)}{M(d+N)} + \frac{(M-N)(N+1)}{M(d+N)} = \frac{dN+N^2+NM+M-N^2-N}{M(d+N)} \tag{A.35}$$

Thus we find

$$\gamma = \frac{1}{1-\frac{1}{d}}\left(\frac{dN+N^2+NM+M-N^2-N}{M(d+N)} - \frac{1}{d}\right) = \frac{d}{d-1}\left(\frac{dN+N^2+NM+M-N^2-N}{M(d+N)} - \frac{1}{d}\right) \tag{A.36}$$

From which we can deduce

$$\gamma = \frac{1}{d-1}\cdot\frac{1}{M(d+N)}\left(d^2N + dN^2 + dNM + dM - dN^2 - dN - dM - NM\right) \tag{A.37}$$

Cancelling the dN^2 and dM terms, we find:

$$\gamma = \frac{1}{d-1} \cdot \frac{1}{M(d+N)} \left(d^2N + dNM - dN - NM\right) \tag{A.38}$$

the term in the brackets nicely factors into $(d-1)(dN+NM)$, thus completing the proof:

$$\gamma = \frac{dN+NM}{M(d+N)} = \frac{N}{d+N} \cdot \frac{d+M}{M} \tag{A.39}$$

□

A.6. Proof that the supremum $\hat{\mathcal{F}}$ is attained

Theorem A.6.1. *There exist quantum operations $\hat{T}_*$ such that*

$$\mathcal{F}(\hat{T}_*) = \hat{\mathcal{F}} := \sup_{T_*} \mathcal{F}(T_*) \tag{A.40}$$

We prove that $\mathcal{F}$ is an upper semicontinuous function, and the set of quantum operations is compact, which proves that $\hat{\mathcal{F}}$ is indeed attained for some cloning map T_*.

A.6.1. Proof that the set of quantum operations is compact

We need to prove that

$$\Gamma := \left\{ T_* \;\middle|\; T_* : \mathcal{B}(\mathcal{H}_+^{\otimes N}) \to \mathcal{B}(\mathcal{H}^{\otimes M}) \text{ and } T_* \text{ is linear and CPTP} \right\} \tag{A.41}$$

is compact. As we work on finite dimensional Hilbert spaces, we can use Heine-Borel: we need to prove that Γ is closed and bounded.

Proof that the set is bounded

Note that we are free to choose whichever norm we prefer, as we work finite-dimensionally, and thus all norms are equivalent. We are thus free to choose the naturally induced supremum norm on cloning machines:

$$\|T_*\| := \sup\left\{ \|T_*(A)\|_{\mathcal{B}(\mathcal{H}^{\otimes M})} \;:\; A \in \mathcal{B}\left(\mathcal{H}_+^{\otimes N}\right) \;,\; \|A\|_{\mathcal{B}(\mathcal{H}_+^{\otimes N})} = 1 \right\} \tag{A.42}$$

We are again free to choose a norm on $\mathcal{B}(\mathcal{H}^{\otimes M})$ and $\mathcal{B}(\mathcal{H}_+^{\otimes N})$. We choose again the induced supremum norm:

$$\|A\|_{\mathcal{B}(\mathcal{H}^{\otimes M})} := \sup\left\{ \|A\psi\|_{\mathcal{H}^{\otimes M}} \;:\; \psi \in \mathcal{H}^{\otimes M} \;,\; \|\psi\|_{\mathcal{H}^{\otimes M}} = 1 \right\} \tag{A.43}$$

and similarly the norm on $\mathcal{B}(\mathcal{H}_+^{\otimes N})$. Now we can use the fact that Hilbert space come equipped with a canonical inner product:

$$\|\psi\|_{\mathcal{H}^{\otimes M}} = \sqrt{\langle \psi \mid \psi \rangle} \qquad \psi \in \mathcal{H}^{\otimes M} \tag{A.44}$$

and similarly for vectors in $\mathcal{H}_+^{\otimes M}$. To shorten notation, we will use $\|\cdot\|_{B,M}$ to denote the norm on $\mathcal{B}(\mathcal{H}^{\otimes M})$, $\|\cdot\|_{B,N}$ to denote the norm on $\mathcal{B}(\mathcal{H}_+^{\otimes N})$, $\|\cdot\|_M$ to denote the norm on $\mathcal{H}^{\otimes M}$, and $\|\cdot\|_N$ to denote the norm on $\mathcal{H}_+^{\otimes N}$.

