

Bachelor Thesis 2017

Optimized Fidelity Estimation in Purification for the Fastest Bootstrap of a Quantum Link

迅速な量子リンク作成のための純粋化におけるフィデリティ推定の最適化

Keio University, Faculty of Environment and Information Studies
Takafumi Oka

Optimized Fidelity Estimation in Purification for the Fastest Bootstrap of a Quantum Link

Quantum networking has increasingly become significant for a variety of its applications such as quantum key distribution (QKD). In quantum networking reliability of a connection depends on the quality of Bell pairs (a type of quantum state) used. When the fidelity is not sufficiently high, we need to conduct purification to increase the fidelity. However, determining the quality of a given Bell pair is by no means a trivial process. Nevertheless, literature established on quantum networking often presupposes the knowledge of the fidelity of the state in question without reference to actual means of state analysis. While existing quantum state tomography methods proposed in e.g. [1] could achieve the purpose, they are not designed to function in synchronization with nodes involved in the link, being redundant and inefficient when employed for operational link creation in quantum networking, and thus far from optimal for our purpose. The thesis will present an optimized configuration of state analysis and purification, tailored for our very situation, with a view toward the quickest possible link creation. Simulation of physical equipment, state analysis, and evaluation of the proposal are implemented in Python.

Keywords :

1. Quantum networking, 2. Quantum computing, 3. Quantum state tomography,

Keio University, Faculty of Environment and Information Studies

Takafumi Oka

Contents

1	Introduction	1
1.1	Background I: Importance of Quantum Information Technology	1
1.2	Background II: Challenges in Quantum Information Technology	1
1.3	Problem Definition	2
1.4	Research Contribution	2
1.5	Thesis structure	3
1.6	Notations and Symbols	3
2	Introduction to Quantum Information Technology	4
2.1	Quantum States and Their Representations	4
2.1.1	Quantum Bits	4
2.1.2	Density Matrix	6
2.1.3	Bloch Sphere	6
2.1.4	Fidelity	7
2.2	Operations on Quantum States	7
2.2.1	Measurements	7
2.2.2	Quantum Gates	9
2.3	Distributed Quantum States	11
2.3.1	Entanglement	11
2.3.2	Quantum Teleportation	12
2.3.3	Entanglement Swapping	14
2.4	Quantum Networking	15
2.4.1	Purification	15
2.4.2	Quantum Networks	17
2.4.3	Quantum Link	18
2.5	Quantum State Tomography	19
2.5.1	Maximum Likelihood Technique	22
2.5.2	Error Estimation	23
3	Ideas and Designs	24
3.1	Key Ideas	24
3.2	Design of the Protocol for Creating a Link	24
3.3	Design of the Optimized Fidelity Estimation	28

4	Implementation	32
4.1	Structure of the Simulator	32
4.2	God Channel Module	33
4.2.1	Implementation of Quantum States Representations	33
4.2.2	Implementation of CNOT Gate with Errors	33
4.3	Tomography Module	35
4.4	Simulator Module	35
5	Evaluation	37
5.1	Criteria for Evaluation	37
5.2	Evaluation for Full State Tomography	37
5.2.1	Behavior of Actual Fidelities with Purifications	38
5.2.2	Behavior of Reconstruction Fidelities with Purifications	41
5.3	Evaluation for the Proposed Fidelity Estimation	42
6	Conclusion	47
6.1	State Reconstruction	47
6.2	Purification	47
6.3	Proposed Method for Fidelity Estimation	48
6.4	Future Work	48
	Acknowledgements	49

List of Figures

2.1	Representation of a qubit on the Bloch sphere: every 1-qubit state can be drawn as a point on the surface of the sphere, providing visually perceptible representation.	7
2.2	List of diagram symbols for X, Y, Z, Hadamard, and CNOT gates: these will be frequently used throughout the thesis.	10
2.3	Symbol for the measurement operator in Z axis (the left symbol stands for the right one unless otherwise noted), corresponding to the measurement by the operators M_0 and M_1 (in the notation of 2.2.1).	10
2.4	Symbol for the measurement operator in X axis, corresponding to the measurement by the operators $M_{ 0\rangle+ 1\rangle/\sqrt{2}}$ and $M_{ 0\rangle- 1\rangle/\sqrt{2}}$	11
2.5	Symbol for the measurement operator in Y axis, corresponding to the measurement by the operators $M_{ 0\rangle+i 1\rangle/\sqrt{2}}$ and $M_{ 0\rangle-i 1\rangle/\sqrt{2}}$	11
2.6	A Bell pair, with two photons entangled: measurements of one photon affects measurements of the other. Local operations on one photon immediately affects the other at a distant location!	12
2.7	Circuit diagram of quantum teleportation: Bob applies his operation depending on the measurement result at Alice.	12
2.8	Circuit diagram of entanglement swapping	14
2.9	Entanglement swapping: initial state. Node 1 and 2 share one entangled photon pairs, and Node 2 and 3 also share another entangled photon pair, with two photons in total at Node 2.	14
2.10	Entanglement swapping: teleporting the state of one particle of Node 2 to Node 3 using the same procedure as quantum teleportation.	15
2.11	Entanglement swapping: the particle at Node 1 is now entangled to the particle at Node 3, resulting in a longer entanglement.	15
2.12	Extended purification circuit: now capable of suppressing both bit flip and phase flip errors.	17
2.13	Multiple rounds of purification, increasing the fidelity still further after each round.	17
2.14	A scheme of two nodes sharing an entangled photon pair: the photon 1 and 2 constitute the entanglement, both having been emitted by the Entangle Photon Pair Sender in the middle.	18
2.15	A quantum link with Node Controllers: the Controllers are responsible for making operational decisions such as choosing measurement bases and fidelity assessment of states, involving state estimation methods.	19

2.16	Fidelity and the process of state reconstruction in tomography: looking at the state from different angles enables reconstruction of the state . .	20
2.17	Measurement bases and their respective points on the Bloch sphere: measurements with respect to these bases “project” a given state to their respective points on the sphere probabilistically.	21
2.18	State tomography for 1-qubit: the actual fidelity is between the ideal state and the actual state (the latter of which cannot be seen) and the reconstruction fidelity is between the state reconstructed by the maximum likelihood (see Section 2.5.1) and a set of states generated by the error estimation routine (see Section 2.5.2), representing accuracy of the reconstruction.	21
3.1	Flowchart at Node 1 in the distributed model: both Node 1 and 2 conduct tomography concurrently, exchanging each other’s reconstructed density matrices.	26
3.2	Flowchart at Node 1 in the master-slave model: only Node 1 conducts tomography and is responsible for choosing measurement bases and state reconstruction.	27
3.3	Flowchart at Node 2 in the master-slave model: Node 2 receives the tomography result and follows the decision of Node 1 regarding whether to proceed for applications.	27
3.4	Flowchart of the bootstrap procedure of a quantum link: the number of purifications increases until leading to the state being of a sufficient fidelity.	28
3.5	Circuit diagram to realize the proposed fidelity estimation method: ρ ’s are four identical initial Bell pairs of which we estimate the fidelity. . .	29
4.1	Software Architecture of the whole program: the modules are separated by their respective roles.	33
5.1	Relationship between Actual Fidelity and Reconstruction Fidelity based on actual experimental data provided by Kwiat et. al., with no purification conducted.	38
5.2	Diagram of two types of fidelities: the blue and orange arrows correspond to the arrows of their respective color in subsequent graphs	39
5.3	Relations between the actual fidelity and the number of purifications with no gate errors: the fidelity smoothly approaches to 1.	40
5.4	Relations between the actual fidelity and the number of purifications with CNOT gate errors present: the fidelity stagnates between 0.8 and 0.9.	40
5.5	Relations between the reconstruction fidelity and the number of purifications with no gate errors: the reconstruction fidelity increases as the actual fidelity increases	41
5.6	Relations between the reconstruction fidelity and the number of purifications with CNOT gate errors present: the reconstruction fidelity also fluctuates as the actual fidelity does.	42

5.7	The state reconstruction performance for $\rho = 0.7 \Phi^+\rangle \langle \Phi^+ + 0.1 \Psi^+\rangle \langle \Psi^+ + 0.1 \Psi^-\rangle \langle \Psi^- + 0.1 \Phi^-\rangle \langle \Phi^- $ with full state tomography employed. . .	43
5.8	The state reconstruction performance for $\rho = 0.7 \Phi^+\rangle \langle \Phi^+ + 0.1 \Psi^+\rangle \langle \Psi^+ + 0.1 \Psi^-\rangle \langle \Psi^- + 0.1 \Phi^-\rangle \langle \Phi^- $ with full state tomography employed. The scale of the vertical axis is adjusted to focus on the reconstruction fidelity. 43	
5.9	The state reconstruction performance for $\rho = 0.7 \Phi^+\rangle \langle \Phi^+ + 0.1 \Psi^+\rangle \langle \Psi^+ + 0.1 \Psi^-\rangle \langle \Psi^- + 0.1 \Phi^-\rangle \langle \Phi^- $ with the proposed method employed. The solid line represents the data of the proposed method, while the dotted line correspond to the data of full state tomography.	44
5.10	The variance of the actual fidelities for $\rho = 0.7 \Phi^+\rangle \langle \Phi^+ + 0.1 \Psi^+\rangle \langle \Psi^+ + 0.1 \Psi^-\rangle \langle \Psi^- + 0.1 \Phi^-\rangle \langle \Phi^- $ with the proposed method employed. The red line indicates the actual fidelities estimated using the proposed method, and the black line those from full state tomography. The proposed method has an obvious advantage of less fluctuation, compensating for a slight deterioration in the reconstruction fidelity.	45
5.11	The variance of the reconstruction fidelities for $\rho = 0.7 \Phi^+\rangle \langle \Phi^+ + 0.1 \Psi^+\rangle \langle \Psi^+ + 0.1 \Psi^-\rangle \langle \Psi^- + 0.1 \Phi^-\rangle \langle \Phi^- $ with the proposed method employed. The red line indicates the reconstruction fidelities estimated using the proposed method, and the black line those from full state tomography. A slight deterioration in the reconstruction fidelity is much smaller than the large fluctuation of the actual fidelities present while using full state tomography, and hence compensated for.	46

List of Tables

1.1	Notations and Symbols	3
2.1	Correspondence between Alice's measurement outcomes and Bob's state at the time Alice obtained each outcome	13
2.2	Possible combinations of the states Alice and Bob have when only bit flip errors occur: when the first and last cases occur the round of purification is considered successful, while the second and third cases lead to failure of the round.	16
3.1	Possible measurement outcomes at the measurement setting 1 and their respective probabilities in terms of the coefficients of ρ	30
3.2	Possible measurement outcomes at the measurement setting 2 and their respective probabilities in terms of the coefficients of ρ	30
3.3	Possible measurement outcomes at the measurement setting 3 and their respective probabilities in terms of the coefficients of ρ	31

Chapter 1

Introduction

1.1 Background I: Importance of Quantum Information Technology

Quantum information technology is known for its great potential in realizing things that are not feasible in classical information technology. Quantum computing, for instance, features surprising algorithms such as Shor's algorithm that enables computing factorization of a number to prime numbers in polynomial time [2]. Quantum networking also has a wide range of applications; one of the most practically beneficial is *quantum key distribution*, or *QKD*, which enables more secure key distribution compared to classical [3]. In fact, the so-called E91 protocol [4] of QKD utilizes *entanglement* (see Section 2.3.1). Another interesting application of quantum networking utilizes distributed quantum states such as *Bell states* or *GHZ states* to realize decision-making among multiple nodes with essentially fewer steps of communication [5]. Furthermore, algorithms and schemes that make use of distributed quantum computing are proposed (e.g. [6]). *Quantum repeaters* are nodes that hold distributed quantum states, that are capable of applying certain operations to the states, and that are responsible for maintaining consistency in conjunction with other nodes for the involved nodes to function as a whole (as explained in Chapter 2.)

1.2 Background II: Challenges in Quantum Information Technology

All these applications have one vital requirement in common: delivery of and operation to entangled quantum states, with as small noises and loss to the states as possible. It should first be noted that precise operation to quantum states is prohibitively difficult as opposed to operation to classical bits (some of the examples of an actual experiment are done in e.g. [7, 8], which tell how large the obstacles are). In addition, another difficulty appears in an attempt to assess how well such delivery and operation has been done. This is attributed to the property of quantum states that a quantum state initiates a probabilistic collapse when measured, unlike classical bits, thereby requiring a myriad of measurements to reconstruct a given state, resorting to both analytical

and statistical reconstruction processes (called *quantum state tomography*, which will be introduced in Chapter 2). In particular, for quantum networking, we need to manage delivery and operation of resources (i.e. entangled states) in a real-time fashion.

This research project is intended to serve as an aid to solve the latter of those two challenges.

1.3 Problem Definition

It is worthwhile to devise a new method of state estimation that is particularly tailored for our quantum networking purpose. In order for the proposed method to be “tailored” it needs to meet the following two requirements: that it keeps consistency with other nodes’ estimations that run concurrently and that the state estimation finishes rapidly enough to be used for bootstrapping a network. The former problem has been dealt with in the workshop paper [9], which proposes a master-slave protocol that supports two nodes about to initiate a quantum communication, with full state tomography embedded as a state estimation method.

This thesis addresses the latter problem and aims to propose an optimized state estimation method that can substitute for full state tomography. The evaluation of the proposed method will be based on the amount of time that it takes for two nodes to become ready for proceeding to further applications (e.g. QKD). Because the most time-consuming step involved is repeated generation, transmission, and measurement of Bell states, shortening the amount of time requires fewer generations of Bell pairs, hence in turn demanding a state analysis method of sufficient accuracy with fewer measurement results.

Of course generation of Bell states, latency of transmission, and measurement efficiency depend upon particular equipment, and assumptions have to be made to evaluate proposals.

1.4 Research Contribution

Upon completion of this research scholars will be able to adopt the proposed method for state analysis and to utilize quantitative data provided in the thesis to anticipate resource consumptions they need to allow for in an attempt to create a link. Furthermore, by combining the proposed protocol to support distributed state estimation, they will be able to sketch a model that they want to realize in reality, with the level of concreteness enough to calculate an amount of bootstrap time and latency caused during the course of bootstrap, provided the error rate in gates and Bell state initial fidelities (that depend on particular physical apparatus) are available. This set of information becomes particularly significant once applications former quantum networking (e.g. QKD) have been launched for practical use, where fidelity of the Bell pairs used dictate the applications’ proper function.

1.5 Thesis structure

Chapter 2 presents a concise introduction to quantum information technology with particular emphasis put on the knowledge of frequent use in this thesis. It is divided into five sections: Quantum States and Their Representations, Operations on Quantum States, Distributed Quantum States, Quantum Networking, and Quantum State Tomography. The Chapter is organized so as to move from local notions regarding quantum bits to global concepts used in conjunction with quantum states at distant locations.

Chapter 3 introduces several underpinning ideas and designs essential in this project, namely: a protocol that supports *distributed* state estimation and an optimized fidelity estimation method that is tailored for quantum networking.

Chapter 4 presents how the simulator used in this project works and how it is organized. It briefly lists the consisting modules and their respective roles, then picks major functions from each of the modules, with detailed explanation provided.

Chapter 5 presents the results obtained from the simulator. It first shows how state reconstruction looks like based on actual tomography and experimental data. Then the relations between the number of purifications and the actual resultant fidelity are presented both in the case some errors are embraced and the case where there is no error. Finally, the evaluation of performance of the proposed fidelity estimation is presented in context of comparison to full state tomography.

Chapter 6 sums up the evaluations in Chapter 5, and yields conclusions that we have drawn from the research. Outlooks for future work will also be in Chapter 6.

1.6 Notations and Symbols

\mathbb{R}	The set of real numbers
\mathbb{C}	The set of complex numbers
X^n	The Cartesian product of n of X 's as sets
$M_n(\mathbb{R})[M_n(\mathbb{C})]$	The set of n -by- n matrices whose entries are in \mathbb{R} (or in \mathbb{C} , respectively).
$ \psi\rangle$	Arbitrary pure quantum state in Dirac's ket notation (i.e. $ \psi\rangle \in \mathbb{C}^{2^n}$ for some n)
ρ	Pure or mixed quantum state in density matrix form (i.e. $\rho \in M_{2^n}(\mathbb{C})$ for some n)

Table 1.1: Notations and Symbols

Notations and symbols used throughout the thesis are summarized in Table 1.1.

Chapter 2

Introduction to Quantum Information Technology

This chapter is a concise presentation of preliminary knowledge necessary to understand this research.

2.1 Quantum States and Their Representations

2.1.1 Quantum Bits

A *quantum bit* (henceforth *qubit*) is represented by a minimum unit of particles — atoms, electrons, or photons — to serve as the most fundamental computational unit in quantum information technology just as *classical* bits, each being 0 or 1 do, in classical computers. The essential difference of qubits lies in the fact that the particle involved can be in *superposition*: it holds two distinct states until measured, when it collapses into one of the two states probabilistically. We utilize this property of qubits for further applications.

One representation of a qubit is in the form of *state vector*, wherein the qubit $|\psi\rangle$ is written as follows:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad (2.1.1.1)$$

where α and β are complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$ and $|0\rangle$ and $|1\rangle$ are defined to be the basis vectors

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (2.1.1.2)$$

These $|0\rangle$ and $|1\rangle$ correspond to the two distinct states in superposition. The $|\psi\rangle$ collapses into $|0\rangle$ with probability $|\alpha|^2$ and into $|1\rangle$ with probability $|\beta|^2$.

More generally, when n qubits are available, n sets of each two distinct states in superposition form 2^n possible combinations, represented by the equation

$$|\psi'\rangle = \alpha_0 |00 \dots 0\rangle + \alpha_1 |00 \dots 1\rangle + \dots + \alpha_{2^n-1} |11 \dots 1\rangle \quad (2.1.1.3)$$

where each α_i is a complex number, $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$ and $|k_1 k_2 \dots k_n\rangle$ (each k_i is either 0 or 1) is the standard unit vector whose m -th component is 1 and other components are 0 where $m = \sum_{i=0}^n 2^i k_i$, the decimal representation of the binary digit $k_1 k_2 \dots k_n$.

This $|\rangle$ notation is called *Dirac's ket notation* [5]. For each $|\psi\rangle$, $\langle\psi|$ is defined to be the transpose with complex conjugate taken for each entry: if

$$|\psi\rangle = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}, \quad (2.1.1.4)$$

then $\langle\psi|$ is defined to be

$$\langle\psi| = (\overline{c_1} \quad \dots \quad \overline{c_n}). \quad (2.1.1.5)$$

where $\overline{c_i}$ is the complex conjugate of c_i .

