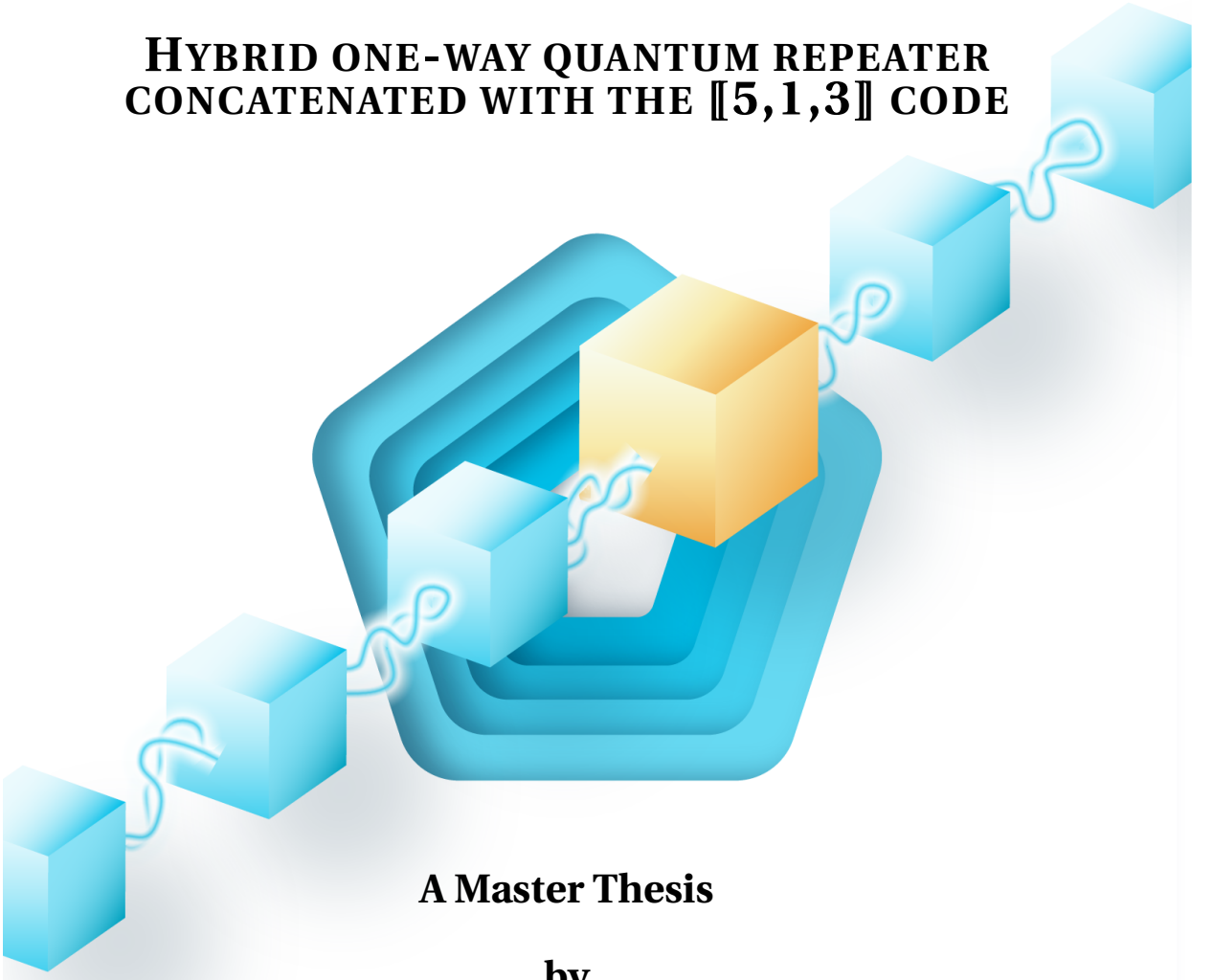
HYBRID ONE-WAY QUANTUM REPEATER CONCATENATED WITH THE ⟦5,1,3⟧ CODE



A Master Thesis

by

Kah Jen Wo

TU Delft Delft University of Technology

QuTech

HYBRID ONE-WAY QUANTUM REPEATER CONCATENATED WITH THE ⟦5,1,3⟧ CODE

Master Thesis

To obtain the degree of Master of Science
at Delft University of Technology, the Netherlands.
To be defended publicly on Tuesday, 12th April 2022, at 10:00

by

Kah Jen Wo

Bachelor of Science in Applied Physics,
City University of Hong Kong, Hong Kong SAR,
born in Kuala Lumpur, Malaysia.

The thesis committee consists of:

Prof. dr. J. Borregaard,	QuTech, Delft University of Technology (*supervisor*)
Prof. dr. B.M. Terhal,	QuTech, Delft University of Technology
Prof. dr. E. Greplová,	Quantum Nanoscience, Delft University of Technology

Project start date: 1st September 2021

Project end date: 31st March 2022

Cover design by: K.J. Wo

ISBN 978-94-6366-536-0

An electronic version of this master thesis is available at
https://repository.tudelft.nl/.

ABSTRACT

An improvement to the existing one-way quantum repeater network using the tree cluster state as the quantum error correcting code is presented. Namely, the $[\![5,1,3]\!]$ quantum error correcting code is introduced as an outer code while the tree code becomes the inner code. Using this approach, we present a novel hybrid one-way quantum repeater architecture with more than one type of quantum repeater in its network. We considered both the non-fault-tolerant and fault-tolerant variants of the $[\![5,1,3]\!]$ code in our study of the hybrid repeater network. A novel improvement to the $[\![5,1,3]\!]$ code is also presented, where we also consider using it for quantum erasure correction. Additionally, we introduced a novel method of extrapolating an approximate fidelity of a quantum state after arbitrary applications of a noisy quantum channel. With these, we see magnitudes of order of boost in the resulting secret key rate in our approach.

ACKNOWLEDGEMENTS

This thesis is the culmination of countless hours of work which I have put into and it would not have been possible if not for my supervisor Prof. Johannes Borregaard whose unparalleled guidance and support has only helped me in my research. The weekly meetings and discussions we had were nothing but an absolute intellectual treat where I was given intriguing questions to consider. This research was also made possible with resources and a scholarship from QuTech.

Together with Prof. Johannes, I also had Prof. Anders Sørensen, Prof. Liang Jiang, and Dr. Filip Rozpędek to thank for the wonderful bi-weekly meetings which provided priceless insights in the field of quantum repeaters, some of which even ended up in this thesis. The most notable moment is when they helped me in forming the secret key rate expression for the hybrid repeater architecture used in the thesis — something that I am immensely thankful for.

I would also like to thank everyone in the Borregaard group for the great weekly meetings which provided me with plenty of deep questions to ponder about. Thanks especially to Yunzhe Zheng for accompanying me in campus while we worked on our own thesis projects.

I also owe a huge debt of gratitude to both Johannes Borregaard and Fenglei Gu for helping with editing this thesis. Thank you for taking your time, patience, and advice.

A huge thank you to my friends, Ali, Amis, Andrew, and Madhava for being there and distract me from my work when I needed it. A huge thank you to my family and my partner, who had given me only unconditional love and support despite being physically so far away.

Thank you for everything,
Kah Jen Wo

CONTENTS

1

INTRODUCTION

THE study of quantum physics is a pursuit of far-reaching impact since the development of nearly all modern technologies has always depended on the principles of quantum mechanics. For example, transistors, photovoltaic cells, and lasers are some of the many results of the *first quantum revolution* which occurred last century. These technological inventions have had a massive transformative effect on society and ultimately led us into the *information age*. While the first quantum revolution involved using fundamental quantum mechanics knowledge, the *second quantum revolution*, which we are in the midst of, covers the development of advanced technologies and methods that exploit it even further [1]. The most notable properties of quantum mechanics being leveraged in this revolution are the quantum entanglement and quantum superposition, which led to the possibility of solving problems that are exceedingly difficult to be undertaken by classical computers. Such problems include the simulation of entangled many-body systems [2], prime factorisation of large integers [3, 4], and the transmission of secured information [5, 6]. The study related to these quantum mechanics principles is also known as quantum information theory, which in itself is a broad field. Generally, it can be divided into several subfields, including but not limited to:

- Quantum communication [7],
- Quantum sensing [8, 9],
- Quantum computation and simulation [2–4].

Let us now focus on the field of quantum communication, which also encompasses quantum key distribution (QKD), first proposed by Wiesner in 1983 [10]. Since then, many others have built on top of Wiesner's work; e.g., Bennett and Brassard developed the famous BB84 protocol based on Wiesner's *"conjugate observables"* [11]. It is clear that QKD is of great interest since it allows us to guarantee the confidentiality of information transmitted between two or more parties by employing principles of quantum mechanics, e.g., any attempts at intercepting the message become exposed to the communicating parties. The classical counterpart of QKD, however, relies on the fact that the used

encryption schemes are computationally hard to be broken, which implies that there is a non-zero chance of the corresponding encrypted keys being retrospectively broken.

Furthermore, the long-term vision in quantum communication is to establish the *quantum internet* — transmission of quantum signals/qubits, usually in the form of photons, between any two parties on Earth [12]. The establishment of the quantum internet is a significant step in scientific and technological advancement as it enables large-scale distributed quantum computation. However, such a network would have connections between parties/nodes that span large distances, which often are beyond the capabilities of optical fibres in which the photonic qubits travel through. This brings us to *quantum repeaters*, which are not only important but also necessary to enable long-distance connections by placing them in-between the communicating parties, dividing the connection into multiple shorter links. This division allows us to circumvent the loss of photons (loss errors) in the optical fibres, which grows exponentially due to attenuation [13].

There have been proposals of quantum repeaters with fundamentally different architectures over the years, each of which handles loss errors and operational errors (errors associated with quantum gate operations) using distinct principles. In fig. 1.1, the quantum repeaters are categorised into three groups, namely, 1^{st}, 2^{nd}, and 3^{rd} generation quantum repeaters [14, 15].

The main challenge of the 1^{st} generation quantum repeaters is that they require quantum memories with long coherence times if the repeaters are far apart from each other due to the slow two-way communication needed for both heralded entanglement generation (HEG) and purification (HEP) [13]. This problem is ameliorated in the 2^{nd} generation quantum repeaters by replacing HEP with quantum error correction (QEC) which requires encoding multiple physical qubits to protect against operational errors [15–17]. Although the need for long coherence time quantum memories has decreased, the 2^{nd} generation quantum repeaters still require operations of significant depth due to encoding and hence have a lower tolerance for relatively high gate errors.

This brings us to the 3^{rd} generation quantum repeaters (also called one-way quantum repeaters) which operates fully under one-way communication with QEC. In this generation, the logical qubits are specifically encoded using a large number of photons under a loss tolerant code [15]. Loss errors that occurred in the optical fibres are corrected in the following repeater station, where the encoded state is decoded and reencoded. Since both loss and operational errors are handled using the one-way QEC scheme, there is no longer a need for long-lived quantum memories, resulting in a significant increase in the distribution rate [14]. Owing to the appealing nature of the 3^{rd} generation quantum repeaters, this class of quantum repeaters would be the focus of this thesis.

In fact, a one-way quantum repeater architecture using the *tree cluster state* encoding as the multi-photon quantum error correcting code that is loss tolerant was recently proposed by Borregaard *et al.* [18]. This approach uses minimal physical resources, i.e., three spins per station, and was able to yield a repeater network of total distance ~ 1000 km while still maintaining relatively high secret key rates provided the error rate in the system is sufficiently low. This feat was achieved despite that the tree cluster state is not fault-tolerant owing to the root qubit of the tree state not being protected against

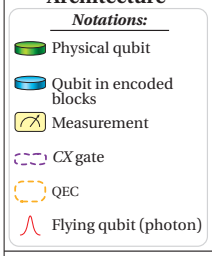
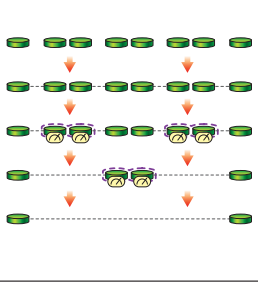
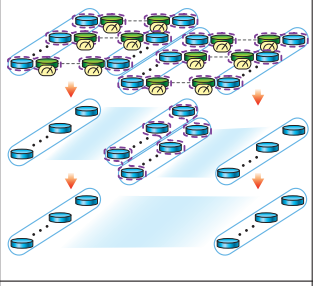
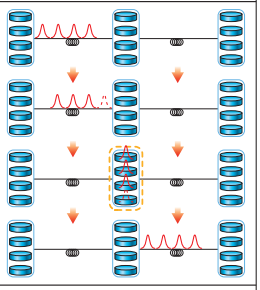
	1st gen. quantum repeater	2nd gen. quantum repeater	3rd gen. quantum repeater
Schematic Architecture 			
Loss Error	HEG (two-way signaling)	HEG (two-way signaling)	QEC (one-way signaling)
Operation Error	HEP (two-way signaling)	QEC (one-way signaling)	QEC (one-way signaling)
Procedure	1. Create entangled pairs over L_0 between adjacent stations. 2. At k^{th} level, connect two pairs over L_k and extend to $L_{k+1}=2L_k$, followed by HEP. 3. After n nesting levels, obtain high-fidelity pair over $L_{\text{tot}}=2^n\times L_0$.	1. Prepare encoded states $\|0_L\rangle$ and $\|+_L\rangle$. 2. Use teleportation-based non-local CX gates to create encoded Bell pairs between adjacent stations. 3. Connect intermediate stations to create long distance encoded Bell pair.	1. Encode information with a block of qubits that are sent through a lossy channel. 2. Use QEC to correct both loss and operation errors. 3. Relay the encoded information to the next station, and repeat steps 2 & 3.