Norm inequality for positive operators We will first prove that for any **positive** operator $X \in \mathcal{B}(\mathcal{H}_+^{\otimes N})$ we have (where we write $X = A^*A$ for some operator A):

$$\|T_*(X)\|_{B,M} = \|T_*(A^*A)\|_{B,M} \leq \|A\|_{B,N}^2 = \|A^*A\|_{B,N} = \|X\|_{B,N} \tag{A.45}$$

We know that for any operator A, we have $A^*A \geq 0$. We claim that then also:

$$\|A\|_{B,N}^2 \mathrm{Id}_{\mathcal{H}_+^{\otimes N}} - A^*A \geq 0 \iff \langle \psi \mid \|A\|_{B,N}^2 \mathrm{Id}_{\mathcal{H}_+^{\otimes N}} - A^*A \mid \psi \rangle \geq 0 \;\forall \psi \in \mathcal{H}_+^{\otimes N} \;,\; \|\psi\|_N = 1 \tag{A.46}$$

$$\iff \|A\|_{B,N}^2 - \|A\psi\|_N^2 \geq 0 \;\forall \psi \in \mathcal{H}_+^{\otimes N} \;,\; \|\psi\|_N = 1 \tag{A.47}$$

and the last statement holds by definition of the supremum norm.

But then, as T_* is CPTP, we can surely write:

$$T_*\left(\|A\|_{B,N}^2 \mathrm{Id}_{\mathcal{H}_+^{\otimes N}} - A^*A \right) \geq 0 \iff \|A\|_{B,N}^2 \mathrm{Id}_{\mathcal{H}^{\otimes M}} \geq T_*(A^*A) \tag{A.48}$$

from which our claim follows.

Norm inequality for general operators Now that we can estimate the norm of T in the case of positive operators, we focus on decomposing general operators into (linear combinations of) positive operators. In general, for an operator X, we can decompose:

$$X = \frac{X + X^*}{2} + i\frac{X - X^*}{2i} := H + iH' \tag{A.49}$$

where one can check that H and H' are both Hermitian. Consider H. We can decompose this self-adjoint operator into the difference of two positive operators. To see this, construct an orthonormal basis $\{|\psi_\lambda\rangle\}_{\lambda\in\sigma(H)}$ of H (where $\sigma(H)$ denotes the spectrum of H) and write:

$$H = \sum_{\lambda\in\sigma(H)} \lambda\,|\psi_\lambda\rangle\,\langle\psi_\lambda| = \left(\sum_{\lambda>0} \lambda\,|\psi_\lambda\rangle\,\langle\psi_\lambda|\right) - \left(\sum_{\lambda\leq 0} -\lambda\,|\psi_\lambda\rangle\,\langle\psi_\lambda|\right) = A_1 - A_2 \tag{A.50}$$

where by construction it is evident that both A_1 and A_2 are positive operators. We repeat this process for H' and decompose it into $A_3 - A_4$. But then we have

$$\|T_*(X)\|_{B,M} \leq \sum_{k=1}^{4} \|T(A_k)\|_{B,M} \leq \sum_{k=1}^{4} \|A_k\|_{B,N} \tag{A.51}$$

where the first inequality follows from the properties of any norm, and the second inequality follows from our previous proof because each A_k is a positive operator. Finally, we need to find an estimate for each A_k in terms of X. We first rewrite this to norms over H and H'. Note that

$$\|H\|_{B,N} = \max\{|\lambda| \;:\; \lambda\in\sigma(H)\} = \max\{\|A_1\|_{B,N}, \|A_2\|_{B,N}\} \tag{A.52}$$

thus, we can safely write (analogously for H'):

$$\|A_1\|_{B,N} + \|A_2\|_{B,N} \leq 2\|H\|_{B,N} \qquad ; \qquad \|A_3\|_{B,N} + \|A_4\|_{B,N} \leq 2\|H'\|_{B,N} \tag{A.53}$$