We define a few operations for state vectors in Dirac's notation. Let

$$|\psi_1\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \quad (2.1.1.6)$$

and

$$|\psi_2\rangle = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}. \quad (2.1.1.7)$$

Then the *outer product* of $|\psi_1\rangle$ and $|\psi_2\rangle$, $|\psi_1\rangle \langle\psi_2|$, is defined to be [5]

$$|\psi_1\rangle \langle\psi_2| \equiv \begin{pmatrix} a_1 \overline{b_1} & a_1 \overline{b_2} & \dots & a_1 \overline{b_n} \\ \vdots & \ddots & \dots & \vdots \\ a_n \overline{b_1} & a_n \overline{b_2} & \dots & a_n \overline{b_n} \end{pmatrix}; \quad (2.1.1.8)$$

the *tensor product* of $|\psi_1\rangle$ and $|\psi_2\rangle$ is

$$|\psi_1\rangle \otimes |\psi_2\rangle \equiv \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ \vdots \\ a_1 b_n \\ a_2 b_1 \\ a_2 b_2 \\ \vdots \\ a_2 b_n \\ \vdots \\ a_n b_1 \\ a_n b_2 \\ \vdots \\ a_n b_n \end{pmatrix}; \quad (2.1.1.9)$$

and the *inner product* of $|\psi_1\rangle$ and $|\psi_2\rangle$ is

$$\langle\psi_1|\psi_2\rangle \equiv \sum_{i=1}^n \overline{a_i} b_i. \quad (2.1.1.10)$$

As is done in usual linear algebra, it is possible to consider *change of basis* for state vectors. In fact, the basis set $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$ is called *computational basis*, one of the most frequently used basis set for 1-qubit states. Another basis set of as frequent use is called *Bell basis*, which consists of $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, and $|\Psi^-\rangle$; for the formal definition of these four states, see Section 2.3.1.

2.1.2 Density Matrix

A *density matrix* is another representation of a quantum state. When a state is part of a larger system and cannot be described as a superposition of known pure states that lie inside the system, the state is said to be *mixed* and expressed as a linear sum of pure states that we *do* know lie within the system, with a classical probability multiplied to each pure state in the sum. Density matrices are used to represent such states. To make the formal definition, let $\{p_i\}$ be the set of classical probabilities and let the state be a combination $\sum_i p_i |\psi_i\rangle$. The density matrix representing this state is defined to be

$$\rho \equiv \sum_i p_i |\psi_i\rangle \langle \psi_i|. \quad (2.1.2.1)$$

Note that, when there are n qubits, each $|\psi_i\rangle$ is a 2^n -dimensional complex vector and thus $|\psi_i\rangle \langle \psi_i|$ is a $2^n \times 2^n$ -complex matrix. In particular, when 1 is the only element in $\{p_i\}$, the ρ is just $|\psi\rangle \langle \psi|$ and represents nothing but a pure state. Because we do not know the whole system (which is ultimately the universe) that surrounds us and the state of interest, every quantum state we face in reality needs to be represented as a density matrix.

2.1.3 Bloch Sphere

A visually useful representation for 1-qubit states is the *Bloch sphere*. Let us represent the state $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ in this sphere. Rewriting $|\psi\rangle$ as

$$|\psi\rangle = \exp(i\theta)(|\alpha| |0\rangle + \exp(-i\theta)\beta |1\rangle) \quad (2.1.3.1)$$

where $\alpha = \exp(i\theta)|\alpha|$, and thanks to the fact that we may ignore *global phase* in measurement — a complex number of absolute value 1 multiplied to $|\psi\rangle$ — that does not affect measurement outcomes, we may assume that

$$|\psi\rangle = |\alpha| |0\rangle + \exp(-i\theta)\beta |1\rangle. \quad (2.1.3.2)$$

Using the identity $|\alpha|^2 + |\beta|^2 = 1$, the equation above can be written as

$$|\psi\rangle = \cos \varphi_1 + \exp(i\varphi_2) \sin \varphi_1 \quad (2.1.3.3)$$

where $\cos \varphi_1 = |\alpha|$, $\varphi_2 = \arg(\beta) - \theta$, $\arg(\beta)$ is the angle at which β lies with respect to the x -axis in the complex plane. This one-to-one correspondence between 1-qubit state vectors and points on the surface of the unit sphere allows us to depict a given 1-qubit state on the sphere as in Figure 2.1.

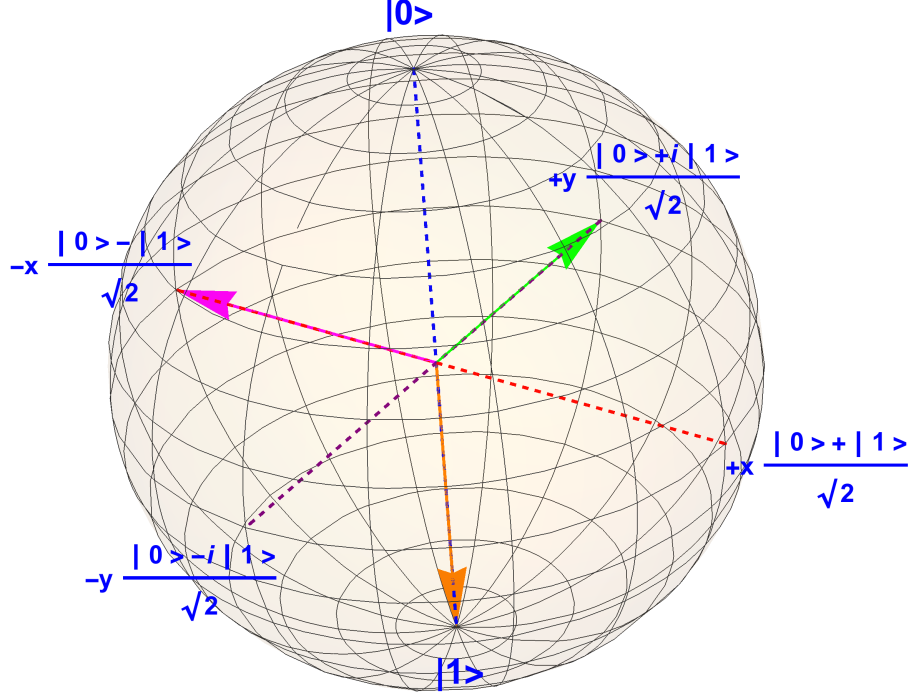


Figure 2.1: Representation of a qubit on the Bloch sphere: every 1-qubit state can be drawn as a point on the surface of the sphere, providing visually perceptible representation.

2.1.4 Fidelity

We introduce one of the quantities of frequent use in further chapters. *Fidelity* is a quantity that derives from given two mixed states, ranging from 0 to 1, and represents “similarity” between the states. More precisely, given density matrices ρ_1 and ρ_2 , the fidelity between them is defined to be [1]

$$F(\rho_1, \rho_2) \equiv \left\{ \text{Tr} \left(\sqrt{\sqrt{\rho_1} \rho_2 \sqrt{\rho_1}} \right) \right\}^2. \quad (2.1.4.1)$$

2.2 Operations on Quantum States

2.2.1 Measurements

As mentioned in Section 2.1.1, qubits collapse into either 0 or 1 probabilistically. This collapse is invoked by *measurement*. An operation of measurement to a quantum state is, in mathematical terms, defined to be a linear transformation called a *measurement operator*. We can thus regard each measurement operator as a matrix that transforms the state vector into another. We need to choose a *measurement basis* to conduct measurement. For 1-qubit measurement, we may choose any 1-qubit state vector for a

measurement basis, and the corresponding measurement operator M_ψ is defined to be

$$M_\psi \equiv |\psi\rangle \langle\psi| \quad (2.2.1.1)$$

with the choice of basis $|\psi\rangle$. The probability of measuring the outcome $|\psi\rangle$ is then defined to be

$$p_\psi \equiv \langle\psi| M_\psi^* M_\psi |\psi\rangle. \quad (2.2.1.2)$$

where M_ψ^* is defined to be the conjugate transpose of M_ψ . The preceding illustration of "probabilistic collapse" of $|\psi\rangle$ made in Section 2.1.1 is precisely the measurement operation with basis $|0\rangle$ and $|1\rangle$. In fact, following the definitions, the corresponding measurement operators become

$$M_0 = |0\rangle \langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad (2.2.1.3)$$

and

$$M_1 = |1\rangle \langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \quad (2.2.1.4)$$

In this setting, we measure 0 in probability $\langle 0| M_0^* M_0 |0\rangle$ and 1 in $\langle 0| M_0^* M_0 |0\rangle$. An easy calculation will show they are equal to $|\alpha|^2$ and $|\beta|^2$, respectively.

Another important notion is *orthogonality*. Two state vectors $|\psi\rangle$ and $|\varphi\rangle$ are said to be *orthogonal* if the relation

$$\langle\psi|\varphi\rangle = 0 \quad (2.2.1.5)$$

holds. Consider an arbitrary 1-qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Since we have the identity $|\alpha|^2 + |\beta|^2 = 1$, the probability of measuring 0 for $|\psi\rangle$ is the complementary event of measuring 1. In fact, for any *orthonormal* basis $\{|v_1\rangle, |v_2\rangle\}$, which is, for any basis set whose elements are of norm 1 and orthogonal, we can write $|\psi\rangle = \alpha'|v_1\rangle + \beta'|v_2\rangle$ with some suitable $\alpha' \in \mathbb{C}$ and $\beta' \in \mathbb{C}$, and the relation

$$|\alpha'|^2 + |\beta'|^2 = 1 \quad (2.2.1.6)$$

still holds, for any basis transformation between orthonormal bases preserves the norm.

More generally, for any n -qubit states, there always exist 2^n vectors, v_0, \dots, v_{2^n-1} in \mathbb{C}^{2^n} , such that any two of them are orthogonal and they are all of norm 1. For an n -qubit state $|\psi\rangle$, the analogous relation

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1 \quad (2.2.1.7)$$

holds where $|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$, where $|i\rangle$ are the orthonormal basis for \mathbb{C}^{2^n} . Because of the orthogonality, theoretically we need only $2^n - 1$ probabilities to represent the state $|\psi\rangle$. The notion of orthogonality will be necessary in Chapter 4.

2.2.2 Quantum Gates

In quantum computing we have an analogous notion for circuits in classical computing, *quantum circuits*, where a set of quantum states pass through *quantum gates*, being transformed by effects of the gates, until they are finally measured to yield outcomes.

Given that state vectors are complex vectors of norm 1, complex matrices that preserve norms, namely *unitary matrices*¹, transform state vectors to state vectors. Therefore it is natural to consider quantum gates that are unitary transformations.

The quantum gate of most frequent use throughout this research is *Controlled-not gate*, or *CNOT gate*. CNOT gate takes two qubits, the first qubit being called *control qubit* and the second *target qubit*. Let the control qubit and the target qubit be expressed as

$$|\psi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle \quad (2.2.2.1)$$

and

$$|\psi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle, \quad (2.2.2.2)$$

respectively. Then the two qubit state is written as

$$\begin{aligned} |\psi\rangle &= |\psi_1\rangle |\psi_2\rangle \\ &= \alpha_1 \alpha_2 |00\rangle + \alpha_1 \beta_2 |01\rangle + \beta_1 \alpha_2 |10\rangle + \beta_1 \beta_2 |11\rangle. \end{aligned}$$

The CNOT gate exchanges the two terms of first qubit 1 in $|\psi\rangle$ each other:

$$\begin{aligned} &\alpha_1 \alpha_2 |00\rangle + \alpha_1 \beta_2 |01\rangle + \beta_1 \alpha_2 |10\rangle + \beta_1 \beta_2 |11\rangle \\ \xrightarrow{CNOT} &\alpha_1 \alpha_2 |00\rangle + \alpha_1 \beta_2 |01\rangle + \beta_1 \alpha_2 |11\rangle + \beta_1 \beta_2 |10\rangle. \end{aligned}$$

Recalling that the states above are vectors in \mathbb{C}^4 (see Section 2.1.1 in this Chapter), this operation is clearly a linear transformation of \mathbb{C}^4 and thus written in matrix form as

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \quad (2.2.2.3)$$

We will see in a subsequent section that this CNOT gate plays an essential role in a procedure called *purification*.

Hadamard gate is another gate for 1-qubit states that is used in *quantum teleportation*, and in turn, *entanglement swapping*, which will be formally introduced in Section 2.3.2 and 2.3.3, respectively. This gate takes $|0\rangle$ to $(|0\rangle + |1\rangle)/\sqrt{2}$, and $|1\rangle$ to $(|0\rangle - |1\rangle)/\sqrt{2}$; in matrix form it is expressed as [5]

$$Hadamard = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (2.2.2.4)$$

Other 1-qubit gates of as frequent use are *X gate*, *Y gate*, and *Z gate*. These are defined as the following [5]:

¹There are several equivalent definitions for unitary matrices, one of which is the one used here, to require the matrix preserve the norm of any vector being transformed.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad (2.2.2.5)$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad (2.2.2.6)$$

and

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (2.2.2.7)$$

These basic gates have commonly used symbols for circuit diagrams as in Figure 2.2.

$$\begin{aligned} \text{---} \boxed{\text{X}} \text{---} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \text{---} \bullet \text{---} \bigoplus \text{---} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\ \text{---} \boxed{\text{Y}} \text{---} &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ \text{---} \boxed{\text{Z}} \text{---} &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ \text{---} \boxed{\text{H}} \text{---} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{aligned}$$

Figure 2.2: List of diagram symbols for X, Y, Z, Hadamard, and CNOT gates: these will be frequently used throughout the thesis.

In addition, measurement operators (with respect to Z, X, and Y axes) are also represented by similar symbols as illustrated in Figure 2.3, 2.4, and 2.5. These symbols will repeatedly appear in the rest of the thesis.

$$\text{---} \boxed{\text{Measurement}} \text{---} \quad \left(= \boxed{\text{Measurement}_Z} \right)$$

Figure 2.3: Symbol for the measurement operator in Z axis (the left symbol stands for the right one unless otherwise noted), corresponding to the measurement by the operators M_0 and M_1 (in the notation of 2.2.1).

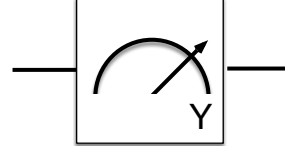
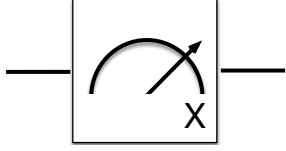


Figure 2.4: Symbol for the measurement operator in X axis, corresponding to the measurement by the operators $M_{|0\rangle+|1\rangle/\sqrt{2}}$ and $M_{|0\rangle-|1\rangle/\sqrt{2}}$. Figure 2.5: Symbol for the measurement operator in Y axis, corresponding to the measurement by the operators $M_{|0\rangle+i|1\rangle/\sqrt{2}}$ and $M_{|0\rangle-i|1\rangle/\sqrt{2}}$.

2.3 Distributed Quantum States

2.3.1 Entanglement

Entanglement refers to a state of superposition of more than one particle such that the outcome of measurement of one qubit is dependent on the outcome of the measurement of another qubit. For example, let

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (2.3.1.1)$$

Observe that measuring 0 (or 1) for the first qubit immediately gives the knowledge of the outcome of the second qubit, 0 (or 1, respectively), *without actually measuring the second one*. This is an example of entanglement of quantum states.

One of the most frequently used type of entangled states in quantum networking is *EPR pairs*, or *Bell pairs*. They are 2-qubit states of one of the forms

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad (2.3.1.2)$$

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \quad (2.3.1.3)$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad (2.3.1.4)$$

and

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \quad (2.3.1.5)$$

All these four are called Bell pairs. Figure 2.6 conceptually illustrates this.

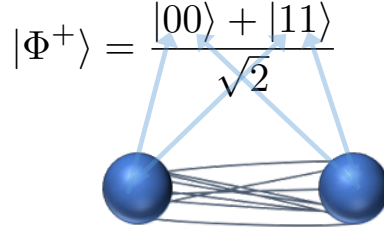


Figure 2.6: A Bell pair, with two photons entangled: measurements of one photon affects measurements of the other. Local operations on one photon immediately affects the other at a distant location!

2.3.2 Quantum Teleportation

Quantum teleportation [10] exemplifies how entanglement can be practically useful. Briefly speaking, a set of local operations² to an entangled state as well as to a given state $|\psi\rangle$, enable “teleportation” of the state $|\psi\rangle$. We explain how a qubit is teleported using an entangled state. The whole procedure of quantum teleportation is drawn in circuit form in Figure 2.7.

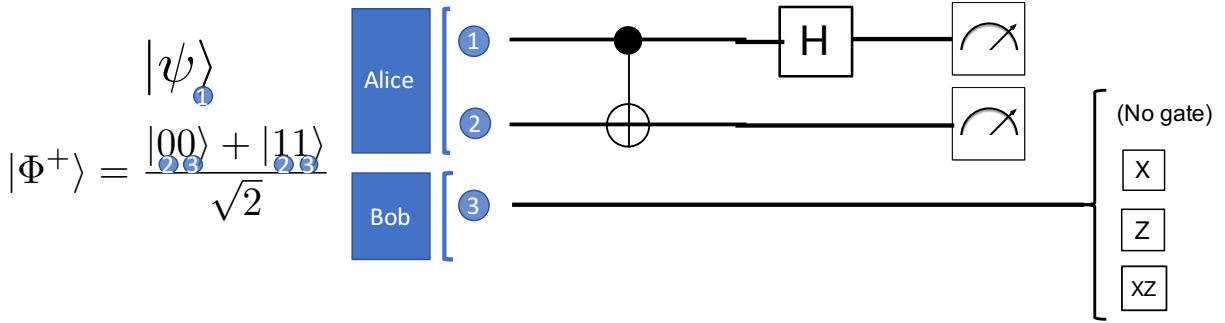


Figure 2.7: Circuit diagram of quantum teleportation: Bob applies his operation depending on the measurement result at Alice.

Assume that Alice wants to teleport a qubit to Bob. Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ be the state that Alice wants to teleport and let the entangled state be the Bell pair³ $|\varphi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ with the first qubit owned by Alice and the second by Bob; thus Alice has two qubits and Bob has one. The whole state is expressed as

$$|\psi\rangle |\Phi^+\rangle = \frac{1}{\sqrt{2}} \left(\alpha|0\rangle (|00\rangle + |11\rangle) + \beta|1\rangle (|00\rangle + |11\rangle) \right). \quad (2.3.2.1)$$

First Alice performs a CNOT gate, setting her qubit $|\psi\rangle$ as the controlling bit and the first qubit of $|\Phi^+\rangle$ as the target bit, the result of which will be

$$|\psi\rangle |\Phi^+\rangle \xrightarrow{\text{CNOT Alice}} \frac{1}{\sqrt{2}} \left(\alpha|0\rangle (|00\rangle + |11\rangle) + \beta|1\rangle (|10\rangle + |01\rangle) \right). \quad (2.3.2.2)$$

²Operation here means application of quantum gates to states and *local operations* imply that the operations are made at the location where each of the qubits lies.