Figure 1.1: Comparison of the three generations of quantum repeaters. Adapted and modified from [14].

operational errors.

The fact that the tree cluster state encoding is not fault-tolerant is an *outstanding challenge*, which means that the one-way quantum repeater scheme using the tree code is limited by the errors introduced by the noisy two-qubit gate operations during QEC. In this thesis, we circumvent this limitation by proposing a novel hybrid one-way quantum repeater scheme in which we take the existing lost tolerant tree code as the inner code and concatenate it with an outer quantum error correcting code that can correct for arbitrary Pauli errors. The $[\![5,1,3]\!]$ code, as well as its fault-tolerant variant that uses flag qubits [19–21], were chosen to be the outer quantum error correcting code in our hybrid repeater scheme. Furthermore, it was shown that any t error correcting code is also a $2t$ erasure/loss correcting code [22, 23] and an experimental protocol for treating the $[\![4,2,2]\!]$ code as a quantum erasure correcting code has been proposed [24]. Utilising these facts, we showed that it is possible to correct for loss errors by applying the same principle on the $[\![5,1,3]\!]$ code. Additionally, we introduced a novel method to extrapolate the approximate fidelity of a quantum state after applying a noisy quantum channel an arbitrary number of times.

Our hybrid repeater approach resulted in a boost in the secret key rate by orders of magnitude relative to state-of-the-art values and extended the theoretical total distance up to 10000 km, albeit at a cost of more physical resources needed. Nevertheless, this aids us in inching the world a step closer towards intercontinental QKD and the quantum internet. The remainder of this thesis is divided into five chapters:

- **Chapter 2** The mathematical preliminaries for this thesis are introduced.

- **Chapter 3** The concept of quantum error correction, fault tolerance using flag qubits, and graph states are introduced and discussed in the context of the $[\![5,1,3]\!]$ code. Noise models that will be used in the hybrid repeater chain are presented. A novel method of extrapolating the approximate fidelity of a state after applying a noisy quantum channel arbitrary number of times is also derived.
- **Chapter 4** The loss tolerant tree cluster state encoding is revisited and a novel protocol for quantum erasure correction using the $[\![5,1,3]\!]$ code is outlined using an existing theorem.
- **Chapter 5** The six-state BB84 protocol from the QKD field is explained briefly in the context of calculating the secret key rate.
- **Chapter 6** The hybrid one-way quantum repeater scheme, which is the *core* of this thesis, is outlined using sequential and parallel scheduling schemes with their required physical resources in mind. The hybrid repeater scheme uses concepts explored throughout the thesis.

2

PRELIMINARIES

2.1. MATHEMATICAL DEFINITIONS

In this section we provide mathematical definitions in linear algebra which are relevant in the context of this thesis so that the readers can be acquainted with them. These definitions are also used ubiquitously in the field of quantum mechanics and quantum information and we assume the readers possess some level of familiarity with the mathematical framework associated with these fields of study. If the readers wish to deepen their knowledge in the preliminaries of quantum mechanics and quantum information, we recommend [25–29].

Definition 2.1.1. $\mathcal{H}$ represents a Hilbert space, in which pure states of a system lie. $|\psi\rangle \in \mathcal{H}$ represents a column vector ("ket") of the Hilbert space $\mathcal{H}$ whereas $\langle\psi| \in \mathcal{H}^\dagger$ represents a row vector ("bra") of the Hilbert space $\mathcal{H}$. $\mathcal{H}^\dagger$ is also known as the *dual* of $\mathcal{H}$.
Let J be an index set and the complex number space be denoted by $\mathbb{C}$. A set of vectors $\{\varphi_j | j \in J\} \subset \mathcal{H}$ is called linearly independent if the following is true for each finite subset $\{\varphi_k | k \in \{0,\ldots,n\}\}$ and $a_k \in \mathbb{C}$:

$$\sum_{k=0}^{n} a_k \varphi_k = 0,$$

which holds only if $a_k = 0, \forall k$.

Definition 2.1.2. $\langle\psi|\phi\rangle \in \mathbb{C}$ denotes the scalar product (also known as inner product) between vectors $|\psi\rangle$ and $|\phi\rangle$.
A basis of $\mathcal{H}$ is formed by a linearly independent set of vectors and each vector of

such set is called a basis vector. A basis satisfying the following condition:

$$\langle \varphi_j | \varphi_k \rangle = \delta_{jk} := \begin{cases} 0, & \text{for } j \neq k \\ 1, & \text{for } j = k \end{cases},$$

is called an orthonormal basis.

Remark. For brevity, we will refer each instance of orthonormal basis in this thesis as basis.

Definition 2.1.3. The adjoint (also called Hermitian conjugate) of an operator O on $\mathcal{H}$ is denoted as $O^\dagger$.

Definition 2.1.4. An operator U on $\mathcal{H}$ is called unitary iff $UU^\dagger = U^\dagger U = I$, where I is the identity matrix.

Definition 2.1.5. An operator H on $\mathcal{H}$ is called Hermitian iff $H = H^\dagger$.

Definition 2.1.6. $\mathrm{Tr}[A]$ denotes the trace of operator A.

Definition 2.1.7. A density matrix $\rho \in \mathcal{H} \otimes \mathcal{H}^\dagger$ can be expressed as a sum of each of its elements as follows:

$$\rho = \sum_j p_j |\varphi_j\rangle\langle\varphi_j|,$$

where p_j is the probability of getting a measurement outcome of $|\varphi_j\rangle$. An operator is called a density matrix if the following conditions are fulfilled:

- The trace of a density matrix is unity, i.e. $\mathrm{Tr}[\rho] = 1$.
- It is a positive matrix, i.e., $\rho > 0$.

Definition 2.1.8. The purity of a state described by a density matrix ρ is defined as $\mathrm{Tr}[\rho^2]$ and it is bounded by the dimension d of $\mathcal{H}$ such that $\mathrm{Tr}[\rho^2] \in [d^{-1}, 1]$. A state described by a density matrix ρ is classified as a pure state only if $\mathrm{Tr}[\rho^2] = 1$ or as a mixed state when $\mathrm{Tr}[\rho^2] < 1$.

Remark. It is possible to represent a pure state with either only *kets* or a density matrix while a mixed state can only be represented with a density matrix.

Definition 2.1.9. Let ρ_{ab} be a density matrix with subspaces a and b. To take the partial trace of ρ_{ab} over a, we write:

$$\mathrm{Tr}_a[\rho_{ab}] = \langle 0|_a \rho_{ab} |0\rangle_a + \langle 1|_a \rho_{ab} |1\rangle_a .$$

Definition 2.1.10. The fidelity between a pure state $|\psi\rangle$ and an arbitrary state $\sigma = |\phi\rangle\langle\phi|$ is defined as:

$$F(|\psi\rangle, \sigma) = \langle\psi|\sigma|\psi\rangle .$$

Remark. The definition of fidelity differs in some literature by a power of 2. For example, in Chapter 9 of Nielsen and Chuang's *Quantum Computation and Quantum Information* textbook [25], the fidelity was taken to be the square root of the overlap between ψ and σ, i.e., $\sqrt{\langle\psi|\sigma|\psi\rangle}$, while in [30] no square root is present. It is thus important to note this discrepancy to avoid confusion. In definition 2.1.10, we follow the convention without the square root.

2.2. QUANTUM INFORMATION

2.2.1. QUBIT

Compared to a classical bit, which can only exist in either state 0 or 1, a qubit exists in a linear superposition of both states within a 2-dimensional complex Hilbert space and can be represented using Dirac notation as:

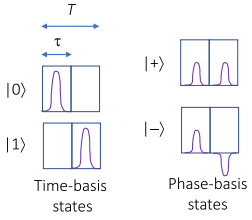
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle , \tag{2.1}$$

where $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$, $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$, and $\alpha, \beta \in \mathbb{C}$ are probability amplitudes and they satisfy the requirement $|\alpha|^2 + |\beta|^2 = 1$, i.e., eq. (2.1) is normalised. This is crucial because $|\alpha|^2$ ($|\beta|^2$) represents the probability of getting a measurement outcome of $|0\rangle$ ($|1\rangle$). The act of measuring the qubit in state $|\psi\rangle$ collapses it into a specific state depending on the measurement outcome.

Example 2.2.1. The time of detection of a photon can be used to encode a qubit as such:

$$|0\rangle \leftrightarrow |e\rangle \text{ and } |1\rangle \leftrightarrow |l\rangle ,$$

where $|e\rangle$ ($|l\rangle$) denotes the *early* (*late*) state. This is also known as the *time-bin* encoding. In practice, the photon pulse is localised within a time-bin of duration $\tau = T/2$. Measurements in the X-basis, i.e., $\{|+\rangle, |-\rangle\}$, correspond to measuring the phase of the photons, which are defined as the superposition of the early and late states, i.e., $|\pm\rangle = (|e\rangle \pm |l\rangle)/\sqrt{2}$. Therefore, the X-basis is sometimes referred to as *phase*-basis in the context of time-bin encoding. An illustration of how the time-basis and phase-basis states' profiles are detected by the single photon detectors is shown below (adapted from [28]).



Remark. With photons, there is also the *polarisation* encoding where the state of the qubit is encoded in the polarisations of the photon. However, the optical fibres in

which photons travel through induce polarisation-dependent loss and polarisation mode dispersion, which results in poor transmission distance [31]. Hence, the time-bin encoding is the choice of the photon encoding for our hybrid one-way quantum repeater scheme, later introduced in chapter 6. In fact, the time-bin encoding was also chosen in the homogeneous one-way quantum repeater scheme proposed by Borregaard *et al.* [18].

In accordance with definition 2.1.2, the vectors $|0\rangle$ and $|1\rangle$ form a basis and for this particular pair of vectors a special name was given, namely *computational basis* because this basis is commonly used in quantum computation.

While still satisfying the normalisation constraint $|\alpha|^2 + |\beta|^2 = 1$, the complex amplitudes in eq. (2.1) can be parametrised as follows:

$$\alpha = \cos\frac{\theta}{2}, \quad \beta = e^{i\phi}\sin\frac{\theta}{2}, \tag{2.2}$$

where $i = \sqrt{-1}$ is the imaginary unit, $e = 2.718\ldots$ is Euler's number, $\theta \in [0,\pi]$ is a polar angle and $\phi \in [0,2\pi)$ is an azimuthal angle. With this, all possible realisations of states that a single qubit can take on can be represented on the Bloch sphere (see fig. 2.1) with the Bloch vector being defined as:

$$\mathbf{v}_{\text{Bloch}} = \begin{bmatrix} \cos(\phi)\sin(\theta) \\ \sin(\phi)\sin(\theta) \\ \cos(\theta) \end{bmatrix}. \tag{2.3}$$

Using eq. (2.2), eq. (2.1) can be rewritten as:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle. \tag{2.4}$$

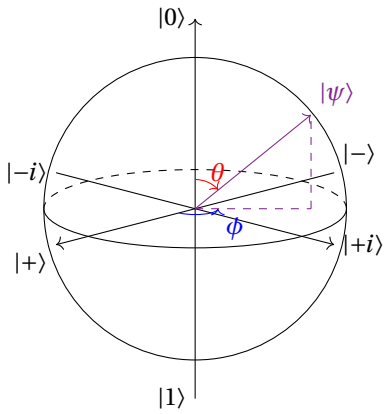


Figure 2.1: Bloch sphere representation of a qubit.