But for H and H' we have

$$\|H\|_{B,N} = \left\|\frac{X + X^*}{2}\right\|_{B,N} \leq \frac{1}{2}\|X\|_{B,N} + \frac{1}{2}\|X^*\|_{B,N} \tag{A.54}$$

To calculate $\|X^*\|_{B,N}$, note that for any $\psi \in \mathcal{H}_+^{\otimes N}$ with $\|\psi\|_N = 1$:

$$\|X^*\psi\|_N^2 = \langle X^*\psi \mid X^*\psi\rangle = \langle\psi \mid XX^*\psi\rangle \leq \|\psi\|_N \cdot \|XX^*\psi\|_N \leq \|XX^*\|_{B,N} = \|X\|_{B,N}^2 \tag{A.55}$$

where we have used Cauchy-Schwarz in the first equality, then the fact that $\|\psi\|_N = 1$ and the definition of the supremum norm.

Putting this together, we have now found that (analogous for H'):

$$\|H\|_{B,N} \leq \|X\|_{B,N} \qquad ; \qquad \|H'\|_{B,N} \leq \|X\|_{B,N} \tag{A.56}$$

But then we indeed have

$$\|T(X)\|_{B,M} \leq \sum_{k=1}^{4} \|A_k\|_{B,N} \leq 2\|H\|_{B,N} + 2\|H'\|_{B,N} \leq 4\|X\|_{B,N} \tag{A.57}$$

from which it directly follows that $\|T\| \leq 4$ and thus surely the set is bounded.

Proof that the set is closed

We prove that Γ is closed. We can construct this as follows:

$$\Gamma = \bigcap_{k\geq 1} \Gamma_k \qquad ; \qquad \Gamma_k = \left\{T_* \;\middle|(T_* \otimes \mathrm{Id}_k) \geq 0 \;;\; T_* \text{ linear and TP}\right\} \tag{A.58}$$

i.e. the intersection of all maps that are k-positive for all k. We can prove that Γ_k is closed for any $k \in \mathbb{Z}_{>0}$. Let $(T_{*n})_{n\geq 1}$ a convergent sequence in Γ_k, and let $T_* = \lim_{n\to\infty} T_{*n}$ (where the limit is taken in the operator norm specified above). We then see:

- T_* is linear:

$$\lim_{n\to\infty} T_{*n}(\rho+\sigma) = \lim_{n\to\infty} \left(T_{*n}(\rho)+T_{*n}(\sigma)\right) = \lim_{n\to\infty} T_{*n}(\rho) + \lim_{n\to\infty} T_{*n}(\sigma) = T_*(\rho)+T_*(\sigma) \quad \text{(A.59)}$$

  for any $\rho, \sigma \in \mathcal{B}(\mathcal{H}_+^{\otimes N})$.

- T_* is trace preserving:

$$\mathrm{Tr}\left[T_*(\rho)\right] = \mathrm{Tr}\left[\lim_{n\to\infty} T_{*n}(\rho)\right] = \lim_{n\to\infty} \mathrm{Tr}\left[T_{*n}(\rho)\right] = 1 \quad \text{(A.60)}$$

  for any $\rho \in \mathcal{B}(\mathcal{H}_+^{\otimes N})$, where we can swap limit and trace as the trace is a linear operator.

- T_* is k-positive:

$$\rho \geq 0 \implies \left(T_{*n}\otimes \mathrm{Id}_k\right)(\rho) \geq 0 \; \forall n \in \mathbb{Z}_{>0} \implies \lim_{n\to\infty} \left(T_{*n}\otimes \mathrm{Id}_k\right)(\rho) \geq 0 \quad \text{(A.61)}$$

  this claim holds by a notion of continuity: the characteristic polynomial of $(T_{*n}\otimes \mathrm{Id}_k)$ must converge to the characteristic polynomial of $(T_*\otimes \mathrm{Id}_k)$, and thus so must the eigenvalues. As for each n, all eigenvalues are nonnegative, their limit must be as well, and thus the limit map is in turn positive.

  and thus

$$\rho \geq 0 \implies \left(\lim_{n\to\infty} T_{*n}\otimes \mathrm{Id}_k\right)(\rho) \geq 0 \implies \left(T_*\otimes \mathrm{Id}_k\right)(\rho) \geq 0 \quad \text{(A.62)}$$

  where we can swap the tensor product and the limit, which can be seen if we would write out all matrix elements: the limit of the tensor product $T_{*n}\otimes \mathrm{Id}_k$ is then the tensor product of the limit of T_{*n} and Id_k.

