Quantum State Purification

by

Honghao Fu

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Computer Science, Quantum Information Option

Waterloo, Ontario, Canada, 2016

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Statement of Contributions

This project started in the summer of 2014 when Andrew Childs and his intern Vedang Vyas became interested in Simon's problem with a faulty oracle. During their research, they developed the idea of using the swap-test in purification procedures and proved that the sample complexity of such procedure is of oder $O(\text{poly}(\frac{1}{\epsilon}))$. This is the foundation for the new analysis of the swap-test procedure by me and my advisors and it provides a tighter upper bound on its sample complexity.

Later, when we moved on to study the optimal purification procedure, Aram Harrow provided us with the idea to formulate the purification problem as an optimization problem using the symmetries of the Choi matrices. Based on his idea, Maris Ozols derived and proved the constraints in this optimization problem. Section 4.2 is based on Aram's idea and Maris' work. I solved the purification problem for qubit and qutrit and analyzed the optimal fidelity in these two cases with help from my advisors.

Beyond the specific technical contributions, my advisors Andrew Childs and Debbie Leung provided countless new ideas and insight that made this thesis possible.

Abstract

Quantum state purification is a process in which decoherence is partially reversed by using multiple copies of the input states that have been subject to the same decoherence effect. This thesis focuses on purifying the decoherence caused by the depolarizing channel. In the first half of the thesis, the purification problem is formally introduced and one efficient purification procedure featuring the swap-test is presented and analyzed. The rest of the thesis formulates the optimal purification problem as an optimization problem and applies it to qubit and qutrit purification.

The first half (Chapter 1 and 2) is devoted to the study of a practical quantum purification procedure based on the swap-test. Before the procedure is introduced, the purification problem is formulated and parameterized in Chapter 1. The procedure and the analysis of its sample complexity are presented in Chapter 2. Chapter 2 ends by applying this procedure to the Simon's problem with a faulty oracle.

The second half of this thesis (Chapter 3 to 5) is built on the Schur-Weyl duality which is the decomposition of space $(\mathbb{C}^d)^{\otimes N}$ into carrier spaces of symmetric group S_n and unitary group $U(d)$ irreducible representations. Necessary background information on it and Schur-Weyl duality itself are introduced in Chapter 3. Chapter 4 focuses on each irreducible representation of $U(d)$ and formulates the purification of the state on this subspace as an optimization problem over all the covariant quantum channels. The constraints implied by the covariance condition and quantum channel properties are derived to make the optimization complete and solvable. In Chapter 5, the method to solve this optimization problem for qubit and qutrit is presented and the implications of the result are also discussed.

Acknowledgements

I first want to thank Andrew Childs and Debbie Leung for their help and guidance throughout my master's program. Without them, little of the work I have done in the last two years would have been possible.

I am also indebted to Maris Ozols who joined this project despite his busy work schedule and made consistent contributions to it which included formal derivation of the constraints of the optimization problem and exploration of the general d-dimensional case. Thanks to Aram Harrow who met with Maris and told us the way to formulate the optimal purification problem as an optimization problem when we lost our research direction. I am grateful to Vedang Vyas whose initial work on this project in summer 2014 laid the foundation of all the future work.

I also want to thank Zhengfeng Ji, Nengkun Yu and Mo Zhou for inspiring and fruitful discussions about this project.

Dedication

This thesis is dedicated to my parents and my teachers.

Table of Contents

List of Figures

Chapter 1

Introduction

1.1 Motivation and previous work

Since the discovery of Shor's Factoring algorithm[20], we have seen increasingly many new quantum algorithms. In theory, we could assume the implementations of the algorithms are perfect. However, in reality, decoherence from thermal noise or interaction with further degrees of freedom could make each step of the quantum algorithms prone to errors. Therefore, one important task is to make sure quantum algorithm implementations still work ideally under the influence of decoherence. One approach is to make the implementations robust and resistant to decoherence. Another approach is to reverse the effect of decoherence on the quantum states produced by such implementations. This thesis is devoted to studying the second approach.

Decoherence has the effect to produce mixed states out of pure states. Thus one of our goals is to partially reverse the effect of decoherence and produce purer states out of mixed ones. It is impossible to achieve such goal with a single copy of the noisy state as both the original state and the type of decoherence are unknown. However, with the presence of multiple copies of the same noisy state, which are produced from the same pure state and subject to the same decoherence process, it is possible to reconstruct a state that is close to the original state by analyzing the properties of the combined states. As we will see in this thesis, the quality of the state we reconstructed gets higher if we are provided with more copies of the noisy state. In the extreme case of analyzing infinite copies of the noise state, we will be able to reconstruct the original state perfectly.

This question was first studied by Cirac, Ekert and Macchiavello [9]. They were inspired by the studies of entanglement purification [5] and studied the problem of purifying depo-

larized qubit and proved the purification procedure proposed in their publication achieves highest output fidelity. They also noticed the connection between the purification procedure and the quantum cloner for a certain type of cloning problem. Later, Keyl and Werner summarized the work by Cirac *et al.* and studied the purification problem for qubit under different criteria [15]. The criteria range from requiring one output state or multiple output states to measuring the fidelity by picking one output state or selecting all the output states. They also found out that the optimal purification procedure is the same as the cloning procedure proposed in [13]. However, the questions that whether such procedure is generalizable to the higher-dimensional case and whether the generalized procedure is optimal remain open. Later in this thesis, we will see that such procedure is not likely to be optimal for higher-dimensional quantum states and we will propose a way to study the optimal purification procedure for higher-dimensional states.

One drawback of [9] is that the calculations and proofs were only outlined. Since their procedure is the starting point of our study, we will give detailed calculation and proof in Chapter 4. In the next section, we will formally state the problem and give necessary parameterization.

1.2 Problem setup

In the general purification problem, we are given multiple copies of the initial d-dimensional noisy state which is of the following form:

$$\rho_0 = (1 - e_0) |\psi\rangle \langle\psi| + \frac{e_0}{d} I, \quad e_0 \in (0, 1). \tag{1.1}$$

We add the subscript 0 to stress the fact that no purification has been performed. The symbol e_0 represents the probability that the state is disturbed and it is called the error parameter. Since it also represents a level of error in the state, we use letter e to save letter p for other purpose. The constraint on e_0 is that it cannot be too close to 1.

When we study the optimal purification procedure, we will make use of the eigenvalues of ρ_0. We will label the target state $|\psi\rangle$ by $|d\rangle$ and the other eigenstates will be denoted by $|1\rangle, \ldots, |d-1\rangle$. The corresponding eigenvalues are

$$\alpha_d = 1 - \frac{d-1}{d} e_0 \text{ and}$$
$$\alpha_1 = \cdots = \alpha_{d-1} = \frac{e_0}{d}.$$

Let $\mathcal{P}$ denote a purification procedure which consists of a set of operations and measurements on the N qudits and perhaps on additional ancillas. After performing purification procedure $\mathcal{P}$, we calculate the fidelity by the following formula:

$$f = \langle\psi| \mathcal{P}(\rho_0^{\otimes N}) |\psi\rangle . \tag{1.2}$$

We are interested in the number of initial states required when the final fidelity is at least $1 - \epsilon$ for a given ϵ.

As the purification problem is introduced, we will outline the structure of this thesis in the next section.

1.3 Summary of results

This thesis is divided into two halves: Chapter 2 discusses a practical purification procedure based on the swap-test and Chapter 3 to 5 present a formulation of optimal purification procedure for general d-dimensional quantum states (or *qudits*).

Chapter 2 introduces a practical quantum state purification procedure for qudits. Moreover, an upper bound on the number of initial noisy states is derived to show that the procedure is efficient.

Chapter 3 introduces the necessary background of representation theory of unitary group and symmetric group that leads to the Schur-Weyl duality. The Schur-Weyl duality will help us understand the properties of combining identical quantum states.

Chapter 4 reduces the problem of finding the optimal fidelity to an optimization problem over quantum channels. We will review the known optimal qubit procedure first and provide a detailed optimality proof. Then we will re-frame the purification problem for general qudits. The complete set of constraints will be derived. It turns out that the problem is a linear programming problem. As we derive the constraints, we will introduce Gel'fand-Tsetlin patterns and Clebsch-Gordan coefficients.

Chapter 5 applies the new formulation to the qubit and qutrit case. The known optimal fidelity of qubit procedure will be reproduced as the solution to the optimization problem developed in Chapter 4. Then we will give the expression for the optimal fidelity for qutrit purification. Based on this fidelity, we will derive a lower bound on the number of input states needed for purification.

Chapter 2

Purification based on the swap-test

This chapter will focus on a purification procedure based on the swap-test [8]. We will introduce basic properties of the pairwise swap-test [6] in the first section. In the following sections, we will list and explain the steps of the procedure and give an upper bound on the number of input states. In the last section, we will discuss one application of this procedure which is Simon's problem [21] with a faulty oracle. Based on this procedure, we can solve the noisy version of Simon's problem with quadratic query complexity and polynomial time complexity.

2.1 The swap-test

The swap-test we used is depicted in the following figure where the input states are two copies of the noisy state $\rho_0 = (1 - e_0) |\psi\rangle \langle\psi| + \frac{e_0}{d} I$ and an ancilla state $|0\rangle$.

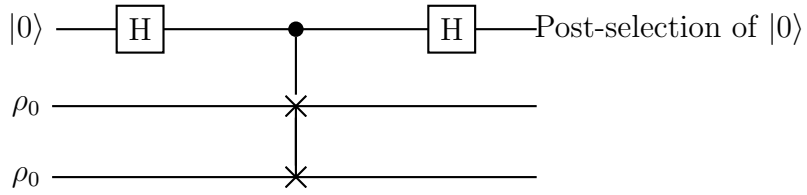

Figure 2.1: The swap-test used in our procedure

In the end, we will measure the first register. If we measure 0, we will only keep the

second register as the output state. Otherwise, we will declare failure and discard both the second and third registers.

This circuit will work as follows:

1. After the first Hadamard gate, the state becomes

$$\frac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|) \otimes \rho_0 \otimes \rho_0. \tag{2.1}$$

Note that for a state $\rho_0 = (1-e_0)\,|\psi\rangle\,\langle\psi| + \frac{e_0}{d}I$, we can extend $|\psi\rangle$ to an orthonormal basis $\{|v_1\rangle, \ldots, |v_d\rangle\}$ of the d-dimensional space such that $|v_1\rangle = |\psi\rangle$. Hence ρ_0 can be written as

$$\rho_0 = (1 - \frac{d-1}{d}e_0)\,|v_1\rangle\,\langle v_1| + \sum_{i=2}^{d} \frac{e_0}{d}\,|v_i\rangle\,\langle v_i|\,. \tag{2.2}$$

Let $\lambda_1 = (1 - \frac{d-1}{d}e)$, $\lambda_2 = \frac{e}{d}$ and $|\Psi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. We could view the input as a probability distribution:

- with probability λ_1^2, we have input state $|\Psi_+\rangle\,|v_1\rangle\,|v_1\rangle$;
- with probability $\lambda_1\lambda_2$, we have input state of the form $|\Psi_+\rangle\,|v_1\rangle\,|v_i\rangle$ or $|\Psi_+\rangle\,|v_i\rangle\,|v_1\rangle$ for some $i \in \{2, 3, \ldots, d\}$;
- with probability λ_2^2, we have input state of the form $|\Psi_+\rangle\,|v_i\rangle\,|v_j\rangle$ for some $i, j \in \{2, 3, \ldots, d\}$.

2. After the controlled-swap gate denoted by U_{c-swap} we have the following states:

$$U_{c-swap}\,|\Psi_+\rangle\,|v_i\rangle\,|v_i\rangle = |\Psi_+\rangle\,|v_i\rangle\,|v_i\rangle \quad \text{and} \quad ,$$
$$U_{c-swap}\,|\Psi_+\rangle\,|v_i\rangle\,|v_j\rangle = \frac{1}{\sqrt{2}}\Big(\,|\Psi_+\rangle\,\frac{|v_i\rangle\,|v_j\rangle + |v_j\rangle\,|v_i\rangle}{\sqrt{2}} + |\Psi_-\rangle\,\frac{|v_i\rangle\,|v_j\rangle - |v_j\rangle\,|v_i\rangle}{\sqrt{2}}\Big) \text{ for } i \neq j$$

3. After the last Hadamard gate, we have the following states:

$$(H \otimes I \otimes I)\,|\Psi_+\rangle\,|v_i\rangle\,|v_i\rangle = |0\rangle\,|v_i\rangle\,|v_i\rangle\,,$$
$$(H \otimes I \otimes I)\frac{1}{\sqrt{2}}\Big(\,|\Psi_+\rangle\,\frac{|v_i\rangle\,|v_j\rangle + |v_j\rangle\,|v_i\rangle}{\sqrt{2}} + |\Psi_-\rangle\,\frac{|v_i\rangle\,|v_j\rangle - |v_j\rangle\,|v_i\rangle}{\sqrt{2}}\Big),$$
$$= \frac{1}{\sqrt{2}}\Big(\,|0\rangle\,\frac{|v_i\rangle\,|v_j\rangle + |v_j\rangle\,|v_i\rangle}{\sqrt{2}} + |1\rangle\,\frac{|v_i\rangle\,|v_j\rangle - |v_j\rangle\,|v_i\rangle}{\sqrt{2}}\Big) \text{ for } i \neq j.$$

For each possible input state, we could calculate the probability to measure state $|0\rangle$ in the first register and the state after the selection. Combining the results, we have that the probability to measure $|0\rangle$ or the success probability p_s is

$$p_s = 1 - \frac{d-1}{d}e_0 + \frac{d-1}{2d}e_0^2. \tag{2.3}$$

The output state will be of the form

$$\rho_1 = (1 - e_1)\,|\psi\rangle\,\langle\psi| + \frac{e_1}{d}I \tag{2.4}$$

with new error parameter

$$e_1 p_s = \frac{e_0}{2} + \frac{e_0^2}{2d}. \tag{2.5}$$

2.2 Steps of the procedure

Our procedure involves recursively applying the prescribed swap-test, hence, we will denote it by P_{swap}.

The procedure starts with preparing many copies of initial states, ρ_0, and applying the pre-described swap-test to them pairwise. When the swap-test succeeds, we collect all the copies of the output stateρ_1 for the next step of the procedure. The failed swap-test will be rejected until we have more than two copies of ρ_1.

After we have collected two copies of ρ_1, we will apply the swap-test to get state ρ_2. From Equation (2.5), the fidelity of ρ_2 can be determined. If it is above $1 - \epsilon$, then it is the output state of the procedure, otherwise, we proceed.

We could view the procedure as a binary tree where initial states ρ_0's are the leaves and other output states are the internal nodes. At the i-th level starting at the botttom, we will have state ρ_i. The subscript i is denoting the steps of the procedure. Here ρ_i is of the form:

$$\rho_i = (1 - e_i)\,|v_1\rangle\,\langle v_1| + e_i\frac{I}{d}, \tag{2.6}$$

where e_i is defined recursively by

$$e_i p_i = \frac{e_{i-1}}{2} + \frac{e_{i-1}^2}{2d}, \tag{2.7}$$

and p_i is the success probability of step i which also depends on the error parameter e_{i-1} by the formula:

$$p_i = 1 - \frac{d-1}{d} e_{i-1} + \frac{d-1}{2d} e_{i-1}^2. \tag{2.8}$$

The choice of proceeding or stop is still depended on the fidelity of ρ_i.

It is always possible that at some step the swap-test will fail and in that case, the procedure will restart and consume more of ρ_0. This procedure will always produce one final state ρ_n which can meet the fidelity criterion. We could see that this procedure is one of the Las Vegas algorithms which could be converted to one of the Monte Carlo algorithms by running the procedure multiple times and each time supplying the procedure with the expected number of copies.

In the next section, we will analyze how many copies of the initial state are expected to produce the final state ρ_n.

2.3 Expected cost

Let $C(P)$ denote the cost of procedure P. Our result is the following theorem.

Theorem 2.3.1 *For P_{swap}, if the final fidelity is at least $1-\epsilon$, then the expected cost is of order $O(\frac{1}{\epsilon})$.*

First of all, we need to get an expression of the expected cost which will be presented in the following lemma.

Lemma 2.3.2 *Assuming the whole process takes l steps, the expected cost of P_{swap} is*

$$\mathbb{E}(C(P_{swap})) = \frac{2^l}{\prod_{i=1}^{l} p_i} \tag{2.9}$$

Proof To prove the lemma, we will use induction starting at the end of the procedure.

If we look at the expected cost of the last step of the procedure, the last step can succeed with probability p_l, then in expectation, we need to run it $1/p_l$ times to succeed. Since each time we run the test, the cost is two states, the expected cost is $2/p_l$.

Assume in expectation, the last i steps cost $\frac{2^i}{\prod_{j=l-i+1}^{l} p_j}$ states. For each of state served as input state to the last i steps, the expected cost is $\frac{2}{p_{l-i}}$. Hence, the expected cost of the last $i+1$ steps is

$$\frac{2^i}{\prod_{j=l-i+1}^{l} p_j} \times \frac{2}{p_{l-i}} = \frac{2^{i+1}}{\prod_{j=l-i}^{l} p_j}$$

Hence, by the principle of inductive proof, the expected cost of all the l steps is as in Equation (2.9). ■

Since the whole process can be described by two sequences $\{e_0, e_1, \ldots, e_l\}$ and $\{p_1, p_2, \ldots, p_l\}$, we will state some properties of P_{swap} derived from these two sequences. The first property is the following lemma.

Lemma 2.3.3 *For P_{swap}, purification of larger-dimensional dimensional quantum states costs more initial states.*

Proof We could rewrite p_i as

$$p_i = 1 - e_{i-1} + \frac{e_{i-1}^2}{2} + \frac{1}{d} e_{i-1}(1 - \frac{e_{i-1}}{2}).$$

For fixed e_{i-1}, p_i decreases as d increases which means that each step will be less likely to succeed for higher dimension.

For e_i, we view it as a function with variables e_{i-1} and d. Even though e_i only takes on discrete values of d but we will see it is monotonic by taking partial derivative against d,

$$\begin{aligned}\frac{\partial e_i}{\partial d} =& \frac{\partial}{\partial d}\left(\frac{\frac{e_{i-1}}{2} + \frac{e_{i-1}^2}{2d}}{1 - \frac{d-1}{d} e_{i-1} + \frac{d-1}{2d} e_{i-1}^2}\right) \\ =& \frac{e_{i-1}^3(1 - e_{i-1})}{2d^2(1 - \frac{d-1}{d} e_{i-1} + \frac{d-1}{2d} e_{i-1}^2)^2} > 0.\end{aligned}$$

The interpretation is that for a given step, output error parameter will grow as d increases but we want the state after each step to have error parameter as small as possible.

Larger error parameter implies that the next step will be harder to succeed and the whole process will possibly be longer. Hence, this two observation combined show that state in larger dimension is harder to purify. ■

Based on Lemma (2.3.3), we can prove the following lemma

Lemma 2.3.4 *For P_{swap}, if the final output state has fidelity $1-\epsilon$, then the number of steps of the procedure in expectation is of order $O(\log(\frac{1}{\epsilon}))$.*

Proof By Lemma (2.3.3), we only need to consider the case that d is infinite to derive the upper bound of the number of steps, n.

If we take d to be inifinite, the parameters are

$$e'_i = \lim_{d\to+\infty} e_i = \frac{e'_{i-1}}{2 - 2e'_{i-1} + e'^2_{i-1}}, \tag{2.10}$$

$$p'_i = \lim_{d\to+\infty} p_i = 1 - e'_{i-1} + \frac{e'^2_{i-1}}{2}. \tag{2.11}$$

However, the sequence $\{e'_i\}$ is not easy to analyze directly, so we upper bound it by a new sequence $\{e''_i\}$ which is defined by

$$e''_0 = e'_0 = e_0 \text{ and} \tag{2.12}$$

$$e''_{i+1} = \frac{e''_i}{2 - 2e''_i}. \tag{2.13}$$

The first property of $\{e''_i\}$ to show is that $e''_i > e_i$ for all $i > 0$.

In the base case,

$$e''_1 = \frac{e''_0}{2 - e''_0} > \frac{e''_0}{2 - 2e''_0 + e''^2_0} = e'_1 > e_1.$$

Assuming it is true for all i up to n. Then we can think of e''_i as a function of e''_{i-1} and notice that

$$\frac{de''_{n+1}}{de''_n} = \frac{1}{2(1-e''_n)^2} > 0.$$

Therefore, we could replace e''_n in the expression of e''_{n+1} by e'_n which is known to be smaller and get a lower bound of e''_{n+1}

$$e''_{n+1} = \frac{e''_n}{2 - 2e''_n} > \frac{e'_n}{2 - 2e'_n} > e'_{n+1} > e_{n+1}.$$

By the principle of induction, we know $e''_n > e_n$ for all $n > 0$.

The reason to choose sequence $\{e''_i\}$ is that we can give closed form expression for this sequence. Since

$$\frac{1}{e''_{n+1}} = \frac{2}{e''_n} - 2,$$

the closed form expression is

$$\frac{1}{e''_n} = 2^n(\frac{1}{e_0} - 2) + 2.$$

Now we can use $\{e''_n\}$ to derive a upper bound on the number of steps. If we set $e''_m = \epsilon$, then $e_m < \epsilon$. This m would be an upper bound on the number of steps. The condition $e''_m = \epsilon$ implies that

$$m = \log(\frac{e_0}{\epsilon} - 2e_0) - \log(1 - 2e_0),$$

which will be an upper bound of the real number of steps, n. Hence, the number of steps is of order $O(\log(\frac{1}{\epsilon}))$. ■

Remark The proof above only holds for $e_0 < \frac{1}{2}$.

To have a complete proof of Theorem (2.3.1), we need to show another property of the sequence $\{e'_i\}$.

Proposition 2.3.5

$$e'_n \leq \frac{e_0}{(2 - 2e_0 + e_0^2)^n}. \tag{2.14}$$

Proof This proof will be inductive as well.

The base case is that $e'_1 = \frac{e_0}{(2-2e_0+e_0^2)}$.

Assume the proposition is true for all the i up to n, then consider $i = n + 1$,

$$\begin{aligned} e'_{n+1} =& \frac{e'_n}{(2 - 2e'_n + e'^2_n)} \\ \leq& \frac{e_0}{(2 - 2e_0 + e_0^2)^n} \frac{1}{2 - 2e'_n + e'^2_n} \\ \leq& \frac{e_0}{(2 - 2e_0 + e_0^2)^{n+1}}. \end{aligned}$$

In the first inequality, we applied the induction hypothesis on e'_n.