³The choice of a Bell pair among the four types is immaterial. It only affects which type of gate Bob applies at the end of this procedure to complete the teleportation process.

Alice's outcome	Bob's state
00	$\alpha 0\rangle + \beta 1\rangle$
01	$\alpha 1\rangle + \beta 0\rangle$
10	$\alpha 0\rangle - \beta 1\rangle$
11	$\alpha 1\rangle - \beta 0\rangle$

Table 2.1: Correspondence between Alice's measurement outcomes and Bob's state at the time Alice obtained each outcome

Next Alice applies a Hadamard gate to $|\psi\rangle$, obtaining

$$|\psi\rangle |\Phi^+\rangle \xrightarrow[\text{Hadamard Alice}]{\text{CNOT Alice}} \frac{1}{2} \left(\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle) \right). \quad (2.3.2.3)$$

Rewriting Equation (2.3.2.3) gives

$$|\psi_{final}\rangle = \frac{1}{2} \left(|00\rangle (\alpha |0\rangle + \beta |1\rangle) + |01\rangle (\alpha |1\rangle + \beta |0\rangle) + |10\rangle (\alpha |0\rangle - \beta |1\rangle) + |11\rangle (\alpha |1\rangle - \beta |0\rangle) \right).$$

Observe that there are four possible outcomes in the measurement of Alice and that each of the outcomes exactly corresponds to measurement outcomes of Bob, which also consists of four patterns. The precise correspondence is shown in Table 2.1. Now the interesting part comes: Bob can recover the state $|\psi\rangle$, which Alice previously held, by applying an appropriate gate depending on the measurement outcome of Alice.

In fact, Bob does not need any operation if Alice's result is 00; if it is 01, then Bob has $\alpha |1\rangle + \beta |0\rangle$ and applying X gate

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (2.3.2.4)$$

to the state

$$\begin{pmatrix} \beta \\ \alpha \end{pmatrix} \quad (2.3.2.5)$$

will recover the original state $|\psi\rangle$; if it is 10, then applying Z gate

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (2.3.2.6)$$

will do; and if 11, then applying X gate first and then Z gate, which is equivalent to the matrix

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad (2.3.2.7)$$

will yield the original state [11].

Recalling that any unitary transformation is mathematically legitimate to be a quantum gate (see Section 2.2.2), all these operation involved at Bob are application of quantum gates. Thus the unknown state $|\psi\rangle$ is “teleported” by a set of local operations to the shared Bell pair and to the state $|\psi\rangle$.

2.3.3 Entanglement Swapping

Entanglement swapping [12] is an application of quantum teleportation of great significance in quantum networking. We have seen how to transfer an unknown state to a distant location in the previous section. We now apply this method to “connect and lengthen” two entangled states. The whole process of entanglement swapping is depicted in the circuit diagram (Figure 2.8).

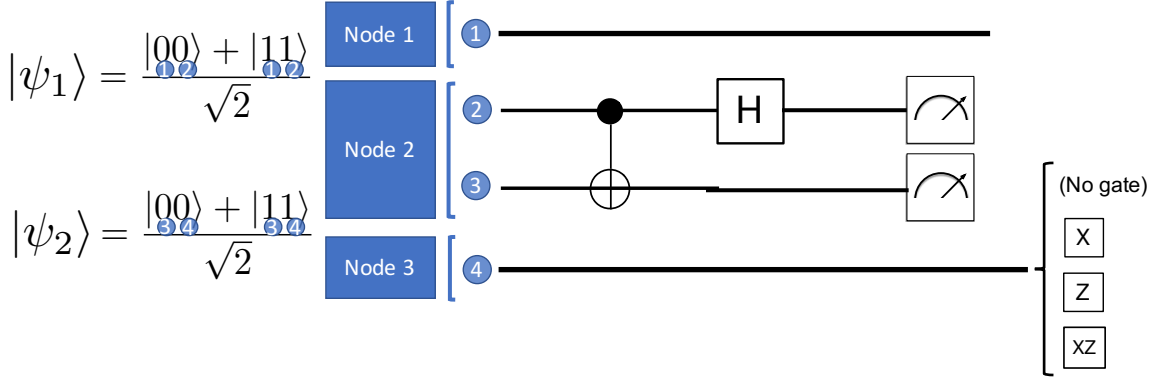


Figure 2.8: Circuit diagram of entanglement swapping

Let us assume that we have three nodes, Node 1 through 3, and Node 1 and 2 have one particle each of the Bell pair $|\psi_1\rangle$ and Node 2 and 3 have one particle each of the other Bell pair $|\psi_2\rangle$, as illustrated in Figure 2.9.

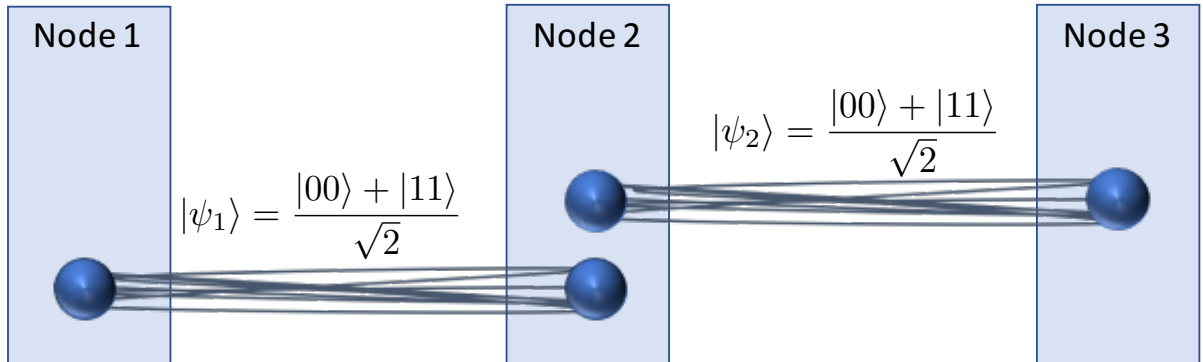


Figure 2.9: Entanglement swapping: initial state. Node 1 and 2 share one entangled photon pairs, and Node 2 and 3 also share another entangled photon pair, with two photons in total at Node 2.

Now Node 2 transfers the state of one particle to Node 3 by using the Bell pair owned by and entangled between Node 2 and 3 (Figure 2.10):

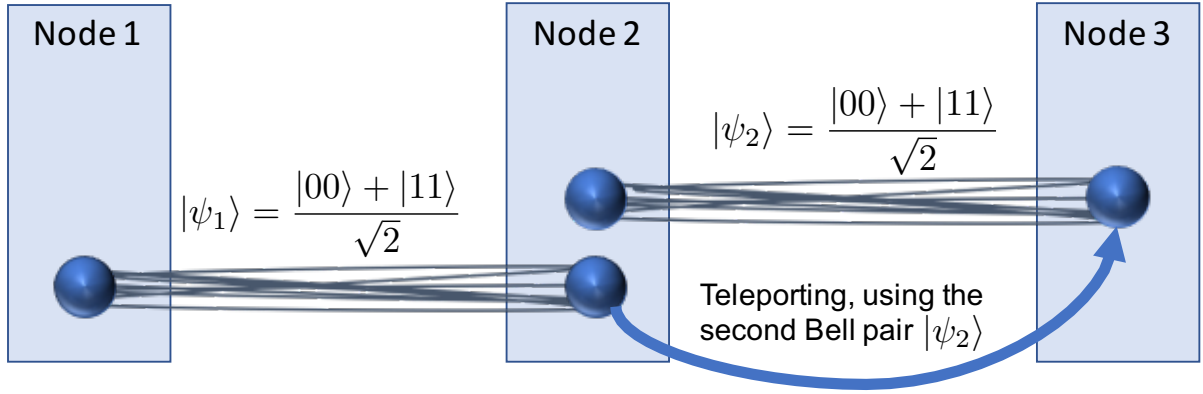


Figure 2.10: Entanglement swapping: teleporting the state of one particle of Node 2 to Node 3 using the same procedure as quantum teleportation.

This operation changes $|\psi_2\rangle$ to some other state, and the two physical qubits in Node 2 are now disentangled from the pair of interest. The result is as depicted in Figure 2.11:

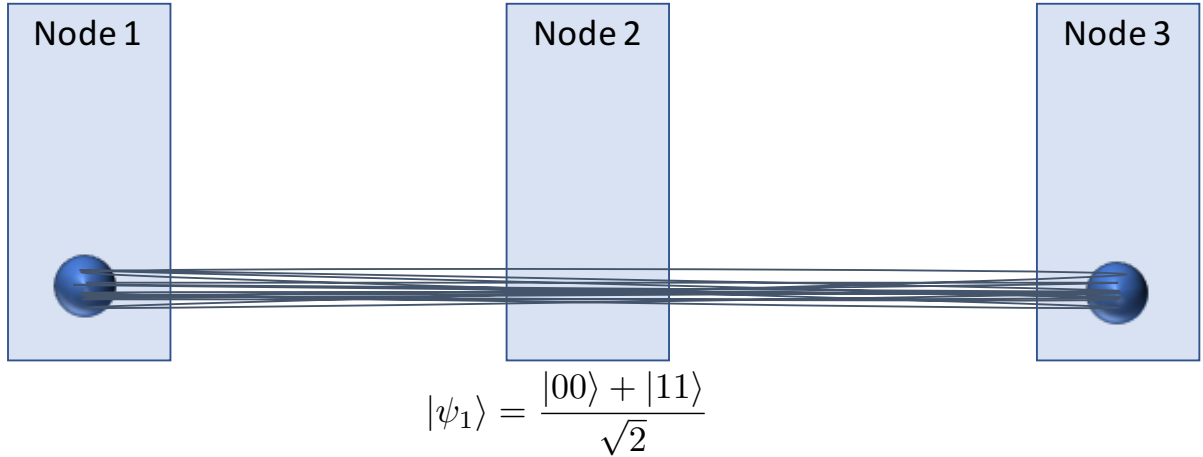


Figure 2.11: Entanglement swapping: the particle at Node 1 is now entangled to the particle at Node 3, resulting in a longer entanglement.

This is not only one of the most quintessential applications of the principle of quantum teleportation, but also a keystone that enables *quantum repeater networks*, as will be seen later.

2.4 Quantum Networking

2.4.1 Purification

Purification is a method to increase the fidelity of a given Bell pair by consuming another Bell pair. Recall that Bell pairs in reality always have errors. Let us consider the simplest case where there is only one type of error, the *bit flip error* in the Bell

Probability	Alice	Bob
F^2	$ \Phi^+\rangle$	$ \Phi^+\rangle$
$F(1 - F)$	$ \Phi^+\rangle$	$ \Psi^+\rangle$
$F(1 - F)$	$ \Psi^+\rangle$	$ \Phi^+\rangle$
$(1 - F)^2$	$ \Psi^+\rangle$	$ \Psi^+\rangle$

Table 2.2: Possible combinations of the states Alice and Bob have when only bit flip errors occur: when the first and last cases occur the round of purification is considered successful, while the second and third cases lead to failure of the round.

pair. At the beginning we have two identical Bell pairs. The density matrix of the Bell pair ρ with bit flip errors described as

$$\rho = F |\Phi^+\rangle \langle \Phi^+| + (1 - F) |\Psi^+\rangle \langle \Psi^+|. \quad (2.4.1.1)$$

where $0 < F < 1$.⁴ Assume that two parties, Alice and Bob, each have the identical Bell pair ρ above with Alice having the first qubit of each of the Bell pairs and Bob the second qubit of each of the Bell pairs. Let ρ_1 denote Alice's and ρ_2 Bob's. They are 4 possible combinations of the states they have, as in Table 2.2.

First Alice applies CNOT gate with the control qubit set to her first qubit and the target qubit to her second qubit; then Bob applies CNOT with the control qubit set to his first qubit and the target qubit to his second, similarly. Alice and Bob each measure their second qubit. If their results are identical (which is, both measured 0's and 1's), then purification *succeeded* and their first Bell pair will have a higher fidelity. The first Bell pair will be used either for further purification or an application; the second pair will always be discarded because of the collapse the measurement caused. If they measured different values, then the purification is said to have *failed*, both Bell pairs will be discarded, and another purification will be attempted. The steps listed in this paragraph is counted as one round of purification.

In practice, many rounds of purification are conducted until the fidelity increases to above a certain “threshold” (Figure 2.13). The value of this threshold depends on subsequent applications.

The version of the purification implemented in the simulator can deal with phase flip errors as well, and the circuit is depicted in Figure 2.12. This circuit uses two Bell pairs to detect bit flips on two other Bell pairs (left half), resulting in two higher-fidelity Bell pairs with potential phase flip errors remaining. The phase flip errors are then suppressed (right half), leaving a single, high-fidelity Bell pair.

⁴In general, there can be multiple types of error and the density matrix $|\Psi^+\rangle \langle \Psi^+|$ multiplied by $1 - F$ in the equation above can be more complex, and subsequent explanations will be more complicated as well.

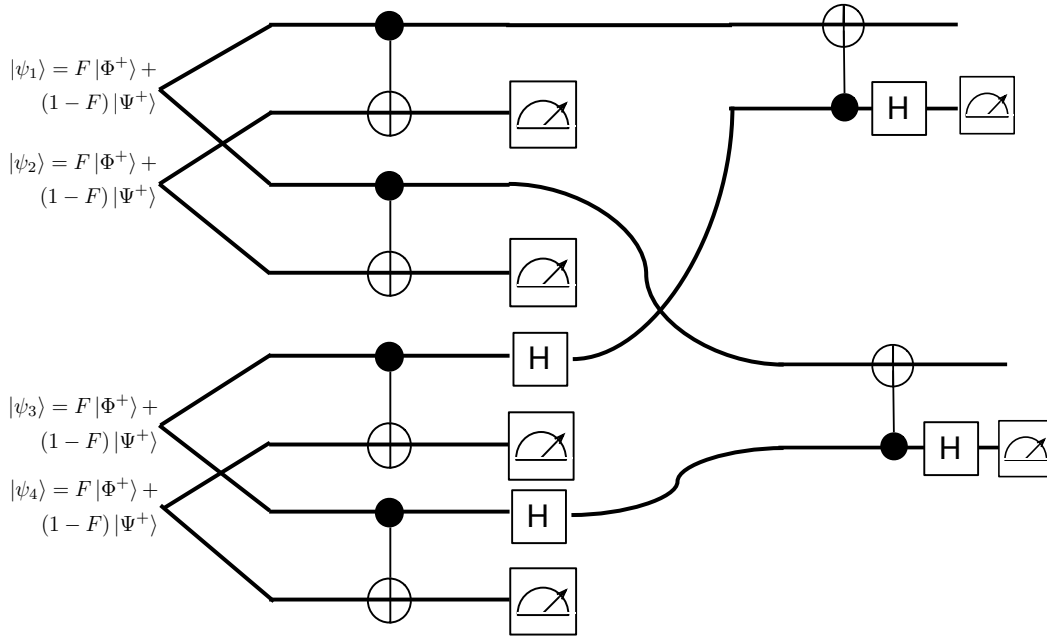


Figure 2.12: Extended purification circuit: now capable of suppressing both bit flip and phase flip errors.

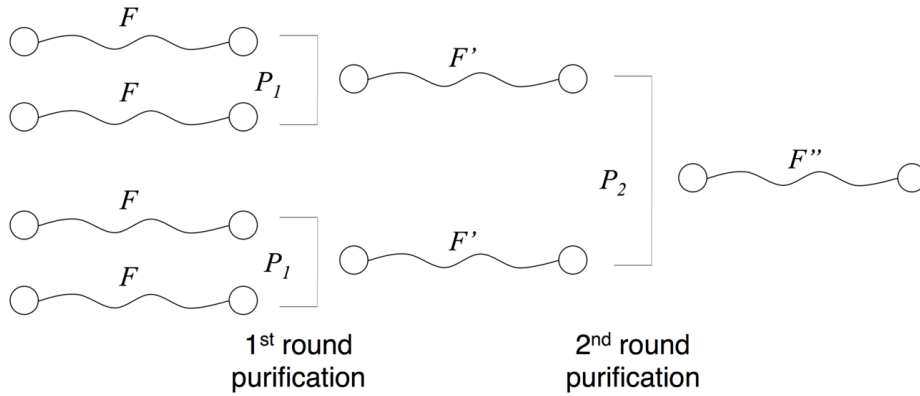


Figure 2.13: Multiple rounds of purification, increasing the fidelity still further after each round.

2.4.2 Quantum Networks

A *quantum repeater network* refers to a network of distributed quantum computing nodes [13]. Entangled states (such as Bell states) play a wide variety of roles in e.g. executing quantum gates remotely and quantum key distribution (QKD) [13]. This thesis lies in the context of building a large-scale quantum network, where delivering entangled states is thus essential. Unlike classical networks, however, transmission of entangled states suffers loss and noises while being delivered, regardless of length of

nodes, and assessing the degree of degeneration of the states requires complex procedures [13], of which quantum state tomography stands as a possible choice. Since every quantum network is essentially a set of node-to-node links, considering the case of sending entangled states is therefore the most fundamental step for our goal of realizing quantum networks. We will take a closer look at such single links in quantum networking in the following section.

2.4.3 Quantum Link

Quantum link refers to a state where two parties (let us call them Alice and Bob here) have one entangled photon pair with one qubit at Alice and the other at Bob, as in Figure 2.14. The entanglement is essential for subsequent applications.

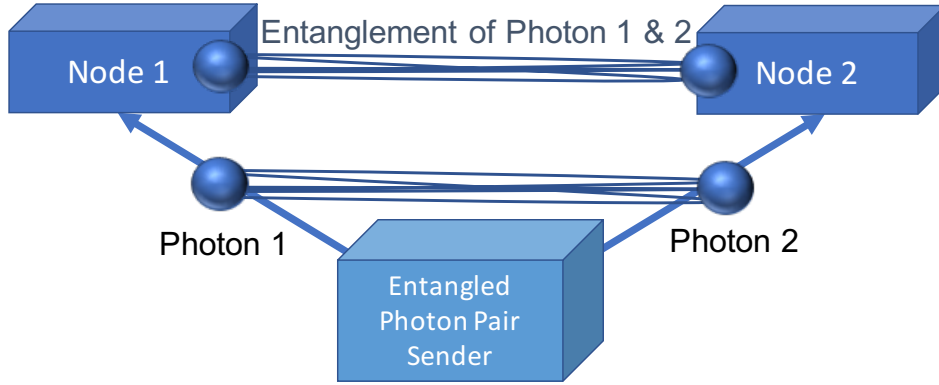


Figure 2.14: A scheme of two nodes sharing an entangled photon pair: the photon 1 and 2 constitute the entanglement, both having been emitted by the Entangle Photon Pair Sender in the middle.