Owing to definition 2.1.2, each pair of antipodal points on the Bloch sphere corresponds to a pair of orthonormal vectors which forms a basis. Besides the computational

basis, two other commonly used basis are formed from the vectors along the x- and y-axes. As seen in fig. 2.1, the x-basis is formed from $\{|+\rangle, |-\rangle\}$ while the y-basis is formed from $\{|+i\rangle, |-i\rangle\}$. Here, the states $|\pm\rangle$ and $|\pm i\rangle$ are defined as:

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), \quad |\pm i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i\,|1\rangle). \tag{2.5}$$

Definition 2.2.1. The Kronecker product denoted by the symbol $\otimes$ acts on two matrices of arbitrary dimension. The result of applying it on a $i \times k$ matrix A and a $j \times l$ matrix B is as shown below:

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1k}B \\ \vdots & \ddots & \vdots \\ a_{i1}B & \cdots & a_{ik}B \end{bmatrix},$$

where the resulting matrix $A \otimes B$ has dimension $ij \times kl$.

To write the state of multiple qubits, one can use the Kronecker product as defined in definition 2.2.1. However, in this thesis we omit the use of the symbol $\otimes$ for brevity, e.g.:

$$|00\ldots0\rangle = |0\rangle \otimes \ldots \otimes |0\rangle. \tag{2.6}$$

2.2.2. GATES

SINGLE-QUBIT GATES

The Pauli matrices, which are both Hermitian and unitary, are shown in eq. (2.7) together with their corresponding quantum gate representation. The X, Y, and Z gates correspond to rotation of the Bloch vector in π radians about the x, y, and z axis, respectively.

$$\boxed{X} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \boxed{Y} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \boxed{Z} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2.7}$$

Besides the Pauli matrices, two other commonly used single-qubit gates are the Hadamard (H) and Phase (S) gates:

$$\boxed{H} \quad H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \boxed{S} \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}. \tag{2.8}$$

TWO-QUBIT GATES

The 2 two-qubit controlled gates used in this thesis are the controlled-NOT (CX) and controlled-phase (CZ) gates. Each of these two gates has two different quantum gate representations shown below, the latter of which is more commonly used in literature.

$$\boxed{X} \text{ or } \quad CX = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad \boxed{Z} \text{ or } \quad CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}. \tag{2.9}$$

In this thesis, we use both quantum gate representations interchangeably.

2.2.3. BELL STATES

Definition 2.2.2. An entangled state, usually composed of two or more qubits, is a state which cannot be expressed in terms of Kronecker product of its individual independent components.

Let us consider the preparation of two-qubit entangled states, also known as Bell states or Einstein-Podolsky-Rosen (EPR) pairs by using the gates introduced in the previous section. The preparation of such states in the form of a quantum circuit can be seen in fig. 2.2, where $p, q \in \{0, 1\}$.

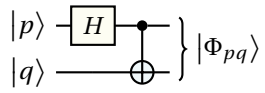


Figure 2.2: Circuit of Bell state preparation, where $p, q \in \{0, 1\}$.

In total there are four possible inputs and corresponding outcomes of this circuit and their states are written explicitly below:

$$|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$
$$|\Phi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad |\Phi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{2.10}$$

In the following section, we demonstrate the entanglement property of the Bell state $|\Phi_{pq}\rangle$ via density matrix calculation.

2.2.4. MEASUREMENTS

All single-qubit measurements considered in this thesis are performed in the computational basis unless stated otherwise. In quantum computing, we often measure whether a qubit in some general state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is in state $|0\rangle$ or $|1\rangle$, i.e., measuring the qubit in the computational basis. For example, if we measured that $|\psi\rangle$ is $|0\rangle$, then the qubit state collapses into state:

$$\frac{P_0|\psi\rangle}{\sqrt{\langle\psi|P_0|\psi\rangle}} = |0\rangle, \tag{2.11}$$

where operator $P_0 = |0\rangle\langle 0|$. If we had multiple copies of $|\psi\rangle$, we can perform repeated measurements and find that the probability of obtaining outcome $|0\rangle$ is $\langle\psi|P_0^\dagger P_0|\psi\rangle = |\alpha|^2$. Similarly, we can do this for the operator $P_1 = |1\rangle\langle 1|$. In fact, the operators P_0 and P_1 are also projectors since they satisfy the property that $P_i^2 = P_i$, $\forall i$. We can combine these two projectors to introduce an observable M, which is Hermitian:

$$M = m_0 P_0 + m_1 P_1, \tag{2.12}$$

where $m_0 = +1$ ($m_1 = -1$) is the eigenvalue associated with the projector P_0 (P_1). Now, we consider the case where we have a state that describes an arbitrary number of qubits:

$$|\psi\rangle = \sum_j \alpha_j |\psi_j\rangle, \text{ such that } \langle\psi_j|\psi_k\rangle = \delta_{jk}, \tag{2.13}$$

where $\{|\psi_j\rangle\}$ forms an orthonormal basis and α_j are the probability amplitudes which satisfy the property $\sum_j |\alpha_j|^2 = 1$. The corresponding observable M is now:

$$M = \sum_j m_j P_j = \sum_j m_j |\psi_j\rangle\langle\psi_j|. \tag{2.14}$$

The probability of obtaining a result corresponding to j after a measurement is:

$$p(j) = \langle\psi|P_j|\psi\rangle\,. \tag{2.15}$$

Thus, in the event of obtaining outcome j, the state of the quantum system immediately collapses into:

$$\frac{P_j|\psi\rangle}{\sqrt{\langle\psi|P_j^\dagger P_j|\psi\rangle}} = \frac{P_j|\psi\rangle}{|\langle\psi_j|\psi\rangle|}. \tag{2.16}$$

If we describe our quantum system via the density matrix formulation, i.e., set $\rho = |\psi\rangle\langle\psi|$, then the probability of obtaining a result corresponding to j after a measurement is:

$$p(j) = \mathrm{Tr}\Big[P_j \rho P_j^\dagger\Big], \tag{2.17}$$

and the quantum system will be left in the following state:

$$\frac{P_j \rho P_j^\dagger}{\mathrm{Tr}\Big[P_j \rho P_j^\dagger\Big]}. \tag{2.18}$$

A nice property that projective measurements have is that the average/expected value corresponding to an observable M can be easily calculated, and it is given by:

$$\begin{aligned}\langle M\rangle &= \sum_j m_j \langle\psi|P_j|\psi\rangle\,,\\ &= \langle\psi|\Big(\sum_j m_j P_j\Big)|\psi\rangle\,,\\ &= \langle\psi|M|\psi\rangle\,.\end{aligned} \tag{2.19}$$

Below, we show some examples using the concepts introduced in this section accompanied by quantum circuit representation for clarity.

Example 2.2.2. We want to measure the input state $\rho = |+\rangle\langle+|$ and obtain the output state ρ'. Since we are measuring the computational basis, the only possible outcomes are either $|0\rangle$ or $|1\rangle$.

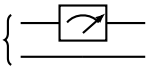
$\rho = |+\rangle\langle+|$ —[measurement]— ρ'

Let $P_j = |j\rangle\langle j|$ be the projector with $j \in \{0,1\}$. Here, j represents all the possible outcomes of the measurement. Then, we can perform the calculation as follows:

$$\rho' = \frac{P_j \rho P_j^\dagger}{\mathrm{Tr}\Big[P_j \rho P_j^\dagger\Big]} = |j\rangle\langle j|.$$

Example 2.2.3. We are presented with one of the Bell states from eq. (2.10) as the input state and we want to measure only the top qubit.

$$\rho = |\Phi_{00}\rangle\langle\Phi_{00}| \left\{ \right. \quad \left. \right\} \rho'$$



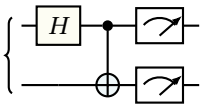
In this case, the projector can be written as $P_j = |j\rangle\langle j| \otimes I$ with $j \in \{0,1\}$. Then, the calculation is as follows:

$$\rho' = \frac{P_j \rho P_j^\dagger}{\mathrm{Tr}\left[P_j \rho P_j^\dagger\right]} = |j\,j\rangle\langle j\,j|$$

Remark. The result obtained in example 2.2.3 is significant because it shows that by measuring only the top qubit, we can determine the state of the other qubit to be exactly the same as the measured qubit. The two qubits are said to be perfectly correlated and this is a demonstration of the entanglement property of the Bell states.

Example 2.2.4. To distinguish between the four Bell states, one can perform the Bell state measurement (BSM), which is also sometimes referred to as *measurement in the Bell basis*. The circuit for performing BSM is shown below.

$$\rho = |\Phi_{pq}\rangle\langle\Phi_{pq}| \left\{ \right. \quad \left. \right\} \rho'$$



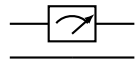
Let $U = (CX)(H \otimes I)$ be the gates acting on the input state. Then, the calculation can be performed as follows:

$$\rho' = \frac{U\rho U^\dagger}{\mathrm{Tr}\left[U\rho U^\dagger\right]} = |pq\rangle\langle pq|.$$

Besides performing measurements on pure states, measurement can also be performed on mixed states using projectors. The act of measuring the mixed state projects it onto a pure state. We recommend reading [24] as it contains a good demonstration of this.

Example 2.2.5. We are presented with a partially mixed state $\rho = \frac{I}{2} \otimes |0\rangle\langle 0|$ and we want to project it onto a pure state ρ' depending on the measurement outcome of the top qubit.

$$\rho = \tfrac{I}{2} \otimes |0\rangle\langle 0| \left\{ \begin{array}{c} \frac{I}{2} \\ |0\rangle\langle 0| \end{array} \right. \quad \left. \right\} \rho'$$



Let $P = |j\rangle\langle j| \otimes I$ be a projector with $j \in \{0,1\}$. Then, the calculation is as follows:

$$\rho' = \frac{P_j \rho P_j^\dagger}{\mathrm{Tr}\left[P_j \rho P_j^\dagger\right]} = |j0\rangle\langle j0|.$$

It can be checked that $\mathrm{Tr}\left[(\rho')^2\right] = 1$.

3

QUANTUM ERROR CORRECTION

3.1. QUANTUM CHALLENGES

Compared with classical error correction, its quantum counterpart is more sophisticated to carry out due to a number of difficulties specific to quantum error correction. The difficulties for quantum error correction are as follows:

- It is not possible to duplicate arbitrary quantum states due to the no-cloning theorem [32]. In other words, there exists no unitary U such that $U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$. In classical error correction, however, one can duplicate an arbitrary state without restrictions.
- A qubit is a linear superposition of a pair of basis vectors and the errors that it is subjected to exist on a continuum. A classical bit, on the other hand, is only subjected to discrete errors, i.e., a bit flip.
- Measurements in quantum systems causes their state to collapse, unlike in classical systems where measurements do not disturb their state.

Fortunately, these challenges can be overcome by carefully designing the quantum error correcting code (QECC). A QECC consists of four major components: encoding, error detection, error correction, and decoding. An example of a QECC can be seen in [25, 28, 33]. In section 3.4, we discuss the perfect $[\![5,1,3]\!]$ code in the context of the four major components in detail.

The mechanism where a qubit undergoes an error can vary depending on which type of technology is being used, e.g., superconducting qubits, ion trapped qubits, etc. It is therefore instructive to begin with examining coherent errors.

Definition 3.1.1. A coherent error on a qubit is an error which transform a qubit state on the Bloch sphere's surface to another point on the surface.

In general, a coherent error is described by the following unitary [33] acting on a

general qubit state $|\psi\rangle$ (see eq. (2.4)):

$$U(\delta\theta,\delta\phi)|\psi\rangle = \cos\frac{\theta+\delta\theta}{2}|0\rangle + e^{i(\phi+\delta\phi)}\sin\frac{\theta+\delta\theta}{2}|1\rangle, \tag{3.1}$$

which shows that the possible errors that could occur to a qubit are continuous, which is one of the difficulties described above. However, eq. (3.1) can be rewritten in the Pauli basis, i.e., in terms of the matrices I, X, Y, Z. By noting that Y is equivalent to XZ up to some global phase, the new expression is then:

$$U(\delta\theta,\delta\phi)|\psi\rangle = \alpha_I I|\psi\rangle + \alpha_X X|\psi\rangle + \alpha_{XZ} XZ|\psi\rangle + \alpha_Z Z|\psi\rangle, \tag{3.2}$$

where $\alpha_I, \alpha_X, \alpha_{XZ}, \alpha_Z$ are the Pauli expansion coefficients. This implies that any coherent error can be corrected by using only X and Z gates.