Note that function $f(x) = 2 - 2x + x^2$ decreases on the interval $(0, 1)$, so in the second inequality we used the fact $e'_n < e_0$ and the monotonicity of $f(x)$ on interval $(0, 1)$ to get $\frac{1}{2-2e'_n+e'^2_n} \leq \frac{1}{(2-2e_0+e_0^2)}$.

By the principle of induction proof, we have completed the proof. ■

Remark Proposition (2.3.5) can also be used to prove the number of steps is of order $O(\log(\frac{1}{\epsilon}))$.

Now we can prove the main theorem of this section

Proof of Theorem (2.3.1) By Lemma (2.3.2) we know that the expected cost can be bounded by analyze its numerator and denominator separately.

By Lemma (2.3.4), we can bound the numerator part by

$$2^l \leq 2^{\log(\frac{e_0}{\epsilon}-2e_0)-\log(1-2e_0)} = \frac{1}{\epsilon}\frac{e_0 - 2e_0\epsilon}{1-2e_0}. \tag{2.15}$$

Then we need a lower bound of the denominator. Following Proposition (2.3.5), we can derive a lower bound on p'_{i+1} first

$$\begin{aligned} p'_{i+1} =& 1 - e'_i + \frac{e'^2_i}{2} \\ >& 1 - e'_i \\ \geq& 1 - \frac{e_0}{(2 - 2e_0 + e_0^2)^i}. \end{aligned}$$

Hence, the denominator can be rewritten as

$$\begin{aligned} \prod_{i=1}^{n} p'_i >& \prod_{i=0}^{n-1}(1 - \frac{e_0}{(2 - 2e_0 + e_0^2)^i}) \\ >& \prod_{i=0}^{\infty}(1 - \frac{e_0}{(2 - 2e_0 + e_0^2)^i}) \\ =& \frac{(e_0; \frac{e_0}{(2-2e_0+e_0^2)})_\infty}{1 - e_0}. \end{aligned}$$

where $(a;q)_\infty$ is the q-Pochhammer symbol which is defined as

$$(a;q)_\infty = \prod_{j=0}^{\infty}(1-aq^j). \tag{2.16}$$

When $\frac{1}{1-e_0} \in O(1)$, the q-Pochhammer symbol $(e_0; \frac{e_0}{(2-2e_0+e_0^2)})_\infty$ is also of order $O(1)$.

Combining all the results we have derived so far, we have

$$\mathbb{E}(C) \leq \frac{1}{\epsilon}\frac{1-e_0}{(e_0; 1/(2-2e_0+e_0^2))_\infty}\frac{e_0-2e_0\epsilon}{1-2e_0} \in O(\frac{1}{\epsilon}). \tag{2.17}$$

Since this upper bound is derived for the infinite dimension case which is the hardest, the upper bound applies to all possible dimensions. ∎

2.4 Application: Simon's problem with a faulty oracle

Quantum purification procedures and especially P_{swap} can be applied to improve accuracy of quantum algorithms querying faulty oracles, for example, Simon's problem [21]. In this section, we will introduce Simon's problem with a faulty oracle and show how P_{swap} solves it.

In Simon's problem [21], we are given a function $f : \{0,1\}^n \to \{0,1\}^n$ implemented as a black-box oracle U_f such that for a given input state $|x\rangle$ and ancilla state $|y\rangle$, $U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$. It has a special property that there exists a hidden string $s \in \{0,1\}^n$ such that $f(x) = f(y)$ if and only if $x = y$ or $x \oplus y = s$. The goal is to find s.

In the ideal case, we will solve this problem by preparing initial state $\sum_{x=0}^{2^n-1} |x\rangle |0\rangle$, and then querying the oracle with the initial state followed by the Hadamard transform. In the end, when we measure the first register, we will get some $y \in \{0,1\}^n$ such that $y \cdot s = 0$. By repeating such steps $O(n)$ times, we could determine the special string s.

What if the oracle only works with a certain probability and depolarize the input state otherwise? That is, we have a quantum channel

$$D_p(\rho) = (1-p)U_f \rho U_f^\dagger + p\frac{I}{2^{2n}} \tag{2.18}$$

where $p \in (0,1)$ represents the probability that oracle will depolarize the input state. In this case, If we follow the algorithm above, we will get a state of the form:

$$\rho = (1-p)\,|\Psi\rangle\langle\Psi| + p\frac{I}{2^{2n}} \tag{2.19}$$

where

$$|\Psi\rangle = \frac{1}{\sqrt{2^n(n-1)}} \sum_{x=0}^{2^n} \sum_{y \cdot s=0} |y\rangle |f(x)\rangle . \tag{2.20}$$

If we measure the first register of ρ, with probability $(1-p)$ we could get y satisfying $y \cdot s = 0$ but with probability p, we will get a random string z. Then determining the quantum query complexity is a difficult "learning with error" problem [18]. It could be solved with $O(n)$ equations, hence $O(n)$ queries, by the maximum likelihood algorithm but the drawback is that the time complexity will be exponentially large [19] which made us think whether it is possible to achieve polynomial gate complexity as well.

The other strategy would be to perform quantum state purification to the output state before measuring the first register so that the error probability can be as small as possible. We will see this strategy will achieve both polynomial query complexity and gate complexity.

If we collect M copies of ρ and apply P_{swap} on them, the procedure P_{swap} will produce one output state $\rho' = (1-\epsilon) |\Psi\rangle \langle\Psi| + \epsilon \frac{I}{2^{2n}}$. At this point, we could measure the first register and with probability at least $(1-\epsilon)$ we will have a string y satisfying the condition $y \cdot s = 0$. Then we could repeat such process, to get more strings perpendicular to string s.

To make sure the error is within a certain threshold c, we will choose $\epsilon = \frac{c}{n}$. By the subadditivity of error, which is discussed in Chapter 4 of [16], it suffices to pick such ϵ. By Theorem (2.3.1), we know that $M \in O(\frac{1}{\epsilon}) = O(n)$. Since we will need $O(n)$ unique strings perpendicular to s, we need to repeat such process $O(n)$ times. Overall, the gate complexity and query complexity will be $O(n^2)$.

This is just one application of P_{swap}. It can also be applied to quantum algorithms involving parallel queries or sequential queries of length $O(1)$ to some faulty oracle. However, applying P_{swap} to algorithm with longer sequential queries to the oracle will result in very large query and sample complexity. Hence, more sophisticated procedure should be designed to control the noise in the sequential algorithms, if possible.

Chapter 3

Representation theory and Schur-Weyl duality

This chapter will introduce necessary representation theory background which will lead to Schur-Wely duality and Schur-Weyl duality is the foundation of studying the optimal purification procedure.

Generally speaking, representation theory is the study of mapping group members to matrices so that the group properties are preserved. Representation theory consists of many topics and the topic we are interested in is Schur-Weyl duality. It is about how to decompose vector space $(\mathbb{C}^d)^{\otimes n}$ into irreducible representation of symmetric group S_n and unitary group $U(d)$. The corresponding transformation is called *Schur transform*.

Schur-Weyl duality is widely used in quantum information research and I noticed many applications of Schur-Weyl duality during my research. It can be applied to the study of symmetric properties of tensor product of multiple identical quantum states by Alicki, Rudnicki and Sadowski [2]. In that publication [2], Alicki and his colleagues calculated the probability distribution over subspaces in the Schur decomposition of $(\mathbb{C}^d)^{\otimes n}$ and gave mathematical description of the shape of this distribution. Later, this technique was applied to the study of optimal qubit purification ([9] and [15]), optimal cloning [13] and estimation of the spectrum of a density operator [14]. In recent years, Haah, Harrow, Ji, Wu and Yu applied it to quantum tomography [12]. Besides application in quantum information research, it can also be applied to quantum computation research. In 2005, an efficient quantum circuit for implementing Quantum Schur transform was invented [4]. The Schur transform is also known as Schur sampling which was applied to the study of the Hidden subgroup problem (HSP) [3] to get better understanding of the general HSP

[7].

This chapter is organized as follows. We will first review many important concepts of representation theory which will lead to the introduction of Schur-Weyl duality. Then in the last section, we will examine the concept and properties of Schur transform. More detailed explanation and proof can be found in [10].

3.1 Related concepts of representation theory

In this section we will give formal definitions of several representation theory concepts which will be used in the rest of the thesis.

Representation: A representation $\boldsymbol{R}$ of a group G on a vector space V associates with each element $g \in G$ a linear map:

$$\boldsymbol{R}(g) : V \to V : v \to \boldsymbol{R}(g)v$$

such that

$$\begin{aligned} &\boldsymbol{R}(gh) = \boldsymbol{R}(g)\boldsymbol{R}(h) \ \ \forall g, h \in G \ , \\ &\boldsymbol{R}(e) = I \end{aligned}$$

where e is the identity element of the group G and I is the identity map on V. V is called the carrier space of the representation $\boldsymbol{R}$. The set of all the linear maps from V to itself is defined as $End(V)$ and such linear maps are called *endomorphisms*. Thus a representation is a map from G to $End(V)$ satisfying aforementioned properties. If $\boldsymbol{R}(g)$ is unitary for all group members g, then $\boldsymbol{R}$ is a unitary representation. Moreover, if the vector space V associated with representation $\boldsymbol{R}$ is finite-dimensional, then we say the representation $\boldsymbol{R}$ is finite-dimensional. In this thesis, we will focus on finite-dimensional unitary representation over complex numbers. The reason is that a d-dimensional quantum system corresponds to a unit vector in a d-dimensional carrier space.

The convention that we will follow is that bold letter is used for the representation, for example, $\boldsymbol{R}$. Normal capital letter is for the carrier space of the representation, for example, V. To refer to a particular representation, it is necessary to give both the mapping and the carrier space so the notion will be $(\boldsymbol{R}, V)$. When the carrier space is clear from the context, we may omit the carrier space and only keep the mapping for convenience.

Irreducible Representation: For every representation $(\boldsymbol{R}, V)$, there exist a subspace W of its carrier space V such that for all $w \in W$ and all $g \in G$, $\boldsymbol{R}(g)w \in W$. This subspace

is called an *invariant subspace*. A representation $\boldsymbol{r}$ is an *irreducible representation*, or an *irrep*, if the only invariant subspaces of it are its carrier space and $\{0\}$. The convention we follow is that bold lower-case letter denotes the mapping of an irrep.

In this thesis, we are particularly interested in the irreps of the symmetric group and unitary group. Symmetric group S_n is the group of all the permutations of n distinct objects. Unitary group $U(d)$ is the group of all $d \times d$ unitary matrices.

A finite-dimensional unitary representation over complex number can be decomposed into a direct sum of irreps. Thus, for any $g \in G$, we could find a change of basis such that $\boldsymbol{R}(g)$ is block-diagonal and each block on the diagonal corresponds to an operator over an irrep. This will lead to the next concept.

Isotypic decomposition: Let $\hat{G}$ denote the set of irreps of G. Then for a reducible finite-dimensional representation $\boldsymbol{R}$, there exist a change of basis such that

$$\boldsymbol{R}(g) \cong \bigoplus_{\boldsymbol{r} \in \hat{G}} \boldsymbol{r}(v) \otimes I_{n_{\boldsymbol{r}}} \tag{3.1}$$

where $\boldsymbol{r}$ is an irrep of $\boldsymbol{R}$; $n_{\boldsymbol{r}}$ is the multiplicity of the irrep $\boldsymbol{r}$ in the decomposition and $\cong$ is denoting the matrix similarity. Following this decomposition, we can decompose the carrier space V of $\boldsymbol{R}$ in the similar way:

$$V \cong \bigoplus_{\boldsymbol{r} \in \hat{G}} V_{\boldsymbol{r}} \otimes \mathbb{C}^{n_{\boldsymbol{r}}}. \tag{3.2}$$

Such decomposition is called the *isotypic decomposition*.

3.2 Schur-Weyl duality

The two groups with particular interest for us are the symmetric group, S_n and unitary group, $U(d)$. The two groups can both have representation on the space $(\mathbb{C}^d)^{\otimes n}$ denoted by $\boldsymbol{P}_n$ for S_n and $\boldsymbol{Q}_n^d$ for $U(d)$. Here we include a superscript d to stress the fact that U acts on d-dimensional vector-space.

The representation $(\boldsymbol{P}_n, (\mathbb{C}^d)^{\otimes n})$ is defined by

$$\boldsymbol{P}_n(s) \left|i_1\right\rangle \otimes \left|i_2\right\rangle \otimes \cdots \otimes \left|i_n\right\rangle = \left|i_{s^{-1}(1)}\right\rangle \otimes \left|i_{s^{-1}(2)}\right\rangle \otimes \cdots \otimes \left|i_{s^{-1}(n)}\right\rangle \tag{3.3}$$

where $s \in S_n$ denotes some permutation, $s(i)$ describe how it permute item i. Vector $\left|i_j\right\rangle$ with $j \in \{1, 2, \ldots, n\}$ denotes some basis vector in $\mathbb{C}^d$. This is a natural way to

represent a permutation as it only permutes the vectors and leaves the content of the vector unchanged. To illustrate it by an example, let s be the transposition $(1,2)$ of group S_3 which exchanges the first and second item and leaves the third item still. Then $\boldsymbol{P}_3(s)\,|i_1\rangle \otimes |i_2\rangle \otimes |i_3\rangle = |i_2\rangle \otimes |i_1\rangle \otimes |i_3\rangle$.

The representation $(\boldsymbol{Q}_n^d, (\mathbb{C}^d)^{\otimes n})$ is defined by

$$\boldsymbol{Q}_n^d(U)\,|i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle = U\,|i_1\rangle \otimes U\,|i_2\rangle \otimes \cdots \otimes U\,|i_n\rangle \tag{3.4}$$

for any $U \in U(d)$. In this representation, U is applied to each vector $|i_j\rangle$ but the order of the vectors is not changed. In this representation, U is represented by $U^{\otimes n}$.

In general, $\boldsymbol{P}_n$ and $\boldsymbol{Q}_n^d$ are reducible representations, so we can use Equation (3.1) to decompose them as

$$\boldsymbol{P}_n(s) \cong \bigoplus_{\alpha} \boldsymbol{p}_\alpha(s) \otimes I_{n_\alpha} \quad \text{and}$$
$$\boldsymbol{Q}_n^d(U) \cong \bigoplus_{\beta} \boldsymbol{q}_\beta(U) \otimes I_{m_\beta}$$

where α, β are labels of the irreps $\boldsymbol{p}_\alpha$, $\boldsymbol{q}_\beta$ and n_α,m_β denote the multiplicities. Then the question whether we can decompose the product of the two representations arises. Indeed, beyond this decomposition, there are further structures. From the description above, we can see that $\boldsymbol{P}_n(s)\boldsymbol{Q}_n^d(U) = \boldsymbol{Q}_n^d(U)\boldsymbol{P}_n(s)$. By Schur's Lemma, if we expand the product of two representations, each $\boldsymbol{p}_\alpha(s)$ can only act on I_{m_β}, otherwise the commutation relation will not hold. Similarly for each $\boldsymbol{q}_\beta^d(U)$, it only acts on I_{n_α}. Hence we can decompose

$$\boldsymbol{Q}_n^d(U)\boldsymbol{P}_n(s) = \bigoplus_{\alpha,\beta} I_{m_{\alpha,\beta}} \otimes \boldsymbol{q}_\beta^d(U) \otimes \boldsymbol{p}_\alpha(s). \tag{3.5}$$

Now consider the algebra generated by $\boldsymbol{P}_n$ which is $A = \boldsymbol{P}_n(C[S_n]) = \text{span}\{\boldsymbol{P}_n(s)\}$. The set of all the operators commute with every element of A can be proved to be $B = \boldsymbol{Q}_n^d(C[U(d)]) = \text{span}\{\boldsymbol{Q}_n^d(U)\}$ which is the algebra generated by $\boldsymbol{Q}_n^d$. Similarly, for B, the set of all the commuting operators is A. This means the multiplicity factors in Equation (3.5), $m_{\alpha,\beta}$, are either 0 or 1 and it leads to the actual decomposition

$$\boldsymbol{Q}_n^d(U)\boldsymbol{P}_n(s) \cong \bigoplus_{\lambda} \boldsymbol{q}_\lambda^d(U) \otimes \boldsymbol{p}_\lambda(s). \tag{3.6}$$

For details of the proof, one can find it in the book [10].

The set of all the irrep labels is also specified by Schur-Weyl duality. It turns out λ should be a partition of integer n into d parts. More specifically, it should be in the set $I_{d,n} = \{\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_d) | \lambda_1 \geq \lambda_2 \geq \ \ldots \ \geq \lambda_d \geq 0 \ , \sum_{i=1}^{d} \lambda_i = n\}$. For labels of S_n irreps, the number of parts can vary, so the set of labels is $I_{n,n} = I_n$. One thing to note is that two partitions which only differ by trailing 0's are considered the same. One can see this point in the following visualization of the label. For labels of $U(d)$ irrep, d is fixed but n can vary, so there are infinitely many such labels and irreps. Since the same λ belonging to different partition set $I_{d,n}$ corresponds to different irrep, we add the superscript d to $\boldsymbol{q}_\lambda^d$ and $\boldsymbol{Q}_n^d$. In the decomposition in Equation (3.6), both n and d are fixed, so we are only looking at a subset of all the possible irreps. The decomposition in Equation (3.6) also means that there is a basis that can simultaneously decompose $P_n(s)$ and $Q_n^d(U)$, hence we can decompose the carrier space $(\mathbb{C}^d)^{\otimes n}$ as follows

$$(\mathbb{C}^d)^{\otimes n} \cong \bigoplus_{\lambda} Q_\lambda^d \otimes P_\lambda \tag{3.7}$$

where Q_λ^d and P_λ are the corresponding carrier space of $\boldsymbol{q}_\lambda^d$ and $\boldsymbol{p}_\lambda$ respectively. The basis is called *Schur basis*. This transform is called *Schur transform*. The term $Q_\lambda^d \otimes P_\lambda$ could be interpreted as a direct sum with $\dim P_\lambda$ number of terms where each term is a unitarily equivalent but orthogonal unitary group irrep.

3.3 Young diagram and Schur basis

In this section, we will introduce the structure of P_λ and Q_λ^d. Before that, we will introduce a way to visualize a partition λ which is called *Young diagram*.

For $\lambda \in I_{d,n}$, the corresponding Young diagram is a diagram with d rows and the i-th row has λ_i boxes. For example, the Young diagram associates with $(4, 2, 1)$ is

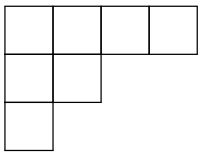

Figure 3.1: Young tableau corresponding to $L_{(3,1)}^{(1)}$

If we fill the boxes with numbers $1, 2, \ldots \ , n.$ such that the numbers in each row are increasing and similarly for numbers in each column , then such diagram is defined to be *standard Young tableaux*. For example, one standard Young tableaux of shape $(4, 2, 1)$ is

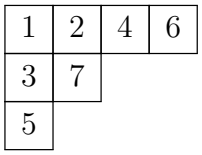

Figure 3.2: standard Young tableau of shape $(4, 2, 1)$

It could be proven that the dimension of P_λ is the number of such standard Young tableau of shape λ. For example, the trivial representation of dimension 1 has label (n). The sign representation has label $(1, 1, \ldots, 1)$. When we use Schur-Weyl duality to study optimal quantum purification procedure, we do not need the basis states of such irrep. We only need to use the expression of the dimension which is known as the Hook Length formula.

To introduce the Hook length formula, we need to assign each box in the Young diagram λ a coordinate (i, j) meaning the box is on the i-th row and j-th column. For example, the top left box has coordinate $(1, 1)$. Then we define $h_\lambda(i, j)$ to be the number of boxes to the right of the box (i, j) plus the number of boxes below it plus 1. If $\lambda = (4, 2, 1)$, then $h_{(4,2,1)}(1, 1) = 6$. The Hook length formula says

$$\dim P_\lambda = \frac{n!}{\prod h_\lambda(i, j)} \tag{3.8}$$

where the product is over all the possible coordinate of boxes in the Young diagram labelled by λ. For Young diagram with only two or three rows, the expression of the dimension can be simplified and we will use the simplified expression in the following chapters.

There is another way to fill the boxes of a Young diagram. For shape $\lambda \in I_{d,n}$, if the boxes are filled with numbers $1, 2, \ldots, d$ so that the integers are increasing from top to bottom in each column and non-decreasing from left to right in each row, such Young tableaux is called *semi-standard Young tableaux*. For example, a semi-standard Young tableaux of shape $(4, 2, 1) \in I_{3,7}$ is depicted in the following figure.

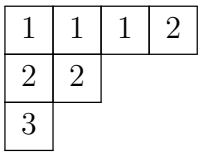

Figure 3.3: semi-standard Young tableau of shape $(4, 2, 1)$

It turns out that for a given λ, each semi-standard Young tableaux has an associated basis vector. The association is by the so called *Young symmetrizer*. For a standard Young tableaux T, define $Row(T)$ to be the set of permutations of integers in each row of T; similarly define $Col(T)$ to be the set of permutations of integers in each column. Now the *Young symmetrizer* $\Pi_{\lambda:T}$ is defined as

$$\Pi_{\lambda:T} = \Big(\sum_{c \in Col(T)} \mathrm{sgn}(c) \boldsymbol{P}_n(c) \Big) \Big(\sum_{r \in Row(T)} \boldsymbol{P}_n(r) \Big) \tag{3.9}$$

where $\mathrm{sgn}(c)$ is the sign of the permutation c.

Young symmetrizer is the projector onto a subspace isomorphic to Q^d_λ. Hence, the way to find the basis of Q^d_λ is to choose one standard Young tableaux T first and then apply $\Pi_{\lambda:T}$ to all the computational basis states. The remaining non-zero states will be the basis states. We will demonstrate this technique in an example. This example can be generalized to help us understand how the optimal qubit purification procedure is designed.