We assume a concrete scenario throughout the research (Figure 2.15), while the details in actual node-to-node links could be in different forms. We consider the scenario with the timeframe spanning from when we began to create a link up to the moment we confirmed that the link is actually ready for use in further applications.

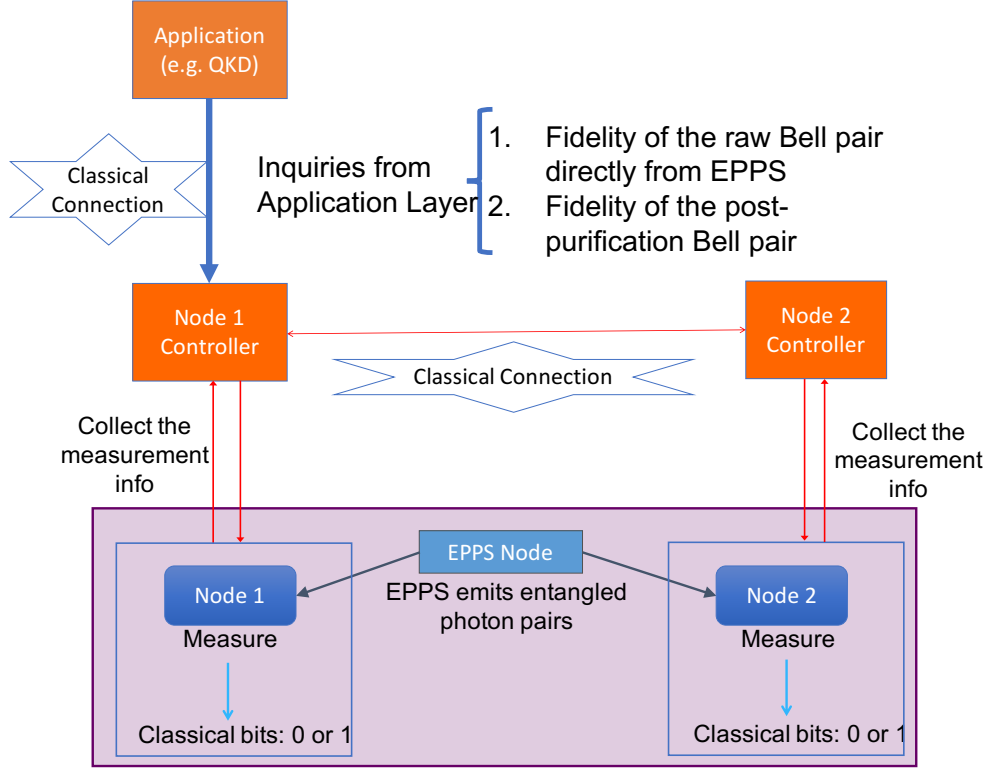


Figure 2.15: A quantum link with Node Controllers: the Controllers are responsible for making operational decisions such as choosing measurement bases and fidelity assessment of states, involving state estimation methods.

We have one *entangled photon pair sender* (EPPS henceforth), that emits entangled photon pairs; two Nodes, Node 1 and 2, that receive entangled photon pairs from the EPPS, which take part in actual communication using Bell pairs; and corresponding controller Nodes, Node Controller 1 and 2, that direct and manage the link creation between the two Nodes. The Node Controllers are classical computers that communicate via classical channel and function as controllers by e.g. monitoring and managing Bell pair emission, conducting state reconstruction, making decisions as to whether the Nodes are ready to use the Bell pairs being made, and if not, whether they need to purify it, and how many times we need to purify to make the pairs ready for use, etc. We will take a closer look at each of the tasks mentioned here. Of course each Bell pair consists of two photons, one of which is owned by Node 1 and the other by Node 2. Moreover, the EPPS in this scenario is assumed to emit the same type of Bell pairs throughout the process, one of the four states presented at the end of Section 2.3.1.

2.5 Quantum State Tomography

Quantum state tomography refers to a procedure by which we can reconstruct a given mixed state, typically in the form of density matrix, with a certain accuracy. Because of its probabilistic behavior in measurement, we cannot directly gain the information of the state itself, but rather need to make a “guess” from a set of measurement outcomes

we obtain by measuring the state with different bases, as in Figure 2.16. For photons, $|H\rangle$, $|V\rangle$, $|D\rangle$, $|A\rangle$, $|R\rangle$ and $|L\rangle$ are the horizontal, vertical, diagonal, antidiagonal, right and left bases, corresponding to $|0\rangle$, $|1\rangle$, $(|0\rangle + |1\rangle)/\sqrt{2}$, $(|0\rangle - |1\rangle)/\sqrt{2}$, $(|0\rangle + i|1\rangle)/\sqrt{2}$ and $(|0\rangle - i|1\rangle)/\sqrt{2}$, respectively, in terms of the Bloch sphere (Figure 2.17). Measuring the state with different bases is analogous to seeing an object at several different angles to grasp the whole image when the object is hard to see as a whole (imagine looking at a huge mountain). Measurement with one basis will give only a partial knowledge of the state. The accuracy of state reconstruction depends on the number of measurement conducted, and generally becomes higher as we increase the number of measurements.

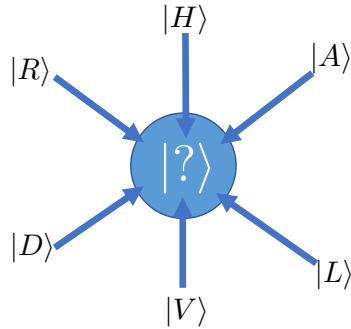


Figure 2.16: Fidelity and the process of state reconstruction in tomography: looking at the state from different angles enables reconstruction of the state

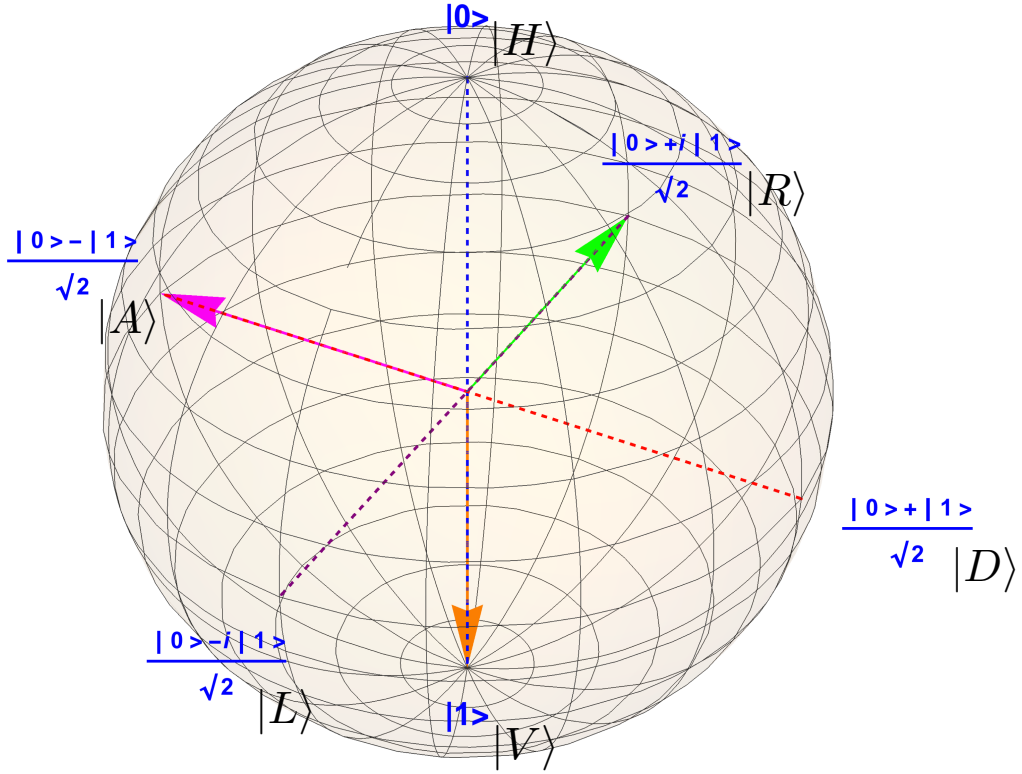


Figure 2.17: Measurement bases and their respective points on the Bloch sphere: measurements with respect to these bases “project” a given state to their respective points on the sphere probabilistically.

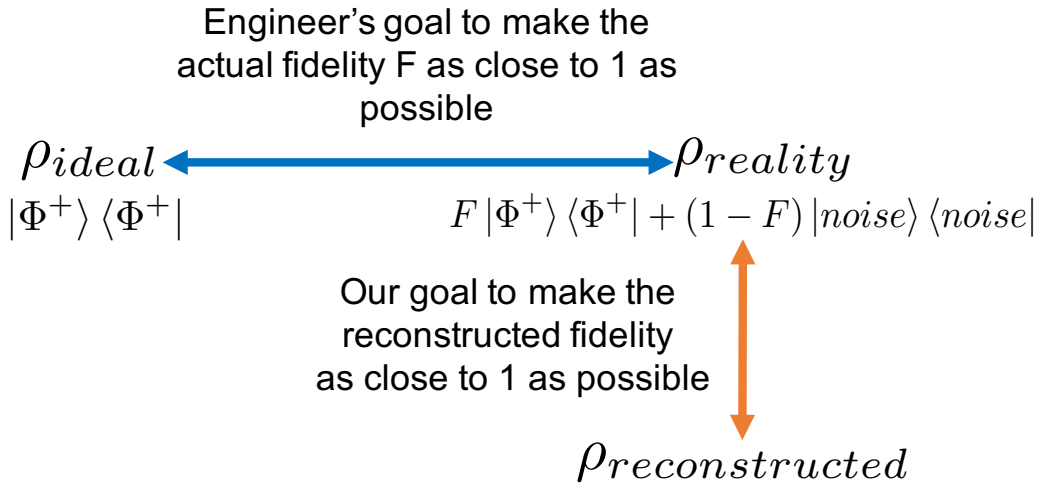


Figure 2.18: State tomography for 1-qubit: the actual fidelity is between the ideal state and the actual state (the latter of which cannot be seen) and the reconstruction fidelity is between the state reconstructed by the maximum likelihood (see Section 2.5.1) and a set of states generated by the error estimation routine (see Section 2.5.2), representing accuracy of the reconstruction.

We adopt the tomography procedure presented by Kwiat et. al. in [1] as the cornerstone for comparison and the basis for our proposal. The tomography implementation used in the simulator (which will be formally presented in a subsequent chapter) has been created based on the implementation developed by the authors of [1].

Two fidelities are used in this state tomography: the actual fidelity, ρ_{reality} , and the reconstruction fidelity, $\rho_{\text{reconstruction}}$ (Figure 2.18). The former one is between the ideal state and the reconstructed state that have derived from the maximum likelihood without error estimation. The latter one is the mean fidelity between the reconstructed state and the numerically generated states that are as likely to have come from the same set of measured data. While the actual fidelity converges to the fidelity of the *actual* state (of which we cannot gain direct information) as we increase the number of measurement, the reconstruction fidelity converges to 1 as we reduce the error range in state reconstruction by increasing the number of measurements.

The tomography procedure presented in [1] is two-fold: one is *maximum likelihood*, an analytical search for the density matrix that is most likely to have come from the given set of data obtained in the experiment; the other is error estimation to assess how accurately the state was reconstructed by the maximum likelihood, involving *Monte Carlo* technique to gain error distributions for each error source in measurement.

2.5.1 Maximum Likelihood Technique

We explain the maximum likelihood technique in more detail here. Let us first make a few assumptions and definitions. Assume we have n qubits. Let $n_{\nu,r}$ be the measurement result for the ν -th measurement setting on the r -th detector combination, as in [1]. A complex matrix A is said to be *Hermitian* if it satisfies the relation

$$AA^* = A^*A \quad (2.5.1.1)$$

where A^* is the conjugate transpose of A as defined in 2.2.1. A complex matrix A is said to be *nonnegative definite* if, for any complex vector $|\psi\rangle$, the relation

$$\langle\psi|A|\psi\rangle \geq 0 \quad (2.5.1.2)$$

holds.

As density matrices are required to be non-negative definite Hermitian matrices of trace one, we first introduce a parametrized matrix $T(t)$ with the parameter $t \in \mathbb{R}^{4^n}$, defined by

$$T(t) \equiv \begin{pmatrix} t_1 & 0 & \cdots & 0 \\ t_{2^n+1} + it_{2^n+2} & t_2 & \cdots & 0 \\ \cdots & \vdots & \ddots & 0 \\ t_{4^n-1} + it_{4^n} & t_{4^n-3} + it_{4^n-2} & \cdots & t_{2^n} \end{pmatrix} \quad (2.5.1.3)$$

and

$$t \equiv \begin{pmatrix} t_1 \\ \vdots \\ t_{4^n} \end{pmatrix}. \quad (2.5.1.4)$$

as in [1]. Note that any matrices of the form TT^* are non-negative definite. The relation $(TT^*)^* = (T^*)^*T^* = TT^*$ implies TT^* is Hermitian as well. By dividing by the trace of itself, TT^* becomes non-negative, Hermitian, and of trace one, thereby formulating a parametrized density matrix

$$\rho(t) = \frac{T(t)T^*(t)}{\text{Tr}\{T(t)T^*(t)\}}. \quad (2.5.1.5)$$

Now let $\hat{n}_{\nu,r}$ be the result that would be expected from a given density matrix $\rho(t)$ ⁵; thus the family $\{\hat{n}_{\nu,r}\}$ with ν and r running through appropriate sets determined by measurement configurations can be regarded as a mapping from $\rho(t)$, and thus a function of t . Assuming the counting statistics follow Gaussian distribution (as in [1]), the probability that $\rho(t)$ yields the counts $\{n_{\nu,r}\}$ is given by

$$P(\{n_{\nu,r}\}) = C \prod_{\nu,r} \exp\left\{-\frac{(\hat{n}_{\nu,r} - n_{\nu,r})^2}{2\hat{n}_{\nu,r}}\right\} \quad (2.5.1.6)$$

where C is a constant to normalize the right hand side. Applying logarithm to the right hand side and then negating, we get

$$\sum_{\nu,r} \frac{(\hat{n}_{\nu,r} - n_{\nu,r})^2}{2\hat{n}_{\nu,r}}. \quad (2.5.1.7)$$

Notice that maximizing the right hand side of (2.5.1.6) with respect to t is equivalent to minimizing the left hand side of . Our maximum likelihood approach is thus reduced to finding the solution $t = t_{min}$ for which the left hand side of Equation attains a minimum [1].

2.5.2 Error Estimation

The error estimation method used in the paper [1] is based on the assumption that count statistics obey Poisson distribution (page 47 and 48). The error estimation will be used in this research as it is, the details of which will be explained in the following paragraphs.

⁵ $\hat{n}_{\nu,r}$ is expressed as a function of t , together with several physical constants that depend on the particular measurement apparatus. For the complete definition, see Page 40 of [1].

Chapter 3

Ideas and Designs

3.1 Key Ideas

Recall that state tomography is designed to reconstruct a completely unknown state without prior knowledge of the state. While it is true that this full tomography can be used to reconstruct Bell states used in quantum networking, we may be able to “cut short” by using the fact that we use Bell states in quantum networking, which comprise only four types. In other words, we can reduce the possibility of the given state, which could be completely unknown in general, to one of those Bell pairs. In addition, we do not need the information of the whole state, but we need to know the *fidelity* of the state with the ideal state we want to achieve. This also suggests a possibility of reducing the number of measurement bases, thereby shortening the bootstrap time. That is, we could greatly accelerate the process by limiting the scope of state analysis to our particular situation in quantum link creation.

The goal of this project is to propose such an optimized fidelity estimation method concretely. Before moving on to the goal, let us first consider how two nodes about to share an entangled state should behave in detail.

3.2 Design of the Protocol for Creating a Link

In this section we discuss how the whole procedure is arranged in link creation. Let us assume that we are at the beginning of the link creation. First the EPPS starts to emit Bell pairs to each Node. After the Bell pairs arrive, each Node controller chooses a measurement basis for its Node, and tells the Node to measure its qubit with the specified basis. Repeating the procedure from the Bell pair emission to the measurement sufficiently many times will give us a reasonably large collection of measurement outcomes. The next step is to reconstruct the state by using the collected data. This is done by the tomography routine implemented in both Node 1 and 2 Controllers, and these Node Controllers conduct tomography independently.

One might suspect that we do not need to run the tomography at more than one location if it is fed with the same input data, since the tomography routine will then give the same reconstruction. However, this is not true because the tomography involves

probabilistic estimation in part, and thus it is not guaranteed that they always give identical output, even though they will yield *almost* identical results.

To probe into the problem, let us suppose that we have two nodes that share a Bell pair and they are going to conduct tomography to check the state is of sufficient fidelity. There are two models regarding the way the tomography is conducted: *distributed model* (Figure 3.1) and *master-slave model* (Figure 3.2 and 3.3). In the distributed model, two separate tomography instances are conducted at each node concurrently. In the master-slave mode, on the other hand, tomography is conducted at only one node; the node at which tomography is conducted then sends the information of the reconstructed state to the other node. While the distributed model has an obvious advantage of being simple, it also has a risk of disagreement between the two nodes. That is, it could happen that one node's tomography leads to a result that indicates the shared Bell state is of sufficiently high fidelity, and thus decides to use the state, while the other node yields a slightly different result in tomography that implies the fidelity of the shared state is marginally under the required threshold. In such an case the nodes disagree on whether they are ready to proceed, resulting in an operational inconsistency. If we use the master-slave model, we need to consider a way to maintain consistency in decision-making, which is crucial for quantum networking to function properly. This is one of the essential properties required for quantum networking, which is not present in the stand-alone state tomography experimented in a laboratory. Thus it is significant to propose a protocol that supports the tomography in quantum networking, one of novelty in this research.