3.2. STABILISER CODES

A stabiliser code is often denoted concisely as an $[\![n,k,d]\!]$ code, which states that codes with distance d use n data/physical qubits (the terms *data* and *physical* qubits are used interchangeably) to encode k logical qubits. An example of such a code is the $[\![5,1,3]\!]$ code which is discussed throughout this thesis.

Definition 3.2.1. The distance d of a quantum error correction code is defined as the minimum weight error (see definition 3.4.1) that will transform a logical state to another, which means that such error will go undetected by the error correction procedure.

Example 3.2.1. Consider the following rudimentary 3-qubit encoding scheme:

$$\alpha|0_L\rangle + \beta|1_L\rangle = \alpha|000\rangle + \beta|111\rangle,$$

with $\alpha,\beta \in \mathbb{C}$ and $|\alpha|^2+|\beta|^2 = 1$. It takes only an error of weight $w = 1$ (e.g., $E_{w=1} = ZII$ error) to switch from a logical state to another orthogonal logical state, which makes it impossible to detect the error because the resulting state is still a $+1$ eigenstate of each of the stabiliser generators of the code (see definition 3.2.3).

$$E_{w=1}|+_L\rangle = |-_L\rangle,$$

where $|\pm_L\rangle = (|0_L\rangle \pm |1_L\rangle)/\sqrt{2}$. Therefore, we say that this 3-qubit code has distance $d = 1$.

Definition 3.2.2. A subset of QECC are stabiliser codes, which have the property that they can be completely described by their respectively stabiliser group [34].

Definition 3.2.3. The stabiliser group $\mathcal{S}$ for a quantum error correcting code C contains stabiliser generators g_i, each of which satisfies $g_i|\psi\rangle = |\psi\rangle, \forall|\psi\rangle \in C$. We say C is stabilised by $\mathcal{S}$.

Example 3.2.2. The stabiliser generators of the $[\![5,1,3]\!]$ code can be seen in eq. (3.3).

3.3. GRAPH STATES

In quantum computing, a convenient way of representing a particular type of multi-qubit states is through the graph representation. Such states are also known as graph states or cluster states and each vertex of the graph represents a qubit while the connecting edge between the vertices represents entanglement between them. For an in-depth graph state description, the readers are recommended to check references [35–40]. In this section, it is useful to recall the basic definition of a graph.

Definition 3.3.1. A graph $G = (V, E)$ consists of n vertices V and l edges E. The points or dots of the graph are the vertices, denoted by $V(G) \in \{1, \ldots, n\}$. The connection between each vertex in the graph are the edges, denoted by $E(G) \in \{e_1, \ldots, e_l\}$.

Remark. All graphs considered in this thesis are *undirected graphs*.

In the graph representation for quantum states, each of the vertices of the graph $V(G)$ represents a qubit in the $|+\rangle$ state while the edges represents a CZ gate between the connected vertices.

Example 3.3.1. Below we show the state of two qubits connected through a CZ gate in the graph representation, as well as its corresponding quantum circuit.

where $|G\rangle = CZ|{+}{+}\rangle_{12}$. The vertices and the quantum circuit registers are labelled to distinguish between qubits 1 and 2.

Definition 3.3.2. A graph state, usually denoted by $|G\rangle$, is a stabiliser state where each of its stabiliser generators can be described by the following expression:

$$K_v = X_v \prod_{b \in \mathcal{N}_v} Z_b,$$

where v denotes a vertex of the graph while $\mathcal{N}_v$ denotes the set of vertices which are adjacent to the vertex v. The subscript of the Pauli matrices indicates which vertex (qubit) of the graph they are acting on, e.g., X_v is the Pauli-X gate acting on the v^{th} qubit. Each of these generators satisfies the following relation:

$$K_v |G\rangle = |G\rangle .$$

Remark. This shows that such graph states $|G\rangle$ are eigenstates with eigenvalue $+1$ of the stabilisers K_v, which implies that by performing measurements on a subset of qubits of a graph state, whose basis is set according to a stabiliser generator, it is possible to predict the intended outcome of the remaining unmeasured qubit with certainty. This is shown in examples 3.3.2 and 3.3.3.

Example 3.3.2. Consider the following graph state:

which can also be written mathematically as:

$$|G\rangle = CZ\,|{+}{+}\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle).$$

By using definition 3.3.2, we can find that the stabiliser generators of this graph state are given by:

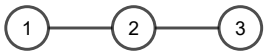
$$K_1 = X_1 Z_2,$$
$$K_2 = X_2 Z_1.$$

Since they are the stabiliser generators of this graph state, it follows that:

$$X_1 Z_2\,|G\rangle = X_2 Z_1\,|G\rangle = |G\rangle\,,$$

which indicates that if we perform the measurement of qubit 1 in the X-basis, then we can infer what the measurement outcome of qubit 2 in the Z-basis would be, *even if qubit 2 is lost.* This implies that such states can tolerate losses.

Example 3.3.3. Consider the following graph state:



where its state can be written mathematically as:

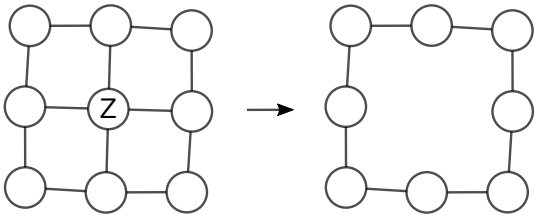
$$\begin{aligned}|G\rangle &= CZ_{12}CZ_{23}\,|{+}{+}{+}\rangle_{123}\\ &= \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle + |101\rangle - |110\rangle + |111\rangle).\end{aligned}$$

Just as in the example above, the stabiliser generators for this state are given by:

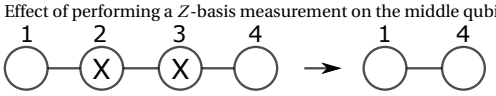
$$K_1 = X_1 Z_2,$$
$$K_2 = Z_1 X_2 Z_3,$$
$$K_3 = Z_2 X_3,$$

and they satisfy the relation $K_v\,|G\rangle = |G\rangle\,, \forall\, v \in \{1,2,3\}$. Take K_1 for example, we see that if we measure qubit 1 in the X-basis, we can then infer what the measurement outcome of qubit 2 in the Z-basis would be, *even if qubit 2 is lost.* This applies also to K_2 and K_3.

So far, we have only looked at simple cases with small graph states. For larger graph states with complicated entanglements (e.g., large tree cluster states, see section 4.1), it may seem infeasible to work out the resulting state after a measurement has been performed. Fortunately, it is possible to visualise the effects of performing X- and Z-basis measurements on a graph state by noting how such measurements affect the edges and vertices. Such visualisations can be seen in fig. 3.1 below. For a more rigorous mathematical representation of effects of measurements on graph states, one can refer to the thesis by Mor Ruiz [41].



(a) Effect of performing a Z-basis measurement on the middle qubit.



(b) Effect of performing an X-basis measurement on each of qubits 2 and 3.

Figure 3.1: (a) The resulting state after a Z-basis measurement on the middle qubit is equivalent to its removal from the graph state as well as the bonds which were previously attached with the removed qubit. (b) The act of performing X-basis measurements on qubit 2 and 3 results in a graph state where the measured qubits are removed but direct bonds are formed between their neighbours.

3.4. PERFECT ⟦5,1,3⟧ CODE

The ⟦5,1,3⟧ code or five qubit code is a *perfect quantum code* because it satisfies the *quantum Hamming inequality* with an equality sign [28]. It is also the smallest distance $d = 3$ code which can correct arbitrary single-qubit errors. In other words, the set of correctable errors of the ⟦5,1,3⟧ code contains all Pauli errors of weight $w = 1$ (see table 3.1).

Definition 3.4.1. Error of weight w is the number of qubits subjected to error.

Example 3.4.1. The error $IIIXI$ has weight $w = 1$ whereas the error $IXIXI$ has weight $w = 2$.

The ⟦5,1,3⟧ code is stabilised by the following four stabiliser generators:

$$XZZXI, \quad IXZZX, \quad XIXZZ, \quad ZXIXZ. \tag{3.3}$$

A general logical state encoded in the ⟦5,1,3⟧ code can be written as the superposition of the following two orthogonal logical states or *quantum codewords*:

$$|\psi_L\rangle = \alpha|0_L\rangle + \beta|1_L\rangle, \tag{3.4}$$

where $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$, and the states $|0/1_L\rangle$ are given by:

$$\begin{aligned}
|0_L\rangle = \frac{1}{4}(&|00000\rangle - |00011\rangle + |00101\rangle - |00110\rangle + |01001\rangle + |01010\rangle - |01100\rangle - |01111\rangle \\
&- |10001\rangle + |10010\rangle + |10100\rangle - |10111\rangle - |11000\rangle - |11011\rangle - |11101\rangle - |11110\rangle), \\
|1_L\rangle = \frac{1}{4}(&|00001\rangle + |00010\rangle + |00100\rangle + |00111\rangle + |01000\rangle - |01011\rangle - |01101\rangle + |01110\rangle \\
&+ |10000\rangle + |10011\rangle - |10101\rangle - |10110\rangle + |11001\rangle - |11010\rangle + |11100\rangle - |11111\rangle).
\end{aligned} \tag{3.5}$$

All superpositions shown in eq. (3.4) are all +1 eigenstates of each of the stabiliser generators in eq. (3.3). It is interesting to note that the logical state $|0_L\rangle$ ($|1_L\rangle$) is the superposition of all the 5-qubit states with even (odd) parity. Then, it is obvious that the two codewords are orthogonal to each other and that $|1_L\rangle = \bar{X}|0_L\rangle$, where $\bar{X} = XXXXX$ is the logical X operator. Another logical operator of the $[\![5,1,3]\!]$ code is the logical Z operator $\bar{Z} = ZZZZZ$. Additionally, the logical H and S operator for the $[\![5,1,3]\!]$ code are defined to be the application of the single-qubit H and S gates, respectively, followed by permutations of the data qubits as shown in fig. 3.2 below [19, 34, 42].

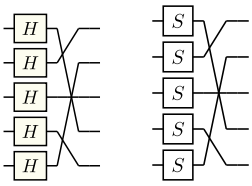


Figure 3.2: (Left) Logical H operator and (right) logical S operator for the $[\![5,1,3]\!]$ code. Adapted from [19].

To encode an arbitrary state with the $[\![5,1,3]\!]$ code and obtain the resulting state as shown in eq. (3.4), we begin with the logical state $|+_L\rangle = (|0_L\rangle + |1_L\rangle)/\sqrt{2}$, which can also be represented as a graph state (see section 3.3) as shown in fig. 3.3 below [36]. In the language of *graph theory*, this graph state is also known as the cycle graph of C_5 [43, 44].

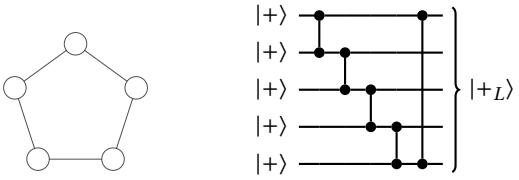


Figure 3.3: (Left) Graph state representation of the $[\![5,1,3]\!]$ code logical state $|+_L\rangle$ (*this particular graph is also known as the C_5 graph in graph theory*) and (right) its quantum circuit representation. Adapted from [36].

Then, we introduce an additional qubit, which we will encode its state into the graph state of C_5. In fig. 3.4, we outline the main encoding step in graph state representation where the additional qubit is entangled with the rest of the 5 data qubits via the CZ gate application, followed by its measurement in the X-basis. The resulting state would then be a logical state which depends on the original state of the measured additional qubit (up to a logical operator correction). The corresponding quantum circuit representation is shown in fig. 3.5. This particular encoding protocol which we are describing in this section is shown in [36]. However, there are also alternative ways to perform encoding for the $[\![5,1,3]\!]$ code as others have proposed [19, 41, 45].

Depending on the physical implementation of the qubits, one encoding protocol may be better than the other. For example, consider a diamond defect based architecture with ^{13}C nuclear-spin qubits and a 'central' electron spin, where we use 5 ^{13}C nuclear-spin qubits as the data qubits. In such a system that uses electron-nuclear two-qubit

gates, it is not possible to perform the encoding scheme as shown in fig. 3.3 since two-qubit gates cannot be easily performed between ^{13}C nuclear-spins. Instead, a heralded approach via repeated stabiliser measurements and a flag qubit is used [19].