But then each Γ_k is closed, and thus Γ is closed.

A.6.2. Proof that the fidelity $\mathcal{F}$ is upper semicontinuous

By [CDA06, page 43] , a functional $f : A \to \mathbb{R}$ on a topological space A is upper semicontinuous if

$$\forall c \in \mathbb{R} \;:\; \{x \in A \;:\; f(x) \geq c\} \text{ is closed} \quad \text{(A.63)}$$

With this, we prove the following lemma:

Lemma A.6.2. *Let $f_\alpha : A \to \mathbb{R}$ be a collection of upper semicontinuous functionals labelled by $\alpha \in \mathcal{I}$ for some index set $\mathcal{I}$. Then $f(a) := \inf_{\alpha\in\mathcal{I}} f_\alpha(a)$ is also upper semicontinuous*

Proof. Observe that, for any $c \in \mathbb{R}$:

$$\bigcap_{\alpha\in\mathcal{I}} \{x \in A \;:\; f_\alpha(x) \geq c\} = \{x \in A \;:\; f(x) \geq c\} \quad \text{(A.64)}$$

Note that, for any $c \in \mathbb{R}$, the set on the left-hand side is closed as each f_α is upper semicontinuous and intersections of closed sets are closed. But then the right-hand side is closed for all $c \in \mathbb{R}$, and thus f is indeed upper semicontinuous. □

To apply the lemma, we write

$$\mathcal{F}(T_*) = \inf_\sigma \mathrm{Tr}\left[\sigma^{\otimes M} T_*\left(\sigma^{\otimes N}\right)\right] := \inf_\sigma f_\sigma(T_*) \qquad ; \qquad f_\sigma(T_*) = \mathrm{Tr}\left[\sigma^{\otimes M} T_*\left(\sigma^{\otimes N}\right)\right] \quad \text{(A.65)}$$

Then clearly, each $f_\sigma(T_*)$ is continuous in T_*, as the trace is a linear operator and thus continuous. But continuous functions are also upper semicontinuous, so we can apply our lemma to $\mathcal{F}$. Thus, $\mathcal{F}$ is upper semicontinuous.

A.7. Proof that ξ is continuous

Theorem A.7.1. *Given $V : \mathcal{H}_+^{\otimes M} \to \mathcal{H}_+^{\otimes N} \otimes \mathcal{K}$, and given that for any $\psi^{\otimes M} \in \mathcal{H}_+^{\otimes M}$:*

$$V\psi^{\otimes M} = \psi^{\otimes N} \otimes \xi(\psi) \qquad ; \qquad \xi(\psi) \in \mathcal{K} \tag{A.66}$$

Then ξ must depend continuously on ψ.

Proof. Recall that we have already proven, for any $\phi, \psi \in \mathcal{H}$ with $\langle \phi \mid \psi \rangle \neq 0$:

$$\langle \xi(\phi) \ , \ \xi(\psi) \rangle = \langle \phi \mid \psi \rangle^{M-N} \tag{A.67}$$

We construct the map T_ψ for any $\psi \in \mathcal{H}_+^{\otimes N}$:

$$T_\psi : \mathcal{H}_+^{\otimes N} \otimes \mathcal{K} \to \mathcal{K} \qquad ; \qquad a \in \mathcal{H}_+^{\otimes N} \ , \ b \in \mathcal{K} \ : \ T_\psi(a \otimes b) = \langle \psi \mid a \rangle \cdot b \tag{A.68}$$

By construction, T_ψ is linear in a and b, and anti-linear in ψ. Thus, T_ψ is continuous for any ψ. We can choose $\psi = \phi^{\otimes N}$ for any $\phi \in \mathcal{H}$. We then have:

$$T_{\phi^{\otimes N}} \left(V\phi^{\otimes M} \right) = T_{\phi^{\otimes N}} \left(\phi^{\otimes N} \otimes \xi(\phi) \right) = \langle \phi^{\otimes N} \mid \phi^{\otimes N} \rangle \cdot \xi(\phi) = \langle \phi \mid \phi \rangle^N \xi(\phi) \tag{A.69}$$