Since we will be working with qubits, d is set to be 2. To give a simple example, we set $n = 4$ and $\lambda = (3, 1)$. The standard Young tableaux is chosen to be $T = \begin{array}{|c|c|c|}\hline 1 & 3 & 4 \\ \hline 2 \\ \cline{1-1} \end{array}$. To denote the permutations, we will use the cycle structure. For example (1) means no permutation and (12) means switching the first and second item. Here the corresponding Young symmetrizer is

$$\begin{aligned} \Pi_{(3,1):T} = &(\boldsymbol{P}_4((1)) - \boldsymbol{P}_4((12))) \\ &\times (\boldsymbol{P}_4((1)) + \boldsymbol{P}_4((13)) + \boldsymbol{P}_4((14)) + \boldsymbol{P}_4((34)) + \boldsymbol{P}_4((134)) + \boldsymbol{P}_4((143))). \end{aligned}$$

Then the basis states are?

$$\begin{aligned} \Pi_{(3,1):T} |1211\rangle &\propto \frac{1}{\sqrt{2}}(|12\rangle - |21\rangle) \otimes |11\rangle \ , \\ \Pi_{(3,1):T} |1212\rangle &\propto \frac{1}{\sqrt{2}}(|12\rangle - |21\rangle) \otimes \frac{1}{\sqrt{2}}(|12\rangle + |21\rangle) \ , \\ \Pi_{(3,1):T} |1222\rangle &\propto \frac{1}{\sqrt{2}}(|12\rangle - |21\rangle) \otimes |22\rangle \ . \end{aligned}$$

For all the other computational basis states, one can easily check that the projector will destroy those states. Upon closer examining of the form of the non-zero basis states, one can see a pattern. All the basis states have the first two quantum systems in the singlet

state, $\frac{1}{\sqrt{2}}(|12\rangle - |21\rangle)$, and the last two systems in a symmetric state. In general, one could show that for qubit and $\lambda = (\lambda_1, \lambda_2)$, one particular basis consists of states with λ_2 singlet states and last $\lambda_1 - \lambda_2$ states in symmetric state. This structure leads to the discovery of optimal quantum purification procedure of qubits.

With the knowledge of the basis states of unitary group irrep, we will give one example of the Schur transform matrix. Considering the decomposition of $(\mathbb{C}^2)^{\otimes 2}$ which is of dimension four. The two possible partition of 2 are $(2, 0)$ and $(1, 1)$. Hence we could write the decomposition as

$$(\mathbb{C}^2)^{\otimes 2} = (Q^2_{(2,0)} \otimes P_{(2,0)}) \oplus (Q^2_{(1,1)} \otimes P_{(1,1)}). \tag{3.10}$$

As we have explained before, $P_{(2,0)}$ and $P_{(1,1)}$ are of dimension 1. The basis state of $Q_{(1,1)}$ is $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. The three basis states of $Q_{(2,0)}$ are $|00\rangle$, $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ and $|11\rangle$. In the Schur transform matrix, from left to right each column corresponds to $|00\rangle$,$|01\rangle$, $|10\rangle$ and $|11\rangle$ respectively. The first row corresponds to the basis of $Q_{(1,1)}$. The second, third and fourth rows correspond to the basis states of $Q_{(2,0)}$. Hence the transform matrix can be expressed as

$$U_{\text{Sch}} = \begin{bmatrix} 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{3.11}$$

Chapter 4

Optimal purification procedure

In this chapter, we will introduce the optimal qubit purification procedure first. In the paper by Ekert *et al.* [9], the optimal purification procedure was presented for the first time. This procedure has some very important properties which should be preserved by higher-dimensional quantum states purification procedures. Following these properties we will formulate the optimal purification problem for higher-dimensional case as an optimization problem and derive all the constraints for this optimization problem.

4.1 Optimal qubit procedure

Before introducing the procedure, we will introduce some parameterization of the irrep labels and irrep basis states first. Assume we are working with $N = 2J$ noisy qubits, then all the partitions can be written as $(J + j, J - j)$ for $j \in \{0, 1, \ldots, J\}$. (The case when $N = 2J + 1$ is very similar, we only need to change the range of j to $\{1/2, 3/2, \ldots, N/2\}$.) Following Equation 3.7. we have

$$(\mathbb{C}^2)^{\otimes N} = \bigoplus_{j=0}^{J} Q^2_{(J+j,J-j)} \otimes P_{(J+j,J-j)}. \tag{4.1}$$

In this decomposition, we will abbreviate $Q^2_{(J+j,J-j)}$ as Q^2_j and $P_{(J+j,J-j)}$ as P_j. As we have discussed before, $Q^2_j \otimes P_j$ can be written as $\bigoplus_{\alpha=1}^{\dim P_j} Q^2_{j:\alpha}$ where α represents an order of all the standard Young tableau of shape $(J + j, J - j)$. Here the order can be implicit except when $\alpha = 1$. The standard Young tableaux with $\alpha = 1$ has the integers 1 though N filled

in the diagram column by column, for example, $\begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 \\ \cline{1-1}\end{array}$. This way of filling will make sure that the first $J-j$ pair of qubits will be in the singlet state.

For a given irrep $Q^2_{j:\alpha_j}$, the basis state are labelled as $|j,m,\alpha_j\rangle$ with $m=-j,-j+1,\ldots,j-1,j$. It is easy to check that the dimension or the number of the semi-standard Young tableau is $2j+1$ for $\lambda=(J+j,J-j)$. When $\alpha_j=1$, the basis state is of the form:

$$|j,m,1\rangle = |\Psi_-\rangle^{\otimes J-j}\otimes|j,m\rangle \tag{4.2}$$

where $|\Psi_-\rangle=\frac{1}{\sqrt{2}}(|12\rangle-|21\rangle)$ is the singlet state and $|j,m\rangle$ is the symmetric state with $j-m$ states in $|1\rangle$ and $j+m$ states in $|2\rangle$. When $\alpha_j>1$,

$$|j,m,\alpha_j\rangle = U_{j:\alpha_j}|j,m,1\rangle \tag{4.3}$$

where U_{j,α_j} is a linear combination of permutation operators $\boldsymbol{P}_n(\pi)$ with $\pi\in S_n$ that will also map the Young symmetrizer $\Pi_{(J+j,J-j):1}$ to $\Pi_{(J+j,J-j):\alpha_j}$.

Then we can introduce one important property shared by all the purification procedures. Here we use ρ to represent the input state and assume the procedure P will output M quantum states.

Definition Let P be a procedure on N d-dimensional quantum states and possibly on additional ancillas and output M quantum systems. We say procedure P is symmetric if

1. the reduced density operator on each output register is the same;
2. the map P is convariant, meaning

$$P[(U\rho U^\dagger)^{\otimes N}] = U^{\otimes M}P(\rho^{\otimes N})(U^\dagger)^{\otimes M} \tag{4.4}$$

for all $U\in U(d)$.

The symmetric condition implies that qubit purification procedure P is invariant under the group actions of S_n and $U(2)$ and the procedure should work for any qubits.

Here the criteria of optimality is that after applying P, it is impossible to increase fidelity even at the cost of fewer output states.

Given the setup, we can introduce the steps of the optimal procedure P_{opt}.

1. Perform quantum measurement defined by the set of projectors (Young symmetrizers): $\{\Pi_{j:\alpha}|j\in\{0,1,\ldots,J\}\ ,\alpha_j\in\{1,2,\ldots,\dim P_j\}\}$.

2. Given the measurement result j and α_j, perform $U^\dagger_{j,\alpha_j}$ on the post-measurement state ρ_{j,α_j} to get state $\rho_{j,1}$ in the space $Q^2_{j,1}$.

3. Discard the first $J-j$ singlet states and get state ρ_j.

4. Trace out all but one states on ρ_j.

We will first show that P_{opt} satisfies the symmetric condition. After the last step, we will have state ρ_j which is in the symmetric subspace and can be expressed as

$$\rho_j = \frac{\alpha_2 - \alpha_1}{\alpha_2^{2j+1} - \alpha_1^{2j+1}} \sum_{m=-j}^{j} \alpha_1^{j-m}\alpha_2^{j+m} \left|j,m\right\rangle \left\langle j,m\right| \tag{4.5}$$

where $|j,m\rangle$ is as introduced before.

The reduced density operator is the same for all output states, so the procedure satisfies the first property of the symmetric condition.The covariance property is built on the fact that $U^{\otimes N}$ and $\Pi_{j:\alpha}$ commute.

$$\begin{aligned}
&\Pi_{j,\alpha} U^{\otimes N} \rho^{\otimes N} (U^\dagger)^{\otimes N} \Pi^\dagger_{j,\alpha} \\
=&U^{\otimes N} \Pi_{j,\alpha} \rho^{\otimes N} \Pi^\dagger_{j,\alpha} (U^\dagger)^{\otimes N} \\
=&U^{\otimes N} \rho_{j,\alpha} (U^\dagger)^{\otimes N}.
\end{aligned}$$

If we discard the first few singlet states, it becomes $U^{\otimes 2j}\rho_j(U^\dagger)^{\otimes 2j}$. In the next subsection, we will give the optimality proof of this procedure.

4.1.1 Optimality proof

The major result of [9] is the following theorem. In the paper, the authors only gave outline of the optimality proof. We will fill in the details below. Later in Chapter 5, we will give a different proof using Clebsch-Gordan transform.

Theorem 4.1.1 *The procedure P_{opt} is the optimal purification procedure for $N = 2j$ depolarized qubits.*

Before that we will state a lemma which is used in the proof.

Lemma 4.1.2 *The state ρ_j is of the form*

$$\rho_j = \frac{\alpha_2 - \alpha_1}{\alpha_2^{2j+1} - \alpha_1^{2j+1}}(2j+1)\int \frac{d\Omega}{4\pi} n(\theta)^{2j} (|\Psi(\theta,\phi)\rangle \langle\Psi(\theta,\phi)|)^{\otimes 2j} \tag{4.6}$$

where

$$\begin{aligned} n(\theta) &= \alpha_2 \cos(\theta/2)^2 + \alpha_1 \sin(\theta/2)^2, \\ |\Psi(\theta,\phi)\rangle &= \sqrt{\alpha_2}\frac{\cos(\theta/2)}{\sqrt{n(\theta)}}|1\rangle + \sqrt{\alpha_1}\frac{\sin(\theta/2)}{\sqrt{n(\theta)}e^{i\phi}}|0\rangle \end{aligned}$$

.

Proof of Lemma 4.1.2 We will omit the common factor $\frac{\alpha_2-\alpha_1}{\alpha_2^{2j+1}-\alpha_1^{2j+1}}$ throughout the proof, so it is equivalent to show

$$(2j+1)\int \frac{d\Omega}{4\pi} n(\theta)^{2j} (|\Psi(\theta,\phi)\rangle \langle\Psi(\theta,\phi)|)^{\otimes 2j} = \sum_{m=-j}^{j} \alpha_1^{j-m}\alpha_2^{j+m} |j,m\rangle \langle j,m| . \tag{4.7}$$

First of all

$$\begin{aligned} & n(\theta) |\Psi(\theta,\phi)\rangle \langle\Psi(\theta,\phi)| \\ =& C_{11}|1\rangle\langle 1| + C_{00}|0\rangle\langle 0| + C_{10}|1\rangle\langle 0| + C_{01}|0\rangle\langle 1|, \end{aligned}$$

with

$$\begin{aligned} C_{00} &= \alpha_1 \sin^2\frac{\theta}{2} & C_{11} &= \alpha_2\cos^2\frac{\theta}{2}, \\ C_{01} &= \sqrt{\alpha_1\alpha_2}\cos\frac{\theta}{2}\sin\frac{\theta}{2}e^{-i\phi} & C_{10} &= \sqrt{\alpha_1\alpha_2}\cos\frac{\theta}{2}\sin\frac{\theta}{2}e^{i\phi}. \end{aligned}$$

Since

$$(|\Psi(\theta,\phi)\rangle \langle\Psi(\theta,\phi)|)^{\otimes 2j} = \sum_{\substack{a,b,c,d \\ a+b+c+d=2j}} C_{11}^a C_{00}^b C_{10}^c C_{01}^d \rho_{a,b,c,d} \tag{4.8}$$

where $\rho_{a,b,c,d}$ contains all the ordering of a copies of $|1\rangle\langle 1|$, b copies of $|0\rangle\langle 0|$, c copies of $|1\rangle\langle 0|$ and d copies of $|0\rangle\langle 1|$. For example, if $j=1$, $a=c=1$ and $b=d=0$, then $\rho_{1,0,1,0} = |11\rangle\langle 10| + |11\rangle\langle 01|$.

Hence we could rewrite the integration as

$$(2j+1)\sum_{\substack{a,b,c,d\\ a+b+c+d=2j}}\int\frac{d\Omega}{4\pi}n(\theta)^{2j}C_{11}^{a}C_{00}^{b}C_{10}^{c}C_{01}^{d}\rho_{a,b,c,d}. \tag{4.9}$$

To prove Equation (4.7), we only need to show the coefficient of one state in $\rho_{k,l,m,n}$ matches the corresponding state in $|j,m\rangle\langle j,m|$.

The integration on the coefficient (the order of $|0\rangle$ and $|1\rangle$ will not affect the coefficient) is

$$\frac{2j+1}{4\pi}\int_0^{\pi}d\theta\sin\theta\alpha_2^{a+\frac{c+d}{2}}\alpha_1^{b+\frac{c+d}{2}}\cos^{2a+c+d}\frac{\theta}{2}\sin^{2b+c+d}\frac{\theta}{2}\int_0^{2\pi}e^{i(d-c)\phi}d\phi.$$

If $c\neq d$, $\int_0^{2\pi}e^{i(c-d)\phi}=0$, so the integration can be reduced to

$$\begin{aligned}&\frac{2j+1}{4\pi}\int_0^{2\pi}d\phi\int_0^{\pi}d\theta\alpha_2^{a+c}\alpha_1^{b+c}\sin\theta\cos^{2a+2c}\frac{\theta}{2}\sin^{2b+2c}\frac{\theta}{2}\\ =&(2j+1)\alpha_2^{a+c}\alpha_1^{b+c}\int_0^{\frac{\pi}{2}}\sin 2\theta\cos^{2a+2c}\theta\sin^{2b+2c}\theta d\theta\\ =&2(2j+1)\alpha_2^{a+c}\alpha_1^{b+c}\int_0^{\frac{\pi}{2}}\cos^{2a+2c+1}\theta\sin^{2b+2c+1}\theta d\theta\end{aligned}$$

with $a+b+2c=2j$. Let $a+c=j+m$ then $b+c=j-m$.The last integration can be written as

$$(4j+2)\alpha_2^{j+m}\alpha_1^{j-m}\int_0^{\frac{\pi}{2}}\cos^{2j+2m+1}\theta\sin^{2j-2m+1}\theta d\theta=\alpha_2^{j+m}\alpha_1^{j-m}\frac{(j+m)!(j-m)!}{(2j)!}. \tag{4.10}$$

The last part is derived from the Beta function for $-j<m<j$ [1]. We could also see that

$$\rho_{a,b,c,d}=\binom{2j}{j+m}|j,m\rangle\langle j,m| \tag{4.11}$$

where $\binom{2j}{j+m}$ is the normalization factor of $|j,m\rangle\langle j,m|$.

When $n=j$ or $n=-j$, the integration can be evaluated as $\int_0^{\frac{\pi}{2}}\cos^{4j+1}\theta\sin\theta d\theta=\int_0^{\frac{\pi}{2}}\cos\theta\sin^{4j+1}\theta d\theta=\frac{1}{4j+2}$.

Therefore, the coefficient of $|j,m\rangle\langle j,m|$ derived from the left-hand side of Equation (4.7) would be

$$\binom{2j}{j+m}\alpha_2^{j+m}\alpha_1^{j-m}\frac{(j+m)!(j-m)!}{(2j)!} = \alpha_2^{j+m}\alpha_1^{j-m}$$

which matches what is given in Eqaution 4.5. ∎

This lemma is showing how to express a state in the symmetric subspace as an integral. More information about symmetric subspace is presented in [23]. With this lemma proved, we could move on to the proof of Theorem (4.1.1). The calculation of the optimal fidelity achievable on each Q_j^2 is included in the proof.

Proof of Theorem 4.1.1 Assume input states are of the form

$$\rho = \alpha_1 |1\rangle\langle 1| + \alpha_2 |2\rangle\langle 2| \tag{4.12}$$

where $|2\rangle$ is the target state that we want to purify. Define p_{j,α_j} to be the probability to measure states in Q_{j,α_j}, that is

$$p_{j,\alpha_j} = \mathrm{Tr}(\Pi_{j,\alpha_j}\rho^{\otimes N}). \tag{4.13}$$

By [2], it has been shown that

$$p_{j,\alpha_j} = p_j = (\alpha_2\alpha_1)^{J-j}\frac{\alpha_2^{2j+1}-\alpha_1^{2j+1}}{\alpha_2-\alpha_1}. \tag{4.14}$$

Now we define

$$\rho_{j,\alpha_j} = \frac{1}{p_j}\Pi_{j,\alpha_j}\rho^{\otimes N}\Pi_{j,\alpha_j}^{\dagger}. \tag{4.15}$$

After transferring ρ_{j,α_j} to $\rho_{j,1}$ and discarding the singlet states, we are left with ρ_j then the fidelity for each j is measured by $f_j = \langle 2|\,\mathrm{Tr}_{2j-1}(\rho_j)\,|2\rangle$ where Tr_{2j-1} means tracing out the last $(2j-1)$ states. We can calculate that

$$f_j = \frac{1}{2j}\Big[\frac{(2j+1)\alpha_2^{2j+1}}{\alpha_2^{2j+1}-\alpha_1^{2j+1}} - \frac{\alpha_2}{\alpha_2-\alpha_1}\Big]. \tag{4.16}$$

Note that the equation above only works for $j > 0$, when $j = 0$, P_{opt} will produce no output state, hence $f_0 = 0$.

Since $\rho^{\otimes N}$ can be expressed as

$$\rho^{\otimes N} = \sum_{j=0}^{J} p_j \sum_{\alpha_j=1}^{\dim P_j} \rho_{j,\alpha_j} \tag{4.17}$$

to prove P_{opt} is indeed optimal, we only need to show that f_j is the highest fidelity one can achieve on each irrep labelled by $(J+j, J-j)$.

Now, consider all the procedures that can be applied to ρ_{j,α_j}. Since ρ_{j,α_j} can be constructed from ρ_j, it is equivalent to consider all the procedures applied to ρ_j with only one output state. We denote such a covariant procedure by P_1 where the subscript 1 is to stress the fact that only one output state will be produced.

Since P_1 is covariant, for any unitary $U \in U(2)$, the application of P_1 on any input state $(U\rho U^\dagger)^{\otimes 2j}$ is

$$P_1((U\rho U^\dagger)^{\otimes 2j}) = U P_1(\rho^{\otimes 2j}) U^\dagger.$$

Let U_Ψ represent a rotation in the bloch sphere around $|\Psi\rangle\langle\Psi|$, then $U_\Psi |\Psi\rangle\langle\Psi| U_\Psi^\dagger = |\Psi\rangle\langle\Psi|$ and $U_\Psi \left|\Psi^\perp\right\rangle\left\langle\Psi^\perp\right| U_\Psi = \left|\Psi^\perp\right\rangle\left\langle\Psi^\perp\right|$ where $\langle\Psi|\Psi^\perp\rangle = 0$. We have

$$\begin{aligned} & U_\Psi P_1((|\Psi\rangle\langle\Psi|)^{\otimes 2j}) U_\Psi^\dagger \\ =& P_1((U_\Psi |\Psi\rangle\langle\Psi| U_\Psi^\dagger)^{\otimes 2j}) \\ =& P_1((|\Psi\rangle\langle\Psi|)^{\otimes 2j}). \end{aligned}$$

This means the state produced by the mapping P_1 applied to $2j$ copies of $|\Psi\rangle\langle\Psi|$ commutes with U_Ψ, so the output state in the bloch sphere is on the line joining $|\Psi\rangle\langle\Psi|$ and $\left|\Psi^\perp\right\rangle\left\langle\Psi^\perp\right|$, therefore, we have

$$P_1((|\Psi\rangle\langle\Psi|)^{\otimes 2j}) = x|\Psi\rangle\langle\Psi| + y\left|\Psi^\perp\right\rangle\left\langle\Psi^\perp\right|, \quad x, y \geq 0, x+y \leq 1. \tag{4.18}$$

By Lemma 4.1.2 we have

$$\begin{aligned} P_1(\rho_j) =& \frac{\alpha_2 - \alpha_1}{\alpha_2^{2j+1} - \alpha_1^{2j+1}} (2j+1) \int \frac{d\Omega}{4\pi} n(\theta)^{2j} P_1(|\Psi(\theta,\phi)\rangle\langle\Psi(\theta,\phi)|^{\otimes 2j}) \\ =& \frac{\alpha_2 - \alpha_1}{\alpha_2^{2j+1} - \alpha_1^{2j+1}} (2j+1) \int \frac{d\Omega}{4\pi} n(\theta)^{2j} \left(x|\Psi(\theta,\phi)\rangle\langle\Psi(\theta,\phi)| + y\left|\Psi(\theta,\phi)^\perp\right\rangle\left\langle\Psi(\theta,\phi)^\perp\right| \right) \end{aligned}$$

where

$$\left|\Psi(\theta,\phi)^\perp\right\rangle = \sqrt{\alpha_1}\frac{\sin\frac{\theta}{2}}{\sqrt{n(\theta)}}|2\rangle - \sqrt{\alpha_2}\frac{\cos\frac{\theta}{2}e^{i\phi}}{\sqrt{n(\theta)}}|1\rangle.$$

Because $\int_0^{2\pi} e^{i\phi} d\phi = 0$, we can drop the terms with $e^{i\phi}$ or $e^{-i\phi}$ which are the terms associated with $|1\rangle\langle 2|$ and $|2\rangle\langle 1|$. Hence, we have

$$\begin{aligned} P_1(\rho_j) =& \frac{\alpha_2 - \alpha_1}{\alpha_2^{2j+1} - \alpha_1^{2j+1}}(2j+1) \text{ and} \\ & \times \int_0^{\pi} \frac{\sin\theta}{2} d\theta n(\theta)^{2j-1} (x\alpha_2 \cos^2\frac{\theta}{2} + y\alpha_1 \sin^2\frac{\theta}{2}) |2\rangle\langle 2| + (x\alpha_1 \sin^2\frac{\theta}{2} + y\alpha_2 \cos^2\frac{\theta}{2}) |1\rangle\langle 1| . \end{aligned}$$

Consider the coefficient of $|2\rangle\langle 2|$ as the fidelity is calculated as $f = \langle 2| P_1(\rho_j) |2\rangle$. The coefficient is

$$\begin{aligned} f &= \int_0^{\pi} \frac{\sin\theta}{2} d\theta n(\theta)^{2j-1} (x\alpha_2 \cos^2\frac{\theta}{2} + y\alpha_1 \sin^2\frac{\theta}{2}) d\theta \\ &= \int_0^{\pi} (x\alpha_2 \cos^3\frac{\theta}{2} \sin\frac{\theta}{2} + y\alpha_1 \cos\frac{\theta}{2} \sin^3\frac{\theta}{2})(\alpha_2 \cos^2\frac{\theta}{2} + \alpha_1 \sin^2\frac{\theta}{2})^{2j-1} d\theta. \end{aligned}$$

Since $(\alpha_2 \cos^2\frac{\theta}{2} + \alpha_1 \sin^2\frac{\theta}{2})^{2j-1} = \sum_{i=0}^{2j-1} \binom{2j-1}{i} \alpha_2^i \cos^{2i}\frac{\theta}{2} \alpha_1^{2j-1-i} \sin^{4j-2i-2}\frac{\theta}{2}$, we have

$$f = \sum_{i=0}^{2j-1} \binom{2j-1}{i} \alpha_2^i \alpha_1^{2j-1-i} \int_0^{\pi} x\alpha_2 \cos^{2i+3}\frac{\theta}{2} \sin^{4j-2i-1}\frac{\theta}{2} + y\alpha_1 \cos^{2i+1}\frac{\theta}{2} \sin^{4j-2i+1}\frac{\theta}{2} d\theta. \tag{4.19}$$

By properties of the Beta function, we can get

$$\int_0^{\pi} \cos^{2i+3}\frac{\theta}{2} \sin^{4j-2i-1}\frac{\theta}{2} d\theta = \frac{(i+1)!(2j-i-1)!}{(2j+1)!}, \tag{4.20}$$

$$\int_0^{\pi} \cos^{2i+1}\frac{\theta}{2} \sin^{4j-2i+1}\frac{\theta}{2} d\theta = \frac{i!(2j-i)!}{(2j+1)!} \tag{4.21}$$

Plugging Equations (4.20 and 4.21) into Equation (4.19), we will get

$$\begin{aligned} f =& \int_0^{\pi} \frac{\sin\theta}{2} d\theta n(\theta)^{2j-1} (x\alpha_2 \cos^2\frac{\theta}{2} + y\alpha_1 \sin^2\frac{\theta}{2}) d\theta \\ =& \frac{1}{2j(2j+1)} \Big(x \sum_{i=0}^{2j-1} (i+1)\alpha_2^{i+1} \alpha_1^{2j-i-1} + y \sum_{i=0}^{2j-1} \alpha_2^i \alpha_1^{2j-i} (2j-i) \Big) \\ =& \frac{1}{2j(2j+1)} \Big(x \sum_{i=1}^{2j} i\alpha_2^i \alpha_1^{2j-i} + y \sum_{i=0}^{2j-1} \alpha_2^i \alpha_1^{2j-i} (2j-i) \Big) \\ =& \frac{\alpha_1^{2j}}{2j(2j+1)} \Big(x \sum_{i=1}^{2j} i(\frac{\alpha_2}{\alpha_1})^i + y \sum_{i=0}^{2j-1} (\frac{\alpha_2}{\alpha_1})^i (2j-i) \Big). \end{aligned}$$

Maximizing f is a simple linear programming problem. Let $A = \sum_{i=1}^{2j} i(\frac{\alpha_2}{\alpha_1})^i$ and $B = \sum_{i=0}^{2j-1}(2j-i)(\frac{\alpha_2}{\alpha_1})^i$, then

$$\begin{aligned} & A > 0 \;\; B > 0 \;\text{ and} \\ A - B &= \sum_{i=0}^{2j}(2i-2j)(\frac{\alpha_2}{\alpha_1})^i \\ &= \sum_{i=0}^{j-1} 2i\Big((\frac{\alpha_2}{\alpha_1})^{2j-i} - (\frac{\alpha_2}{\alpha_1})^i\Big) > 0 \end{aligned}$$

as $\alpha_2 > \alpha_1$ and $i < j$, the maximum of $Ax + By$ is attained at $x = 1, y = 0$.