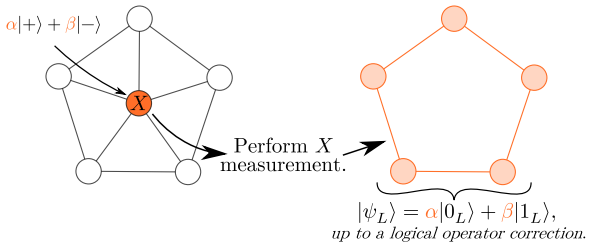


Figure 3.4: Procedure of encoding a qubit of arbitrary state into the ⟦5,1,3⟧ logical state. The graph on the left is also known as the W_5 graph in graph theory [44].

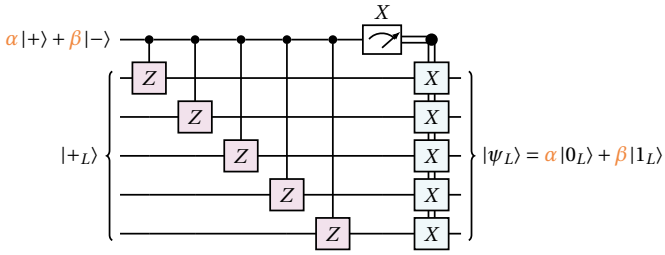


Figure 3.5: Quantum circuit for encoding a qubit of arbitrary state into the 5 data qubits. If a -1 eigenstate is measured in the X-basis measurement, then the $\bar{X} = XXXXX$ logical operator will be performed additionally. Adapted from [36].

The quantum circuit for measuring the error syndrome of the ⟦5,1,3⟧ code needs $n-k = 5-1 = 4$ ancilla qubits (see fig. 3.6). In total, 9 qubits are needed (4 ancilla qubits + 5 data qubits).

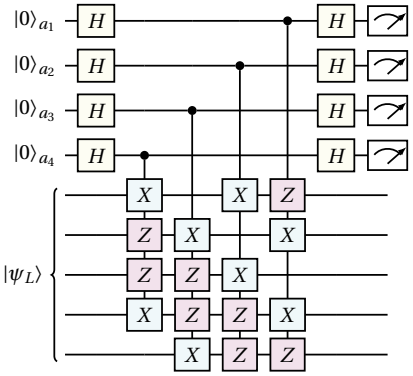


Figure 3.6: Quantum circuit for obtaining the error syndrome by measuring the stabiliser generators of the perfect $[\![5,1,3]\!]$ code. The top four qubits are the ancillas for obtaining the error syndrome while the bottom five are the data qubits.

The $[\![5,1,3]\!]$ code has in total $2^4 = 16$ possible syndromes, each of which corresponds to a distinct single-qubit error or lack thereof. All the possible syndromes and their corresponding corrections are tabulated in table 3.1 below.

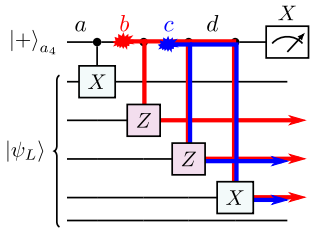
a_1	a_2	a_3	a_4	Correction
0	0	0	0	I
0	0	0	1	X_2
0	0	1	0	Z_5
0	0	1	1	X_3
0	1	0	0	Z_3
0	1	0	1	Z_1
0	1	1	0	X_4
0	1	1	1	Y_3
1	0	0	0	X_1
1	0	0	1	Z_4
1	0	1	0	Z_2
1	0	1	1	Y_2
1	1	0	0	X_5
1	1	0	1	Y_1
1	1	1	0	Y_5
1	1	1	1	Y_4

Table 3.1: Corrections of $w \leq 1$ to the five physical qubits depending on the ancilla outcomes. $a_i = 0$ ($a_i = 1$) corresponds to a measurement outcome of $+1$ (-1) eigenstate.

3.4.1. FAULT-TOLERANCE WITH FLAG QUBIT

The circuit depicted in fig. 3.6 is not fault-tolerant because errors happening at the ancilla qubits would propagate to the data qubits via the two-qubit gates. In fig. 3.7a, we show the subcircuit of the stabiliser generator $XZZXI$ as an example. The errors propagated by the a gate and d gate are not considered in the fault-tolerant protocol because they induce only uncorrelated errors [20]. The errors which occur in gates b and c, however, do induce correlated errors on the data qubits, i.e., errors of weight $w = 2$

(see fig. 3.7b and fig. 3.7c). The data qubit errors shown in fig. 3.7b and fig. 3.7c can be derived similarly for subcircuits of the three remaining stabiliser generators and their results are compiled in table 3.2. One can 'catch' and correct these propagated errors by introducing an additional qubit, which is also known as a *flag qubit* as shown in fig. 3.8. When the flag qubit is triggered (i.e., a measurement resulting in the -1 eigenstate), then we know that the data qubits are subjected to weight $w \leq 2$ errors. Thus, the error syndrome needs to be interpreted differently when the flag qubit is triggered. In fact, each of these propagated weight $w = 2$ errors has their own distinct syndrome, and therefore can be corrected (see table 3.2 and definition 3.4.2).



(a)

b gate error	Data error
X_{a_4}	$Z_2 Z_3 X_4 \sim X_1$
$X_{a_4} X_2$	$Y_2 Z_3 X_4 \sim X_1 X_2$
$X_{a_4} Y_2$	$X_2 Z_3 X_4 \sim X_1 Y_2$
$X_{a_4} Z_2$	$Z_3 X_4$

(b)

c gate error	Data error
X_{a_4}	$Z_3 X_4$
$X_{a_4} X_3$	$Y_3 X_4$
$X_{a_4} Y_3$	$X_3 X_4$
$X_{a_4} Z_3$	X_4

(c)

Figure 3.7: (a) Error propagation visualised in part of the non-fault-tolerant ⟦5,1,3⟧ circuit. (b-c) The two-qubit gate errors at sites b and c with their corresponding effective weight $w \leq 2$ errors on the data qubits. E.g., the error $Z_2 Z_3 X_4$ is effectively a weight $w = 1$ error (i.e., $Z_2 Z_3 X_4 \sim X_1$) by multiplying it with the stabiliser generator $XZZXI$.

Definition 3.4.2. The protocol for the flagged ⟦5,1,3⟧ circuit is as follows:
Begin with the circuit in fig. 3.8 and proceed to the application of the two-qubit gates, flag qubit measurements and syndrome extraction. Depending on the result of the measurements at each subcircuit of a stabiliser generator, one would need to make the following decisions:

1. If $f_i = a_i = +1$ (i.e., flag and ancilla not triggered), then continue using the flagged circuit and extract a_{i-1} and f_{i-1}. If all four flag qubits and four ancilla qubits were not triggered, then we are finished with no corrections needed.
2. If $f_i = -1$ and $a_i = \pm 1$ (i.e., flag triggered regardless of syndrome outcome), then switch to the unflagged circuit and measure a'_1, a'_2, a'_3, a'_4. Finish by applying weight $w \leq 2$ corrections as shown in table 3.2.
3. If $f_i = +1$ and $a_i = -1$ (i.e., flag not triggered and ancilla triggered), then switch to the unflagged circuit and measure a'_1, a'_2, a'_3, a'_4. Finish by applying weight $w \leq 1$ corrections as shown in table 3.1.

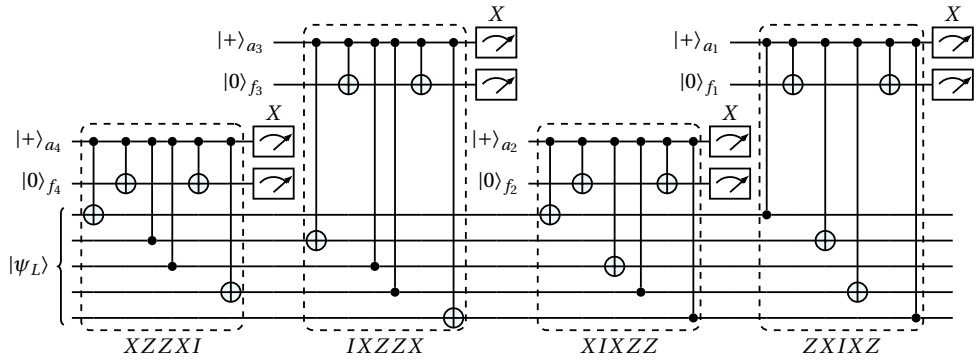


Figure 3.8: The flagged variant of the perfect $[\![5,1,3]\!]$ code quantum circuit. The flag qubits are labelled f_i with $i \in \{1,2,3,4\}$.

				Correction			
a'_1	a'_2	a'_3	a'_4	Triggered: f_1	f_2	f_3	f_4
0	0	0	0	I	I	I	I
0	0	0	1	X_2	X_2	X_2	Y_3X_4
0	0	1	0	Z_5	Z_5	X_2X_3	Z_3X_4
0	0	1	1	X_3	X_3	Y_4X_5	X_1Y_2
0	1	0	0	X_4Z_5	X_4Z_5	Z_3	Z_3
0	1	0	1	Z_1	Z_1	Z_4X_5	X_3X_4
0	1	1	0	X_4	X_4	X_1Y_5	X_4
0	1	1	1	Y_3	Y_3	Y_3	Y_3
1	0	0	0	X_1	X_1	X_1	X_1
1	0	0	1	Z_4	Z_4	Z_4	X_1X_2
1	0	1	0	Z_2	Z_2	X_4X_5	Z_2
1	0	1	1	Z_4Z_5	Z_4Z_5	Y_2	Y_2
1	1	0	0	X_5	X_1Z_3	X_5	X_5
1	1	0	1	Y_4Z_5	Y_4Z_5	Y_1	Y_1
1	1	1	0	Z_1Y_2	Y_5	Y_5	Y_5
1	1	1	1	Z_1Z_2	X_1Y_3	Y_4	Y_4

Table 3.2: Corrections of $w \leq 2$ to the five data qubits depending on the ancilla outcomes and which flag was triggered. $a'_i = 0$ ($a'_i = 1$) corresponds to a measurement outcome of $+1$ (-1) eigenstate.

3.5. NOISE MODELS

To study the performance of a quantum error correcting code, we need to introduce a *quantum channel* which introduces noise. In theory, there are multiple types of noise models to consider, i.e., the bit-flip channel or the phase-flip channel. In this thesis, we consider the depolarising noise channel.

Definition 3.5.1. A *quantum channel* is a completely positive and trace-preserving (CPTP) map, which takes a given density matrix to another density matrix [25].

3.5.1. SINGLE-QUBIT DEPOLARISING CHANNEL

To model depolarisation with error rate ϵ on a single qubit, we can use the single-qubit depolarising channel, $\Lambda_{(1)}$, which is given below:

$$\Lambda_{(1)}(\epsilon) = (1-\epsilon)\rho_{(1)} + \frac{\epsilon}{3}\left(X\rho_{(1)}X + Y\rho_{(1)}Y + Z\rho_{(1)}Z\right), \tag{3.6}$$

where $\rho_{(1)}$ is a density matrix which describes one qubit and X, Y, Z are the Pauli matrices.

3.5.2. TWO-QUBIT DEPOLARISING CHANNEL

To model a noisy two-qubit gate operation, U, we consider the following depolarising channel with error rate ϵ, $\Lambda_{(2)}$, where the second term represents the sum of all possible Pauli operators acting on each of the qubit, except for *identity on both qubits*:

$$\begin{aligned}\Lambda_{(2)}(\epsilon) &= (1-\epsilon)U\rho_{(2)}U^\dagger + \frac{\epsilon}{15}\left(\sum_{i=1}^{4}\sum_{j=1}^{4}\left(\sigma_1^i\sigma_2^j\rho_{(2)}\sigma_1^i\sigma_2^j\right) - \rho_{(2)}\right)\\ &= (1-\epsilon)U\rho_{(2)}U^\dagger + \frac{\epsilon}{15}\left(X_1\rho_{(2)}X_1 + Y_1\rho_{(2)}Y_1 + Z_1\rho_{(2)}Z_1\right.\\ &\quad + X_1X_2\rho_{(2)}X_1X_2 + X_1Y_2\rho_{(2)}X_1Y_2 + X_1Z_2\rho_{(2)}X_1Z_2\\ &\quad + Y_1X_2\rho_{(2)}Y_1X_2 + Y_1Y_2\rho_{(2)}Y_1Y_2 + Y_1Z_2\rho_{(2)}Y_1Z_2\\ &\quad + Z_1X_2\rho_{(2)}Z_1X_2 + Z_1Y_2\rho_{(2)}Z_1Y_2 + Z_1Z_2\rho_{(2)}Z_1Z_2\\ &\quad \left. + X_2\rho_{(2)}X_2 + Y_2\rho_{(2)}Y_2 + Z_2\rho_{(2)}Z_2\right),\end{aligned} \tag{3.7}$$

where σ_k^1, σ_k^2, σ_k^3, and σ_k^4 are the operators X, Y, Z, and I acting on the k^{th} qubit, respectively and $\rho_{(2)}$ is a density matrix which describes two qubits. In eq. (3.7), U can be any two-qubit gate, but we will only look at the case for $U = CX$ and $U = CZ$ since those are the only two-qubit gates which are used in this thesis.