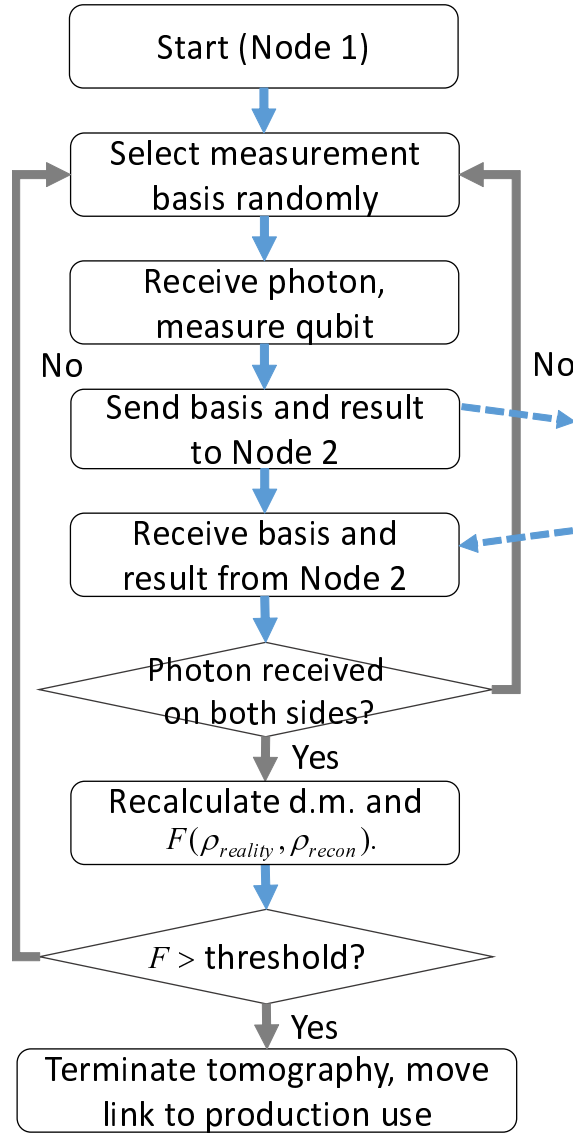


Figure 3.1: Flowchart at Node 1 in the distributed model: both Node 1 and 2 conduct tomography concurrently, exchanging each other's reconstructed density matrices.

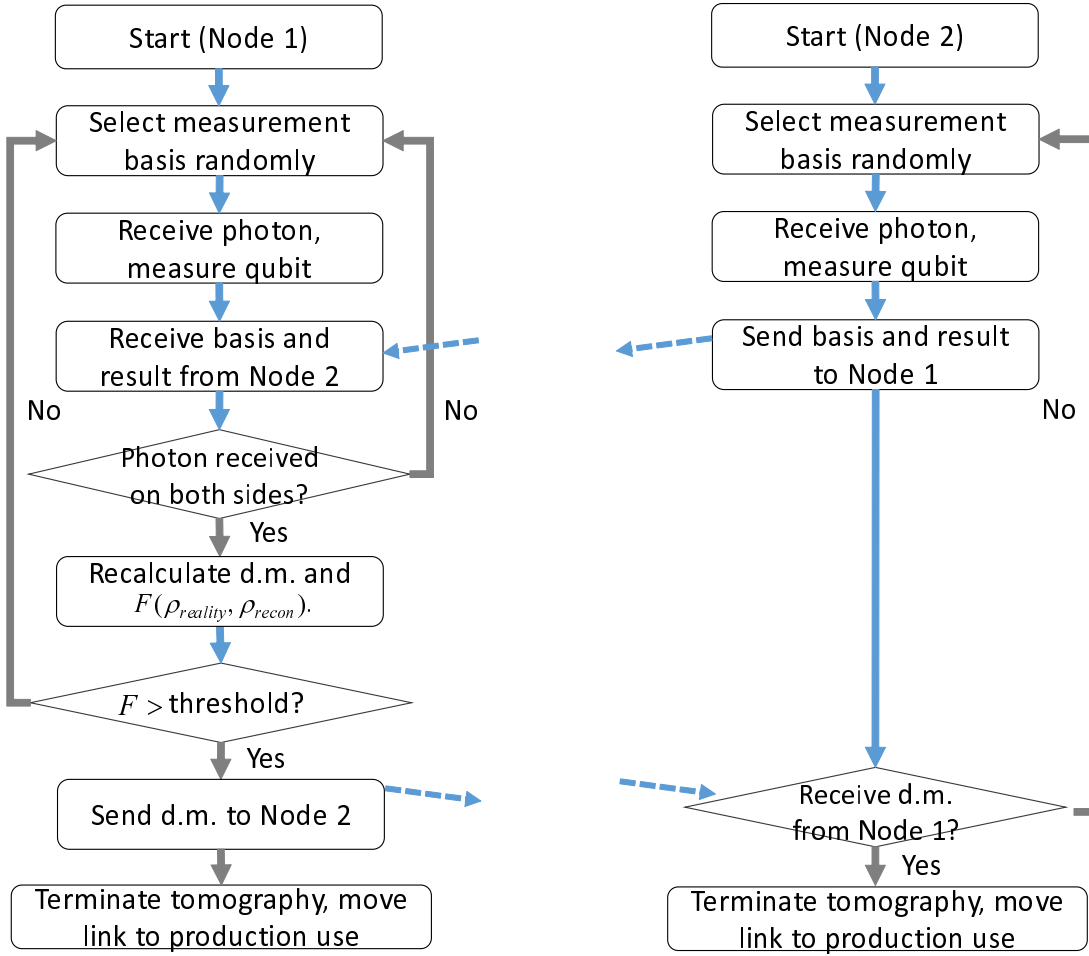


Figure 3.2: Flowchart at Node 1 in the master-slave model: only Node 1 conducts tomography and is responsible for choosing measurement bases and state reconstruction. Figure 3.3: Flowchart at Node 2 in the master-slave model: Node 2 receives the tomography result and follows the decision of Node 1 regarding whether to proceed for applications.

With the results from tomography we calculate the reconstruction fidelity, by which we can determine whether we have reconstructed the state accurately enough. If the accuracy is sufficient, then we can calculate the fidelity between the reconstructed state and the ideal state, $\rho_{reality}$ in the notation in Section 2.5. If $\rho_{reality}$ is high enough for use in further applications, then we are ready to use the link and the procedure terminates. If not, we need to purify it to achieve a higher fidelity. Recall that we need to conduct a state analysis every time when we try to know the state; thus we start again from the phase of measuring the state many times, but this time *with one purification conducted before every measurement*. We increase the number of purifications until we are confident that the fidelity is sufficiently high with that number of measurements. This whole procedure is illustrated in the flowchart (Figure 3.4).

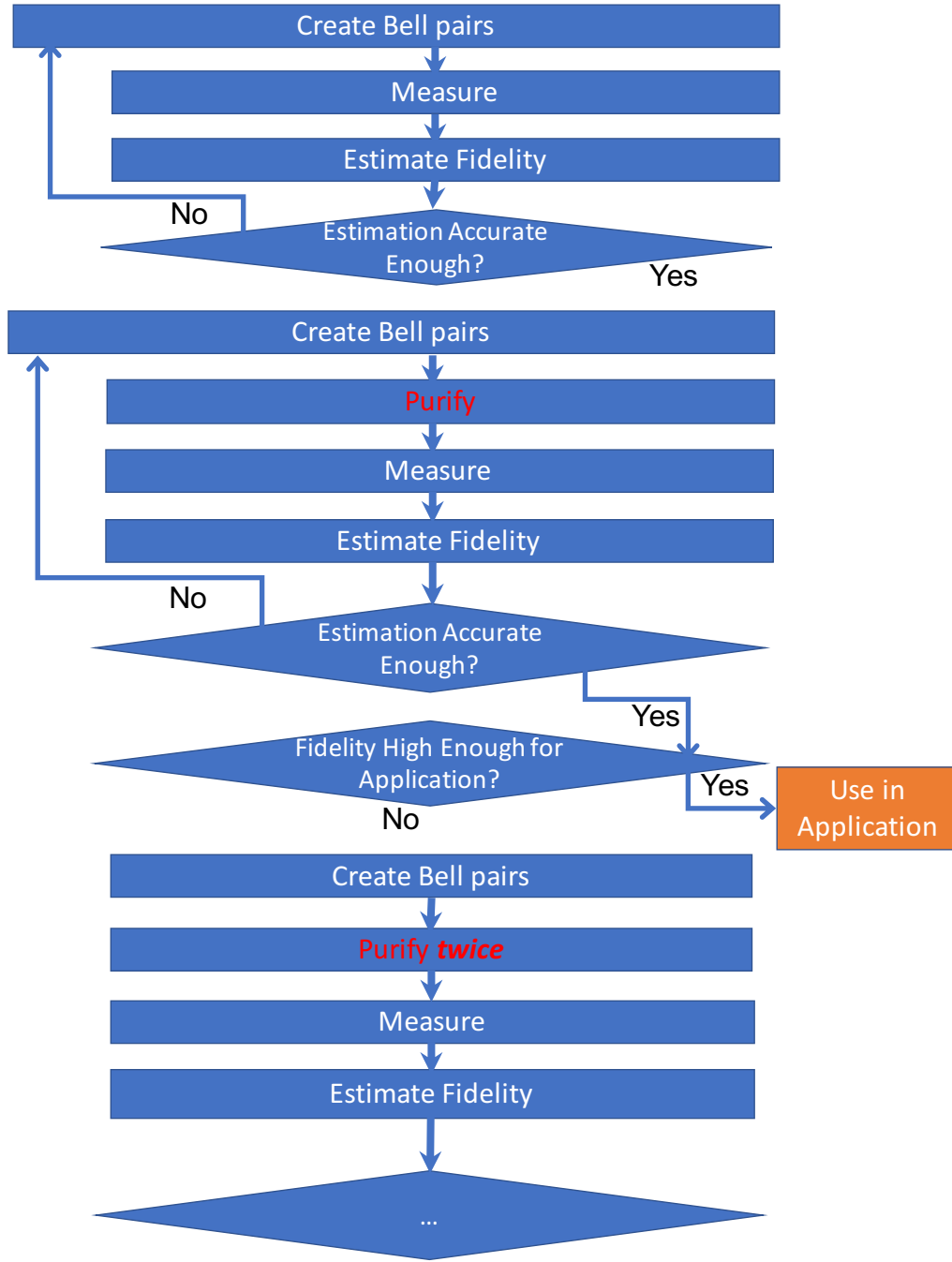


Figure 3.4: Flowchart of the bootstrap procedure of a quantum link: the number of purifications increases until leading to the state being of a sufficient fidelity.

3.3 Design of the Optimized Fidelity Estimation

In this section a thorough exposition of the optimized fidelity estimation method proposed will be presented.

The proposed fidelity estimation method is realized as part of the circuit that is identical to the one we have used for purification, except choice of bases in some of the

measurement operations involved (Figure 3.5).

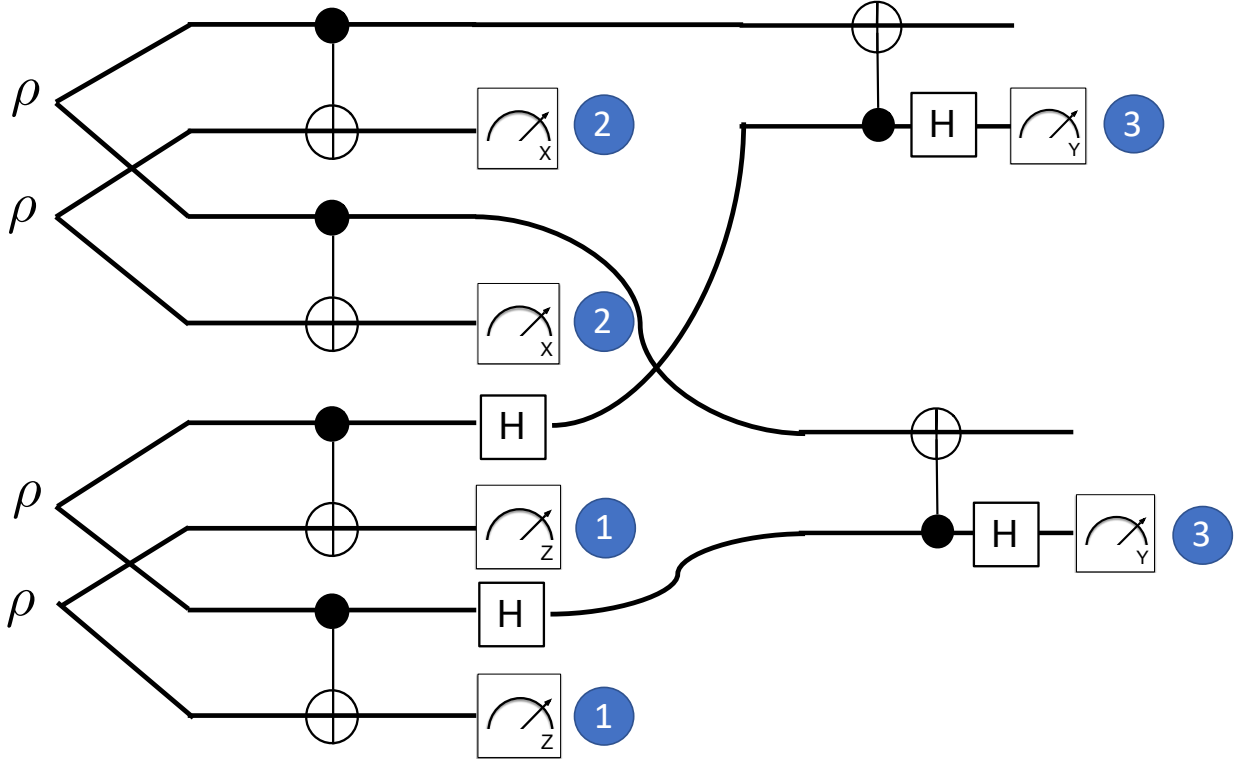


Figure 3.5: Circuit diagram to realize the proposed fidelity estimation method: ρ 's are four identical initial Bell pairs of which we estimate the fidelity.

Let us suppose that the initial state is represented by the density matrix ρ , defined by

$$\rho = A |\Phi^+\rangle \langle \Phi^+| + B |\Psi^+\rangle \langle \Psi^+| + C |\Psi^-\rangle \langle \Psi^-| + D |\Phi^-\rangle \langle \Phi^-|. \quad (3.3.0.1)$$

We will collect the measurement outcomes obtained at the measurement settings 1, 2, and 3, each of which corresponds to the circled numbers in Figure 3.5, to estimate the coefficients A , B , C , and D of ρ , hence the fidelity between ρ and $|\Phi^+\rangle \langle \Phi^+|$.

Recall that we have four possible patterns for a measurement outcome of 2-qubit states, namely 00, 01, 10, and 11. Following the circuit above, the possible outcomes and corresponding probabilities at the measurement setting 1 is as in Table 3.1. It is reasonable to expect, as the number of total measurements increases, that the proportion of the number of measurements with outcomes of the same parity (00 or 11) to the total number of measurements will converge to $(A + D)^2 + (B + C)^2$. We define P_1 to be this proportion.

Outcome at 1	Probability
00	$\{(A + D)^2 + (B + C)^2\} / 2$
01	$(A + D)(B + C)$
10	$(A + D)(B + C)$
11	$\{(A + D)^2 + (B + C)^2\} / 2$

Table 3.1: Possible measurement outcomes at the measurement setting 1 and their respective probabilities in terms of the coefficients of ρ .

In view of the relation

$$A + D = 1 - (B + C), \quad (3.3.0.2)$$

set $x = A + D$ to obtain an equation of x

$$P_1 = x^2 + (1 - x)^2. \quad (3.3.0.3)$$

Solving the equation (3.3.0.3) leads to the expressions in terms of P_1

$$A + D = \frac{1 + \sqrt{2P_1 - 1}}{2} \quad (3.3.0.4)$$

$$B + C = \frac{1 - \sqrt{2P_1 - 1}}{2}. \quad (3.3.0.5)$$

The possible outcomes and corresponding probabilities at the measurement setting 2 is in Table 3.2

Outcome at 2	Probability
00	$\{(A + B)^2 + (A + B)(C + D)\} / 2$
01	$\{(C + D)^2 + (A + B)(C + D)\} / 2$
10	$\{(C + D)^2 + (A + B)(C + D)\} / 2$
11	$\{(A + B)^2 + (A + B)(C + D)\} / 2$

Table 3.2: Possible measurement outcomes at the measurement setting 2 and their respective probabilities in terms of the coefficients of ρ .

We similarly define P_2 to be $\{(A + B)^2 + (A + B)(C + D)\} / 2$. Setting $x = A + B$ this time, the relation (3.3.0.2) yields

$$A + B = P_2 \quad (3.3.0.6)$$

$$C + D = 1 - P_2, \quad (3.3.0.7)$$

for we have $P_2 = x^2 + x(1 - x) = x$.

Finally, we consider the measurement outcomes obtained at the setting 3 to finish the last piece needed to calculate the coefficients of ρ . We introduce another set of

expressions as follows:

$$\begin{aligned}
\tilde{A}_1 &= A^2 + D^2 + AB + CD \\
\tilde{B}_1 &= AC + BD + 2AD \\
\tilde{C}_1 &= AC + BD + 2BC \\
\tilde{D}_1 &= B^2 + C^2 + AB + CD \\
\tilde{A}_2 &= \tilde{A}_1 \\
\tilde{B}_2 &= \tilde{D}_1 \\
\tilde{C}_2 &= \tilde{C}_1 \\
\tilde{D}_2 &= \tilde{B}_1.
\end{aligned}$$

Now the correspondence between the measurement outcomes and their respective probabilities can be written as in Table 3.3.

Outcome at 3	Probability
00	$\{(\tilde{A}_1 + \tilde{C}_1)(\tilde{C}_2 + \tilde{D}_2) + (\tilde{B}_1 + \tilde{D}_1)(\tilde{A}_2 + \tilde{B}_2)\}/2$
01	$\{(\tilde{A}_1 + \tilde{C}_1)(\tilde{A}_2 + \tilde{B}_2) + (\tilde{B}_1 + \tilde{D}_1)(\tilde{C}_2 + \tilde{D}_2)\}/2$
10	$\{(\tilde{A}_1 + \tilde{C}_1)(\tilde{A}_2 + \tilde{B}_2) + (\tilde{B}_1 + \tilde{D}_1)(\tilde{C}_2 + \tilde{D}_2)\}/2$
11	$\{(\tilde{A}_1 + \tilde{C}_1)(\tilde{C}_2 + \tilde{D}_2) + (\tilde{B}_1 + \tilde{D}_1)(\tilde{A}_2 + \tilde{B}_2)\}/2$

Table 3.3: Possible measurement outcomes at the measurement setting 3 and their respective probabilities in terms of the coefficients of ρ .