Then the optimal fidelity is

$$f_{opt} = \frac{\alpha_2^{2j+1}}{\alpha_2^{2j+1} - \alpha_1^{2j+1}} - \frac{1}{2j}\frac{\alpha_2\alpha_1(\alpha_2^{2j} - \alpha_1^{2j})}{(\alpha_2 - \alpha_1)(\alpha_2^{2j+1} - \alpha_1^{2j+1})} = f_j. \tag{4.22}$$

This is matches the expression given in [9]. ∎

4.1.2 Analysis of average fidelity $F_N^{(2)}$

In the previous section, we have shown the optimal fidelity achieved on a particular $U(2)$-irrep labelled by $\lambda = (J+j, J-j)$. Then the next question to ask is that how good is this procedure over all the irreps. That is, we would like to know the fidelity averaged over all the $U(2)$ irrep in the Schur decomposition of $(\mathbb{C}^2)^{\otimes N}$. We will denote the average fidelity by $F_N^{(2)}$.

$$F_N^{(2)} = \sum_{j=1}^{J} d_j p_j f_j \tag{4.23}$$

where d_j is the multiplicity factor of the irrep Q_J^2. The formula for d_j is

$$d_j = \frac{(2J)!(2j+1)}{(J-j)!(J+j+1)!} = \frac{2j+1}{2J+1}\binom{2J+1}{J+j+1}. \tag{4.24}$$

Then the average fidelity can be specified as we substitute Equation (4.22) and Equation (4.24) into Equation (4.23)

$$F_N^{(2)} = \frac{1}{2J+1}\sum_{j=1}^{J}(2j+1)\binom{2J+1}{J+j+1}\Big(\frac{\alpha_1^{J-j}\alpha_2^{J+j+1}}{\alpha_2-\alpha_1} - \frac{\alpha_1^{J-j+1}\alpha_2^{J+j+1} - \alpha_1^{J+j+1}\alpha_2^{J-j+1}}{(2j)(\alpha_2-\alpha_1)^2}\Big). \tag{4.25}$$

Before we start the analysis, we need to state the Chernoff-Hoeffding Theorem which will be used to bound the minor parts of $F_N^{(2)}$.

Theorem 4.1.3 (Chernoff-Hoeffding) *Suppose $X_1, \ldots, X_n$ are i.i.d random variables, taking values in $\{0, 1\}$, let $p = E[X_i]$ and $\epsilon > 0$, then*

$$\Pr(\frac{1}{n}\sum X_i > p + \epsilon) \leq e^{-D(p+\epsilon\|p)n} \tag{4.26}$$

where $D(x\|y) = x\ln(\frac{x}{y}) + (1-x)\ln(\frac{1-x}{1-y})$.

For n independent and identical Bernoulli trial X_i's, the sum $X = \sum_{i=1}^{n} X_i$ is also a random variable which satisfies the binomial distribution, so the theorem is equivalent to

$$\Pr(X > n(p+\epsilon)) \leq e^{-D(p+\epsilon\|p)n} \text{ for } X \sim B(n, p).$$

For approximation, the first step is to break $F_N^{(2)}$ into three parts. Then we can extend the sum to include every term in the corresponding binomial expansion. The three parts are:

$$\begin{aligned}
F_{N,1}^{(2)} &= \sum_{j=1}^{J} \frac{2j+1}{(\alpha_2-\alpha_1)(2J+1)} \binom{2J+1}{J+j+1} \alpha_1^{J-j}\alpha_2^{J+j+1}, \\
F_{N,2}^{(2)} &= -\sum_{j=1}^{J} \frac{\alpha_1}{(\alpha_2-\alpha_1)^2} \frac{2j+1}{(2j)(2J+1)} \binom{2J+1}{J+j+1} \alpha_1^{J-j}\alpha_2^{J+j+1}, \\
F_{N,3}^{(2)} &= \sum_{j=1}^{J} \frac{\alpha_2}{(\alpha_2-\alpha_1)^2} \frac{2j+1}{(2j)(2J+1)} \binom{2J+1}{J+j+1} \alpha_1^{J+j+1}\alpha_2^{J-j}
\end{aligned}$$

so that $F_N^{(2)} = F_{N,1}^{(2)} + F_{N,2}^{(2)} + F_{N,3}^{(2)}$.

For $F_{N,1}^{(2)}$, we could set $k = J - j$ and it can be approximated by

$$\begin{aligned}
F_{N,1}^{(2)} =& \frac{1}{(2J+1)(\alpha_2-\alpha_1)} \sum_{k=0}^{2J+1} \binom{2J+1}{k} \alpha_1^k \alpha_2^{2J+1-k}(2J+1-2k) - \Delta F_{N,1}^{(2)} \\
=& 1 - \Delta F_{N,1}^{(2)}
\end{aligned}$$

where

$$\Delta F_{N,1}^{(2)} = \frac{1}{(2J+1)(\alpha_2-\alpha_1)} \sum_{k=J}^{2J+1} \binom{2J+1}{k} \alpha_1^k \alpha_2^{2J+1-k} (2J+1-2k).$$

Using the fact $2J+1-2k \leq 2J+1$, we can see that

$$\begin{aligned}
\Delta F_{N,1}^{(2)} \leq & \frac{2J+1}{(2J+1)(\alpha_2-\alpha_1)} \sum_{k=J}^{2J+1} \binom{2J+1}{k} \alpha_1^k \alpha_2^{2J+1-k} \\
= & \frac{1}{\alpha_2-\alpha_1} \sum_{k=J}^{2J+1} \binom{2J+1}{k} \alpha_1^k \alpha_2^{2J+1-k} \\
= & \frac{1}{(\alpha_2-\alpha_1)} \Pr(X \geq J) \\
\leq & \frac{1}{\alpha_2-\alpha_1} e^{-D(\alpha_1+\delta \| \alpha_1)(2J+1)} \in O(e^{-N})
\end{aligned}$$

where the last inequality is based on Theorem 4.1.3. Here $\delta = \frac{(\alpha_2-\alpha_1)J-\alpha_1-1}{2J+1}$ and $X \sim B(2J+1, \alpha_1)$.

Hence, we can see that $F_{N,1}^{(2)}$ is very close to 1 as

$$F_{N,1}^{(2)} = 1 - O(e^{-N}). \tag{4.27}$$

For $F_{N,2}^{(2)}$ we have

$$\begin{aligned}
F_{N,2}^{(2)} = & -\sum_{j=1}^{J} \frac{\alpha_1}{(\alpha_2-\alpha_1)^2} \frac{2j+1}{(2j)(2J+1)} \binom{2J+1}{J+j+1} \alpha_1^{J-j} \alpha_2^{J+j+1} \\
= & -\frac{1}{2J+1} \frac{\alpha_1}{(\alpha_2-\alpha_1)^2} \sum_{j=1}^{J} \binom{2J+1}{J+j+1} \alpha_1^{J-j} \alpha_2^{J+j+1} (1+\frac{1}{2j}) \\
= & -S_{2,1} - S_{2,2}
\end{aligned}$$

where

$$S_{2,1} = \frac{1}{2J+1}\frac{\alpha_1}{(\alpha_2-\alpha_1)^2}\sum_{j=1}^{J}\binom{2J+1}{J+j+1}\alpha_1^{J-j}\alpha_2^{J+j+1},$$
$$S_{2,2} = \frac{1}{2J+1}\frac{\alpha_1}{(\alpha_2-\alpha_1)^2}\sum_{j=1}^{J}\binom{2J+1}{J+j+1}\alpha_1^{J-j}\alpha_2^{J+j+1}(\frac{1}{2j}).$$

Here we still follow the convention $k = J - j$, then we estimate $S_{2,1}$ and $S_{2,2}$ separately,

$$\begin{aligned} S_{2,1} =& \frac{1}{2J+1}\frac{\alpha_1}{(\alpha_2-\alpha_1)^2}\sum_{k=0}^{2J+1}\alpha_1^k\alpha_2^{2J+1-k}\binom{2J+1}{k} - \Delta S_{2,1} \\ =& \frac{1}{2J+1}\frac{\alpha_1}{(\alpha_2-\alpha_1)^2} - \Delta S_{2,1}. \end{aligned}$$

Here the sum of the extended terms is

$$\begin{aligned} \Delta S_{2,1} =& \frac{1}{2J+1}\frac{\alpha_1}{(\alpha_2-\alpha_1)^2}\sum_{k=J}^{2J+1}\alpha_1^k\alpha_2^{2J+1-k}\binom{2J+1}{k} \\ =& \frac{1}{2J+1}\frac{\alpha_1}{(\alpha_2-\alpha_1)^2}\Pr(X \geq J) \\ \leq& \frac{1}{2J+1}\frac{\alpha_1}{(\alpha_2-\alpha_1)^2}e^{-D(\alpha_1+\delta\|\alpha_1)(2J+1)} \in O(\frac{1}{N}e^{-N}) \end{aligned}$$

with $X \sim B(2J+1, \alpha_1)$.

Since $\frac{1}{j} \geq \frac{1}{N}$,

$$S_{2,2} = \frac{1}{2J+1}\frac{\alpha_1}{(\alpha_2-\alpha_1)^2}\sum_{j=1}^{J}\alpha_1^{J-j}\alpha_2^{J+j+1}\binom{2J+1}{J+j+1}\frac{1}{2j} \tag{4.28}$$
$$\geq \frac{1}{N(N+1)}\frac{\alpha_1}{2(\alpha_2-\alpha_1)^2}\sum_{j=1}^{J}\binom{2J+1}{J-j}\alpha_1^{J-j}\alpha_2^{J+j+1} \tag{4.29}$$
$$= \frac{1}{N(N+1)}\frac{\alpha_1}{2(\alpha_2-\alpha_1)^2}\sum_{k=0}^{2J+1}\binom{2J+1}{k}\alpha_1^k\alpha_2^{2J+1-k} - \Delta S_{2,2} \tag{4.30}$$
$$= \frac{1}{N(N+1)}\frac{\alpha_1}{2(\alpha_2-\alpha_1)^2} - \Delta S_{2,2} \tag{4.31}$$

with

$$\Delta S_{2,2} = \frac{1}{N(N+1)} \frac{\alpha_1}{2(\alpha_2-\alpha_1)^2} \sum_{k=J}^{2J+1} \binom{2J+1}{k} \alpha_1^k \alpha_2^{2J+1-k} \tag{4.32}$$

$$= \frac{1}{N(N+1)} \frac{\alpha_1}{2(\alpha_2-\alpha_1)^2} \Pr(X \geq J) \tag{4.33}$$

$$\leq \frac{1}{N(N+1)} \frac{\alpha_1}{2(\alpha_2-\alpha_1)^2} e^{-D(\alpha_1+\delta\|\alpha_1)(N+1)}. \tag{4.34}$$

Putting them together, we will have the following equations:

$$F_{N,2}^{(2)} = \frac{1}{N+1} \frac{\alpha_1}{(\alpha_2-\alpha_1)^2} + O(\frac{1}{N^2}), \tag{4.35}$$

$$F_{N,2}^{(2)} \leq \frac{1}{N+1} \frac{\alpha_1}{(\alpha_2-\alpha_1)^2} - \frac{1}{N(N+1)} \frac{\alpha_1}{2(\alpha_2-\alpha_1)^2}. \tag{4.36}$$

Since $\frac{2j+1}{2j} \leq 2$, setting $k = J+j+1$, $F_{N,3}^{(2)}$ can be evaluated as

$$F_{N,3}^{(2)} = \sum_{j=1}^{J} \frac{\alpha_2}{(\alpha_2-\alpha_1)^2} \frac{2j+1}{(2j)(2J+1)} \binom{2J+1}{J+j+1} \alpha_1^{J+j+1} \alpha_2^{J-j} \tag{4.37}$$

$$\leq \frac{\alpha_2}{(\alpha_2-\alpha_1)^2} \frac{2}{2J+1} \sum_{j=1}^{J} \binom{2J+1}{J+j+1} \alpha_1^{J+j+1} \alpha_2^{J-j} \tag{4.38}$$

$$= \frac{\alpha_2}{(\alpha_2-\alpha_1)^2} \frac{2}{2J+1} \sum_{k=J+2}^{2J+1} \binom{2J+1}{k} \alpha_1^k \alpha_2^{2J+1-k}. \tag{4.39}$$

At this point, we could apply Theorem (4.1.3) to conclude that

$$F_{N,3}^{(2)} \in O(\frac{1}{N} e^{-N}). \tag{4.40}$$

Overall, summing $F_{N,1}^{(2)}, F_{N,2}^{(2)}$ and $F_{N,3}^{(2)}$, we have

$$F_N^{(2)} = 1 - \frac{1}{N+1} \frac{\alpha_1}{(\alpha_2-\alpha_1)^2} + O(\frac{1}{N^2}). \tag{4.41}$$

which matches Cirac, Ekert and Macchiavello's result [9].

By setting $F_N^{(2)} = 1-\epsilon$, we can get $N \geq \frac{\alpha_1}{(\alpha_2-\alpha_1)^2} \frac{1}{\epsilon}$. The interpretation is that $\Omega(\frac{1}{\epsilon})$ is the sample complexity for this purification problem and this lower bound on the sample complexity is what we are interested in.

4.1.3 Lower bound on sample complexity of purifying higher-dimensional states

As we know that the complexity of purifying qubit is $\Omega(1/\epsilon)$, we are thinking about the implication of this bound on the d-dimensional case and we reach the following lemma.

Lemma 4.1.4 *Given the final output fidelity is $1-\epsilon$, the sample complexity of purifying d-dimensional state $\rho_0^{(d)}$ is of order $\Omega(\frac{1}{d\epsilon})$*

Proof The idea of this proof is that when we purify N copies of $\rho_0^{(2)} = (1-e_0^{(2)}/2)\left|1\right\rangle\left\langle 1\right| + \frac{e_0^{(2)}}{2}\left|2\right\rangle\left\langle 2\right|$, there are two procedures we can consider:

1. applying the optimal qubit procedure denoted by $P_{\text{opt}}^{(2)}$ on the N copies;
2. embedding each of $\rho_0^{(2)}$ in the d-dimensional space and then applying optimal qudit purification procedure denoted by $P_{\text{opt}}^{(d)}$.

The second procedure will be denoted by $P_{\text{embed}}^{(2)}$ and it cannot outperform the optimal procedure $P_{\text{opt}}^{(2)}$.

The embedded d-dimensional state is

$$\rho_0^{(d)} = (1-q)\rho_0^{(2)} + \frac{q}{d-2}M \tag{4.42}$$

where

$$M = \sum_{i=3}^{d} \left|i\right\rangle\left\langle i\right|. \tag{4.43}$$

We want $\rho_0^{(d)}$ to be of the form

$$\rho_0^{(d)} = (1 - \frac{d-1}{d}e_0^{(d)}\left|1\right\rangle\left\langle 1\right| + \frac{e_0^{(d)}}{d}\sum_{i=2}^{d}\left|i\right\rangle\left\langle i\right|. \tag{4.44}$$

Note that for the simplicity of the proof, we choose $\left|1\right\rangle$ as the target state which is different from the other choices in this thesis.

By equating coefficient of $|1\rangle\langle 1|$ in Equation (4.42) and Equation (4.44), we will get

$$(1-q)(1-\frac{e_0^{(2)}}{2}) = 1 - \frac{d-1}{d}e_0^{(d)}.$$

Then if we equate coefficient of $|2\rangle\langle 2|$ in Equation (4.42) and Equation (4.44), we will get

$$\frac{(1-q)e_0^{(2)}}{2} = \frac{e_0^{(d)}}{d}.$$

For coefficient of $|i\rangle\langle i|$, for $i = 3, \ldots, d$, in Equation (4.42) and Equation (4.44), we will get

$$\frac{q}{d-2} = \frac{e_0^{(d)}}{d}.$$

We will choose $e_0^{(d)}$ as constant, then we can express q and $e_0^{(2)}$ in terms of $e_0^{(d)}$ and d as

$$\begin{aligned} q =& \frac{d-2}{d}e_0^{(d)}, \\ e_0^{(2)} =& \frac{2e_0^{(d)}}{d-(d-2)e_0^{(d)}}. \end{aligned}$$

Let the final output fidelity be F_{embed} and F_{opt} for $P_{\text{embed}}^{(2)}$ and $P_{\text{opt}}^{(2)}$ respectively. Since $P_{\text{embed}}^{(2)}$ cannot outperform $P_{\text{opt}}^{(2)}$, we know that

$$F_{\text{embed}} \leq F_{\text{opt}}. \tag{4.45}$$

From the proof of Theorem (4.1.1), we get the final fidelity $F_{\text{opt}} \leq 1 - \frac{e_0^{(2)}}{2(1-e_0^{(2)})^2}\frac{1}{N}$, so if $F_{\text{embed}} = 1-\epsilon$, we will have

$$\begin{aligned} 1-\epsilon &\leq 1 - \frac{e_0^{(2)}}{2(1-e_0^{(2)})^2}\frac{1}{N}, \\ N &\geq \frac{e_0^{(d)}(d-(d-2)e_0^{(d)})}{d^2(1-e_0^{(d)})^2}\frac{1}{\epsilon} = \frac{e_0^{(d)}}{(1-e_0^{(d)})d\epsilon} + \Theta(\frac{1}{d^2\epsilon}). \end{aligned}$$

This shows that $N \in \Omega(\frac{1}{d\epsilon})$. ∎

This lemma indicates that the lower bound is dependent on d and for larger d we may need fewer copies of the initial states. It also implies that for constant d, the lower bound is $\Omega(\frac{1}{\epsilon})$ which matches the upper bound of P_{swap} sample complexity and P_{swap} is optimal in this case. However, for exponentially large d, P_{swap} might be suboptimal and we need to find better procedures or the optimal procedure.

4.2 Generalization to qudit

In the last section, we have proved a lower bound on the sample complexity of the qudit purification problem. It is unknown whether such lower bound is achievable. However, we know that the only way to reach the lower bound is to study the optimal purification procedure.

The first question we asked was that if it is possible to generalize the optimal qubit procedure to qudits. The qubit procedure is built on the fact that Q_λ^2 is isomorphic to some symmetric subspace. However, this is not true for general unitary group $U(d)$. We will give an example here. Let T be the standard Young tableaux of shape $\lambda = (2,1)$ and $T = \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 \\ \cline{1-1}\end{array}$. Then

$$\Pi_{\lambda:T} |012\rangle \propto (|12\rangle - |21\rangle)|3\rangle - (|23\rangle - |32\rangle)|1\rangle$$

This example made us start to think about a new formulation of the problem.

By Equation (3.7), we could assume the procedure start by measuring λ. Hence, we could focus on studying the optimal fidelity achievable by purifying post-measurement state in space Q_λ^d. We want to optimize the final fidelity over all covariant quantum channels that will produce one output state. Then we can construct the optimal procedure. The optimal purification procedure will apply the channel corresponding to the measurement result λ with the highest fidelity.

Specifically, we want to apply a quantum channel to a state in Q_λ^d to produce a state in $Q_{(1)}^d$ which is the carrier space of the $U(d)$ defining irrep. Thus we are optimizing over all the quantum channels $\Psi : Q_\lambda^d \to Q_{(1)}^d$. Moreover, we want such quantum channel to be covariant and commute with action of $U(d)$ defined by the λ-irrep and defining irrep.