3.6. OBTAINING FIDELITY WITH RECURSION

In this section, we present a novel method of obtaining the fidelity via a recursion relation if we were to apply the quantum error correction procedure multiple times. We begin with letting the combined action of input depolarisation, erroneous gate channels, stabiliser operations with ancilla qubits, and correction, be represented by a quantum channel $\mathcal{C}$. An example using the non-fault-tolerant $[\![5,1,3]\!]$ code is shown below in fig. 3.9. Note that perfect qubit readouts and single-qubit gate applications are assumed.

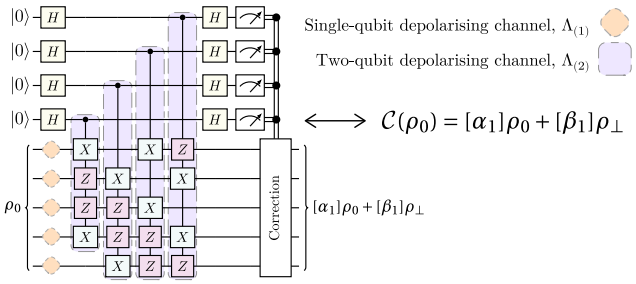


Figure 3.9: Equivalence between the quantum circuit representation and the channel representation. In this figure, the non-fault-tolerant $[\![5,1,3]\!]$ circuit with single-qubit and two-qubit depolarising channels is used as an example. The depolarising channels, $\Lambda_{(1/2)}$, are given in eqs. (3.6) and (3.7). The corrections applied at the end of the circuit depends on the error syndrome measured according to table 3.1.

As shown in fig. 3.9, the action of the channel on an input state ρ_0 can be written as such:

$$\mathcal{C}(\rho_0) = [\alpha_1]\rho_0 + [\beta_1]\rho_\perp, \tag{3.8}$$

where $\rho_0 = |\psi_L\rangle\langle\psi_L|$ is the perfect logical state and $\rho_\perp$ represents the states that are orthogonal to ρ_0. Here, α_1 is the fidelity and $\beta_1 = 1-\alpha_1$ is the error rate. Moving on, it is also important to consider the effect of $\mathcal{C}$ on the orthogonal term, because in the following round of correction, part of it can be corrected back into the logical state ρ_0, i.e.,

$$\mathcal{C}(\rho_\perp) = [\alpha']\rho_0 + [\beta']\rho'_\perp. \tag{3.9}$$

With eq. (3.8) and eq. (3.9), we can then apply the $\mathcal{C}$ channel c times on ρ_0. As a first order approximation, we assume that the second term in eq. (3.9) is completely uncorrectable, and therefore we only keep terms that lead to non-zero fidelity while we discard the others. In this case, we discard terms with β'.

$$\begin{aligned}
\rho_1 = \mathcal{C}(\rho_0) &= [\alpha_1]\rho_0 + [\beta_1]\rho_\perp, \\
\rho_2 = \mathcal{C}(\rho_1) = [\alpha_1]\mathcal{C}(\rho_0) + [\beta_1]\mathcal{C}(\rho_\perp) &= [\alpha_1^2 + \alpha']\rho_0 + [\beta_1\alpha_1]\rho_\perp = [\alpha_2]\rho_0 + [\beta_2]\rho_\perp, \\
&\vdots \\
\rho_c = \mathcal{C}(\rho_{c-1}) &= [\alpha_c]\rho_0 + [\beta_c]\rho_\perp.
\end{aligned} \tag{3.10}$$

After performing the steps in eq. (3.10), we find the terms α_c and β_c to be:

$$\alpha_c = \alpha_1\alpha_{c-1} + \beta_{c-1}\alpha', \quad \beta_c = \beta_1\alpha_{c-1}. \tag{3.11}$$

Since $\beta_1 = 1-\alpha_1$, we can combine the expressions in eq. (3.11) to form:

$$\alpha_c = \alpha_{c-1}\alpha_1 + \alpha_{c-2}(1-\alpha_1)\alpha', \text{ with } \alpha_i = \begin{cases} \alpha_1, & \text{if } i = 1 \\ 1, & \text{if } i = 0 \\ 0, & \text{if } i < 0 \end{cases}. \tag{3.12}$$

Finally, solving for the recursion relation in eq. (3.12) then yields:

$$\mathcal{F}_{\mathcal{C}}^{c,1}[\rho_0] \equiv \alpha_c \equiv \frac{(\alpha_1+\zeta)^{c+1} - (\alpha_1-\zeta)^{c+1}}{2^{c+1}\zeta} \tag{3.13}$$

where $\zeta = \sqrt{\alpha_1^2 + 4(1-\alpha_1)\alpha'}$. We have used $\mathcal{F}_{\mathcal{C}}^{c,k}[\rho_0]$ to denote the *recursive model function* with k^{th} order approximation. In this case, eq. (3.13) is the first order approximation of the fidelity of our logical state ρ_0 after applying the $\mathcal{C}$ channel c times. We see that if we set $\alpha' = 0$, then eq. (3.13) becomes equivalent to the zeroth order approximation:

$$\mathcal{F}_{\mathcal{C}}^{c,0}[\rho_0] \equiv \alpha_c \equiv \alpha_1^c, \tag{3.14}$$

which we call the *pessimistic model* or the *naïve model* because eq. (3.14) assumes that even $\rho_\perp$ is 100% uncorrectable, let alone trying to correct $\rho'_\perp$. However, one question remains: it is clear how to obtain α_1 via numerical calculation, but how does one obtain α'? To begin, we first note that $\rho_1 = \alpha_1\rho_0 + \beta_1\rho_\perp$. Then, we can rewrite this in terms of $\rho_\perp$, yielding us:

$$\rho_\perp = (\rho_1 - \alpha_1\rho_0)/\beta_1. \tag{3.15}$$

From eq. (3.15), we see that we already have ρ_1 at hand from numerical calculation. To obtain α', we simply need to perform another numerical calculation of $\mathcal{C}(\rho_\perp)$.

In chapter 6, we will see that the recursive model function is a great approximation to the exact result. The recursive model is a remarkable find as it allows us to extrapolate the fidelity of a state acted on by a generic channel $\mathcal{C}$ c times just by applying it a few times. The expression for the second order approximation can be seen in eq. (A.5) in appendix A.

4

QUANTUM ERASURE CORRECTION

4.1. TREE CLUSTER STATES

In the previous section, we have introduced the concept of graph states and how simple graph states can be robust against losses using the indirect Z measurement technique as shown in examples 3.3.2 and 3.3.3. However, these simple states are not robust enough against losses since the low number of qubits in the system can all still be lost. To increase redundancy or robustness in the system, we can add more qubits to the graph state to form a tree cluster state, an example of which can be seen in fig. 4.1.

Definition 4.1.1. A tree cluster state is described by a *branching vector* or *tree vector* $\vec{t} = [b_0, b_1, \ldots, b_d]$, where d is the *depth* of the tree.

Remark. Since the tree cluster state is a type of graph state, it is invariant under the operations of stabiliser generators K as shown in definition 3.3.2.

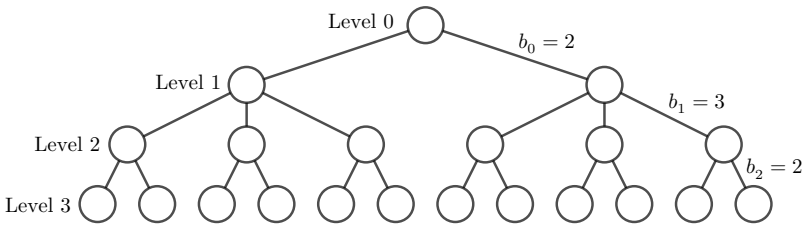
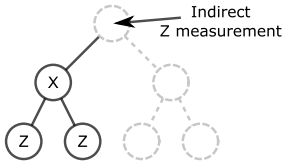


Figure 4.1: A tree cluster state with tree vector $\vec{t} = [2,3,2]$.

Example 4.1.1. Consider a tree cluster state with $\vec{t} = [2,2]$ where one of its branch is lost (indicated by grey colour). We still can recover the information of the root qubit by performing measurements on the remaining subset of qubits which leads to an indirect Z-basis measurement. The graph representation of such state can be seen

below with the dashed lines representing lost qubits.



Remark. An indirect Z-basis measurement can also be performed if it was the left branch that was lost instead. This is known as *redundancy*.

Due to tree cluster states' robustness against loss via redundancy, it is desirable to encode quantum information into such states. To achieve this, we can perform Bell state measurement (BSM) (see example 2.2.4) between the data qubit in an arbitrary state and the root qubit of the tree cluster state (see fig. 4.2). After performing the BSM, we end up a truncated tree cluster state, from which we can recover the data qubit (up to some Pauli correction and global phase) by performing direct/indirect Z-basis measurement on adjacent qubits (see fig. 4.3). From this, we see that we can afford to have some qubits lost as long as we can perform the Z-basis measurements in fig. 4.3. Tree cluster states are therefore able to encode quantum information while being robust against lost due to the redundancy that they provide. Despite the tree cluster states' robustness against loss, they can only tolerate losses up to 50% owing to the no-cloning theorem [32] before it becomes impossible to extract the encoded information.

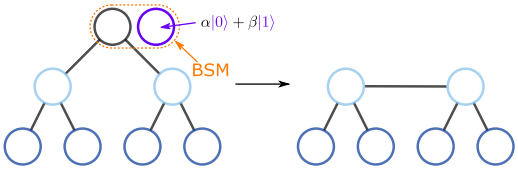


Figure 4.2: Encoding of the data qubit (in purple) into the $\vec{t} = [2,2]$ tree cluster state by performing the Bell state measurement (BSM) between the data qubit and the root qubit of the tree. The colours on the qubits of the tree emphasise the different levels of the qubits.

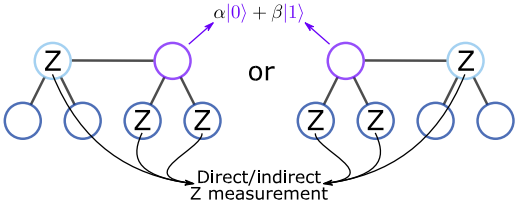
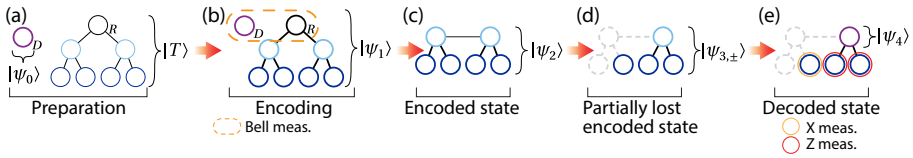


Figure 4.3: Decoding procedure to recover the data qubit. Since the tree is symmetric about a vertical reflection, there are two ways to decode and recover the data qubit up to some Pauli correction.

Example 4.1.2. In the following example, we will illustrate the full procedure of both encoding and decoding a tree using $\vec{t} = [2,2]$ taking loss errors into account.