As V is an isometry, it is linear and thus also continuous. Compositions of continuous maps are contnuous. thus $T_{\phi^{\otimes N}} \circ V$ is continuous. Then, we have for any $\phi \neq 0$:

$$\xi(\phi) = \frac{T_{\phi^{\otimes N}} \left(V\phi^{\otimes M} \right)}{\langle \phi \mid \phi \rangle^N} \tag{A.70}$$

And thus ξ is continuous everywhere, except possibly at 0. Now, for any $\phi \neq 0$ we have $\langle \xi(\phi) \mid \xi(\phi) \rangle = \langle \phi \mid \phi \rangle^{M-N}$, such that $\|\xi(\phi)\| = \|\phi\|^{M-N}$, thus to make ξ continuous everywhere, we set $\xi(0) = 0$. □

Corollary A.7.2. *We have $\langle \xi(\phi) \mid \xi(\psi) \rangle = 0$ for $\langle \phi \mid \psi \rangle = 0$*

Proof. Let $(\phi_n)_{n \geq 1}$ denote the sequence given by $\phi_n = \phi + \frac{1}{n}\psi$, such that $\phi_n \to \phi$ for $n \to \infty$. We then have

$$\langle \xi(\phi) \mid \xi(\psi) \rangle = \langle \lim_{n\to\infty} \xi(\phi_n) \mid \xi(\psi) \rangle = \lim_{n\to\infty} \langle \xi(\phi_n) \mid \xi(\psi) \rangle \tag{A.71}$$

The key insight is now that, as $\langle \phi_n \mid \psi \rangle = \frac{1}{n}\|\psi\|^2 \neq 0$ for any $n \in \mathbb{Z}_{>0}$, we can apply:

$$\lim_{n\to\infty} \langle \xi(\phi_n) \mid \xi(\psi) \rangle = \lim_{n\to\infty} \langle \phi_n \mid \psi \rangle^{M-N} = \langle \phi \mid \psi \rangle^{M-N} = 0 \tag{A.72}$$

□

A.8. Solution to the optimization problem in calculating $\Delta_{\text{ONE}}(T)$

Theorem A.8.1. *Given the optimalisation problem*

$$\max \sum_{i=1}^{d} \lambda_i \left(d\beta_i - 1 \right) \tag{A.73}$$

$$s.t. \quad 0 \leq \lambda_i \leq 1 \qquad \forall i \in \{1, \ldots, d\} \tag{A.74}$$

$$\beta_i \geq 0 \qquad \forall i \in \{1, \ldots, d\} \tag{A.75}$$

$$\sum_{i=1}^{d} \beta_i = 1 \tag{A.76}$$

An optimal solution to this optimalisation problem is $\hat{\lambda}_1 = 1$, $\hat{\beta}_1 = 1$, and $\hat{\lambda}_i = \hat{\beta}_i = 0$ for all $i \in \{2, \ldots, d\}$, which yields a value of $d - 1$.

Proof. [1] First note that for each i, we either have $\hat{\lambda}_i = 0$ or $\hat{\lambda}_i = 1$. This is due to the following: for each i, we have three possibilities:

[1] Largely inspired by the insight of fellow student Nando Leijenhorst

- $d\hat{\beta}_i - 1 < 0$: in this case, decreasing the value of λ_i increases the overall sum, such that we must have $\hat{\lambda}_i = 0$
- $d\hat{\beta}_i - 1 > 0$: in this case, increasing the value of λ_i increases the overall sum, such that we must have $\hat{\lambda}_i = 1$
- $d\hat{\beta}_i - 1 = 0$: in this case, the value of λ_i does not matter, such that we can choose $\hat{\lambda}_i = 1$ for convenience.