For simplicity, we need to introduce a few notions first. The input state is ρ_0 as defined in Section 1.2. The projected state from $\rho_0^{\otimes N}$ onto Q_λ^d is denoted as ρ_λ. We also define $U_\lambda = \boldsymbol{Q}_\lambda^d(U)$.

Tp better present this optimization problem, we divide the content into several subsections. In the first subsection, we will see what the implication of the covariance property is for this optimization problem. To study the covariance condition, some background knowledge will also be introduced in the second subsection Then in the following subsections, we will derive explicit constraints and simplify this optimization problem.

4.2.1 Dual representation and covariance condition

Dual representation: Recall that the dual vector space of V is the set of linear maps from V to $\mathbb{C}$. Vectors in the dual space are usually denoted by bras as contrary to ket notation for vectors in the original space. Moreover, if the vector space has basis vectors $\{|v_1\rangle, |v_2\rangle, \ldots, |v_n\rangle\}$, then the basis for the dual space is $\{\langle v_1|, \langle v_2|, \ldots, \langle v_n|\}$. Now for a representation $\boldsymbol{R}$ with carrier space V, the dual representation is denoted by $\boldsymbol{R}^*$ with carrier space V^*. Moreover, we want to have $\langle v|\,|v\rangle = (\boldsymbol{R}^*(g)\,\langle v|)(\boldsymbol{R}(g)\,|v\rangle)$ for all $g \in G$, then $\boldsymbol{R}^*(g) = \boldsymbol{R}(g^{-1})^T$. When $\boldsymbol{R}$ is a unitary representation, $\boldsymbol{R}^*$ is the conjugate representation where $\boldsymbol{R}^*(g) = \boldsymbol{R}(g)^*$ and $\boldsymbol{R}(g)^*$ is the entrywise complex conjugate of $\boldsymbol{R}(g)$.

After introducing dual representation, we can examine the covariance condition of quantum channel Ψ, which can be stated as

$$\Psi(\rho_\lambda) = U^\dagger \Psi(U_\lambda \rho_\lambda U_\lambda^\dagger) U \quad \forall U \in U(d). \tag{4.46}$$

Now expressing $\Psi(\rho_\lambda)$ in terms of the Choi representation as $\Psi(\rho_\lambda) = \mathrm{Tr}_{Q_\lambda^d}(J(\Psi)(I_{(1)} \otimes \rho_\lambda^T))$ [23],

$$\begin{aligned}
\Psi(\rho_\lambda) &= U^\dagger \,\mathrm{Tr}_{Q_\lambda^d}(J(\Psi)(I_{(1)} \otimes (U_\lambda \rho_\lambda U_\lambda^\dagger)^T))U \\
&= \mathrm{Tr}_{Q_\lambda^d}[(U^\dagger \otimes I_\lambda) J(\Psi)(I_{(1)} \otimes (U_\lambda \rho_\lambda U_\lambda^\dagger)^T)(U \otimes I_\lambda)] \\
&= \mathrm{Tr}_{Q_\lambda^d}[(U^\dagger \otimes U_\lambda^T) J(\Psi)(U \otimes U_\lambda^*)(I_{(1)} \otimes \rho_\lambda^T)].
\end{aligned}$$

Hence the covariance condition can be reduced to this condition on $J(\Psi)$

$$J(\Psi) = (U^\dagger \otimes U_\lambda^T) J(\Psi)(U \otimes U_\lambda^*) \quad \forall U \in U(d). \tag{4.47}$$

For simplicity, we can replace U by U^T and get

$$J(\Psi) = (U^* \otimes U_\lambda) J(\Psi)(U^* \otimes U_\lambda)^\dagger \quad \forall U \in U(d). \tag{4.48}$$

This will be the first constraint on $J(\Psi)$. Since Ψ is a quantum channel, it must be complete positive and trace-preserving, so the other two conditions for $J(\Psi)$ are:

$$J(\Psi) \succeq 0, \tag{4.49}$$

$$\mathrm{Tr}_{Q^*_{(1)}}(J(\Psi)) = I_\lambda, \tag{4.50}$$

The covariance condition depends on the decomposition of tensor product of dual irrep $Q^d_{(1)}$ and Q^d_λ which we will explore after introducing Clebsch-Gorden transform. The trace-preserving condition will be explored after that.

4.2.2 Clebsch-Gordan transform and the first constraint on $J(\Psi)$

What we conclude in this subsection can be summarized in the following proposition.

Proposition 4.2.1 *Let $\Psi : Q^d_\lambda \to (Q^d_{(1)})^*$ be a quantum channel satisfying the covariance condition, then its Choi representation must be of the form:*

$$J(\Psi) = W^\dagger \left[\bigoplus_{\mu \in \{\lambda - \square\}} c_\mu I_\mu \right] W \tag{4.51}$$

for some $c_\mu \geq 0$ and W is the corresponding Clebsch-Gordan transform matrix.

Before proving this proposition, we need to introduce the Clebsch-Gordan transform.

Let $\boldsymbol{R}_1$ and $\boldsymbol{R}_2$ be two representations of group G and let V_1,V_2 be their carrier spaces respectively, then $\boldsymbol{R}_1 \otimes \boldsymbol{R}_2$ is also a representation of group G. Usually, this representation is reducible even if both $\boldsymbol{R}_1$ and $\boldsymbol{R}_2$ are irreducible. This means we can decompose its carrier space $V_1 \otimes V_2$ as

$$V_1 \otimes V_2 \overset{G}{\cong} \bigoplus_{\lambda \in \hat{G}} m^\lambda_{1,2} V_\lambda \tag{4.52}$$

where $m^\lambda_{1,2}$ is the multiplicity factor of the carrier space V_λ of irrep $\boldsymbol{r}_\lambda$. This factor could be zero sometimes. Such decomposition is called *Clebsch-Gordan decomposition*.

In our case, we are particularly interested in the decomposition of $(Q^d_{(1)})^* \otimes Q^d_\lambda$. It turns out

$$(Q^d_{(1)})^* \otimes Q^d_\lambda \overset{U(d)}{\cong} \bigoplus_{\mu \in \{\lambda - \square\}} Q^d_\mu \tag{4.53}$$

where $\{\lambda - \square\}$ denotes the set of valid Young diagrams obtained from λ by removing one box from the end of each possible row. For example, if $\lambda =$  , then the set is $\{$  ,  $\}$. Further notice that, the decomposition we encountered is a special case as the multiplicity factor is 1.

This unitary change of basis is called *Clebsch-Gordan transform* and we will denote it by $W : Q^*_{(1)} \otimes Q^d_\lambda \to \bigoplus_{\mu\in\{\lambda-\square\}} Q^d_\mu$. By Equation 4.53 we know that

$$W(U^* \otimes U_\lambda)W^\dagger = \bigoplus_{\mu\in\{\lambda-\square\}} U_\mu \tag{4.54}$$

where $U_\mu = \boldsymbol{Q}^d_\mu(U)$.

Proof of Proposition (4.2.1) Since $J(\Psi)$ commutes with $(U^* \otimes U_\lambda)$, then under the same Clebsch-Gordan transform, it must be block diagonal with each block being a multiple of identity matrix in the corresponding subspace.

Hence, covariant quantum channel $\Psi : Q^d_\lambda \to (Q^d_{(1)})^*$ must satisfy the following condition:

$$WJ(\Psi)W^\dagger = \bigoplus_{\mu\in\{\lambda-\square\}} c_\mu I_\mu. \tag{4.55}$$

Since we require $J(\Psi) \succeq 0$, we get the first condition on c_μ which is $c_\mu \geq 0$. ∎

This is the first constraint we have on c_μ, the next constraint will be derived from the trace-preserving condition.

4.2.3 The trace-preserving condition

Now we would like to know the implication of the trace-preserving condition on the coefficient c_μ's. The condition is summarized in the following proposition.

Proposition 4.2.2 *Let $\Psi : Q^d_\lambda \to (Q^d_{(1)})^*$ be a quantum channel with Choi representation of the form $J(\Psi) = W^\dagger \left[\bigoplus_{\mu\in\{\lambda-\square\}} c_\mu I_\mu\right] W$, then the trace-preserving condition implies that the coefficients c_μ's must satisfy the following condition*

$$\sum_{\mu\in\{\lambda-\square\}} c_\mu \frac{\dim Q^d_\mu}{\dim Q^d_\lambda} = 1. \tag{4.56}$$

To see it we will introduce a lemma

Lemma 4.2.3 ([17]) *For a given $\mu \in \{\lambda - \square\}$, let $E_\mu \in \mathrm{End}((Q^d_{(1)})^* \otimes Q^d_\lambda)$ be an operator act as I_μ on Q^d_μ and acts as 0 on all the other irrep carrier spaces, then*

$$\mathrm{Tr}_{(Q^d_{(1)})^*}(W^\dagger E_\mu W) = \frac{\dim Q^d_\mu}{\dim Q^d_\lambda} I_\lambda. \tag{4.57}$$

Proof of Lemma (4.2.3) Consider any $U \in U(d)$, we have

$$\begin{aligned} U_\lambda \,\mathrm{Tr}_{(Q^d_{(1)})^*}(W^\dagger E_\mu W) U_\lambda^\dagger &= \mathrm{Tr}_{(Q^d_{(1)})^*}[(U^* \otimes U_\lambda) W^\dagger E_\mu W (U^* \otimes U_\lambda)^\dagger] \\ &= \mathrm{Tr}_{(Q^d_{(1)})^*}[W^\dagger \Big(\bigoplus_{\mu' \in \{\lambda - \square\}} U_{\mu'} \Big) E_\mu \Big(\bigoplus_{\mu'' \in \{\lambda - \square\}} U^\dagger_{\mu''} \Big) W] \\ &= \mathrm{Tr}_{(Q^d_{(1)})^*}(W^\dagger E_\mu W). \end{aligned}$$

By Schur's Lemma, we can conclude that $\mathrm{Tr}_{(Q^d_{(1)})^*}(W^\dagger E_\mu W) \propto I_\lambda$.

Let the coefficient be x, then $\mathrm{Tr}(W^\dagger E_\mu W) = x \,\mathrm{Tr}(I_\lambda)$. Further note that $\mathrm{Tr}(W E_\mu W^\dagger) = \dim Q^d_\mu$ and $\mathrm{Tr}(I_\lambda) = \dim Q^d_\lambda$, we can conclude that $x = \frac{\dim Q^d_\mu}{\dim Q^d_\lambda}$. ∎

Proof of Proposition (4.2.2) Since $\bigoplus_{\mu \in \{\lambda - \square\}} c_\mu I_\mu = \sum_{\mu \in \{\lambda - \square\}} c_\mu E_\mu$, we can have the following equation:

$$\begin{aligned} I_\lambda &= \mathrm{Tr}_{(Q^d_{(1)})^*}(W^\dagger \sum_{\mu \in \{\lambda - \square\}} c_\mu E_\mu W) \\ &= \sum_{\mu \in \{\lambda - \square\}} c_\mu \frac{\dim Q^d_\mu}{\dim Q^d_\lambda} I_\lambda. \end{aligned}$$

Cancelling I_λ from both sides will give us Proposition (4.2.2). ∎

4.2.4 Gel'fand-Tsetlin basis and the objective value

With all the constraints on c_μ's have been derived, the next step is to give an expression of the objective value of this optimization problem. The objective value or the fidelity achieved on Q^d_λ is of the form

$$f_\lambda = \langle d | \,\mathrm{Tr}_{V_\lambda}(J(\Phi_\lambda)(I \otimes \rho_\lambda^T)) \,| d \rangle \tag{4.58}$$

where $|d\rangle$ is the target state and ρ_λ is the state projected onto Q^d_λ. When we calculate the fidelity, we need to know the entries of W. To learn about the transform, we need to introduce the Gel'fand-Tsetlin basis.

In general, suppose $(\boldsymbol{r}, V)$ is an irrep of group G and H is a proper subgroup of G. Restricting the representation $\boldsymbol{r}$ to H will give us an representation of H denoted by $(\boldsymbol{r}\downarrow_H, V\downarrow_H)$. In most of the cases, $\boldsymbol{r}\downarrow_H$ will be reducible and $V\downarrow_H$ can be decomposed as

$$V\downarrow_H \overset{H}{\cong} \bigoplus_{\alpha\in\hat{H}} V_\alpha \otimes \mathbb{C}^{n_\alpha}.$$

where $\hat{H}$ is the set of all the irreps of H and n_α is the branching multiplicity factor of the irrep labelled by α. The case that all the branching multiplicities are either 0 or 1 is called *multiplicity-free branching*.

Such restriction and decomposition can be recursively applied until we reach the trivial subgroup that only contains the identity element and we will have a tower of groups: $G = G_1 \supset G_2 \supset \cdots \supset G_{k-1} \supset G_k = \{e\}$. The recursion starts by decomposing V_1, the carrier space of G_1, under restriction to G_2. Then for each V^2_α appearing in the decomposition of G_1, we further decompose it under restriction to G_3. The process goes on until we reach the trivial group. If we choose orthonormal basis for each multiplicity space, then we will have a complete orthonormal basis for V_1. We label such basis by $|\alpha_2, m_2, \alpha_3, m_3, \ldots, \alpha_k, m_k\rangle$ where α_i is the label of an irrep of G_i and m_i is denoting a basis of the corresponding multiplicity space.

If the branching for each G_i in the tower is multiplicity-free , then we say the tower of subgroup is *canonical*. In this case we don't need to worry about the multiplicity space $\mathbb{C}^{n_\alpha}$ and the basis can be simply labelled by $|\alpha_2, \alpha_3, \ldots, \alpha_k\rangle$. Often we will include the irrep label of G_1 as well to get a complete label of the basis state.

It turns out that the chain of subgroup, $U(d) \supset U(d-1) \supset \cdots \supset U(2) \supset U(1) \supset \{1\}$, is canonical. The embedding is by the fact that $U(i)\oplus 1 = \{U\oplus 1 : U \in U(i)\}$ is a subgroup of $U(i+1)$. For a irrep carrier space Q^d_λ of $U(d)$, the restriction to $U(d-1)$ is reducible and it decomposes as the direct sum of all irreps of $U(d-1)$ with the irrep label satisfying the *betweenness condition*. Let $\lambda = (\lambda_{1,d}, \lambda_{2,d}, \ldots, \lambda_{d,d})$ and $\lambda' = (\lambda_{1,d-1}, \lambda_{2,d-1}, \ldots, \lambda_{d-1,d-1})$,if

$$\lambda_{j,d} \geq \lambda_{j,d-1} \geq \lambda_{j+1,d}, \quad \forall \ \ 1 \leq j \leq d-1, \tag{4.59}$$

then λ' satisfy the betweenness condition and irrep labelled by λ' will appear in the decomposition of Q^d_λ.

The basis we get from the branching is called *Gel'fand-Tsetlin basis*. Since it is labelled by partitions, we will introduce one visualization of such basis:

$$M = \begin{pmatrix} m_{1,d} & & m_{2,d} & \dots & m_{d-1,d} & & m_{d,d} \\ & m_{1,d-1} & \dots & \dots & \dots & m_{22} & \\ & & & \vdots & & & \\ & & m_{1,2} & & m_{2,2} & & \\ & & & m_{1,1} & & & \end{pmatrix} \tag{4.60}$$

where each $m_{i,j}$ is between $m_{i,j-1}$ and $m_{i+1,j-1}$. We shall denote such pattern by $M = (\boldsymbol{m}_d, \boldsymbol{m}_{d-1}, \dots, \boldsymbol{m}_2, \boldsymbol{m}_1)$ with each $\boldsymbol{m}_i$ being a valid partition and bold to stress the fact it is an array of integers. Such pattern is called *Gel'fand-Tsetlin pattern*. One thing to note is that for a given Q^d_λ, the first row of all the Gel'fand-Tsetlin pattern will be the same as λ. When we denote a particular basis state of Q^d_m, we will use the notation $|\boldsymbol{m}, M\rangle$ where M is the corresponding Gel'fand-Tsetlin pattern and we repeat $\boldsymbol{m}$ to stress the label of the irrep, Q^d_m.

There is an one-to-one correspondence between Gel'fand-Tsetlin pattern and semi-standard Young tableaux. Here we will give steps to convert a Gel'fand-Tsetlin pattern to a semistand Young tableaux for a given pattern M:

1. create an empty Young tableaux;
2. extend the first row to length $m_{1,1}$ and fill the newly added boxes with number 1;
3. extend the first row to length $m_{1,2}$ and fill the newly added boxes with number 2;
4. repeat this process by extend i-th row to length $m_{i,j}$ and fill the newly boxes with number j;

The process is finished when all the numbers in the pattern are used. Following the same idea, we can read out the corresponding Gel'fand-Tsetlin pattern from a given semi-standard Young tableaux.

The entries of W matrix are called *Clebsch-Gordan coefficients* which are denoted by $\langle \boldsymbol{m}', M', \boldsymbol{m}'', M'' | \boldsymbol{m}, M \rangle$ and defined by

$$|\boldsymbol{m}, M\rangle = \sum_{M', M''} \langle \boldsymbol{m}', M', \boldsymbol{m}'', M'' | \boldsymbol{m}, M \rangle \, |\boldsymbol{m}', M'\rangle \otimes |\boldsymbol{m}'', M''\rangle \tag{4.61}$$

when the decomposition is $Q^d_{\boldsymbol{m}'} \otimes Q^d_{\boldsymbol{m}''}$ and $Q^d_{\boldsymbol{m}}$ is one of the resulting subspace. The general formula for calculating such coefficients is very complicated, but our case is special. Moreover, the covariance property gives us the freedom to choose a simpler formula in this special case.

Before giving formulas, we need to mention one important property since we are working with dual representation.

Proposition 4.2.4

$$\langle \overline{\boldsymbol{m}'}, \overline{M'}, \boldsymbol{m}, M | \boldsymbol{m}'', M'' \rangle = \frac{\dim Q^d_{\boldsymbol{m}''}}{\dim Q^d_{\boldsymbol{m}}} \overline{\langle \boldsymbol{m}', M', \boldsymbol{m}'', M'' | \boldsymbol{m}, M \rangle} \tag{4.62}$$

where $Q^d_{\overline{\boldsymbol{m}'}} = (Q^d_{\boldsymbol{m}'})^*$, $\overline{\boldsymbol{m}'} = (-m_{d,d}, -m_{d-1,d}, \ldots, -m_{2,d}, -m_{1,d})$ *and* $\overline{M'} = (\overline{\boldsymbol{m}_d}, \overline{\boldsymbol{m}_{d-1}}, \ldots \overline{\boldsymbol{m}_1})$. *The overline above the coefficient is denoting the complex conjugate.*

The proof can be found in Chapter 18 of [22].

For most of combinations of M', M'' and M, the coefficient $\langle \boldsymbol{m}', M', \boldsymbol{m}'', M'' | \boldsymbol{m}, M \rangle$ will be zero. This coefficient will not vanish only if

$$\sum_{i=1}^{j} (m'_{i,j} + m''_{i,j}) = \sum_{i=1}^{j} m_{i,j} \tag{4.63}$$

holds for $j = 1, 2, \ldots, d$.

Expanding the partial trace of Equation (4.58), we can get

$$\begin{aligned} f_\lambda &= \sum_{i=1}^{\dim Q^d_\lambda} \langle d| \langle i| W^\dagger (\bigoplus_\mu c_\mu I_\mu) W (I_d \otimes \rho_\lambda^T) |d\rangle |i\rangle \\ &= \sum_{i=1}^{\dim Q^d_\lambda} \rho_{\lambda,i} \langle d| \langle i| W^\dagger (\bigoplus_\mu c_\mu I_\mu) W |d\rangle |i\rangle \end{aligned}$$

where $|i\rangle$ is a basis state of Q^d_λ and $\rho_{\lambda,i}$ is the (i,i)-th entry of ρ_λ. From the form of Q^d_λ basis states we know that $\rho_{\lambda,i}$ is the i-th entry of the Schur function $s_\lambda(\alpha_1, \alpha_2, \ldots, \alpha_d)$ divided by the Schur function. Hence, we need to introduce Schur function and one important theorem.

Definition Given a partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ where $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ and each $\lambda_i \geq 0$, let

$$a_{(\lambda_1+n-1,\lambda_2+n-2,\ldots,\lambda_n)}(x_1, x_2, \ldots, x_n) = \det \begin{pmatrix} x_1^{\lambda_1+n-1} & x_2^{\lambda_1+n-1} & \ldots & x_n^{\lambda_1+n-1} \\ x_1^{\lambda_2+n-2} & x_2^{\lambda_2+n-2} & \ldots & x_n^{\lambda_2+n-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{\lambda_n} & x_2^{\lambda_n} & \ldots & x_n^{\lambda_n} \end{pmatrix}$$

and

$$a_{(n-1,n-2,\ldots,0)}(x_1, x_2, \ldots, x_n) = \prod_{1 \leq j < k \leq n} (x_j - x_k)$$

then we can define the Schur function labelled by λ as

$$s_\lambda(x_1, x_2, \ldots x_n) = \frac{a_{(\lambda_1+n-1,\lambda_2+n-2,\ldots,\lambda_n)}(x_1, x_2, \ldots, x_n)}{a_{(n-1,n-2,\ldots,0)}(x_1, x_2, \ldots, x_n)}$$

The expression we used $s_\lambda(\alpha_1, \alpha_2, \ldots, \alpha_d)$ is the Schur function evaluated when $x_i = \alpha_i$. This factor represents the probability to measure the state projected onto Q_λ^d by the following theorem by Alicki *et al.* [2].

Theorem 4.2.5 *For a d-dimensional quantum state ρ with eigenvalues $\alpha_1, \alpha_2, \ldots, \alpha_d$, the probability to be projected onto subspace Q_λ^d is*

$$\mathrm{Tr}(\Pi_{\lambda,\alpha} \rho^{\otimes n}) = s_\lambda(\alpha_1, \alpha_2, \ldots, \alpha_d) \;\; \textit{for} \;\; \alpha = 1, 2, \ldots, \dim P_\lambda \tag{4.64}$$

where λ is a valid partition of n.

Now we can further simplify the expression of f_λ. We can write $\bigoplus_\mu c_\mu I_\mu$ as $(\sum_\mu \sqrt{c_\mu} \Pi_\mu)$ where Π_μ's are orthonormal projectors onto irrep subspace Q_μ^d. Then

$$f_\lambda = \sum_{i=1}^{\dim Q_\lambda^d} \rho_{\lambda,i} \sum_{\mu \in \{\lambda - \square\}} \| \sqrt{c_\mu} \Pi_\mu W |d\rangle |i\rangle \|^2 \tag{4.65}$$

$$= \sum_{i=1}^{\dim Q_\lambda^d} \rho_{\lambda,i} \sum_{\mu \in \{\lambda - \square\}} c_\mu \sum_{j=1}^{\dim Q_\mu^d} \| \langle j | W |d\rangle |i\rangle \|^2 \tag{4.66}$$

where $|i\rangle$ and $|j\rangle$ are basis state of Q_λ^d and Q_μ^d respectively.