We define P_3 to be $(\tilde{A}_1 + \tilde{C}_1)(\tilde{C}_2 + \tilde{D}_2) + (\tilde{B}_1 + \tilde{D}_1)(\tilde{A}_2 + \tilde{B}_2)$. Observe that the equation (3.3.0.6) allows B to be expressed in terms of P_2 and A , (3.3.0.7) C to be expressed in terms of P_2 and D , and (3.3.0.4) enables D to be expressed in terms of P_1 and A ; consequently, we can write \tilde{A}_i , \tilde{B}_i , \tilde{C}_i , and \tilde{D}_i , for $i = 1, 2$, in terms of P_1 , P_2 , and A . Further substitution leads to the expression of P_3 in terms of P_1 , P_2 , and A . Messy calculations show that P_3 is in fact

$$\begin{aligned}
P_3 &= -2A(2P_2 - 1)^3 + 4\left(\sqrt{2P_1 - 1} - 3\right)P_2^3 - 6\left(\sqrt{2P_1 - 1} - 1\right)P_2^2 \\
&\quad + \left(3\sqrt{2P_1 - 1} - 1\right)P_2 + \frac{1}{2}\left(1 - \sqrt{2P_1 - 1}\right) + 8P_2^4.
\end{aligned}$$

Since we know the values of P_1 , P_2 , and P_3 estimated by the three sets of repeated measurements, we may solve the linear equation above to obtain the value of A . Using the relations (3.3.0.6), (3.3.0.7), and (3.3.0.4) again, we can revert the values of B , C , and D . The evaluation of accuracy per a given number of measurements will be presented in Chapter 5.

Chapter 4

Implementation

4.1 Structure of the Simulator

The simulator comprises three modules: *God channel* module, *tomography* module, and *simulator* module (4.1). The God channel module serves as the imitation of real physical equipment, examples of its job including creating states, measurements, and applying CNOT gates (i.e. purifications). Many of these operations are essentially probabilistic in the senses that measurements invoke probabilistic collapse of quantum states and that errors in both measurements and CNOT gates embrace fluctuations, which also follow certain probability distributions in classical sense. The God channel thus simulates both quantum and classical operations that in reality derive from the property of quanta and from physical apparatus, respectively.

The tomography module is the collection of routines for conducting tomography. Almost all of this module has been taken from the tomography program which the authors of the paper [1] created without any essential change. The tomography module takes the measured count data and returns the reconstructed density matrix. For the details of this process, see the descriptions in Section 2.5. Using the reconstructed density matrix and the density matrix of the ideal state, this module then computes the fidelity of these two states. We regard the fidelity as indication of the quality of the state.

Finally, the simulator module serves much as an experimenter, using the two modules introduced above to actually yield valuable data for the goal of this research by attempting various different settings. The settings that vary include the number of measurements conducted, types of errors observed in the Bell state, the number of purifications conducted, the degree of errors in measurements, and the degree of errors in CNOT gates. The simulator module passes these sets of parameters to the two modules above to run over different settings.

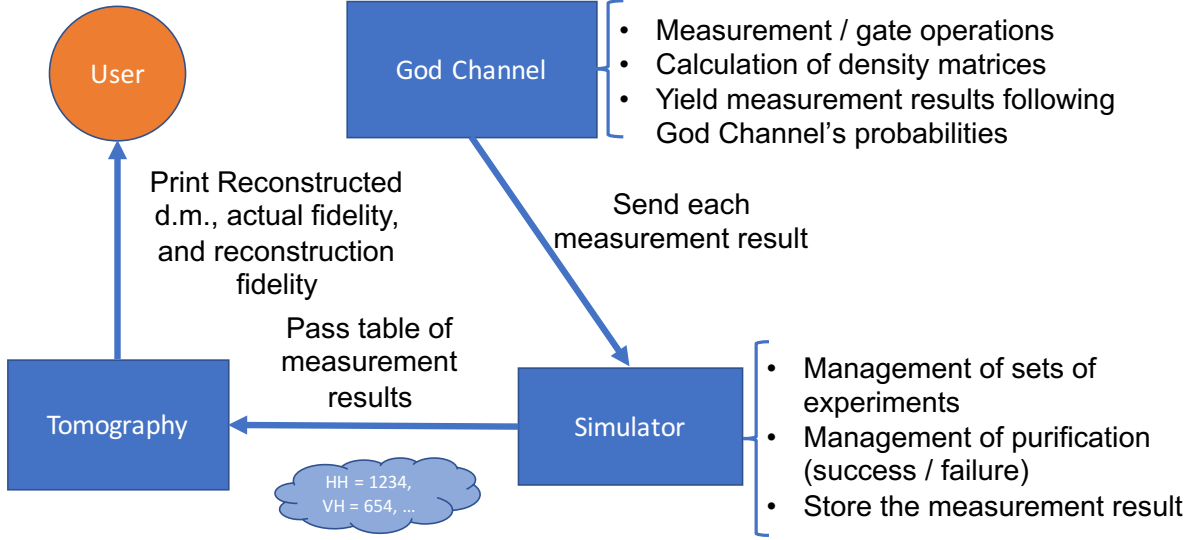


Figure 4.1: Software Architecture of the whole program: the modules are separated by their respective roles.

4.2 God Channel Module

4.2.1 Implementation of Quantum States Representations

Every quantum state recognized in the simulator is first represented as a list that serves as an ensemble of several pure states. For example, this list can contain the elements $[0.64, |\Phi^+\rangle, |\Phi^+\rangle]$, $[0.16, |\Phi^+\rangle, |\Psi^+\rangle]$, $[0.16, |\Psi^+\rangle, |\Phi^+\rangle]$ and $[0.04, |\Psi^+\rangle, |\Psi^+\rangle]$ where $|\Phi^+\rangle$ and $|\Psi^+\rangle$ are arrays $[1,0,0,0]$ and $[0,0,1,0]$, respectively. These array representations of the state vectors are exactly derived from their mathematical representations in *Bell basis*¹, written coefficient by coefficient.

These ensembles are then converted into the corresponding density matrices in order for gates and measurements to be applied.

4.2.2 Implementation of CNOT Gate with Errors

We have seen in Section 2.2.2 that CNOT gate is represented in theory as

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \quad (4.2.2.1)$$

However, there is always imperfection in any real equipment. O'Brien et. al. demonstrated all-optical CNOT gate in experiment, providing actual data of the probabilities that we measure 00, 01, 10, and 11 after each of these states passing through the

¹The Bell basis is a set of basis vectors $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, and $|\Psi^-\rangle$.

demonstrated CNOT (Page 2 in [14]). Based upon this data the author introduced the CNOT gate with errors, whose matrix representation has become

$$CNOT_{error} = \begin{pmatrix} 0.95 & 0.031 & 0.005 & 0.011 \\ 0.023 & 0.94 & 0.011 & 0.0005 \\ 0.024 & 0.0019 & 0.23 & 0.72 \\ 0.0006 & 0.022 & 0.75 & 0.26 \end{pmatrix}. \quad (4.2.2.2)$$

While this matrix faithfully reflects the experimental data on the paper, it has an obvious disadvantage that it can only be applied to 2-qubits states; this is not desirable given that we want to apply this CNOT to arbitrary n -qubit states. For example, we might have 4-qubit states and want to set the first qubit to the control qubit and the third to the target. In such a case, the CNOT matrix must be represented as a matrix that transforms 3-qubit states (containing the operation for the first to the third qubits out of the four), leaving the second qubit as it is, and then must be tensored with the identity matrix I_2 of degree 2 (i.e. 2-by-2 matrix). Therefore we also take into account cases when the control qubit and target qubit are not “adjacent”, other qubits being between the control and the target qubit. The author implemented a function that generates a CNOT matrix with similar level of errors that can be applied for any n -qubit states, with the first qubit set to the control qubit and the n -th the target².

Let us first consider the case when the target qubit comes *after* the control qubit. Let m denote the index of the target qubit and suppose the first qubit is set to the control qubit. This function takes as arguments the index of the target qubit m and the total number of qubits (again, m) involved in *this CNOT operation*, and yields the matrix $CNOT_{1,m} \in M_{2^m}(\mathbb{R})$

$$CNOT_{1,m} = \begin{pmatrix} 0.95 & \frac{1-0.95}{n_0} & \dots & \frac{1-0.95}{n_0} & \frac{1-0.95}{n_0} & \frac{1-0.95}{n_0} \\ \frac{1-0.95}{n_0} & 0.95 & \dots & \frac{1-0.95}{n_0} & \frac{1-0.95}{n_0} & \frac{1-0.95}{n_0} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{1-(0.20+0.75)}{\frac{n_0-1}{1-(0.20+0.75)}} & \dots & 0.20 & 0.75 & \frac{1-(0.20+0.75)}{\frac{n_0-1}{1-(0.20+0.75)}} & \frac{1-(0.20+0.75)}{\frac{n_0-1}{1-(0.20+0.75)}} \\ \frac{1-(0.20+0.75)}{\frac{n_0-1}{1-(0.20+0.75)}} & \dots & 0.75 & 0.20 & \frac{1-(0.20+0.75)}{\frac{n_0-1}{1-(0.20+0.75)}} & \frac{1-(0.20+0.75)}{\frac{n_0-1}{1-(0.20+0.75)}} \\ \frac{1-(0.20+0.75)}{\frac{n_0-1}{1-(0.20+0.75)}} & \dots & \frac{1-(0.20+0.75)}{\frac{n_0-1}{1-(0.20+0.75)}} & \frac{1-(0.20+0.75)}{\frac{n_0-1}{1-(0.20+0.75)}} & 0.20 & 0.75 \\ \frac{1-(0.20+0.75)}{\frac{n_0-1}{1-(0.20+0.75)}} & \dots & \frac{1-(0.20+0.75)}{\frac{n_0-1}{1-(0.20+0.75)}} & \frac{1-(0.20+0.75)}{\frac{n_0-1}{1-(0.20+0.75)}} & 0.75 & 0.20 \end{pmatrix} \quad (4.2.2.3)$$

²Note that, when we have still other qubits that are not involved in CNOT *after* the target qubit, then we only need to take the tensor product of the CNOT matrix given and the identity matrix of the same degree as the number of the rest of the qubits placed after the target qubit. If we assume there are n qubits in total and the first qubit is set to the control qubit and the n -th qubit is to the target, with of course $1 < n < m$, then the desired CNOT matrix is $CNOT_{1,m} \otimes I_{n-m}$, where I_{n-m} denotes the identity matrix of degree $n - m$.

where $n_0 = 2^m - 1$. The (i, j) entry of the matrix above, a_{ij} , can be expressed as

$$a_{ij} = \begin{cases} 0.95 & \text{if } i = j \text{ and } 1 \leq i \leq 2^{m-1} \\ \frac{1-0.95}{n_0} & \text{if } i \neq j \text{ and } 1 \leq i \leq 2^{m-1} \\ 0.75 & \text{if } i \equiv 0 \pmod{2} \text{ and } i = j - 1 \text{ and } 2^{m-1} < i \leq 2^m \\ 0.75 & \text{if } i \equiv 1 \pmod{2} \text{ and } i - 1 = j \text{ and } 2^{m-1} < i \leq 2^m \\ \frac{1-(0.20+0.75)}{n_0-1} & \text{if } i \neq j \text{ and } 2^{m-1} < i \leq 2^m \end{cases} \quad (4.2.2.4)$$

Now let us consider the case when the target qubit is placed *before* the control qubit. Let m denote the index of the *control* qubit and suppose the first qubit is set to the target qubit (notice that the relation is reversed here). This function takes as arguments the index of the control qubit m and the total number of qubits (again, m) involved in *this CNOT operation*, and yields the matrix $CNOT_{m,1} \in M_{2^m}(\mathbb{R})$ defined in the following manner. First let \tilde{a}_{ij} denote the (i, j) entry of the matrix $CNOT_{m,1}$. Next, consider the permutation σ that acts on the set of indices $0, 1, \dots, 2^m - 1$, defined as

$$\sigma(i) \equiv \begin{cases} (-d_1)d_2 \dots d_m & \text{if } d_m \text{ is } 1 \\ d_1d_2 \dots d_m & \text{otherwise} \end{cases} \quad (4.2.2.5)$$

where $d_1d_2 \dots d_m$ denotes the binary representation of the index i and $-d_1$ is the negation of d_1 . Now \tilde{a}_{ij} is defined using σ as ³

$$a_{i\sigma(j)} = \begin{cases} 0.95 & \text{if } i = j \text{ and } i \equiv 0 \pmod{2} \\ \frac{1-0.95}{n_0} & \text{if } i \neq j \text{ and } i \equiv 0 \pmod{2} \\ 0.75 & \text{if } i = j \text{ and } i \equiv 1 \pmod{2} \\ \frac{1-0.75}{n_0} & \text{if } i \neq j \text{ and } i \equiv 1 \pmod{2} \end{cases} \quad (4.2.2.6)$$

where $n_0 = 2^m - 1$ as in the previous case.

4.3 Tomography Module

Tomography module takes count distributions that have come from God Channel module and conducts tomography. This module returns the fidelity between the reconstructed state and the actual state, and the fidelity between the reconstructed state and the ideal state.

4.4 Simulator Module

Simulator module first loads the configuration file from its current directory to load the settings regarding the set of simulations such as the minimum and maximum of the total number of measurements, the minimum and maximum number of purifications

³Note that the set $\{(i, \sigma(j)) \mid 1 \leq i, j \leq n\}$ is equal to the set $\{(i, j) \mid 1 \leq i, j \leq n\}$ when σ is a permutation of elements in the set $\{1, 2, \dots, n\}$. When j runs 1 through n , so does $\sigma(j)$.

conducted, etc. The module then stores the table of measurement results, pass it to the Tomography module, received the reconstructed density matrix and the information of fidelities, and finally it saves the data into an external file for reference.

Chapter 5

Evaluation

5.1 Criteria for Evaluation

Fidelities that ensure proper operation of applications using Bell pairs vary in general. Since this project is not intended to limit the scope of the conclusion to this or that particular application after the fidelity estimation, we need to establish a set of criteria that define “sufficiently high” fidelities. We define the fidelity of a given Bell state to be *sufficiently high* if it is either above 0.99 or above 0.999. Either of these two different criteria will be used each time we take a look at data.

Another set of criteria are still needed to assess to which extent the goal of the project has been fulfilled. We consider the amount of time for two nodes to take in order to be convinced that the fidelity of the Bell state they hold is either over 0.99 or 0.999 with standard error in the estimation under 0.01 or 0.001, respectively.

The configurations for evaluation fall into two categories: the case when no error is present and when CNOT gate errors are present.

5.2 Evaluation for Full State Tomography

Below is the plotted data of the actual fidelities and the reconstruction fidelities with the varying number of total measurements conducted for tomography (Figure 5.1). The data used here is derived from an actual set of experimental data that was provided in the paper [1], while the tomography was (of course) done in software.

The horizontal axis represents the number of measurements. In the vertical axis the actual state fidelities are drawn in red, with the corresponding labeled axis with numbers on the right side of the graph; the reconstruction fidelities are in black with the corresponding axis on the left. Now the statement made at Section 2.5 is verified from the graph quantitatively.

The reconstruction fidelity being constantly above 0.999 requires over 60,000 measurements, with being above 0.99 still demanding over 3,000 measurements. If we assume Bell pair creation rate is 10 per second, the reconstruction fidelity above 0.999 needs more than an hour and a half. This is obviously an unacceptable amount of time for tomography to take for preparation of an entangled state. In the rest of this Section we first consider the case where purification is embedded into the process and

how to circumvent difficulties arising when errors in CNOT gates are present; then we investigate possibilities of reducing the number of measurements (hence the amount of time) needed to prepare an entangled state.

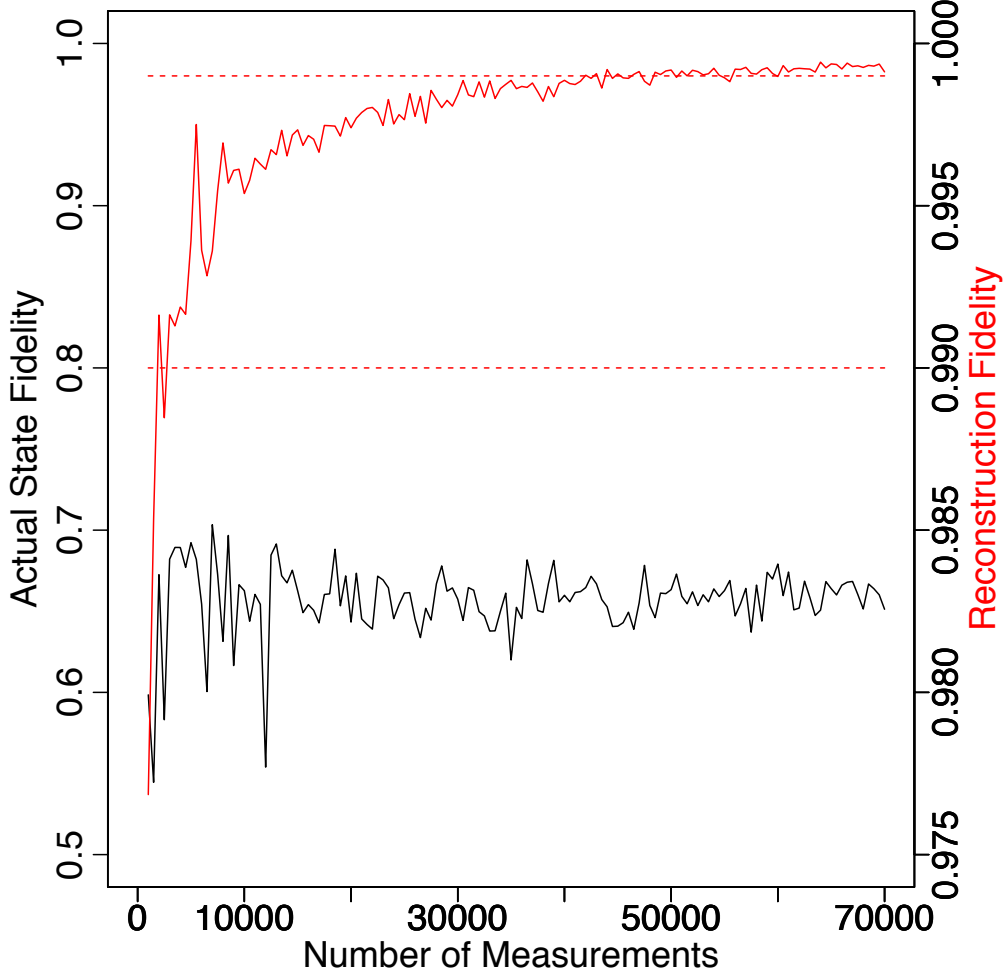


Figure 5.1: Relationship between Actual Fidelity and Reconstruction Fidelity based on actual experimental data provided by Kwiat et. al., with no purification conducted.