We begin with step (a) in which we prepare our data qubit (denoted by D) in state $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$ and our tree in state $|T\rangle = (|0\rangle_R|\tau_+\rangle + |1\rangle_R|\tau_-\rangle)/\sqrt{2}$, with the root qubit denoted by R. Here, $|\tau_\pm\rangle = (|0\rangle|{+}{+}\rangle \pm |1\rangle|{-}{-}\rangle)^{\otimes 2}/2$ is the state of the subtrees, i.e., the qubits below the root qubit. With the preparation done, we can move on to step (b) in which we encode the data qubit into the tree via a BSM between the data and the root qubit, which follows the following application of H and CX gate:

$$|\psi_1\rangle = H_D CX_{DR}|\psi_0\rangle|T\rangle.$$

The resulting state depends on the outcome of the BSM on state $|\psi_1\rangle$, which is characterised by the Bell states $|\Phi_{pq}\rangle$, with $p,q \in \{0,1\}$. After the BSM, we can write the resulting state as follows:

$$|\psi_2\rangle = \alpha\big[(1-q)|\tau_+\rangle + q|\tau_-\rangle\big] + \beta(1-2p)\big[q|\tau_+\rangle + (1-q)|\tau_-\rangle\big],$$

which is the encoded state in step (c). To simplify the subsequent calculations, we assume that we obtained $p = q = 0$ in the BSM, then the state becomes:

$$|\psi_2\rangle = \alpha|\tau_+\rangle + \beta|\tau_-\rangle.$$

Next, in step (d), we assume that we detected some qubits in the tree are lost, e.g., due to lost of photons that were travelling through an optical fibre. This brings the state to:

$$|\psi_{3,\pm}\rangle = \frac{|\pm\rangle}{\sqrt{2}}\big[(\alpha \pm \beta)|0\rangle|{+}{+}\rangle + (\alpha \mp \beta)|1\rangle|{-}{-}\rangle\big].$$

At this stage, we can perform direct/indirect Z-basis measurements in step (e) to project the remaining qubit on the *first-level* into the state:

$$|\psi_4\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{up to some Pauli correction.}$$

This is exactly the state of our original data qubit $|\psi_0\rangle$, though Pauli corrections are needed depending on the outcome of the measurements on the tree qubits in step (e).

Remark. Similar examples were also shown in references [18, 41]. In fact, it was shown that the $\vec{t} = [3,2]$ tree code is *local Clifford* (LC) equivalent to the $[\![9,1,3]\!]$ Shor's code (see [41] for further reading).

So far, we have only talked about the tree cluster states in the context of loss errors. However, the tree cluster state architecture is also robust against general errors to a certain degree. Naïvely, one might think that introducing a large number of qubits in the tree cluster state increases its robustness against loss errors at the expense of increasing

sensitivity towards depolarising errors. This is, however, not the case because in reality, adding the number of qubits also introduces redundancy in the context of depolarising errors. This redundancy against depolarising errors is achieved by adopting the *majority voting strategy*, which significantly reduces the overall error rate [46]. A simple demonstration of majority voting is shown in example 4.1.3.

Example 4.1.3. Consider the tree cluster state as shown in example 4.1.2. Let us imagine that if none of the qubits were lost, then we can simply perform all the Z-basis measurements in a direct manner as shown below.

If there were no errors, the state of the subtree enclosed in the grey box is:

$$|\tau_{\text{no err}}\rangle = |0\rangle|{+}{+}\rangle \pm |1\rangle|{-}{-}\rangle.$$

In a realistic setting, each of the qubits in the tree are subjected to some depolarising error. Consider the case where the left-most qubit in the *first-level* is subject to a Pauli-X error. In this case, we would measure the state:

$$|\tau_{\text{err}}\rangle = |1\rangle|{+}{+}\rangle \pm |0\rangle|{-}{-}\rangle.$$

By comparing $|\tau_{\text{err}}\rangle$ and $|\tau_{\text{no err}}\rangle$, we see that by deduction, an error probably occurred on the left-most qubit on the *first-level*. We can thus apply the correction in post-processing, after which we can then say that we have applied *majority voting*.

Let us now consider a scenario where we encode the data qubit into a tree cluster state with arbitrary tree vector $\vec{t} = [b_0, b_1, \ldots, b_d]$. Assuming each qubit in the tree is subjected to some probability μ of being lost (or being subjected to some other type of detectable error), then the probability of successfully recovering the data qubit from the tree is given by the following recursive formula [18, 46]:

$$P = [(1-\mu+\mu R_1)^{b_0} - (\mu R_1)^{b_0}](1-\mu+\mu R_2)^{b_1}, \tag{4.1}$$

where for $k \leq d$

$$R_k = 1 - [1-(1-\mu)(1-\mu+\mu R_{k+2})^{b_{k+1}}]^{b_k}, \tag{4.2}$$

with $R_{d+1} = 0$ and $b_{d+1} = 0$. The quantity R_i is the probability of successfully performing on indirect Z-basis measurement on a qubit in the i^{th} level. Since $1-\mu$ is the probability of a successful direct Z-basis measurement, then the probability of a successful Z-basis measurement on a qubit in the i^{th} level is given by $1-\mu+\mu R_i$.

4.1.1. TREE GENERATION

The generation of a tree-cluster state with depth $d = 2$ (see definition 4.1.1) is shown in fig. 4.4. In the first step, entanglement between the qubits in state $|+\rangle$ is achieved via the CZ gate. In subsequent steps, the qubits are emitted via the emitter through spontaneous emission until all qubits of the tree cluster state except for the root qubit

are emitted as photons. For an in-depth look into the tree generation, we recommend the references [18, 47, 48].

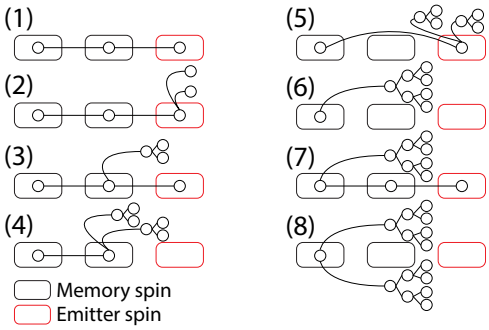


Figure 4.4: A sketch of the steps in generating a $\vec{t} = [2,2,2]$ tree using 2 memory qubits and an emitter. In step 1, the 3 qubits of state $|+\rangle$ are initialised and the CZ gate is applied between them (see section 3.3). In step 2, third-level photons are emitted from the emitter followed by the emission of the corresponding second-level photon in step 3. Steps 1-3 are repeated resulting in the state in step 4. The first-level qubit is transferred to the emitter spin in step 5 before being emitted as photon in step 6. The qubits are re-initialised in step 7 and the entire procedure is repeated for the other branch of the tree, resulting in the $\vec{t} = [2,2,2]$ tree in step 8.

4.2. QUANTUM ERASURE CORRECTING CODES

A single-qubit quantum erasure channel is a channel which erases a qubit with probability γ:

$$\mathcal{E}(\rho_{(1)}) = (1-\gamma)\rho_{(1)} + \gamma|\perp\rangle\langle\perp|, \tag{4.3}$$

where $\rho_{(1)}$ is a density matrix describing one qubit and $|\perp\rangle$ is a state that is orthogonal to all the input states, i.e., $\langle\perp|\rho_{(1)}|\perp\rangle = 0$. This state $|\perp\rangle$ acts as a *flag* since it tells us about the erasure of qubit $\rho_{(1)}$. This is in fact the channel which describes the loss errors we have discussed thus far in this thesis. It is crucial to consider such errors because they often occur in quantum computing especially in the physical implementation of qubits using photons since they can be lost while travelling through an optical fibre.

At first glance, it may seem impossible to use the conventional $[\![n,k,d]\!]$ codes to correct for erasure errors since one or more of the n qubits encoding k logical qubit is completely gone, i.e., erased. However, it was shown by Grassl *et al.* [22] in 1997 that any t arbitrary error correcting codes can also correct for $2t$ known erasure errors which resulted in theorem 4.2.1. Later in 1999, Cleve *et al.* [23] discussed quantum erasure corrections in the context of quantum key distribution with a detailed example using the 3-qutrit encoding scheme. Another few years later, Gingrich *et al.* [24] detailed in 2003 a quantum communication protocol which can correct for 1-erasure error using the $[\![4,2,2]\!]$ encoding scheme.

Theorem 4.2.1. A quantum error correcting code which corrects t arbitrary error(s) is a $2t$-erasure correcting code, provided that we know where each of the $2t$ erasure errors occurred [22].

However, it is imperative to note that in order for such code to be able to correct for

$2t$ known erasure errors, it must follow that there are no additional arbitrary errors on the remaining qubits. In other words, it is not possible to correct for $2t$ erasure errors and any additional arbitrary errors simultaneously. In the following section, we discuss the $[\![5,1,3]\!]$ code in the context of quantum erasure correction.

4.2.1. PERFECT $[\![5,1,3]\!]$ CODE

Since the $[\![5,1,3]\!]$ code can correct for arbitrary single-qubit errors, it can also, according to theorem 4.2.1, correct for erasure errors occurring on up to 2 qubits, provided that the locations of these erasures are known. To outline the erasure correction protocol using the $[\![5,1,3]\!]$ code, we begin by introducing the reset channel $\mathcal{R}$ (used also in [24]) acting on the subspace of a density matrix:

$$\mathcal{R}_a(\rho_{ab}) = |0\rangle\langle 0|_a \rho_{ab} |0\rangle\langle 0|_a + |0\rangle\langle 1|_a \rho_{ab} |1\rangle\langle 0|_a. \tag{4.4}$$

Intuitively, the reset channel can be taught of as the action of swapping the orthogonal state $|\perp\rangle$ in the event of an erasure error with a new qubit initialised in state $|0\rangle$. It can also be seen as the Kronecker product of the partial trace (see definition 2.1.9) of a density matrix and a qubit in state $|0\rangle$, i.e., $\mathcal{R}_a(\rho_{ab}) = |0\rangle\langle 0|_a \otimes \mathrm{Tr}_a[\rho_{ab}]$.

Example 4.2.1. Consider a density matrix of a two qubit system, $\rho_{ab} = |{+}{+}\rangle\langle{+}{+}|_{ab}$. To reset qubit a and return it into state $|0\rangle$, we apply the reset channel as follows:

$$\mathcal{R}_a(\rho_{ab}) = |0{+}\rangle\langle 0{+}|_{ab}.$$

However, applying the reset channel on an entangled system that is initially a pure state transforms it into a mixed state. This is important to consider since the logical codewords of the $[\![5,1,3]\!]$ code are entangled states (see eq. (3.5)).

Example 4.2.2. Consider a density matrix of a maximally entangled two qubit system, $\rho_{ab} = |\Phi_{00}\rangle\langle\Phi_{00}|_{ab}$ with $|\Phi_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. To reset qubit a and return it into state $|0\rangle$, we apply the reset channel as follows:

$$\mathcal{R}_a(\rho_{ab}) = |0\rangle\langle 0|_a \otimes \frac{I_b}{2}.$$

PROTOCOL - 1 ERASURE ERROR

Let us first consider the case where 1 out of the 5 data qubits is lost. To prevent ambiguity, we label each of the 5 data qubits in fig. 4.5 below with one of the qubits being lost/erased. Since we know beforehand where the erasure had happened, e.g., a heralded erasure on qubit D_1, then we can replace the lost qubit with a new qubit in the $|0\rangle$ state. In other words, this combined action of qubit erasure and replacement can be modelled with the reset channel in eq. (4.4). The resulting state ρ'_L after the application of the reset channel can be written mathematically as follows:

$$\rho'_L = \mathcal{R}_{D_1}(\rho_L) = |0\rangle\langle 0|_{D_1} \otimes \rho_L^{(1\text{lost})}, \tag{4.5}$$

where $\rho_L^{(1\text{lost})} = \mathrm{Tr}_{D_1}[\rho_L]$ with $\rho_L = |\psi_L\rangle\langle\psi_L|$. Since ρ'_L is a mixed state, it follows that $\mathrm{Tr}[(\rho'_L)^2] < 1$.

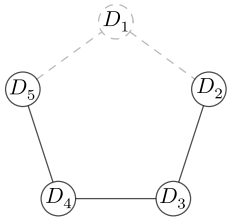


Figure 4.5: Graph state representation of the state $\rho_L^{(1\text{lost})} = \text{Tr}_{D_1}[\rho_L]$ where the data qubit D_1 encoding the logical qubit is lost.

Then, to return the mixed state back into the original logical state ρ_L, we can perform the quantum circuit as laid out in fig. 3.6 but with ρ_L' as the input state. Depending on the measurement outcomes of the ancilla qubits, we can apply Pauli corrections of weight $w \leq 2$ onto the 5 data qubits and thus correct for the erasure error. Furthermore, it was found that the $[\![5,1,3]\!]$ code can additionally tolerate 3 out of 12 Pauli errors on the 4 qubits that were not lost (there are 12 possibilities where single qubit errors can occur, i.e., $X_2, Y_2, Z_2, ..., X_5, Y_5, Z_5$). Taking normalisation into account, we can say that the $[\![5,1,3]\!]$ code can tolerate an additional $\frac{1}{4}$ Pauli errors on the remaining 4 qubits.

Depending on which of the 5 qubits is lost, the error syndromes are interpreted differently. The corresponding corrections are tabulated in table 4.1 below.