4.2.5 Putting together the optimization problem

To make the trace-preserving condition convex, we introduce $\overline{c_\mu} = \frac{\dim Q_\mu^d}{\dim Q_\lambda^d} c_\mu$. Combining Proposition (4.2.1) and (4.2.2) and Equation (4.66), the optimization problem is

$$\begin{aligned} \underset{\overline{c_\mu}}{\text{Max}} \quad & \sum_{\mu \in \{\lambda - \square\}} \overline{c_\mu} \left(\sum_{i=1}^{\dim Q_\lambda^d} \rho_{\lambda,i} \frac{\dim Q_\lambda^d}{\dim Q_\mu^d} \sum_{j=1}^{\dim Q_\mu^d} \| \langle j | W | d \rangle | i \rangle \|^2 l \right) \\ \text{subject to} \quad & \overline{c_\mu} \geq 0 \\ & \sum_{\mu \in \{\lambda - \square\}} \overline{c_\mu} = 1 \end{aligned} .$$

Here c_μ's are the variables of this linear programming problem and the expression $\left(\sum_{i=1}^{\dim Q_\lambda^d} \rho_{\lambda,i} \frac{\dim Q_\lambda^d}{\dim Q_\mu^d} \sum_{j=1}^{\dim} \right.$ is the coefficient for each c_μ which is determined by λ and μ. The norm $\| \langle j | W | d \rangle | i \rangle \|^2$ is the Clesch-Gordan coefficient.

Since this is a convex linear programming problem, the objective value can be replaced by

$$\underset{\mu \in \{\lambda - \square\}}{\text{Max}} \frac{\dim Q_\lambda^d}{\dim Q_\mu^d} \sum_{j=1}^{\dim Q_\mu^d} \sum_{i=1}^{\dim Q_\lambda^d} \rho_{\lambda,i} \| \langle j | W | d \rangle | i \rangle \|^2. \tag{4.67}$$

Here we used the fact that the maximum can only be achieved when one of the c_μ's is 1 and all the others are 0.

To start evaluate such optimization problem, we need to know the expression of $\| \langle j | W | d \rangle | i \rangle \|^2$. By our introduction of Gel'fand-Tsetlin pattern and Clebsch-Gordan coefficients, we know that the non-vanishing terms $\| \langle j | W | d \rangle | i \rangle \|^2$ must have this corresponding Gel'fand-Tsetlin pattern

$$\left(\begin{array}{ccc|c} (\mathbf{0}, -1) & & \boldsymbol{m}_d & \boldsymbol{m}_d - i \\ \mathbf{0} & & \boldsymbol{m}_{d-1} & \boldsymbol{m}_{d-1} \\ & & \vdots & \\ 0 & & m_{11} & 0 \end{array} \right) .$$

Here we used the fact that the Gel'fand-Tsetlin pattern of $|d\rangle$ has all entries being 0 except for the last entry in the first row being -1. The term $\boldsymbol{m}_d - i$ means the i-th entry of $\boldsymbol{m}_d$ was deducted by 1. This means that for each $|i\rangle \in Q_\lambda^d$, there is only one corresponding

state $|j\rangle$ that will produce non-zero Clebsch-Gordan coefficient. Hence, the summation over j can be dropped in the calculation. The summation over i can be further specified by summing over entries in its Gel'fand-Tsetlin pattern. We will see how to do it in the next chapter.

The formula for this coefficient is known. To simplify the expression, we define $l_{j,k} = m_{j,k} - j$, then

$$\left(\begin{array}{cc|c} (\mathbf{0},-1) & \boldsymbol{m}_d & \boldsymbol{m}_d - i \\ \mathbf{0} & \boldsymbol{m}_{d-1} & \boldsymbol{m}_{d-1} \\ & \vdots & \\ 0 & m_{11} & 0 \end{array}\right) = \left|\frac{\prod_{j=1}^{d-1}(l_{j,d-1} - l_{i,d})}{\prod_{j\neq i}(l_{j,d} - l_{i,d})}\right|^{1/2}. \tag{4.68}$$

With this formula we can solve this problem computationally for any given d and N. However, the universal solution for all d and N is unknown. Hence we will start by solving the case when $d = 2$ and $d = 3$ first in the next chapter.

Chapter 5

Optimal purification of qubit and qutrit

In this chapter, we will follow the optimization problem formulation in Equation (4.67) to work out the optimal fidelity achieved by purification of qubits and qutrits on each unitary group irrep. In the qubit case, we will see that the optimal fidelity achievable on each irrep is the same as shown in Equation (4.22). For the qutrit case, we will not only calculate the optimal fidelity achievable on each unitary irrep, we will also consider all such irreps to calculate the average fidelity.

5.1 Qubit case revisited

For unitary group $U(2)$, a particular semi-standard Young tableaux can be represented by the Gel'fand-Tsetlin pattern:

$$\begin{pmatrix} m_{1,2} & & m_{2,2} \\ & m_{1,1} & \end{pmatrix} \tag{5.1}$$

where the shape of the Young diagram is $\lambda = (\lambda_1, \lambda_2)$ and $m_{1,2} = \lambda_1, m_{2,2} = \lambda_2$.

The set of all possible μ's contains only two elements: μ_1 and μ_2 with μ_i defined to be the Young diagram obtained from λ by removing one box from the i-th row. Hence, for a general μ_i the objective value can be expressed as

$$f_\lambda(\mu_i) = \frac{\dim Q_\lambda^2}{\dim Q_{\mu_i}^2} \sum_{i=1}^{\dim Q_\lambda^2} \sum_{j=1}^{\dim Q_{\mu_i}^2} \rho_{\lambda,i} |\langle j| W |2\rangle |i\rangle|^2 \tag{5.2}$$

and we need to compare $f_\lambda(\mu_1)$ and $f_\lambda(\mu_2)$.

In the dual space of defining representation, state $|2\rangle$ has the following Gel'fand-Tsetlin pattern

$$\begin{pmatrix} 0 & & -1 \\ & 0 & \end{pmatrix}.$$

If $|i\rangle \in Q^2_\lambda$ has Gel'fand-Tsetlin pattern of the form (5.1), then the only $|j\rangle \in Q^2_{\mu_1}$ which will give non-trivial Clebsch-Gordan coefficient must be of the form

$$\begin{pmatrix} m_{1,2}-1 & & m_{2,2} \\ & m_{1,1} & \end{pmatrix}.$$

For μ_2, the first row of the non-vanish state $|j\rangle$ will be $(m_{1,2}, m_{2,2}-1)$ and its second row will be unchanged.

To evaluate $f_\lambda(\mu_i)$, we first need to find the expression of $\rho_{\lambda,i}$ which is the eigenvalue of ρ_λ on state $|i\rangle \in Q^2_\lambda$. Recall that $\alpha_2 = 1 - \frac{e_0}{2}$ is the eigenvalue of $|2\rangle$ of ρ and $\alpha_1 = \frac{e_0}{2}$ is the eigenvalue of $|1\rangle$. Assume the Gel'fand-Tsetlin pattern of $|i\rangle \in Q^2_\lambda$ is as shown in Equation (5.1), then we have

$$\rho_{\lambda,i} = \frac{\alpha_1^{m_{1,1}} \alpha_2^{m_{1,2}-m_{1,1}+m_{2,2}}}{s_\lambda(\alpha_1, \alpha_2)}. \tag{5.3}$$

In general, the Schur function $s_{(\lambda_1,\lambda_2)}(x_1, x_2)$ is defined as

$$s_{(\lambda_1,\lambda_2)}(x_1, x_2) = \frac{x_1^{\lambda_2} x_2^{\lambda_2} (x_1^{\lambda_1-\lambda_2+1} - x_2^{\lambda_1-\lambda_2+1})}{x_1 - x_2}$$

and the denominator of Equation (5.3) is the corresponding Schur function evaluated when $x_1 = \alpha_1$ and $x_2 = \alpha_2$. However, in the comparison, we will omit this denominator as it is always positive and will not affect the relation between $f_\lambda(\mu_1)$ and $f_\lambda(\mu_2)$.

To get closed-form expressions of $f_\lambda(\mu_1)$ and $f_\lambda(\mu_2)$, we further assume that $N = \lambda_1 + \lambda_2$. Note that when λ is fixed, each Gel'fand-Tsetlin pattern can be uniquely described by its value of $m_{1,1}$. Rewriting Equation (5.2), we can simplify the sum to be over possible values

of $m_{1,1}$.

$$\begin{aligned}
f_\lambda(\mu_1) =& \frac{\lambda_1-\lambda_2+1}{\lambda_1-\lambda_2}\sum_{m_{11}=\lambda_2}^{\lambda_1-1}\alpha_1^{m_{11}}\alpha_2^{N-m_{11}}\frac{\lambda_1-m_{11}}{\lambda_1-\lambda_2+1}\\
=& \frac{\lambda_1-\lambda_2+1}{\lambda_1-\lambda_2}\alpha_2^N\sum_{m_{11}=\lambda_2}^{\lambda_1-1}q^{m_{11}}\frac{\lambda_1-m_{11}}{\lambda_1-\lambda_2+1}\\
=& \frac{\alpha_2^N}{\lambda_1-\lambda_2}\sum_{m_{11}=\lambda_2}^{\lambda_1-1}q^{m_{11}}(\lambda_1-m_{11})\\
=& \frac{\alpha_2^N}{\lambda_1-\lambda_2}\frac{(\lambda_1-\lambda_2)(1-q)q^{\lambda_2}-q(q^{\lambda_2}-q^{\lambda_1})}{(1-q)^2}
\end{aligned}$$

where $q=\frac{\alpha_1}{\alpha_2}$.

Similarly, the other fidelity is

$$\begin{aligned}
f_\lambda(\mu_2) =& \frac{\lambda_1-\lambda_2+1}{\lambda_1-\lambda_2+2}\alpha_2^N\sum_{m_{11}=\lambda_2}^{\lambda_1}q^{m_{11}}\frac{m_{11}+1-\lambda_2}{\lambda_1-\lambda_2+1}\\
=& \frac{\alpha_2^N}{\lambda_1-\lambda_2+2}\sum_{m_{11}=\lambda_2}^{\lambda_1}q^{m_{11}}(m_{11}+1-\lambda_2)\\
=& \frac{\alpha_2^N}{\lambda_1-\lambda_2+2}\frac{q^{\lambda_2}-(\lambda_1+2-\lambda_2)q^{\lambda_1+1}+(\lambda_1+1-\lambda_2)q^{\lambda_1+2}}{(1-q)^2}.
\end{aligned}$$

The comparison reveals that

Proposition 5.1.1 $f_\lambda(\mu_1) > f_\lambda(\mu_2)\ \ \forall\ \ \lambda\vdash N,\ \ e_0\in(0,1)$.

Proof We will do the comparison directly by calculating the difference and then show this difference is always positive. The difference is

$$\begin{aligned}
&f_\lambda^{(2)}(\mu_1)-f_\lambda^{(2)}(\mu_2)\\
=&\frac{(\lambda_1+1-\lambda_2)q^{\lambda_2}}{(\lambda_1+2-\lambda_2)(\lambda_1-\lambda_2)(1-q)^2}(-2q(1-q^{\lambda_1-\lambda_2})+(\lambda_1-\lambda_2)(1-q)(1+q^{\lambda_1-\lambda_2+1})).
\end{aligned}$$

We are interested in the behaviour of $-2q(1-q^{\lambda_1-\lambda_2})+(\lambda_1-\lambda_2)(1-q)(1+q^{\lambda_1-\lambda_2+1})$ since the factor in front of it is always positive.

Let $l = \lambda_1 - \lambda_2$ and define an auxillary function:

$$g(q, l) = -2q(1 - q^l) + l(1 - q)(1 + q^{l+1}). \tag{5.4}$$

Taking partial derivative of q on its domain $(0, 1)$, we have

$$\frac{\partial g^2}{\partial^2 q} = l(l + 1)(l + 2)(q^{l-1} - q^l) > 0,$$

so the maximum of $\frac{\partial g}{\partial q}$ is achieved at $q = 1$. However, the maximal value of $\frac{\partial g}{\partial q}$ is

$$\frac{\partial g}{\partial q}\Big|_{q=1} = \left(-2 - l + (l + 1)(l + 2)q^l - l(l + 2)q^{l+1}\right)\Big|_{q=1} = 0$$

which means $\frac{\partial g}{\partial q} < 0$ and the minimum of $g(q, l)$ for any given l is achieved at $q = 1$.

For any give $l > 0$, $g(1, l) = 0$ so we have proved $f_\lambda^{(2)}(\mu_1) > f_\lambda^{(2)}(\mu_2)$. ∎

There are other ways to prove it. The reason we choose this method is that this method is similar to the method used for the qutrit case.

Let $2j = \lambda_1 - \lambda_2$ and adding back the Schur function factor we omitted, the optimal fidelity is

$$\begin{aligned}&\frac{f_\lambda(\mu_1)}{s_{(\lambda_1,\lambda_2)}(\alpha_1, \alpha_2)}\\ =&\frac{\alpha_2(2j\alpha_2^{2j+1} - (2j + 1)\alpha_1\alpha_2^{2j} + \alpha_1^{2j+1})}{2j(\alpha_2 - \alpha_1)(\alpha_2^{2j+1} - \alpha_1^{2j+1})}\end{aligned}$$

which matches the optimal fidelity given in [9]. The average fidelity in [9] can also be re-derived using method presented in Section 4.1.2.

5.2 Qutrit case

In this section, we will first calculate the fidelity achieved on each irrep Q_λ^3 in the first subsection. The second subsection will combine the result from previous subsection to calculate the average fidelity. With average fidelity, we can derive a lower bound on the number of states required to purify a state until it is $\epsilon-$close to original state.

5.2.1 Optimal fidelity achievable on unitary group irrep Q^3_λ

Before we start the calculation, we need to state one fact, which is true for all $\lambda \in I_{d,N}$ and

$$\sum_{\mu\in\{\lambda-\square\}} \frac{\dim Q^d_\mu}{\dim Q^d_\lambda} f_\lambda(\mu) = \sum_{i=1}^{\dim Q^d_\lambda} \rho_{\lambda,i} \sum_{\mu\in\{\lambda-\square\}} \|\Pi_\mu W |d\rangle |i\rangle\|^2 = \sum_{i=1}^{\dim Q^d_\lambda} \rho_{\lambda,i} = s_\lambda(\boldsymbol{\alpha}) \tag{5.5}$$

where Π_μ is the projector onto Q^d_μ and $\boldsymbol{\alpha}$ represents the vector of all the eigenvalues of ρ_0. With this fact, we will be able to calculate the closed-form expressions for $f_\lambda(\mu_1)$,$f_\lambda(\mu_2)$ and $f_\lambda(\mu_3)$, then we can compare them to figure out which one is the largest.

For qutrit, a particular semi-standard Young tableaux can be represented by the Gel'fand-Tsetlin pattern:

$$\begin{pmatrix} m_{1,3} & & m_{2,3} & & m_{3,3} \\ & m_{1,2} & & m_{2,2} & \\ & & m_{1,1} & & \end{pmatrix}. \tag{5.6}$$

The first row is persisted over all such patterns for a given $\lambda = (\lambda_1, \lambda_2, \lambda_3)$ with $m_{1,3} = \lambda_1, m_{2,3} = \lambda_2$ and $m_{3,3} = \lambda_3$.

As in the qubit case, we define

$$f_\lambda(\mu_k) = \frac{\dim Q^3_\lambda}{\dim Q^3_{\mu_k}} \sum_{i=1}^{\dim Q^3_\lambda} \sum_{j=1}^{\dim Q^3_{\mu_k}} \rho_{\lambda,i} |\langle j| W |2\rangle |i\rangle|^2 \quad \text{for} \quad k = 1, 2, 3 \tag{5.7}$$

and we need to compare $f_\lambda(\mu_1)$,$f_\lambda(\mu_2)$ and $f_\lambda(\mu_3)$.

The pattern for state $|3\rangle$ of the dual defining representation is of the form

$$\begin{pmatrix} 0 & & 0 & & -1 \\ & 0 & & 0 & \\ & & 0 & & \end{pmatrix}.$$

Hence for a basis state of Q^3_λ with Gel'fand-Tsetlin pattern in Equation (5.6), the only state in $Q^3_{\mu_1}$ that will give non-zero Clebsch-Gordan coefficient must be of the form:

$$\begin{pmatrix} m_{1,3}-1 & & m_{2,3} & & m_{3,3} \\ & m_{1,2} & & m_{2,2} & \\ & & m_{1,1} & & \end{pmatrix}.$$

To get the Gel'fand-Tsetlin pattern of such states in $Q^3_{\mu_2}$ and $Q^3_{\mu_3}$, we just need to move -1 to $m_{2,3}$ and $m_{3,3}$ respectively. Then the corresponding Clebsch-Gordan Coefficients is

$$\begin{aligned}
&\left\langle \begin{array}{ccc|c} (0^2,-1) & \boldsymbol{m_3} & \boldsymbol{m_3}-i & \\ (0,0) & \boldsymbol{m_2} & \boldsymbol{m_2} & \\ 0 & m_{11} & m_{11} & \end{array} \right\rangle^2 \\
=&\frac{\dim Q^3_{\mu_i}}{\dim Q^3_\lambda} \left\langle \begin{array}{ccc|c} (1,0^2) & \boldsymbol{m_3}-i & \boldsymbol{m_3} & \\ (1,0) & \boldsymbol{m_2} & \boldsymbol{m_2} & \\ 1 & m_{11} & m_{11} & \end{array} \right\rangle^2 \\
=&\frac{\dim Q^3_{\mu_i}}{\dim Q^3_\lambda} \left(\begin{array}{ccc|c} (1,0^2) & \boldsymbol{m_3}-i & \boldsymbol{m_3} & \\ (0,0) & \boldsymbol{m_2} & \boldsymbol{m_2} & \end{array} \right)^2 \\
=&\frac{\dim Q^3_{\mu_i}}{\dim Q^3_\lambda} \left| \frac{\prod_{j=1}^2 (l_{j,2}-l_{i,3}-1)}{\prod_{j\neq i}(l_{j,3}-l_{i,3})} \right|.
\end{aligned}$$

Hence when we do summation over such coefficients, we could sum over $m_{1,2}, m_{2,2}$ and $m_{1,1}$ because the three numbers could uniquely identify the Cledsch-Gordan coefficient.

Similarly, $\rho_{\lambda,i}$ can be expressed in terms of α_1 and α_3. For a given semi-standard Young tableaux, every box filled with 1 or 2 will contribute one copy of α_1 to $\rho_{\lambda,i}$ and each box filled with 3 will contribute one copy of α_3. Expressing it in terms of the Gel'fand-Tsetlin pattern and adding the Schur function factor we get

$$\rho_{\lambda,i} = \frac{\alpha_1^{m_{1,2}+m_{2,2}} \alpha_3^{N-m_{1,2}-m_{2,2}}}{s_\lambda(\alpha_1,\alpha_1,\alpha_3)} \tag{5.8}$$

where

$$\begin{aligned}
&s_\lambda(\alpha_1,\alpha_1,\alpha_3) \\
=&\frac{\alpha_3^N}{(1-q)^2}\Big((\lambda_2-\lambda_3+1)q^{\lambda_2+\lambda_3} - (\lambda_1-\lambda_3+2)q^{\lambda_1+\lambda_3+1} + (\lambda_1-\lambda_2+1)q^{\lambda_1+\lambda_2+2}\Big).
\end{aligned}$$

Here, quotient q is defined as $q = \frac{\alpha_1}{\alpha_3} \in (0,1)$. This Schur function factor will be dropped in the following calculation with the same reason as for the qubit case.