We thus immediately see that $\hat{\beta}_i = 0 \implies \hat{\lambda}_i = 0$. We now prove that the converse also holds. Assume there is a $\hat{\lambda}_i = 0$ for which $\hat{\beta}_i \neq 0$. There must be a j such that $d\hat{\beta}_j - 1 > 0$: the summing condition of β_i cannot hold if all $\beta_i < \frac{1}{d}$, and the situation that all $\hat{\beta}_i = \frac{1}{d}$ is excluded by the fact that our proposed solution in the Lemma has a value of $d - 1 > 0$, whilst this solution has a value of 0. Thus by the previous statement also $\hat{\lambda}_j = 1$. We can now find a better solution by setting $\hat{\beta}_i' = 0$ and $\hat{\beta}_j' = \hat{\beta}_j + \hat{\beta}_i$, as decreasing β_i' does not actually impact the sum as $\hat{\lambda}_i = 0$. But we cannot improve an optimal solution, so our assumption is incorrect. Thus indeed $\hat{\lambda}_i = 0 \implies \hat{\beta}_i = 0$, and so we now have $\hat{\lambda}_i = 0 \iff \hat{\beta}_i = 0$.

As the optimisation problem is invariant under permutation of the indices, we can first sum over all indices for which $\lambda_i = 1$. Say there are k such indices, for $1 \leq k \leq d$. We can forget about all other indices, as we have $\lambda_j = 0$ for these indices, and $\lambda_j = 0 \implies \beta_j = 0$ as proven previously, thus we must still have $\sum_{i=1}^{k} \beta_i = 1$. We thus now have the problem:

$$\max \sum_{i=1}^{k} d\beta_i - 1 \tag{A.77}$$

$$\text{s.t.} \qquad \beta_i \geq 0 \qquad \forall i \in \{1, \ldots, d\} \tag{A.78}$$

$$\sum_{i=1}^{k} \beta_i = 1 \tag{A.79}$$

$$1 \leq k \leq d \tag{A.80}$$

But this problem is rather trivial, as we have

$$\max \sum_{i=1}^{k} d\beta_i - 1 = \max \left[d \left(\sum_{i=1}^{k} \beta_i \right) - k \right] = d \cdot 1 - k = d - k \tag{A.81}$$

where we have used the second constraint. We achieve this maximum by setting $k = 1$, $\beta_1 = 1$. Thus we have found an optimal solution to our original problem: we set $\hat{\beta}_1 = 1$, and thus also $\hat{\lambda}_1 = 1$, and for all other indices i we set $\hat{\beta}_i = 0$ and $\hat{\lambda}_i = 0$, thus proving our proposition. □

A.9. Derivation of the second constraint to $\omega(T_{\alpha\beta})$

Theorem A.9.1. *Given* $\alpha, \beta, \gamma \in \frac{1}{2}\mathbb{Z}_{\geq 0}$. *Given*

$$|\alpha - \beta| \leq \gamma \leq \alpha + \beta \tag{A.82}$$

This is equivalent to

$$|\alpha - \gamma| \leq \beta \leq \alpha + \gamma \tag{A.83}$$

Proof. We expand on the left inequality:

$$|\alpha - \beta| \leq \gamma \iff -\gamma \leq \alpha - \beta \leq \gamma \iff -\gamma - \alpha \leq -\beta \leq \gamma - \alpha \tag{A.84}$$

which is equivalent to $\alpha - \gamma \leq \beta \leq \alpha + \gamma$.

We combine this with the right inequality which reads $\beta \geq \gamma - \alpha$. Firstly, we also have $\beta \geq \alpha - \gamma$, which can be combined to $\beta \geq |\alpha - \gamma|$. We also have $\beta \leq \alpha + \gamma$. Thus, we have

$$|\alpha - \gamma| \leq \beta \leq \alpha + \gamma \tag{A.85}$$

□

A.10. Derivation of the expression for $\max \omega(T_{\alpha\beta})$

Theorem A.10.1. *Given $\alpha = M/2$, $\beta = (M-N)/2$, we have*

$$\omega(T_{\alpha\beta}) = \frac{1}{2} + \frac{1}{2}\frac{\alpha(\alpha+1) - \beta(\beta+1)}{(N/2)(N/2+1)} = \frac{M+2}{N+2} \tag{A.86}$$

Proof.

$$\omega(T_{\alpha\beta}) = \frac{1}{2} + \frac{M^2/4 + M/2 - (M-N)^2/4 - (M-N)/2}{(N/2)(N+2)} = \tag{A.87}$$

$$\frac{(1/2)(N+2)}{(N+2)} + \frac{M^2/4 + M/2 - M^2/4 - N^2/4 + MN/2 - M/2 + N/2}{(N/2)(N+2)} = \tag{A.88}$$

$$\frac{(1/2)(N+2)}{(N+2)} + \frac{(N/2)(M - N/2 + 1)}{(N/2)(N+2)} = \frac{M+2}{N+2} \tag{A.89}$$

□

B

Casimir elements

To look at Casimir elements, we first need to define where they live: in the universal enveloping algebras of a Lie algebra. All following definitions are from [Šn11].