5.2.1 Behavior of Actual Fidelities with Purifications

Since our goal is to provide the most efficient scheme of state reconstruction for purification-embedded link creation, it is natural to consider cases where purification is conducted a number of times before tomography. First let us consider the case where the target state suffers only bit flip errors. In particular, let us suppose here that the state in question, denoted by ρ , is

$$\rho = 0.8 |\Phi^+\rangle \langle \Phi^+| + 0.2 |\Psi^+\rangle \langle \Psi^+| \quad (5.2.1.1)$$

in density matrix form¹. Fixing the state to this ρ , simulations were conducted with the number of purifications varying from 1 to 5, and after each of the purifications, fidelity estimation using full state tomography followed.

The first two graphs (Figure 5.3 and 5.4) below indicate the relations between the actual fidelity and the number of purifications conducted varying from 1 to 5, with Figure 5.3 showing the case without gate errors and Figure 5.4 showing the case *with* CNOT gate errors present. The x-axis represents the number of purifications conducted and the y-axis the actual fidelity.

As is seen, the blue line in Figure 5.3 increases (almost) smoothly to 1 as the number of purifications increases, whereas the other one in Figure 5.4 stagnates around somewhere of fidelity 0.8 and begins to show slight fluctuation. The former graph shows evidence that the method of purification works as expected in literature under the assumption that the gates involved have no error. On the other hand, the stagnation and fluctuation in the latter graph can be explained using the following fact: imperfect CNOT gates mix *phase flip errors* even when the initial Bell pair has only bit flip errors. Following the criteria in Section 5.1, purification with imperfect CNOT gates can *never* lift fidelities of the state up to the point of “sufficiently high”.

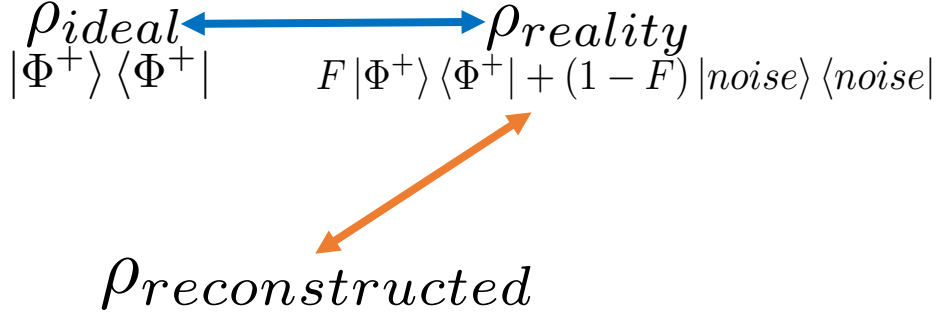


Figure 5.2: Diagram of two types of fidelities: the blue and orange arrows correspond to the arrows of their respective color in subsequent graphs

¹Recall that the term $0.2 |\Psi^+\rangle \langle \Psi^+|$ in Equation (5.2.1.1) is called bit flip error.

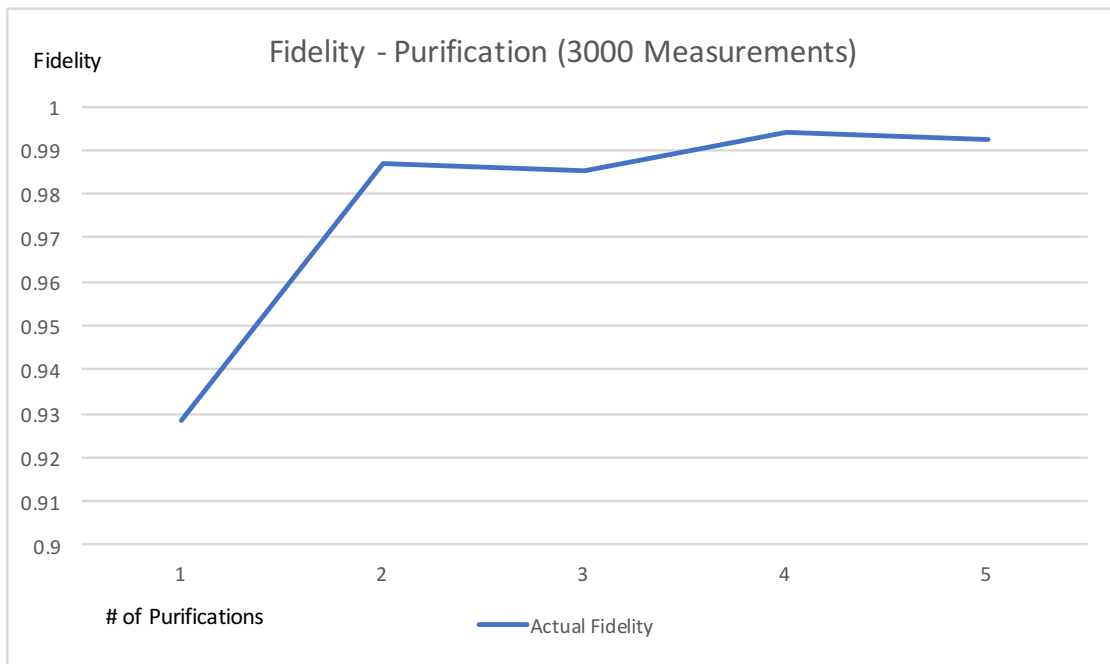


Figure 5.3: Relations between the actual fidelity and the number of purifications with no gate errors: the fidelity smoothly approaches to 1.

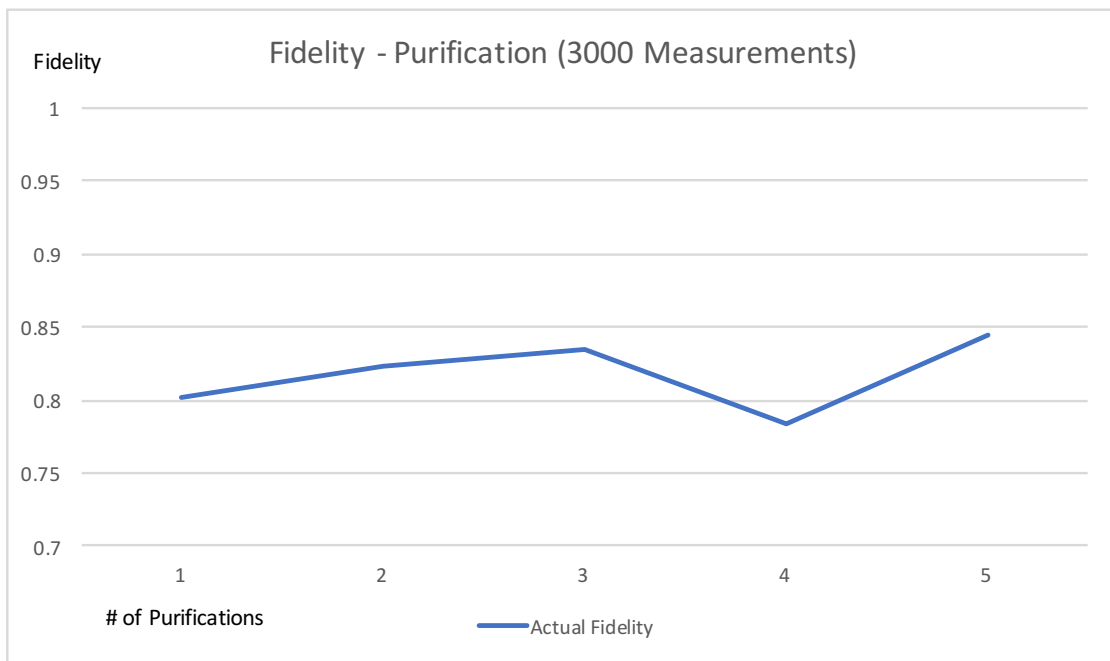


Figure 5.4: Relations between the actual fidelity and the number of purifications with CNOT gate errors present: the fidelity stagnates between 0.8 and 0.9.

5.2.2 Behavior of Reconstruction Fidelities with Purifications

The graphs below (Figure 5.5 and 5.6) are the relations between the reconstruction fidelity and the number of purifications conducted, each drawn from the same set of simulated data as above. The x-axis represents the number of purifications conducted and the y-axis the reconstruction fidelity. The first one is obtained from the case without CNOT gate errors and the second one from the case with CNOT errors.

In general, reconstruction fidelities are expected to approach 1 as the number of measurements (which is not varying in these graphs) increases. It is a question of worth asking whether reconstruction fidelities depend on the actual fidelities themselves of the target state or not. The graphs might show some hints: in the first graph the orange line (reconstruction fidelity) increases as the number of purifications increases. This might suggest that higher actual fidelities lead to higher reconstruction fidelities. This suggestion is not inconsistent if taking into account the second graph, since the fluctuations of the actual fidelities when CNOT gate errors are present seem to make reasonable the fluctuations in the reconstruction fidelities.

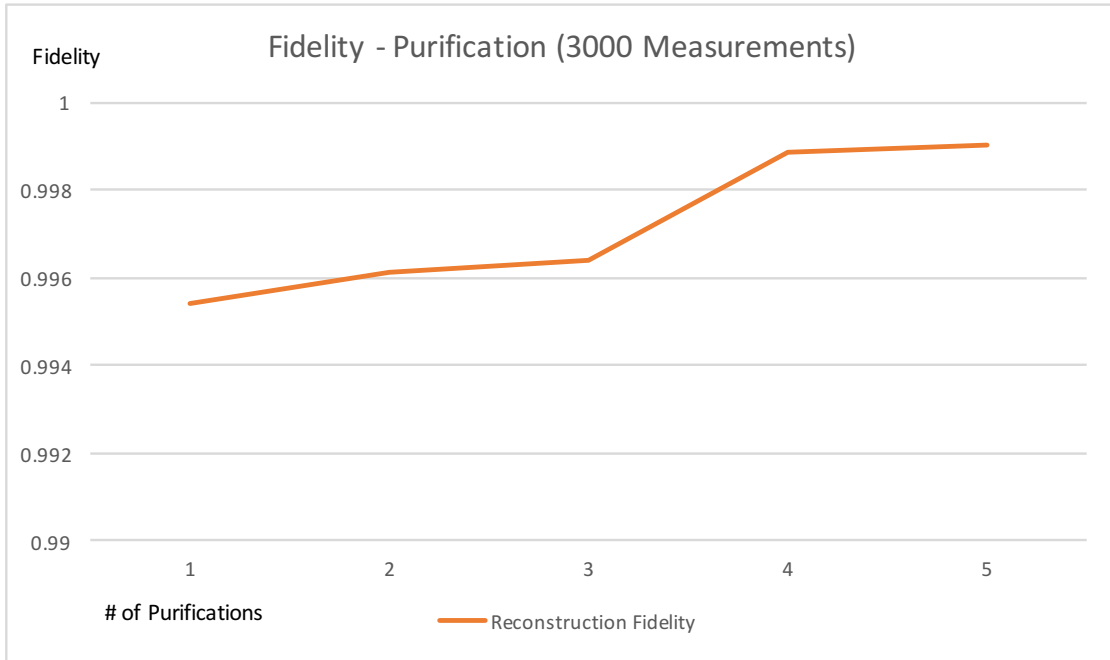


Figure 5.5: Relations between the reconstruction fidelity and the number of purifications with no gate errors: the reconstruction fidelity increases as the actual fidelity increases

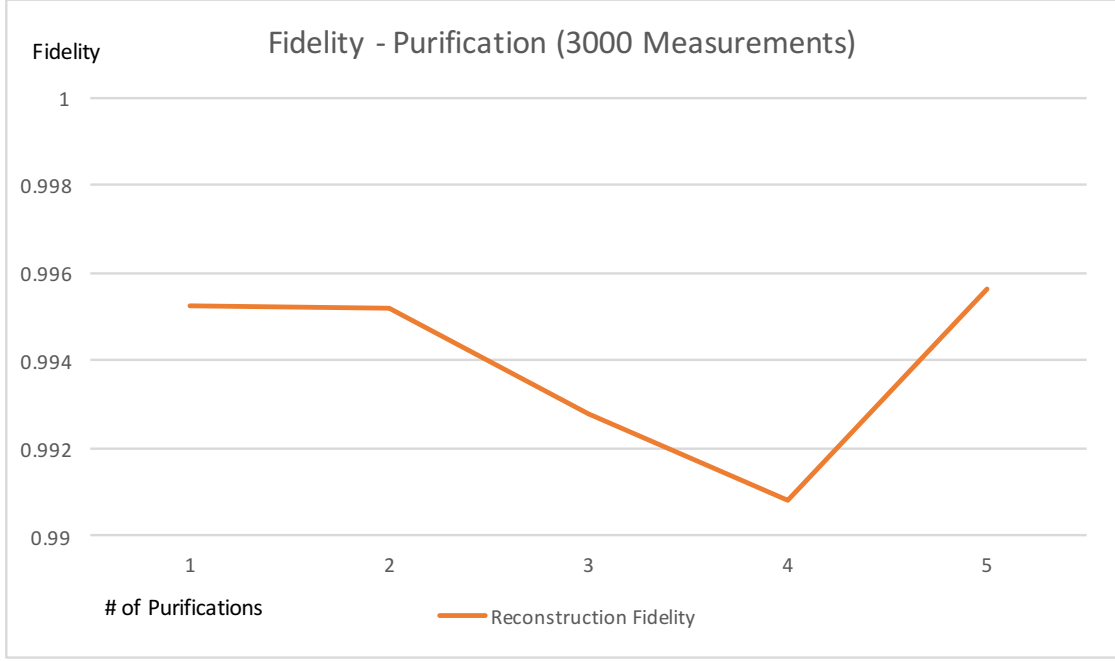


Figure 5.6: Relations between the reconstruction fidelity and the number of purifications with CNOT gate errors present: the reconstruction fidelity also fluctuates as the actual fidelity does.

5.3 Evaluation for the Proposed Fidelity Estimation

In this section, we will see what advantages the proposed fidelity estimation method has over the full state tomography. We have already seen that how the proposed method is realized in Section 3.3. Throughout this section neither measurement errors nor any gate errors are assumed to be present.

We make assumptions for the evaluation: the values $A = 0.7$ and $B = C = D = 0.1$ is used for the initial state $\rho = A|\Phi^+\rangle\langle\Phi^+| + B|\Psi^+\rangle\langle\Psi^+| + C|\Psi^-\rangle\langle\Psi^-| + D|\Phi^-\rangle\langle\Phi^-|$. Before showing the evaluation, we first investigate the performance of the full state tomography with the identical set of assumptions regarding the initial state and whether the errors are present or not.

Figure 5.7 shows the variances of the actual fidelity and the reconstruction fidelity as the number of measurements increases. The horizontal axis represents the number of measurements taken for the state ρ and the vertical axis fidelity. As is more easily seen in the graph in Figure 5.8, around 3000 measurements are needed to reach to the reconstruction fidelity 0.99, and some more than 50,000 measurements enable the reconstruction fidelity above 0.999.

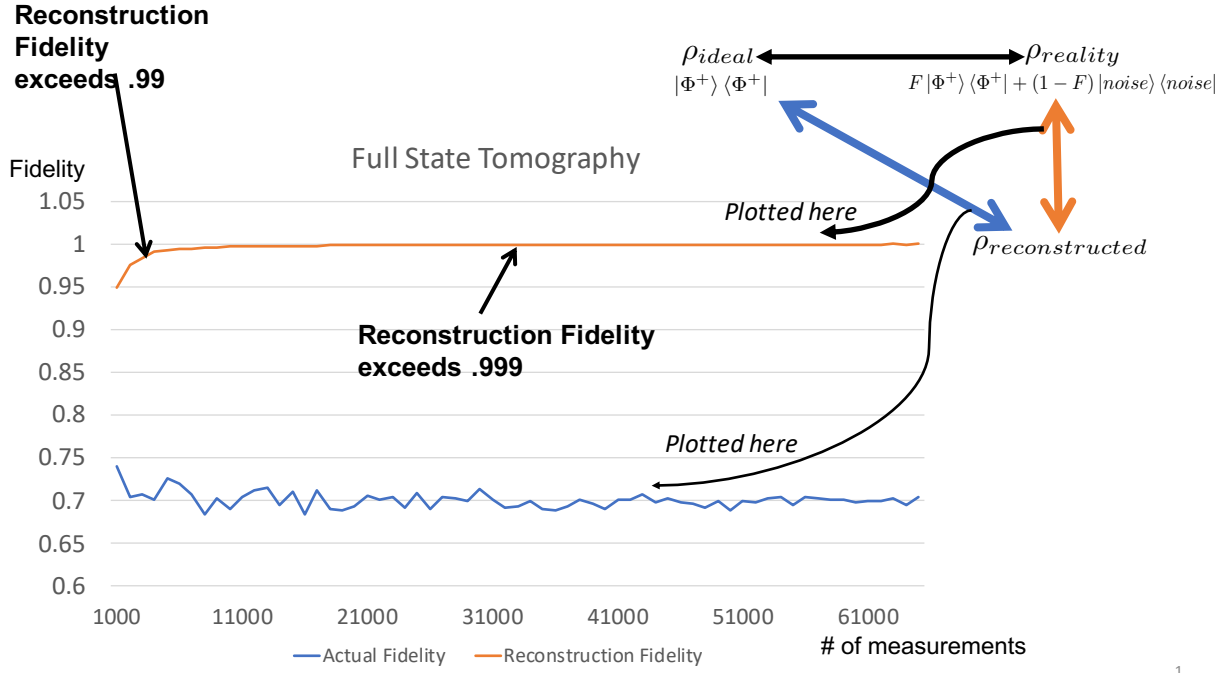


Figure 5.7: The state reconstruction performance for $\rho = 0.7|\Phi^+\rangle\langle\Phi^+| + 0.1|\Psi^+\rangle\langle\Psi^+| + 0.1|\Psi^-\rangle\langle\Psi^-| + 0.1|\Phi^-\rangle\langle\Phi^-|$ with full state tomography employed.