With the expressions above we can derive the formula of the fidelity without the Schur

function factor.

$$
\begin{aligned}
&f_\lambda(\mu_1)\\
=&\sum_{m_{12}=\lambda_2}^{\lambda_1-1}\sum_{m_{22}=\lambda_3}^{\lambda_2}\sum_{m_{11}=m_{22}}^{m_{12}}\alpha_1^{m_{12}+m_{22}}\alpha_3^{N-m_{12}-m_{22}}\frac{(\lambda_1-m_{12})(\lambda_1+1-m_{22})}{(\lambda_1-\lambda_2)(\lambda_1+1-\lambda_3)}\\
=&\frac{\alpha_3^N}{(\lambda_1-\lambda_2)(\lambda_1+1-\lambda_3)}\sum_{m_{12}=\lambda_2}^{\lambda_1-1}\sum_{m_{22}=\lambda_3}^{\lambda_2}q^{m_{12}+m_{22}}(m_{12}-m_{22}+1)(\lambda_1-m_{12})(\lambda_1+1-m_{22})\\
=&\frac{\alpha_3^N}{(1-q)^3}\Big((\lambda_2-\lambda_3+1)q^{\lambda_2+\lambda_3}-\frac{(\lambda_1-\lambda_2+1)(\lambda_1-\lambda_3+2)(\lambda_2-\lambda_3+1)}{(\lambda_1-\lambda_2)(\lambda_1-\lambda_3+1)}q^{\lambda_2+\lambda_3+1}\\
&+\frac{\lambda_1-\lambda_3+2}{\lambda_1-\lambda_2}q^{\lambda_1+\lambda_3+1}-\frac{\lambda_1-\lambda_2+1}{\lambda_1-\lambda_3+1}q^{\lambda_1+\lambda_2+2}\Big).
\end{aligned}
$$

For μ_3, $f_\lambda(\mu_3)$ can be evaluated directly as

$$
\begin{aligned}
&f_\lambda(\mu_3)\\
=&\frac{\alpha_3^N}{(\lambda_1+3-\lambda_3)(\lambda_2+2-\lambda_3)}\sum_{m_{12}=\lambda_2}^{\lambda_1}\sum_{m_{22}=\lambda_3}^{\lambda_2}q^{m_{12}+m_{22}}(m_{12}-m_{22}+1)(m_{12}+2-\lambda_3)(m_{22}+1-\lambda_3)\\
=&\frac{\alpha_3^N}{(1-q)^3}\Big(\frac{\lambda_2-\lambda_3+1}{\lambda_1-\lambda_3+3}q^{\lambda_2+\lambda_3}-\frac{\lambda_1-\lambda_3+2}{\lambda_2-\lambda_3+2}q^{\lambda_3+\lambda_1+1}+(\lambda_1-\lambda_2+1)q^{\lambda_1+\lambda_2+2}\\
&-\frac{(\lambda_2-\lambda_3+1)(\lambda_1-\lambda_2+1)(\lambda_1-\lambda_3+2)}{(\lambda_1-\lambda_3+3)(\lambda_2-\lambda_3+2)}q^{\lambda_1+\lambda_2+3}\Big).
\end{aligned}
$$

Similarly, we can write $f_\lambda(\mu_2)$ as a sum over $m_{1,2}$ and $m_{2,2}$ as

$$
\begin{aligned}
&f_\lambda(\mu_2)\\
=&\frac{\alpha_3^N}{(\lambda_1+2-\lambda_2)(\lambda_2-\lambda_3)}\sum_{m_{12}=\lambda_2}^{\lambda_1}\sum_{m_{22}=\lambda_3}^{\lambda_2-1}q^{m_{12}+m_{22}}(m_{12}-m_{22}+1)(m_{12}+1-\lambda_2)(\lambda_2-m_{22}).
\end{aligned}
$$

However, this value is hard to evaluate directly, so we need to use Equation (5.5) and get

$$\begin{aligned}
&f_\lambda(\mu_2)\\
=&\frac{\dim Q^3_\lambda}{\dim Q^3_{\mu_2}}\Big(s_\lambda(\alpha_1,\alpha_1,\alpha_2)-\frac{\dim Q^3_{\mu_1}}{\dim Q^3_\lambda}f_\lambda(\mu_1)-\frac{\dim Q^3_{\mu_3}}{\dim Q_\lambda}f_\lambda(\mu_3)\Big)\\
=&\frac{\alpha_3^N q^{\lambda_2+\lambda_3}}{(1-q)^3}\Big(\frac{\lambda_2-\lambda_3+1}{\lambda_1-\lambda_2+2}-(\lambda_1-\lambda_3+2)q^{\lambda_1-\lambda_2+1}\\
&+\frac{(\lambda_1-\lambda_3+2)(\lambda_2-\lambda_3+1)(\lambda_1-\lambda_2+1)}{(\lambda_2-\lambda_3)(\lambda_1-\lambda_2+2)}q^{\lambda_1-\lambda_2+2}-\frac{\lambda_1-\lambda_2+1}{\lambda_2-\lambda_3}q^{\lambda_1-\lambda_3+2}\Big).
\end{aligned}$$

Before comparing the three fidelities, we could omit the common factor $C(\lambda,q)=\frac{\alpha_3^N q^{\lambda_2+\lambda_3}}{(1-q)^3}$ and define $\lambda_1-\lambda_2=c$, $\lambda_2-\lambda_3=b$ to simplify the expressions:

$$f_\lambda(\mu_1)=C(\lambda,q)\Big(b+1-\frac{(c+1)(b+c+2)(b+1)}{c(b+c+1)}q+\frac{b+c+2}{c}q^{c+1}-\frac{c+1}{b+c+1}q^{b+c+2}\Big), \tag{5.9}$$

$$f_\lambda(\mu_2)=C(\lambda,q)\Big(\frac{b+1}{c+2}-(b+c+2)q^{c+1}+\frac{(b+c+2)(b+1)(c+1)}{b(c+2)}q^{c+2}-\frac{c+1}{b}q^{b+c+2}\Big), \tag{5.10}$$

$$f_\lambda(\mu_3)=C(\lambda,q)\Big(\frac{b+1}{b+c+3}-\frac{b+c+2}{b+2}q^{c+1}+(c+1)q^{b+c+2}-\frac{(b+1)(c+1)(b+c+2)}{(b+c+3)(b+2)}q^{b+c+3}\Big). \tag{5.11}$$

Proposition 5.2.1

$$f_\lambda(\mu_1)>f_\lambda(\mu_2)>f_\lambda(\mu_3)\ \ \forall\ \ \lambda\vdash N\ \&\ p\in(0,1). \tag{5.12}$$

Proof To compare $f_\lambda(\mu_1)$ and $f_\lambda(\mu_2)$, we define an auxiliary function:

$$\begin{aligned}
g(b,c,q)&=\frac{f_\lambda(\mu_1)-f_\lambda(\mu_2)}{C(\lambda,q)(c+1)}\\
&=\frac{b+1}{c+2}-\frac{(b+c+2)(b+1)}{c(b+c+1)}q+\frac{b+c+2}{c}q^{c+1}\\
&-\frac{(b+c+2)(b+1)}{b(c+2)}q^{c+2}+\frac{c+1}{b(b+c+1)}q^{b+c+2}.
\end{aligned}$$

Note that

$$g(b,c,0) = \frac{b+1}{c+2} > 0,$$
$$g(b,c,1) = 0.$$

At this step, we just need to show $g(b,c,q)$ is decreasing on $q \in (0,1)$ by

$$\frac{1}{b+c+2}\frac{\partial g}{\partial q} = -\frac{b+1}{c(b+c+1)} + \frac{c+1}{c}q^c - \frac{b+1}{b}q^{c+1} + \frac{c+1}{b(b+c+1)}q^{b+c+1}.$$

Note that

$$\frac{\partial g}{\partial q}\Big|_{q=0} = -\frac{(b+c+2)(b+1)}{c(b+c+1)} < 0,$$
$$\frac{\partial g}{\partial q}\Big|_{q=1} = 0.$$

Then we take the second derivative and get

$$\frac{1}{b+c+2}\frac{\partial^2 g}{\partial q^2} = (c+1)q^{c-1}(1 - \frac{b+1}{b}q + \frac{1}{b}q^{b+1}).$$

The minimum of $(1 - \frac{b+1}{b}q + \frac{1}{b}q^{b+1})$ is achieved when $q = 1$ and the minimum is 0, hence, $\frac{\partial g}{\partial q}$ is increasing on $q \in (0,1)$. The maximal value of $\frac{\partial g}{\partial q}$ is at $q = 1$ and the maximal value is 0, so $\frac{\partial g}{\partial q} < 0$ and the minimum of $g(b,c,q)$ is achieved when $q = 1$ and we can see that $g(b,c,q) > 0$.

At this point we can conclude that $f_\lambda(\mu_1) > f_\lambda(\mu_2)$.

Similarly, to compare $f_\lambda(\mu_2)$ and $f_\lambda(\mu_3)$, we define an auxiliary function:

$$\begin{aligned} h(b,c,q) &= \frac{f_\lambda(\mu_2) - f_\lambda(\mu_3)}{C(\lambda,q)(b+1)} \\ &= \frac{b+1}{(c+1)(b+c+3)} - \frac{b+c+2}{b+2}q^{c+1} + \frac{(b+c+2)(c+1)}{b(c+2)}q^{c+2} \\ &- \frac{c+1}{b}q^{b+c+2} + \frac{(c+1)(b+c+2)}{(b+2)(b+c+3)}q^{b+c+3}. \end{aligned}$$

Note that

$$h(b,c,0) = \frac{b+1}{(c+1)(b+c+3)} > 0,$$
$$h(b,c,1) = 0.$$

At this step, we just need to show $h(b,c,q)$ is decreasing on $q \in (0,1)$ as

$$\frac{1}{(b+c+2)(c+1)}\frac{\partial h}{\partial q} = q^c\Big(-\frac{1}{b+2}+\frac{1}{b}q-\frac{1}{b}q^{b+1}+\frac{1}{b+2}q^{b+2}\Big).$$

Note that

$$\Big(-\frac{1}{b+2}+\frac{1}{b}q-\frac{1}{b}q^{b+1}+\frac{1}{b+2}q^{b+2}\Big)\Big|_{q=0} = -\frac{1}{b+2} < 0,$$
$$\Big(-\frac{1}{b+2}+\frac{1}{b}q-\frac{1}{b}q^{b+1}+\frac{1}{b+2}q^{b+2}\Big)\Big|_{q=1} = 0.$$

By taking derivatives we could show $k(b,q) = \Big(-\frac{1}{b+2}+\frac{1}{b}q-\frac{1}{b}q^{b+1}+\frac{1}{b+2}q^{b+2}\Big)$ is increasing on $q \in (0,1)$. Hence $\frac{\partial h}{\partial q} < 0$ on $q \in (0,1)$ and the minimum of $f_\lambda(\mu_2) - f_\lambda(\mu_3)$ is 0.

Combining the two results we have $f_\lambda(\mu_1) > f_\lambda(\mu_2) > f_\lambda(\mu_3)$. ∎

Hence, we have shown that in the qutrit case, the optimal fidelity achievable on Q_λ^3 is

$$\frac{f_\lambda^{(3)}}{s_\lambda(\alpha_1,\alpha_1,\alpha_3)} = \frac{\alpha_3^N q^{\lambda_2+\lambda_3}}{(1-q)^3 s_\lambda(\alpha_1,\alpha_1,\alpha_3)} \times \Big(b+1-\frac{(c+1)(b+c+2)(b+1)}{c(b+c+1)}q+\frac{b+c+2}{c}q^{c+1}-\frac{c+1}{b+c+1}q^{b+c+2}\Big). \quad (5.13)$$

5.2.2 Formula of average fidelity $F_N^{(3)}$

Similar to the qubit case, the qutrit case average fidelity is still calculated by the formula:

$$F_N^{(3)} = \sum_{\lambda\vdash N, \lambda_1\geq\lambda_2\geq\lambda_3} f_\lambda^{(3)} d_\lambda^{(3)} \quad (5.14)$$

where $f_\lambda^{(3)}$ can be substituted from Equation (5.13). $d_\lambda^{(3)}$ is the dimension of symmetric group irrep P_λ and defined by

$$d_\lambda^{(3)} = \frac{(\lambda_1-\lambda_2+1)(\lambda_2-\lambda_3+1)(\lambda_1-\lambda_3+2)}{(N+1)(N+2)(N+3)}\binom{N+3}{\lambda_3,\lambda_2+1,\lambda_1+2}. \quad (5.15)$$

Let $b = \lambda_2 - \lambda_3$,$c = \lambda_1 - \lambda_2$ and $q = \frac{\alpha_1}{\alpha_3}$, then

$$F_N^{(3)} = \sum_{\lambda \vdash N} d_\lambda^{(3)} \frac{\alpha_3^N q^{\lambda_2+\lambda_3}}{(1-q)^3} \times \Big(b+1 - \frac{(c+1)(b+c+2)(b+1)}{c(b+c+1)}q + \frac{b+c+2}{c}q^{c+1} - \frac{c+1}{b+c+1}q^{b+c+2}\Big).$$

We will first break the sum into three parts: $F_{N,1}^{(3)}$, $F_{N,2}^{(3)}$ and $F_{N,3}^{(3)}$ such that

$$F_{N,1}^{(3)} = \sum_{\lambda \vdash N} d_\lambda \frac{\alpha_2^N q^{\lambda_2+\lambda_3}}{(1-q)^3}[b+1 - \frac{(c+1)(b+c+2)(b+1)}{c(b+c+1)}q], \tag{5.16}$$

$$F_{N,2}^{(3)} = \sum_{\lambda \vdash N} d_\lambda \frac{\alpha_2^N q^{\lambda_2+\lambda_3}}{(1-q)^3} \frac{b+c+2}{c} q^{c+1}, \tag{5.17}$$

$$F_{N,3}^{(3)} = -\sum_{\lambda \vdash N} d_\lambda \frac{\alpha_2^N q^{\lambda_2+\lambda_3}}{(1-q)^3} \frac{c+1}{b+c+1} q^{b+c+2} \tag{5.18}$$

with $F_N^{(3)} = F_{N,1}^{(3)} + F_{N,2}^{(3)} + F_{N,3}^{(3)}$. In the following analysis, we will see that $F_{N,1}^{(3)}$ is the dominant part and $F_{N,2}^{(3)}$ and $F_{N,3}^{(3)}$ are the minor parts.

5.2.3 Preliminaries of the analysis of $F_N^{(3)}$

Before we go onto analyze the average fidelity, we need to state the Multinomial theorem and propositions derived from the Multinomial theorem and one corollary derived from Chernoff-HoeffdingTheorem (4.1.3).

Theorem 5.2.2 (Multinomial Theorem) *Let n be a nonnegative integer and m be a positive integer, then*

$$(x_1 + x_2 + \cdots + x_m)^n = \sum_{k_1+k_2+\cdots+k_m=n} \binom{n}{k_1, k_2, \ldots, k_m} x_1^{k_1} x_2^{k_2} \ldots x_m^{k_m} \tag{5.19}$$

where $\binom{n}{k_1,k_2,\ldots,k_m} = \frac{n!}{k_1!k_2!\ldots k_m!}$.

In the calculation, we also need to use some propositions derived from Theorem (5.2.2).

Proposition 5.2.3 *Let n be a nonnegative integer, then the following equations hold:*

$$\sum_{k_1+k_2+k_3=n+4} \binom{n+4}{k_1,k_2,k_3} x_1^{k_1}x_2^{k_2}x_3^{k_3}k_1^2k_2x_3 =$$
$$(n+4)(n+3)(n+2)\Big[(n+1)(x_1+x_2+x_3)^n x_1^2x_2x_3 + (x_1+x_2+x_3)^{n+1}x_1x_2x_3\Big], \quad (5.20)$$

$$\sum_{k_1+k_2+k_3=n+4} \binom{n+4}{k_1,k_2,k_3} x_1^{k_1}x_2^{k_2}x_3^{k_3}k_1^2k_2^2 = (n+4)(n+3)\Big[(n+2)(n+1)$$
$$\times (x_1+x_2+x_3)^n x_1^2x_2^2 + (n+2)(x_1+x_2+x_3)^{n+1}(x_1^2x_2+x_1x_2^2) + (x_1+x_2+x_3)^{n+2}x_1x_2\Big], \quad (5.21)$$

$$\sum_{k_1+k_2+k_3=n+4} \binom{n+4}{k_1,k_2,k_3} x_1^{k_1}x_2^{k_2}x_3^{k_3}k_1^3k_2 = (n+4)(n+3)$$
$$\times\Big[(n+2)(n+1)(x_1+x_2+x_3)^n x_1^3x_2 + 3(n+2)(x_1+x_2+x_3)^{n+1}x_1^2x_2 + (x_1+x_2+x_3)^{n+2}x_1x_2\Big]. \quad (5.22)$$

Proof we will only give the proof of Equation (5.20) as the techniques required to prove the other equations are the same.

Applying the Multinomial Theorem (5.2.2) to the case that $m = 3$, we have that

$$(x_1+x_2+x_3)^{n+4} = \sum_{k_1+k_2+k_3=n+4} \binom{n+4}{k_1,k_2,k_3} x_1^{k_1}x_2^{k_2}x_3^{k_3}. \quad (5.23)$$

Taking partial derivative against x_1 on both sides, we have

$$\frac{\partial}{\partial x_1}(x_1+x_2+x_3)^{n+4} = (n+4)(x_1+x_2+x_3)^{n+3} \quad (5.24)$$

$$\frac{\partial}{\partial x_1}\sum_{k_1+k_2+k_3=n+4} \binom{n+4}{k_1,k_2,k_3} x_1^{k_1}x_2^{k_2}x_3^{k_3} = \sum_{k_1+k_2+k_3=n+4} \binom{n+4}{k_1,k_2,k_3} x_1^{k_1-1}x_2^{k_2}x_3^{k_3}k_1. \quad (5.25)$$

Equating the two equations above and multiplying both sides by x_1, we have

$$(n+4)(x_1+x_2+x_3)^{n+3}x_1 = \sum_{k_1+k_2+k_3=n+4} \binom{n+4}{k_1,k_2,k_3} x_1^{k_1}x_2^{k_2}x_3^{k_3}k_1. \quad (5.26)$$

Taking partial derivative on both sides against x_1 again, we will have

$$\frac{\partial}{\partial x_1}(n+4)(x_1+x_2+x_3)^{n+3}x_1 = (n+4)\Big[(n+3)(x_1+x_2+x_3)^{n+2}x_1 + (x_1+x_2+x_3)^{n+3}\Big] \tag{5.27}$$

$$\frac{\partial}{\partial x_1}\sum_{k_1+k_2+k_3=n+4}\binom{n+4}{k_1,k_2,k_3}x_1^{k_1}x_2^{k_2}x_3^{k_3}k_1 = \sum_{k_1+k_2+k_3=n+4}\binom{n+4}{k_1,k_2,k_3}x_1^{k_1-1}x_2^{k_2}x_3^{k_3}k_1^2. \tag{5.28}$$

Equating the two equations above and multiplying both sides by x_1 we get

$$(n+4)\Big[(n+3)(x_1+x_2+x_3)^{n+2}x_1^2 + (x_1+x_2+x_3)^{n+3}x_1\Big] = \sum_{k_1+k_2+k_3=n+4}\binom{n+4}{k_1,k_2,k_3}x_1^{k_1}x_2^{k_2}x_3^{k_3}k_1^2. \tag{5.29}$$

Taking partial derivative on both sides against x_2 and x_3 we will have

$$\frac{\partial}{\partial x_2}\frac{\partial}{\partial x_3}(n+4)\Big[(n+3)(x_1+x_2+x_3)^{n+2}x_1^2 + (x_1+x_2+x_3)^{n+3}x_1\Big] = \\ = (n+4)(n+3)(n+2)\Big[(n+1)(x_1+x_2+x_3)^{n}x_1^2 + (x_1+x_2+x_3)^{n+1}x_1\Big], \tag{5.30}$$

$$\frac{\partial}{\partial x_2}\frac{\partial}{\partial x_3}\sum_{k_1+k_2+k_3=n+4}\binom{n+4}{k_1,k_2,k_3}x_1^{k_1}x_2^{k_2}x_3^{k_3}k_1^2 = \sum_{k_1+k_2+k_3=n+4}\binom{n+4}{k_1,k_2,k_3}x_1^{k_1}x_2^{k_2-1}x_3^{k_3-1}k_1^2k_2k_3. \tag{5.31}$$

Equating the two equations above and multiplying both sides by x_2 and x_3, we will get the formula

$$\sum_{k_1+k_2+k_3=n+4}\binom{n+4}{k_1,k_2,k_3}x_1^{k_1}x_2^{k_2}x_3^{k_3}k_1^2k_2k_3 = \\ (n+4)(n+3)(n+2)\Big[(n+1)(x_1+x_2+x_3)^{n}x_1^2x_2x_3 + (x_1+x_2+x_3)^{n+1}x_1x_2x_3\Big] \tag{5.32}$$

as we expected. ■

Proposition 5.2.4 *Let N be a positive integer,and x_1, x_2 be some real number, then*

$$\sum_{\substack{k,l,m\geq 0\\ k+l+m=N}} \binom{N}{k,l,m} x_1^k x_2^{l+m} = (2 \sum_{\substack{k>l>m\\ k+l+m=N}} +2 \sum_{\substack{l\geq k, l>m\\ k+l+m=N}} + \sum_{\substack{k\geq 0, l=m\\ k+l+m=N}}) \binom{N}{k,l,m} x_1^k x_2^{l+m}. \quad (5.33)$$

Proof By the Multinomial theorem (5.2.2), we have

$$(x_1 + x_2 + x_2)^N = \sum_{\substack{k,l,m\geq 0\\ k+l+m=N}} \binom{N}{k,l,m} x_1^k x_2^{l+m}. \quad (5.34)$$

Since $\binom{N}{k,l,m} = \binom{N}{k,m,l}$, when $l \neq m$, the partitions (k,l,m) and (k,m,l) will contribute same value to the sum. Hence we could rewrite the sum as

$$\sum_{\substack{k,l,m\geq 0\\ k+l+m=N}} \binom{N}{k,l,m} x_1^k x_2^{l+m} \quad (5.35)$$

$$=(2\sum_{k=0}^{N} \sum_{\substack{l>m\\ l+m=N-k}} +\sum_{k=0}^{N} \sum_{\substack{l=m\\ l+m=N-k}}) \binom{N}{k,l,m} x_1^k x_2^{l+m} \quad (5.36)$$

$$=(2 \sum_{\substack{k>l>m\\ k+l+m=N}} +2 \sum_{\substack{l\geq k, l>m\\ k+l+m=N}} + \sum_{\substack{k\geq 0, l=m\\ k+l+m=N}}) \binom{N}{k,l,m} x_1^k x_2^{l+m} \quad (5.37)$$

. ■

We introduced Proposition (5.2.4) because our strategy will be built on extending the sum $\sum_{\substack{k>l>m\\ k+l+m=N+3}}$ to the full trinomial expansion.

To further simplify the calculation, we need one corollary of Theorem (4.1.3).

Corollary 5.2.5 *For $d \geq 2$, let probabilities $\alpha_1, \alpha_2, \ldots \alpha_d \in (0,1)$, $\alpha_1 + \alpha_2 + \cdots + \alpha_d = 1$, $\alpha_d < \frac{1}{d}$ and indices $i_1 + I_2 + \cdots + i_d = N$ with special condition $i_d > i_j$ for all $j < d$, then*

$$\sum_{\substack{i_d > i_j\\ i_1+i_2+\cdots+i_d=N}} \binom{N}{i_1, i_2, \ldots, i_d} \prod_{k=1}^{d} \alpha_k^{i_k} \in O(e^{-N}) \text{ for large } N \quad (5.38)$$

.