B.1. Universal enveloping algebras

To define the universal enveloping algebra of a Lie representation, we must first define:

Definition B.1.1 (Tensor algebra or free algebra). The tensor algebra over a vector space V over the field $\mathbb{F}$ is the vector space

$$\mathcal{T}(V) := \bigoplus_{k=0}^{\infty} V^{\otimes k} = \mathbb{F} \oplus V \oplus (V \otimes V) \oplus \cdots \oplus V^{\otimes k} \oplus \cdots \tag{B.1}$$

equipped with the associative multiplication:

$$(v_1 \otimes v_2 \otimes \cdots \otimes v_k) \cdot (w_1 \otimes \cdots \otimes w_l) := v_1 \otimes v_2 \otimes \cdots \otimes v_k \otimes w_1 \otimes \cdots \otimes w_l \tag{B.2}$$

In the case that we take the tensor algebra $\mathcal{T}(\mathfrak{g})$ of a Lie algebra $\mathfrak{g}$, we can consider the two-side ideal $\mathcal{I}$:

$$\mathcal{J} := \text{Span}\left\{A \otimes (x \otimes y - y \otimes x - [x,y]) \otimes B \ : \ x, y \in \mathfrak{g} \ , \ A, B \in \mathcal{T}(\mathfrak{g})\right\} \tag{B.3}$$

We now arrive at

Definition B.1.2 (Universal enveloping algebra). The factoralgebra

$$\mathfrak{U}(\mathfrak{g}) := \mathcal{T}(\mathfrak{g})/\mathcal{J} \tag{B.4}$$

is called the universal enveloping algebra of $\mathfrak{g}$

For any representation ρ of $\mathfrak{g}$ on the (finite dimensional) vector space V, we can define a representation $\widetilde{\rho}$ of $\mathcal{T}(\mathfrak{g})$ on the vector space V:

$$\widetilde{\rho}(x_1 \otimes \cdots \otimes x_k) := \rho(x_1) \cdot \rho(x_2) \cdots \rho(x_k) \tag{B.5}$$

Now, as ρ is a representation of a Lie algebra, it must hold that

$$\rho([x,y]) = \rho(x) \cdot \rho(y) - \rho(y) \cdot \rho(x) \tag{B.6}$$

thus we have $\widetilde{\rho}(\mathcal{J}) = 0$. Thus, we can now construct a representation $\hat{\rho}$ of $\mathfrak{U}(\mathfrak{g})$ on V:

$$\hat{\rho}(a) = \widetilde{\rho}(A) \quad , \quad (a \equiv A \mod \mathcal{I}) \in \mathfrak{U}(\mathfrak{g}) \ , \ A \in \mathcal{T}(\mathfrak{g}) \tag{B.7}$$

B.2. Casimir operators

Casimir operators are precisely the elements of $Z\left(\mathfrak{U}(\mathfrak{g})\right)$, i.e. the elements that commute with all elements in the universal enveloping algebra. It is sufficient to have, for an element $c \in \mathfrak{U}(\mathfrak{g})$

$$c \cdot x = x \cdot c \qquad \forall x \in \mathfrak{g} \cong \mathfrak{g}^{\otimes 1} / \mathcal{J} \tag{B.8}$$

to be a Casimir element.

Now, as we have $[\hat{\rho}(c), \rho(x)] = 0$ for all $x \in \mathfrak{g}$, whenever we have an irreducible ρ, we must have that $\hat{\rho}(c) = \lambda \mathrm{Id}$ by Schur's Lemma.

For a more complete overview of the Casimir operators applied to this specific quantum cloning problem, see [KW99, Appendix A.5].

Bibliography

[ABH$^+$03] Gernot Alber, Thomas Beth, Michal Horodecki, Martin Rotteler, and Harald Weinfurter. *Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments*. 2003.