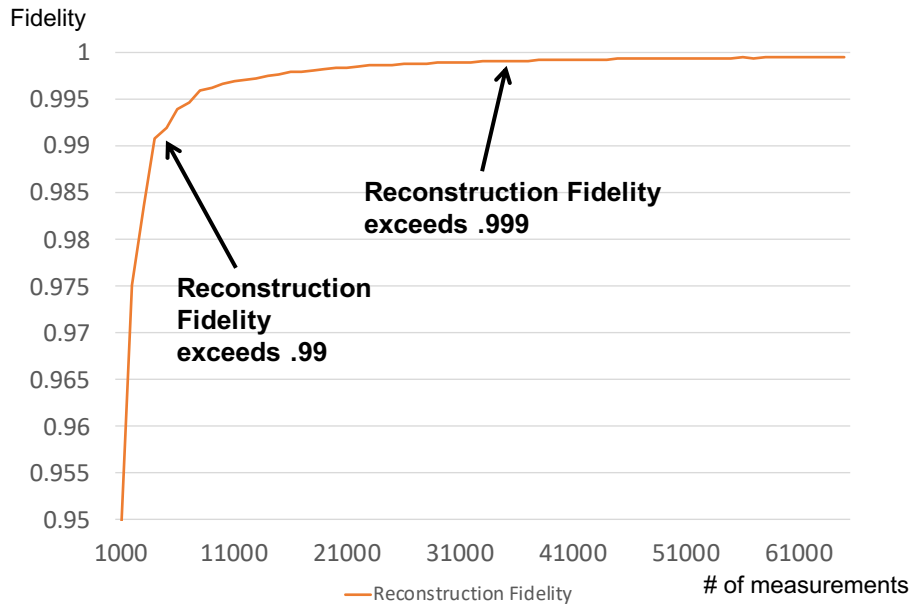


Figure 5.8: The state reconstruction performance for $\rho = 0.7|\Phi^+\rangle\langle\Phi^+| + 0.1|\Psi^+\rangle\langle\Psi^+| + 0.1|\Psi^-\rangle\langle\Psi^-| + 0.1|\Phi^-\rangle\langle\Phi^-|$ with full state tomography employed. The scale of the vertical axis is adjusted to focus on the reconstruction fidelity.

Now let us probe into the performance of the proposed method in question. As drawn in Figure 5.9, the proposed fidelity estimation method exhibits remarkable sta-

bility in the actual fidelities, with a slightly slower convergence in estimation of the fidelity.

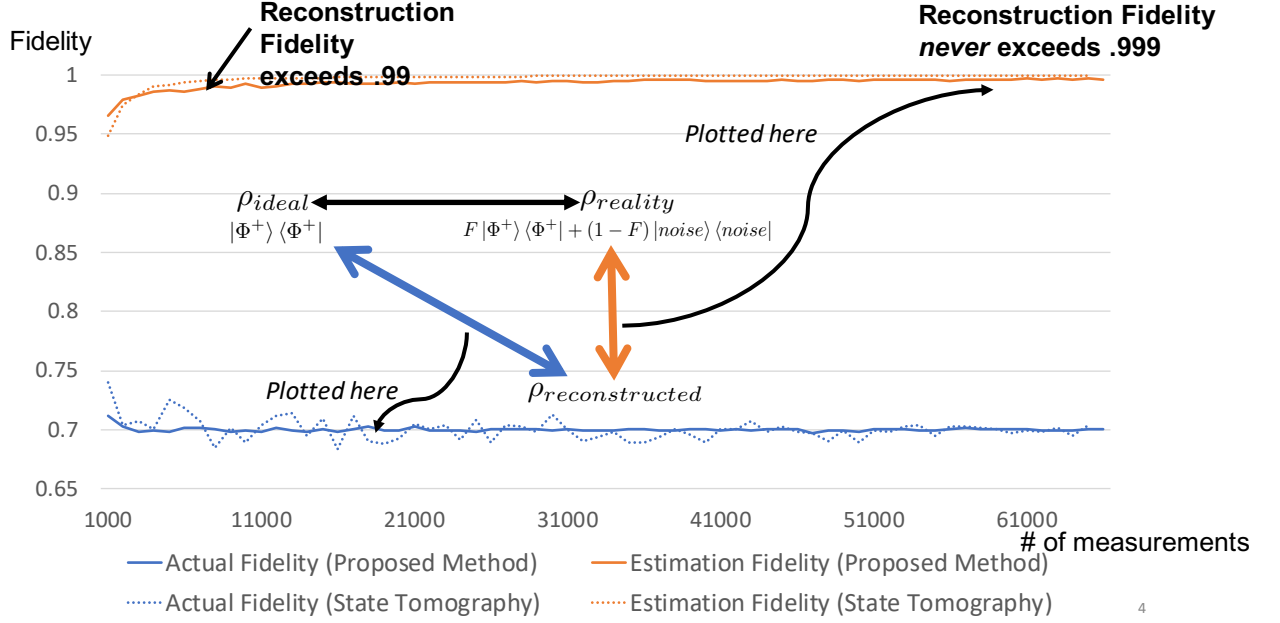


Figure 5.9: The state reconstruction performance for $\rho = 0.7|\Phi^+\rangle\langle\Phi^+| + 0.1|\Psi^+\rangle\langle\Psi^+| + 0.1|\Psi^-\rangle\langle\Psi^-| + 0.1|\Phi^-\rangle\langle\Phi^-|$ with the proposed method employed. The solid line represents the data of the proposed method, while the dotted line correspond to the data of full state tomography.

The more detailed data for the actual fidelity and the reconstruction fidelity are plotted in Figure 5.10 and 5.11.

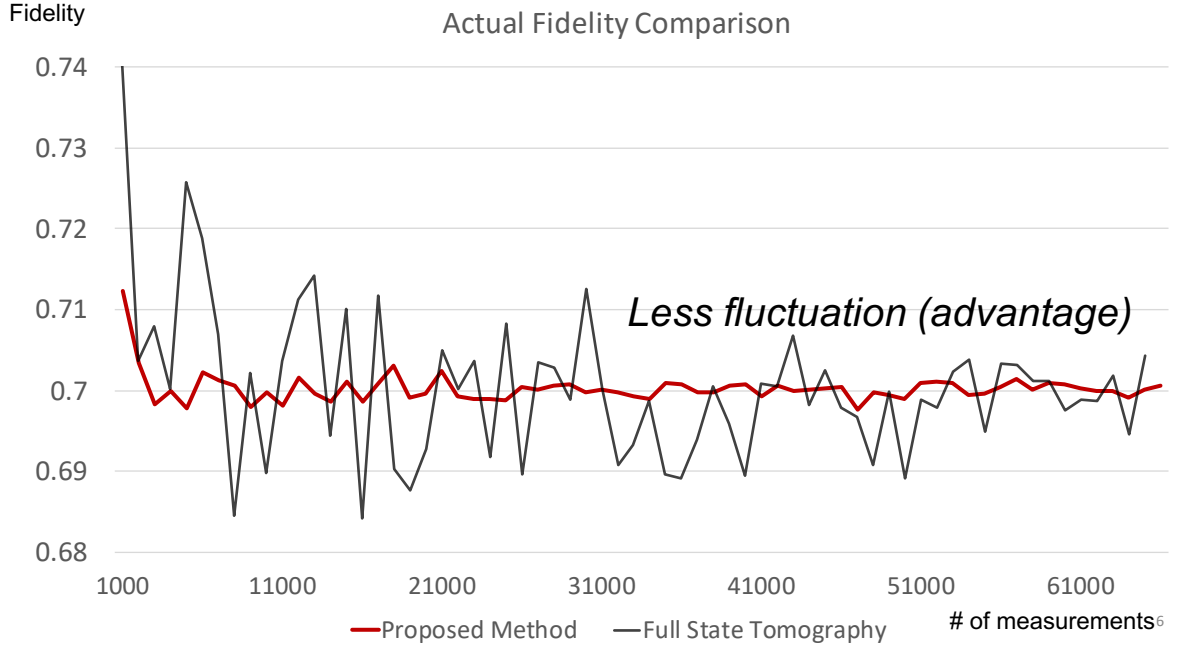


Figure 5.10: The variance of the actual fidelities for $\rho = 0.7 |\Phi^+\rangle \langle \Phi^+| + 0.1 |\Psi^+\rangle \langle \Psi^+| + 0.1 |\Psi^-\rangle \langle \Psi^-| + 0.1 |\Phi^-\rangle \langle \Phi^-|$ with the proposed method employed. The red line indicates the actual fidelities estimated using the proposed method, and the black line those from full state tomography. The proposed method has an obvious advantage of less fluctuation, compensating for a slight deterioration in the reconstruction fidelity.

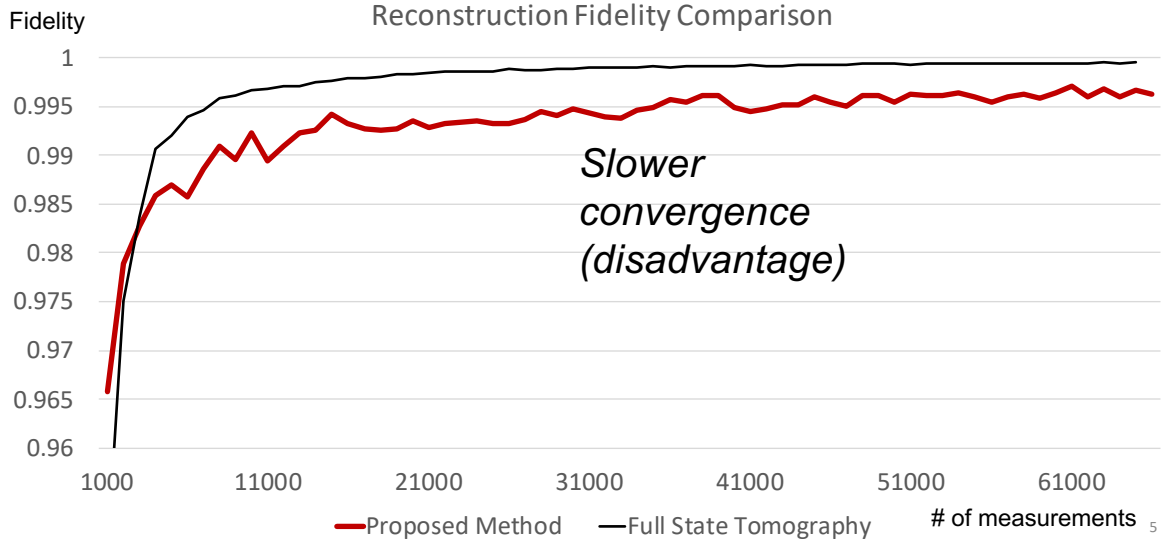


Figure 5.11: The variance of the reconstruction fidelities for $\rho = 0.7|\Phi^+\rangle\langle\Phi^+| + 0.1|\Psi^+\rangle\langle\Psi^+| + 0.1|\Psi^-\rangle\langle\Psi^-| + 0.1|\Phi^-\rangle\langle\Phi^-|$ with the proposed method employed. The red line indicates the reconstruction fidelities estimated using the proposed method, and the black line those from full state tomography. A slight deterioration in the reconstruction fidelity is much smaller than the large fluctuation of the actual fidelities present while using full state tomography, and hence compensated for.

The deviations of the fidelities in full state tomography from the fidelity 0.7, to which the estimation is expected to converge, are often around 0.1, as is seen in Figure 5.10, while the deviations in the proposed method are in most cases below 0.02. On the other hand, as in Figure 5.11, the convergence of the reconstruction fidelities, in the case the proposed method is used, is slightly slower; in particular, the reconstruction fidelities in the proposed method never exceed 0.999. However, the differences of the reconstructed fidelities between the proposed method and full state tomography are in most cases below 0.01. Thus, the difference in reconstruction fidelities is generally much smaller than the observed fluctuation of the actual fidelities in full tomography. In conclusion, the proposed method proves to be more reliable in estimating fidelities because of the smaller fluctuation in the actual fidelities, compensating for the slight deterioration in convergence of reconstruction fidelity.

Chapter 6

Conclusion

6.1 State Reconstruction

For the state reconstruction performance, if full state tomography is employed, then Figure 5.1 in Chapter 5 implies that the number of measurements necessary exceeds 50,000 in order to reach the reconstruction fidelity of 0.999, with the number still above several thousand to reach 0.99. This requires the respective numbers of Bell pairs that are successfully created and measured. In Hucul et. al.'s research [15], for example, 4.5 Bell pairs per second have successfully been measured. Another experiment by a group of researchers in China [16] succeeded in measuring 1.1 Bell pairs per second at a distance of approximately 1200 kilometers¹. With this magnitude of Bell pair generation rates, it takes more than ten thousand seconds, or well above two hours, to repeat 50,000 of Bell pair creation and measurements; to conduct several thousand such procedures still requires a dozen of minutes. This is clearly an unacceptable amount of time for a single bootstrap.

In addition, this implies that changes to the environment faster than this amount of time cannot be compensated for by tomography, and hence must be handled at a lower level. That is, deterioration of states caused by environmental changes within the interval of time smaller than the tomography is done cannot be detected by tomography.

6.2 Purification

When CNOT gates have no error, purification leads to smooth improvement in actual fidelities. The smoothness has also been seen for the reconstruction fidelities. Contrary to the no-error case, however, purification seems to lift the actual fidelity asymptotically to somewhere considerably lower than 1. It thus could be concluded (at least from all the data obtained so far in Chapter 5) that phase flip errors cause persistent deterioration in fidelities that remain to a certain degree after a set of purifications. If the fidelity merely converges to around 0.8, then it is very hard for the resultant Bell pair to be used in applications. To circumvent this problem, some countermeasure, e.g.

¹There are still other researches that managed entanglement creation between some distance (e.g. [17] or [18]).

an enhanced purification method, should be devised.

Furthermore, given that raising fidelities is such a hard job as to call for sophisticated methods, and that whatever fidelity improvement method is used, it is *state estimation* in some form that evaluates those methods' performance, efficient state estimation is really a keystone for realizing quantum networking in reality.

6.3 Proposed Method for Fidelity Estimation

Aside from the resemblance of the circuit involved to the one used in purification, the method has a great merit in that it estimates fidelities more reliably. In other words, the fidelity estimation with full tomography is less reliable due to the great fluctuation in actual fidelities.

6.4 Future Work

While the performance of the proposed fidelity estimation method is advantageous, the simulated experiment has been done without any measurement errors or gate errors. Given that we always have both types of errors in reality, an extended simulation with errors present will resemble better reality, thereby yielding more realistic evaluation of the method. This will be a problem of greatest importance at hand. Another future work can be to devise ways to realize both fidelity estimation and purification at a time, as the circuit involved in the method has another remarkable characteristic of being identical to the circuit that is used for purification (except for some of the measurement bases involved)! The proposed method will be much more advantageous if it can combine both fidelity estimation and purification, thereby greatly reducing the total number of Bell pairs consumed to initiate a quantum communication.

Acknowledgements

First and foremost, I would like to express my most heartfelt gratitude to Associate Professor Rodney Van Meter at Keio University who, despite my procrastination, has ever been providing the best possible supervision on every aspect of my research, as well as guiding me towards plenty of valuable experiences such as presentations at research workshops. It has been a pleasure to be a student of his.

I also thank very much Project Research Associate Satoh Takahiko for his long-term and persistent supervision, through which I gained a variety of new perspectives to look at research topics. I appreciate Doctor Shota Nagayama so much, who has repeatedly helped, supported and guided me on this project, often remotely; at many of such occasions he should have been busier, in fact.

I would like to express great appreciation for other members of AQUA; for Takaaki Matsuo, who has always been more than willing to support and encourage me in any aspect. The on-time submission of the thesis is thanks to the LaTeX template he gave me; for Shinnosuke Ozawa, who has always been cheerful and willing to do jobs in AQUA. It has been nice to talk to him; for Shin Nishio, who has a great passion for a variety of topics such as physics, computer science and mathematics, stimulating my motivation for research; and for Yumeka Kajiwara, who blew a refreshing wind into our group.

Finally, I thank all members of Murai and Tokuda Laboratory, many of whom I enjoyed talking and discussing with, and gained insights from, for all the guidance and supports.

Bibliography

- [1] J.B. Altepeter, E.R. Jeffrey, and P.G. Kwiat. Photonic State Tomography. *Advances In Atomic, Molecular, and Optical Physics*, 52:105–159, 2005.
- [2] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Review*, 41(2):303–332, Jan 1999.
- [3] Peter W. Shor and John Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Physical Review Letters*, 85(2):441–444, Jul 2000.
- [4] Artur K. Ekert. Quantum cryptography based on bell’s theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.
- [5] Rodney Van Meter. *Quantum Networking*. ISTE Ltd, 2014.
- [6] Anocha Yimsiriwattana and Samuel J. Lomonaco. Distributed quantum computing: A distributed Shor algorithm. Mar 2004.
- [7] E. Knill. Quantum computing with realistically noisy devices. *Nature*, 434(7029):39–44, Mar 2005.
- [8] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger. Experimental one-way quantum computing. *Nature*, 434(7030):169–176, Mar 2005.
- [9] Takafumi Oka, Takahiko Satoh, and Rodney Van Meter. A Classical Network Protocol to Support Distributed Quantum State Tomography. In *2016 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6. IEEE, dec 2016.
- [10] Charles H. Bennett, Gilles Brassard, Claude Crepeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.
- [11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.
- [12] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. “event-ready-detectors” bell experiment via entanglement swapping. *Phys. Rev. Lett.*, 71:4287–4290, Dec 1993.

- [13] Rodney Van Meter, Joe Touch, and Clare Horsman. Recursive quantum repeater networks. *Progress in Informatics*, (8):65–79, Mar 2011.
- [14] J L O’Brien, G J Pryde, A G White, T C Ralph, and D Branning. Demonstration of an all-optical quantum controlled-NOT gate. *Nature*, 426:264, nov 2003.
- [15] D Hucul, IV Inlek, G Vittorini, C Crocker, S Debnath, SM Clark, and C Monroe. Modular entanglement of atomic qubits using photons and phonons. *Nature Physics*, 11:37–42, 2014.
- [16] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, Guang-Bing Li, Qi-Ming Lu, Yun-Hong Gong, Yu Xu, Shuang-Lin Li, Feng-Zhi Li, Ya-Yun Yin, Zi-Qing Jiang, Ming Li, Jian-Jun Jia, Ge Ren, Dong He, Yi-Lin Zhou, Xiao-Xiang Zhang, Na Wang, Xiang Chang, Zhen-Cai Zhu, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.
- [17] Bas Hensen, H Bernien, AE Dreau, A Reiserer, N Kalb, MS Blok, J Ruitenberg, RFL Vermeulen, RN Schouten, C Abellan, et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.
- [18] Hou Shun Poh, Siddarth K. Joshi, Alessandro Cere, Adan Cabello, and Christian Kurtsiefer. Approaching Tsirelson ’ s bound in a photon pair experiment. *Phys. Rev. Lett.*, 115:180408, Oct 2015.