Proof The first observation is that if $i_d > i_j$ for all $j < d$, then $i_d > \frac{N}{d}$,

The second observation is that $\sum_{\substack{i_d > i_j \\ i_1+i_2+\cdots+i_d=N}}$ can be relaxed to $\sum_{i_d=\frac{N}{d}+1}^{N} \sum_{\substack{i_1,i_2,\ldots,i_{d-1}\geq 0 \\ i_1+i_2+\cdots+i_{d-1}=N-i_d}}$, then we will have

$$\begin{aligned}
&\sum_{\substack{i_d > i_j \\ i_1+i_2+\cdots+i_d=N}} \binom{N}{i_1, i_2, \ldots, i_d} \prod_{k=1}^{d} \alpha_k^{i_k} \\
\leq &\sum_{i_d > \frac{N}{d}} \binom{N}{i_d} \alpha_d^{i_d} (1-\alpha_d)^{N-i_d} \sum_{i_1+i_2+\cdots+i_{d-1}=N-i_d} \binom{N-i_d}{i_1, i_2, \ldots, i_{d-1}} \frac{\alpha_1^{i_1} \ldots \alpha_{d-1}^{i_{d-1}}}{(1-\alpha_d)^{N-i_d}} \\
= &\sum_{i_d > \frac{N}{d}} \binom{N}{i_d} \alpha_d^{i_d} (1-\alpha_d)^{N-i_d}.
\end{aligned}$$

From the second step to the third step, we have used the Theorem (5.2.2) and reach a point where we can apply Theorem (4.1.3) as

$$\sum_{i_d > \frac{N}{d}} \binom{N}{i_d} \alpha_d^{i_d} (1-\alpha_d)^{N-i_d} \leq e^{-D(\frac{1}{d} \| \alpha_d) N} \in O(e^{-N}).$$

Hence,

$$\sum_{\substack{i_d > i_j \\ i_1+i_2+\cdots+i_d=N}} \binom{N}{i_1, i_2, \ldots, i_d} \prod_{k=1}^{d} \alpha_k^{i_k} \in O(e^{-N}) \tag{5.39}$$

as we expected. ∎

5.2.4 Analysis of the dominant part of $F_N^{(3)}$

We will analyze $F_{N,1}^{(3)}$ first by further splitting $F_{N,1}^{(3)}$. In order to do that, we need to split $\frac{(c+1)(b+c+2)(b+1)}{c(b+c+1)}$ in Equation (5.16) first by

$$\begin{aligned}
&\frac{(c+1)(b+c+2)(b+1)}{c(b+c+1)} \\
=&(1+\frac{1}{c})(1+\frac{1}{b+c+1})(b+1) \\
=&(b+1)+\Big(\frac{b+1}{c}+\frac{b+1}{b+c+1}+\frac{b+1}{c(b+c+1)}\Big).
\end{aligned}$$

Hence we could further split $F^{(3)}_{N,1}$ into two parts $S_{1,1}$ and $S_{1,2}$ where

$$\begin{aligned}
S_{1,1} =& \sum_{\lambda\vdash N} d^{(3)}_\lambda \frac{\alpha_2^N q^{\lambda_2+\lambda_3}}{(1-q)^3}[(b+1)-(b+1)q] \\
=& \sum_{\lambda\vdash N} d^{(3)}_\lambda \frac{\alpha_2^N q^{\lambda_2+\lambda_3}}{(1-q)^2}(b+1), \\
S_{1,2} =& -\sum_{\lambda\vdash N} d^{(3)}_\lambda \frac{\alpha_2^N q^{\lambda_2+\lambda_3}}{(1-q)^3}\Big[\frac{b+1}{c}+\frac{b+1}{b+c+1}+\frac{b+1}{c(b+c+1)}\Big].
\end{aligned}$$

Substituting the expression of $d^{(3)}_\lambda$ into $S_{1,1}$ and rewriting $b+1$ as $\lambda_2-\lambda_3+1$, we get

$$S_{1,1} = \sum_{\lambda\vdash N} \frac{\alpha_3^{\lambda_1+2}\alpha_1^{\lambda_2+\lambda_3}}{(\alpha_3-\alpha_1)^2}\frac{(\lambda_1-\lambda_2+1)(\lambda_2-\lambda_3+1)^2(\lambda_1-\lambda_3+2)}{(N+1)(N+2)(N+3)}\binom{N+3}{\lambda_1+2,\lambda_2+1,\lambda_3}. \tag{5.40}$$

To further simplify $S_{1,1}$ and all the following expressions, we will set $k=\lambda_1+2$, $l=\lambda_2+1$ and $m=\lambda_3$ and then

$$S_{1,1} = \frac{\sum_{k>l>m}^{k+l+m=N+3}\binom{N+3}{k,l,m}\alpha_3^k\alpha_1^{l+m}(k-l)(l-m)^2(k-m)}{(N+3)(N+2)(N+1)\alpha_1(\alpha_3-\alpha_1)^2}. \tag{5.41}$$

Now our strategy is to extend the sum in the expression of $S_{1,1}$ to include every term of the corresponding multinomial expansion and then bound the additional terms. We will use this strategy repeatedly in the following analysis.

Hence, by Proposition (5.2.4) we have

$$S_{1,1} = \frac{\Big[\frac{1}{2}\sum_{k,l,m}-\frac{1}{2}\sum_{l=m}-\sum_{l\geq k,l>m}\Big]\binom{N+3}{k,l,m}\alpha_3^k\alpha_1^{l+m}(k-l)(l-m)^2(k-m)}{(N+3)(N+2)(N+1)\alpha_1(\alpha_3-\alpha_1)^2}. \tag{5.42}$$

The terns in summations with indices $k=l$ or $l=m$ are cancelled because of the factor $(k-l)(l-m)$, so $S_{1,1}$ can be further simplified as

$$\begin{aligned}
S_{1,1} =& \frac{\frac{1}{2}\sum_{k,l,m}\binom{N+3}{k,l,m}\alpha_3^k\alpha_1^{l+m}(k-l)(l-m)^2(k-m)}{(N+3)(N+2)(N+1)\alpha_1(\alpha_3-\alpha_1)^2} && (5.43)\\
& -\frac{\sum_{l>k,l>m}\binom{N+3}{k,l,m}\alpha_3^k\alpha_1^{l+m}(k-l)(l-m)^2(k-m)}{(N+3)(N+2)(N+1)\alpha_1(\alpha_3-\alpha_1)^2} && (5.44)\\
=& 1-\Delta S_{1,1} && (5.45)
\end{aligned}$$

where

$$\Delta S_{1,1} = \frac{\sum_{l>k,l>m} \binom{N+3}{k,l,m} \alpha_3^k \alpha_1^{l+m} (k-l)(l-m)^2(k-m)}{(N+3)(N+2)(N+1)\alpha_1(\alpha_3-\alpha_1)^2} \tag{5.46}$$

and we used the fact that the dominant part of $S_{1,1}$ which is

$$S'_{1,1} = \frac{\sum_{k,l,m} \binom{N+3}{k,l,m} \alpha_3^k \alpha_1^{l+m} (k-l)(l-m)^2(k-m)}{2(N+3)(N+2)(N+1)\alpha_1(\alpha_3-\alpha_1)^2} = 1 \tag{5.47}$$

.

The calculation of $S'_{1,1}$ is as follows. First of all, we need to expand $(k-l)(l-m)^2(k-m)$ to get

$$\begin{aligned}&(k-l)(l-m)^2(k-m)\\ =&k^2l^2 - 2k^2lm + k^2m^2 - kl^3 + kl^2m + klm^2 - km^3 + l^3m - 2l^2m^2 + lm^3.\end{aligned}$$

Then we calculate the numerator of $S'_{1,1}$ by applying Proposition (5.2.3) and get the following:

$$\begin{aligned}&\sum_{k,l,m} \binom{N+3}{k,l,m} \alpha_3^k \alpha_1^{l+m} (k^2l^2 + k^2m^2 - 2m^2l^2)\\ &\qquad = 2(N+3)(N+2)(\alpha_3-\alpha_1)((N+1)N(\alpha_3+\alpha_1)\alpha_1^2 + (N+2)\alpha_1),\end{aligned} \tag{5.48}$$

$$\begin{aligned}&\sum_{k,l,m} \binom{N+3}{k,l,m} \alpha_3^k \alpha_1^{l+m} (-kl^3 - km^3 + l^3m + lm^3)\\ &\qquad = -2(N+3)(N+2)(\alpha_3-\alpha_1)((N+1)N\alpha_1^3 + 3(N+1)\alpha_1^2 + \alpha_1),\end{aligned} \tag{5.49}$$

$$\begin{aligned}&\sum_{k,l,m} \binom{N+3}{k,l,m} \alpha_3^k \alpha_1^{l+m} (-2k^2lm + kl^2m + klm^2)\\ &\qquad = -2(N+3)(N+2)(N+1)N(\alpha_3-\alpha_1)\alpha_3\alpha_1^2.\end{aligned} \tag{5.50}$$

Summing the three equations above, we can get $S'_{1,1} = \frac{N+1-p(N+1)}{(N+1)(\alpha_3-\alpha_1)} = 1$.

Then we will bound the value of $\Delta S_{1,1}$. A closer examine of the summation in the numerator of $\Delta S_{1,1}$ tells us that we could apply Corollary (5.2.5). Using the fact that $(k-l)(l-m)^2(k-m) < N^4$ and Corollary (5.2.5), we could conclude that

$$\Delta S_{1,1} < \frac{N^4 e^{-D(\frac{1}{3}\|\frac{p}{3})(N+3)}}{(N+3)(N+2)(N+1)\alpha_1(\alpha_3-\alpha_1)^2} \in O(Ne^{-N}). \tag{5.51}$$

Summing $S'_{1,1}$ and $\Delta S_{1,1}$, we see that

$$S_{1,1} = 1 - O(Ne^{-N}). \tag{5.52}$$

To complete the analysis of $F^{(3)}_{N,1}$, the last part is $S_{1,2}$ which contains the terms that should be subtracted from $F^{(3)}_{N,1}$. The expression for $S_{1,2}$ is

$$S_{1,2} = -\sum_{\lambda\vdash N} d^{(3)}_\lambda (b+1)(\frac{1}{c} + \frac{1}{b+c+1} + \frac{1}{c(b+c+1)})\frac{\alpha_3^{\lambda_1-1}\alpha_1^{\lambda_2+\lambda_3+1}}{(1-q)^3}. \tag{5.53}$$

We will multiply $d^{(3)}_\lambda$ with the fractional expressions and separate out the integral parts by

$$\begin{aligned}
\frac{d^{(3)}_\lambda}{c} &= \Big[(b+1)(b+c+2) + \frac{1}{c}(b+1)(b+c+2)\Big]\frac{\binom{N+3}{\lambda_1+2,\lambda_2+1,\lambda_3}}{(N+3)(N+2)(N+1)},\\
\frac{d^{(3)}_\lambda}{b+c+1} &= \Big[(b+1)(c+1) + \frac{(b+1)(c+1)}{b+c+1}\Big]\frac{\binom{N+3}{\lambda_1+2,\lambda_2+1,\lambda_3}}{(N+3)(N+2)(N+1)},\\
\frac{d^{(3)}_\lambda}{c(b+c+1)} &= \Big[b+1+\frac{b+1}{c} + \frac{b+1}{b+c+1} + \frac{b+1}{c(b+c+1)}\Big]\frac{\binom{N+3}{\lambda_1+2,\lambda_2+1,\lambda_3}}{(N+3)(N+2)(N+1)}.
\end{aligned}$$

Hence, we could simplify $|S_{1,2}|$ by

$$\begin{aligned}
|S_{1,2}| =& \sum_{\lambda\vdash N}(b+1)^2(b+c+2+c+1+1)\frac{\binom{N+3}{\lambda_1+2,\lambda_2+1,\lambda_3}\alpha_3^{\lambda_1-1}\alpha_1^{\lambda_2+\lambda_3+1}}{(1-q)^3(N+3)(N+2)(N+1)}\\
&+\sum_{\lambda\vdash N}(b+1)^2(\frac{b+c+3}{c} + \frac{c+2}{b+c+1} + \frac{1}{c(b+c+1)})\frac{\binom{N+3}{\lambda_1+2,\lambda_2+1,\lambda_3}\alpha_3^{\lambda_1-1}\alpha_1^{\lambda_2+\lambda_3+1}}{(N+3)(N+2)(N+1)(1-q)^3}.
\end{aligned}$$

Expressing it with $k = \lambda_1 + 2$,$l = \lambda_2 + 1$ and $m = \lambda_3$, we get

$$\begin{aligned}
|S_{1,2}| =& \frac{\sum_{k>l>m\geq 0,\ k+l+m=n+3}\binom{N+3}{k,l,m}\alpha_3^k\alpha_1^{N+3-k}(l-m)^2(2k+1-l-m)}{(N+3)(N+2)(N+1)(\alpha_3-\alpha_1)^3}\\
&+\frac{\sum_{k>l>m\geq 0,\ k+l+m=n+3}\binom{N+3}{k,l,m}\alpha_3^k\alpha_1^{N+3-k}(l-m)^2(\frac{k-m+1}{k-l-1} + \frac{k-l+1}{k-m-1} + \frac{1}{(k-l-1)(k-m-1)})}{(N+3)(N+2)(N+1)(\alpha_3-\alpha_1)^3}\\
=& S'_{1,2} + \Delta S_{1,2}
\end{aligned}$$

where $S'_{1,2}$ is the dominant term of $|S_{1,2}|$ and $\Delta S_{1,2}$ is the minor term.

We will evaluate $S'_{1,2}$ by applying Proposition (5.2.4) in the following way:

$$S'_{1,2} = \frac{\sum_{\substack{k>l>m\geq 0\\ k+l+m=n+3}} \binom{N+3}{k,l,m}\alpha_3^k\alpha_1^{N+3-k}(l-m)^2(2k+1-l-m)}{(N+3)(N+2)(N+1)(\alpha_3-\alpha_1)^3} \tag{5.54}$$

$$= \Big(\frac{1}{2}\sum_{\substack{k,l,m\geq 0\\ k+l+m=n+3}} - \frac{1}{2}\sum_{k\geq 0\ ,l=m} - \sum_{l\geq k\ ,l>m}\Big)\frac{\binom{N+3}{k,l,m}\alpha_3^k\alpha_1^{N+3-k}(l-m)^2(2k+1-l-m)}{(N+3)(N+2)(N+1)(\alpha_3-\alpha_1)^3} \tag{5.55}$$

$$= \Big(\frac{1}{2}\sum_{\substack{k,l,m\geq 0\\ k+l+m=n+3}} - \sum_{l>k\ ,l>m}\Big)\frac{\binom{N+3}{k,l,m}\alpha_3^k\alpha_1^{N+3-k}(l-m)^2(2k+1-l-m)}{(N+3)(N+2)(N+1)(\alpha_3-\alpha_1)^3} \tag{5.56}$$

$$= \frac{\alpha_1}{(N+1)(\alpha_3-\alpha_1)^2} - \sum_{l>k\ ,l>m}\frac{\binom{N+3}{k,l,m}\alpha_3^k\alpha_1^{N+3-k}(l-m)^2(2k+1-l-m)}{(N+3)(N+2)(N+1)(\alpha_3-\alpha_1)^3} \tag{5.57}$$

$$= \frac{\alpha_1}{(N+1)(\alpha_3-\alpha_1)^2} - O(e^{-N}). \tag{5.58}$$

Bounding $\sum_{l>k\ ,l>m}\frac{\binom{N+3}{k,l,m}\alpha_3^k\alpha_1^{N+3-k}(l-m)^2(2k+1-l-m)}{(N+3)(N+2)(N+1)(\alpha_3-\alpha_1)^3}$ is similar to bounding $\Delta S_{1,1}$, as it is also an application of Corollary (5.2.5). The result, which is

$$\frac{1}{2}\sum_{\substack{k,l,m\geq 0\\ k+l+m=n+3}}\frac{\binom{N+3}{k,l,m}\alpha_3^k\alpha_1^{N+3-k}(l-m)^2(2k+1-l-m)}{(N+3)(N+2)(N+1)(\alpha_3-\alpha_1)^3} = \frac{\alpha_1}{(N+1)(\alpha_3-\alpha_1)^2}, \tag{5.59}$$

is also derived from Proposition (5.2.3) and the calculation is similar to that of $S'_{1,1}$.

To finish the analysis of $F^{(3)}_{N,1}$, we need to bound $\Delta S_{1,2}$ where

$$\Delta S_{1,2} = \frac{\sum_{\substack{k>l>m\geq 0\\ k+l+m=n+3}} \binom{N+3}{k,l,m}\alpha_3^k\alpha_1^{N+3-k}(l-m)^2(\frac{k-m+1}{k-l-1}+\frac{k-l+1}{k-m-1}+\frac{1}{(k-l-1)(k-m-1)})}{(N+3)(N+2)(N+1)(\alpha_3-\alpha_1)^3}. \tag{5.60}$$

Since $k-m+1 > k-l-1$, we have $\frac{k-m+1}{k-l-1}+\frac{k-l+1}{k-m-1}+\frac{1}{(k-l-1)(k-m-1)} > 1$, Hence, we will have

$$\Delta S_{1,2} > \frac{\sum_{\substack{k>l>m\geq 0\\ k+l+m=n+3}} \binom{N+3}{k,l,m}\alpha_3^k\alpha_1^{N+3-k}(l-m)^2}{(N+3)(N+2)(N+1)(\alpha_3-\alpha_1)^3} \tag{5.61}$$

$$= \frac{\alpha_1}{(N+2)(N+1)(\alpha_3-\alpha_1)^3} - O(\frac{1}{N}e^{-N}). \tag{5.62}$$

The calculation is similar to that of $S_{1,1}$.

Now $F^{(3)}_{N,1}$ is fully analyzed and we could conclude that

$$F^{(3)}_{N,1} = S_{1,1} + S_{1,2} = 1 - \Delta S_{1,1} - S'_{1,2} - \Delta S_{1,2} \tag{5.63}$$

$$= 1 - \frac{\alpha_1}{(N+1)(\alpha_3 - \alpha_1)^2} + O(\frac{1}{N^2}). \tag{5.64}$$

5.2.5 Analysis of the minor part of $F^{(3)}_N$

The methods to bound $F^{(3)}_{N,2}$ and $F^{(3)}_{N,3}$ are very similar as we only need to show they are exponentially small. We can simplify $F^{(3)}_{N,2}$ as

$$\begin{aligned} F^{(3)}_{N,2} =& \sum_{\lambda \vdash N} d^{(3)}_\lambda \frac{\alpha_2^N q^{\lambda_2+\lambda_3}}{(1-q)^3} \frac{b+c+2}{c} q^{c+1} \\ =& \sum_{\substack{k>l>m\geq 0 \\ k+l+m=n+3}} d^{(3)}_\lambda \frac{k-m}{l-m-1} \frac{\alpha_3^{l+1}\alpha_1^{k+m-1}}{(\alpha_3-\alpha_1)^3} \\ =& \frac{\sum_{k>l>m} \binom{N+3}{k,l,m} \alpha_3^{l+1}\alpha_1^{k+m-1}(k-m)^2(k-l)(l-m)}{(l-m-1)(N+3)(N+2)(N+1)(\alpha_3-\alpha_1)^3}. \end{aligned}$$

Using the fact $\frac{(k-m)^2(k-l)(l-m)}{l-m-1} < N^3$ and Corollary (5.2.5), we will see that

$$F^{(3)}_{N,2} \in O(e^{-N}). \tag{5.65}$$

Similarly for $F^{(3)}_{N,3}$, we have that

$$\begin{aligned} F^{(3)}_{N,3} =& -\sum_{\lambda \vdash N} d^{(3)}_\lambda \frac{\alpha_2^N q^{\lambda_2+\lambda_3}}{(1-q)^3} \frac{c+1}{b+c+1} q^{b+c+2} \\ =& -\sum_{\substack{k>l>m\geq 0 \\ k+l+m=n+3}} d^{(3)}_\lambda \frac{k-l}{k-m-1} \frac{\alpha_3^{m+1}\alpha_1^{k+l-1}}{(\alpha_3-\alpha_1)^3} \\ =& -\frac{\sum_{k>l>m} \binom{N+3}{k,l,m} \alpha_3^{m+1}\alpha_1^{k+l-1}(k-m)(k-l)^2(l-m)}{(k-m-1)(N+3)(N+2)(N+1)(\alpha_3-\alpha_1)^3}. \end{aligned}$$

Using the fact $\frac{(k-m)(k-l)^2(l-m)}{k-m-1} < N^3$ and Corollary (5.2.5), we will see that

$$|F_{N,3}^{(3)}| \in O(e^{-N}). \tag{5.66}$$

Hence, as we expect, $F_{N,2}^{(3)}$ and $F_{N,3}^{(3)}$ are exponentially small. The average fidelity can be expressed as

$$F_N^{(3)} = 1 - \frac{\alpha_1}{(N+1)(\alpha_3 - \alpha_1)^2} + O(\frac{1}{N^2}) \tag{5.67}$$

and we can conclude that if we want to purify qutrit to ϵ-close to the original state, we need at least $\frac{\alpha_1}{\epsilon(\alpha_3-\alpha_1)^2}$ copies of the initial state. However, for the d-dimensional case, any achievable lower bound of the sample complexity of the purification problem is unknown.

To fully understand the optimal purification procedure, the first step is to solve the optimization problem formulated in Chapter 4. Maybe we could avoid explicit analysis of the average fidelity but upper bound the average fidelity achieved by the optimal procedure and then derive the achievable lower bound of the d-dimensional quantum state purification sample complexity.

References

[1] Milton Abramowitz and Irene A Stegun. Handbook of mathematical functions. *Applied mathematics series*, 55:62, 1966.

[2] Robert Alicki, Sl/awomir Rudnicki, and Sl/awomir Sadowski. Symmetry properties of product states for the system of N n-level atoms. *Journal of mathematical physics*, 29(5):1158–1162, 1988.

[3] Dave Bacon, Andrew M Childs, and Wim van Dam. From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS'05)*, pages 469–478. IEEE, 2005.

[4] Dave Bacon, Isaac L Chuang, and Aram W Harrow. The quantum Schur transform: I. efficient qudit circuits. *arXiv preprint quant-ph/0601001*, 2005.

[5] Charles H Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A Smolin, and William K Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Physical review letters*, 76(5):722, 1996.

[6] Harry Buhrman, Richard Cleve, John Watrous, and Ronald De Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001.

[7] Andrew M Childs, Aram W Harrow, and Paweł Wocjan. Weak Fourier-Schur sampling, the hidden subgroup problem, and the quantum collision problem. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 598–609. Springer, 2007.

[8] Andrew M Childs and Vedang Vyas. Note for spring 2014. Personal notes, 2014.

[9] JI Cirac, AK Ekert, and C Macchiavello. Optimal purification of single qubits. *Physical Review Letters*, 82(21):4344, 1999.

[10] Roe Goodman and Nolan R Wallach. *Representations and invariants of the classical groups*, volume 68. Cambridge University Press, 2000.

[11] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219. ACM, 1996.

[12] Jeongwan Haah, Aram W Harrow, Zhengfeng Ji, Xiaodi Wu, and Nengkun Yu. Sample-optimal tomography of quantum states. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing*, pages 913–925. ACM, 2016.

[13] Michael Keyl and Reinhard F Werner. Optimal cloning of pure states, testing single clones. *Journal of Mathematical Physics*, 40(7):3283–3299, 1999.

[14] Michael Keyl and Reinhard F Werner. Estimating the spectrum of a density operator. *Physical Review A*, 64(5):052311, 2001.

[15] Michael Keyl and Reinhard F Werner. The rate of optimal purification procedures. In *Annales Henri Poincare*, volume 2, pages 1–26. Springer, 2001.

[16] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[17] Maris Ozols. Purification. Personal notes, 2015.

[18] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):34, 2009.

[19] Oded Regev. The learning with errors problem. *Invited survey in CCC*, 2010.

[20] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484 – 1509, 1997.

[21] Daniel R Simon. On the power of quantum computation. *SIAM journal on computing*, 26(5):1474–1483, 1997.

[22] N.Ya. Vilenkin and A.U. Klimyk. *Representation of Lie Groups and Special Functions: Volume 3: Classical and Quantum Groups and Special Functions*, volume 75. Springer Science & Business Media, 2013.

[23] John Watrous. Theory of quantum information. 2011.