[Aud06] Koenraad M. R. Audenaert. A Digest on Representation Theory of the Symmetric Group. 2006.

[BDE$^+$98] Dagmar Bruß, David P. DiVincenzo, Artur Ekert, Christopher A. Fuchs, Chiara Macchiavello, and John A. Smolin. Optimal universal and state-dependent quantum cloning. *Physical Review A*, 57(4):2368–2378, apr 1998.

[BEM98] Dagmar Bruss, Artur Ekert, and Chiara Macchiavello. Optimal universal quantum cloning and state estimation. *Physical Review Letters*, 81(12):2598–2601, sep 1998.

[BH96] V. Bužek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Physical Review A*, 54(3):1844–1852, sep 1996.

[BH98] V. Buzek and M. Hillery. Universal optimal cloning of qubits and quantum registers. In *1st NASA Conference on Quantum Computing and Quantum Communications Palm Springs, California, February 17-20, 1998*, 1998.

[CDA06] Kim Border C. D. Aliprantis. *Infinite Dimensional Analysis*. Springer-Verlag Berlin Heidelberg, 2006.

[Dri03] B. K. Driver. Chapter 12: Hilbert spaces, 2003. Lecture Notes.

[Fas11] Lucio Fassarella. Characterization of Positive Operators. 2011.

[Fey82] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6-7):467–488, jun 1982.

[FH04] William Fulton and Joe Harris. *Representation Theory*. Springer New York, 2004.

[Fre12] Alex Freire. Some Multilinear Algebra, January 2012.

[GH97] N. Gisin and B. Huttner. Quantum cloning, eavesdropping and Bell's inequality. *Physics Letters A*, 232(6):463, aug 1997.

[GM97] N. Gisin and S. Massar. Optimal quantum cloning machines. *Physical Review Letters*, 79(11):2153–2156, sep 1997.

[Hal15] Brian C. Hall. *Lie Groups, Lie Algebras, and Representations*. Springer International Publishing, 2015.

[Har13] Aram Wettroth Harrow. The Church of the Symmetric Subspace. 2013.

[Jan10] Bas Janssens. Transformation & Uncertainty. Some Thoughts On Quantum Probability Theory, Quantum Statistics, And Natural Bundles. 2010.

[Jon09] Vaughan F.R. Jones. Von Neumann Algebras, October 2009.

[KS09] Yvette Kosmann-Schwarzbach. *Groups and Symmetries*. Springer-Verlag New York Inc., 2009.

[KW99] M. Keyl and R. F. Werner. Optimal cloning of pure states, testing single clones. *Journal of Mathematical Physics*, 40(7):3283–3299, jul 1999.

[Lan17] Klaas Landsman. *Foundations of Quantum Theory*. Springer International Publishing, 2017.

[Llo96] S. Lloyd. Universal quantum simulators. *Science*, 273(5278):1073–1078, aug 1996.

[LV18] Jonathan D. Lee and Ramarathnam Venkatesan. Rigorous analysis of a randomised number field sieve. *Journal of Number Theory*, 187:92–159, jun 2018.

[Maa04] Hans Maassen. Quantum probability, quantum information theory, quantum computing, 2004.

[NC01] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Pr., 2001.

[Sch13] Kathrin Schäcke. On the Kronecker Product, August 2013. Lecture Notes.

[Scu79] H. Scutaru. Some remarks on covariant completely positive linear maps on c∗-algebras. *Reports on Mathematical Physics*, 16(1):79–87, aug 1979.

[Sho99] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 41(2):303–332, jan 1999.

[Sim95] Barry Simon. *Representations of Finite and Compact Groups (Graduate Studies in Mathematics ; V. 10)*. American Mathematical Society, 1995.

[Sti08] John Stillwell. *Naive Lie Theory*. Springer New York, 2008.

[WEH18] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412):eaam9288, oct 2018.

[Wer98] R. F. Werner. Optimal cloning of pure states. *The American Physical Society*, 58(3):1827–1832, September 1998.

[Wu94] Pei Wu. Additive combinations of special operators. *Banach Center Publications*, 30(1):337–361, 1994.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, oct 1982.

[Šn11] Libor Šnobl. Representations of Lie algebras, Casimir operators and their applications, September 2011. Lecture Notes.