				Correction		
a_1	a_2	a_3	a_4	Lost: $D_{1/2}$	$D_{3/4}$	D_5
0	0	0	0	I	I	I
0	0	0	1	X_2	Y_3X_4	Y_1X_5
0	0	1	0	X_1Z_2	Z_3X_4	Z_5
0	0	1	1	X_1Y_2	X_3	Y_1Y_5
0	1	0	0	Z_1X_2	Z_3	X_1X_5
0	1	0	1	Z_1	X_3X_4	Z_1
0	1	1	0	Y_1Y_2	X_4	X_1Y_5
0	1	1	1	Y_1Z_2	Y_3	Z_1Z_5
1	0	0	0	X_1	Y_3Y_4	X_1
1	0	0	1	X_1X_2	Z_4	Z_1X_5
1	0	1	0	Z_2	X_3Z_4	Z_1X_5
1	0	1	1	Y_2	Z_3Y_4	Z_1Y_5
1	1	0	0	Y_1X_2	X_3Y_4	X_5
1	1	0	1	Y_1	Z_3Z_4	Y_1
1	1	1	0	Z_1Y_2	Y_3Z_4	Y_5
1	1	1	1	Z_1Z_2	Y_4	Y_1Z_5

Table 4.1: Corrections of $w \leq 2$ to the five data qubits depending on the ancilla outcomes and which data qubit was lost. $a_i = 0$ ($a_i = 1$) corresponds to a measurement outcome of $+1$ (-1) eigenstate. This correction look-up table is not unique because syndromes are shared by multiple cases where the additional error occurs on a different qubit that is not lost, e.g., when qubit D_1 is lost the syndrome $a_1, a_2, a_3, a_4 = 0,0,0,1$ corresponds to the cases where either an X_2, Z_3, Z_4, or X_5 error occurred.

However, it is possible to use an alternative approach involving data qubits permutation to simplify the correction table. Since the erasure error is heralded, we can perform permutation of the data qubits such that it always seems like the same qubit is lost from the point of view of the quantum circuit. In fig. 4.6, we show an example where we have

a heralded lost of data qubit D_5 and apply permutation of the data qubits as seen fit.

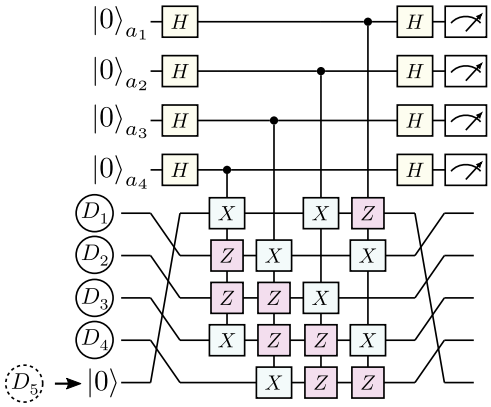


Figure 4.6: The data qubit D_5 that is lost is replaced with a new qubit in state $|0\rangle$. Since the lost detection is heralded, the data qubits can be permutated prior to the operations with the ancilla qubits. After the stabiliser operations, the permutation is undone and then we can apply the corrections as tabulated in table 4.2 to the data qubits.

In table 4.2 below, we find the simplified correction look-up table that uses this permutation technique.

				Correction	
a_1	a_2	a_3	a_4	Lost:	D_k
0	0	0	0		I
0	0	0	1		$X_{\mathcal{K}}$
0	0	1	0		$X_k Z_{\mathcal{K}}$
0	0	1	1		$X_k Y_{\mathcal{K}}$
0	1	0	0		$Z_k X_{\mathcal{K}}$
0	1	0	1		Z_k
0	1	1	0		$Y_k Y_{\mathcal{K}}$
0	1	1	1		$Y_k Z_{\mathcal{K}}$
1	0	0	0		X_k
1	0	0	1		$X_k X_{\mathcal{K}}$
1	0	1	0		$Z_{\mathcal{K}}$
1	0	1	1		$Y_{\mathcal{K}}$
1	1	0	0		$Y_k X_{\mathcal{K}}$
1	1	0	1		Y_k
1	1	1	0		$Z_k Y_{\mathcal{K}}$
1	1	1	1		$Z_k Z_{\mathcal{K}}$

Table 4.2: Corrections of $w \leq 2$ to the five data qubits depending on the ancilla outcomes and which data qubit was lost. The index k is such that $1 \leq k \leq 5$ and $\mathcal{K} = (k \bmod 5)+1$. $a_i = 0$ ($a_i = 1$) corresponds to a measurement outcome of $+1$ (-1) eigenstate.

PROTOCOL - 2 ERASURE ERRORS

For 2 erasure errors, the protocol is similar to that of 1 erasure error shown in the previous section. Since 2 qubits are lost instead of one, the resulting error syndromes have be interpreted differently again. In fig. 4.7 is a graph representation of one such resulting

state from losing 2 qubits. Furthermore, there are now $\binom{5}{2} = 10$ possible ways of losing 2 out of 5 data qubits instead of just 5 in the previous section. Therefore, the correction table is considerably larger (see table 4.3).

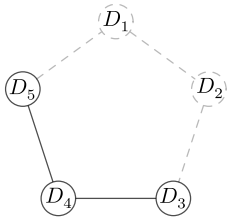


Figure 4.7: Graph state representation of the state $\rho_L^{(2\text{lost})} = \mathrm{Tr}_{D_2}\left[\mathrm{Tr}_{D_1}\left[\rho_L\right]\right]$ where the data qubits D_1 and D_2 encoding the logical qubit is lost.

				Correction										
a_1	a_2	a_3	a_4	Lost:	$D_{1\&2}$	$D_{1\&3}$	$D_{1\&4}$	$D_{1\&5}$	$D_{2\&3}$	$D_{2\&4}$	$D_{2\&5}$	$D_{3\&4}$	$D_{3\&5}$	$D_{4\&5}$
0	0	0	0		I	I	I	I	I	I	I	I	I	I
0	0	0	1		X_2	Z_1Z_3	X_1Z_4	Y_1X_5	X_2	X_2	X_2	Y_3X_4	X_3Z_5	Y_4Y_5
0	0	1	0		X_1Z_2	Z_1Y_3	Y_1Y_4	Z_5	X_2X_3	Y_2Z_4	Z_5	Z_3X_4	Z_5	Z_5
0	0	1	1		X_1Y_2	X_3	Z_1X_4	Y_1Y_5	X_3	Z_2Z_4	X_2Z_5	X_3	X_3	Y_4X_5
0	1	0	0		Z_1X_2	Z_3	Y_1Z_4	X_1X_5	Z_3	Y_2Y_4	Z_2Y_5	Z_3	Z_3	X_4Z_5
0	1	0	1		Z_1	Z_1	Z_1	Z_1	X_2Z_3	Z_2Y_4	Y_2Y_5	X_3X_4	Y_3Z_5	Z_4X_5
0	1	1	0		Y_1Y_2	Z_1X_3	X_4	X_1Y_5	X_2Y_3	X_4	Z_2X_5	X_4	Z_3Z_5	X_4
0	1	1	1		Y_1Z_2	Y_3	X_1Y_4	Z_1Z_5	Y_3	X_2X_4	Y_2X_5	Y_3	Y_3	Z_4Y_5
1	0	0	0		X_1	X_1	X_1	X_1	Y_2X_3	X_2Z_4	Z_2Z_5	Y_3Y_4	Z_3X_5	X_4Y_5
1	0	0	1		X_1X_2	Y_1Z_3	Z_4	Z_1X_5	Z_2X_3	Z_4	Y_2Z_5	Z_4	Y_3Y_5	Z_4
1	0	1	0		Z_2	Y_1Y_3	Z_1Y_4	X_1Z_5	Z_2	Z_2	Z_2	X_3Z_4	Z_3Y_5	X_4X_5
1	0	1	1		Y_2	X_1X_3	Y_1X_4	Z_1Y_5	Y_2	Y_2	Y_2	Z_3Y_4	Y_3X_5	Z_4Z_5
1	1	0	0		Y_1X_2	X_1Z_3	Z_1Z_4	X_5	Y_2Y_3	Z_2X_4	X_5	X_3Y_4	X_5	X_5
1	1	0	1		Y_1	Y_1	Y_1	Y_1	Z_2Y_3	Y_2X_4	X_2X_5	Z_3Z_4	X_3Y_5	Y_4Z_5
1	1	1	0		Z_1Y_2	Y_1X_3	X_1X_4	Y_5	Z_2Z_3	X_2Y_4	Y_5	Y_3Z_4	Y_5	Y_5
1	1	1	1		Z_1Z_2	X_1Y_3	Y_4	Y_1Z_5	Y_2Z_3	Y_4	X_2Y_5	Y_4	X_3X_5	Y_4

Table 4.3: Corrections of $w \leq 2$ to the five data qubits depending on the ancilla outcomes and which data qubits were lost. $a_i = 0$ ($a_i = 1$) corresponds to a measurement outcome of $+1$ (-1) eigenstate.

As shown in the previous section, we can also employ the data qubits permutation approach in the 2-erasure case to simplify the correction table. Figure 4.8 below is a circuit representation of one such example.

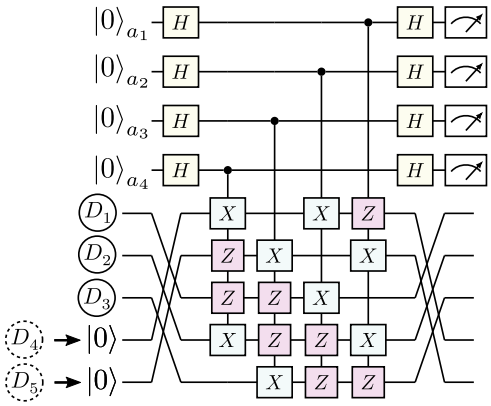


Figure 4.8: The data qubits D_4 and D_5 that are lost are each replaced with a new qubit in state $|0\rangle$. Since the lost detection is heralded, the data qubits can be permutated prior to the operations with the ancilla qubits. After the stabiliser operations, the permutation is undone and then we can apply the corrections as tabulated in table 4.4 to the data qubits.

This permutation of qubits via heralded loss results in a simplified table as shown in table 4.4.

				Correction	
a_1	a_2	a_3	a_4	Lost: $D_{k\&\mathcal{K}_1}$	$D_{k\&\mathcal{K}_2}$
0	0	0	0	I	I
0	0	0	1	$X_{\mathcal{K}_1}$	$Z_k Z_{\mathcal{K}_2}$
0	0	1	0	$X_k Z_{\mathcal{K}_1}$	$Z_k Y_{\mathcal{K}_2}$
0	0	1	1	$X_k Y_{\mathcal{K}_1}$	$X_{\mathcal{K}_2}$
0	1	0	0	$Z_k X_{\mathcal{K}_1}$	$Z_{\mathcal{K}_2}$
0	1	0	1	Z_k	Z_k
0	1	1	0	$Y_k Y_{\mathcal{K}_1}$	$Z_k X_{\mathcal{K}_2}$
0	1	1	1	$Y_k Z_{\mathcal{K}_1}$	$Y_{\mathcal{K}_2}$
1	0	0	0	X_k	X_k
1	0	0	1	$X_k X_{\mathcal{K}_1}$	$Y_k Z_{\mathcal{K}_2}$
1	0	1	0	$Z_{\mathcal{K}_1}$	$Y_k Y_{\mathcal{K}_2}$
1	0	1	1	$Y_{\mathcal{K}_1}$	$X_k X_{\mathcal{K}_2}$
1	1	0	0	$Y_k X_{\mathcal{K}_1}$	$X_k Z_{\mathcal{K}_2}$
1	1	0	1	Y_k	Y_k
1	1	1	0	$Z_k Y_{\mathcal{K}_1}$	$Y_k X_{\mathcal{K}_2}$
1	1	1	1	$Z_k Z_{\mathcal{K}_1}$	$X_k Y_{\mathcal{K}_2}$

Table 4.4: Corrections of $w \leq 2$ to the five data qubits depending on the ancilla outcomes and which data qubits were lost. Here, $\mathcal{K}_j = (k + j - 1 \bmod 5) + 1$ and $a_i = 0$ ($a_i = 1$) corresponds to a measurement outcome of $+1$ (-1) eigenstate.

5

QUANTUM KEY DISTRIBUTION

5.1. INTRODUCTION

In the previous chapters, we dealt with the concepts of quantum error and erasure correction which are relevant to the hybrid repeater scheme outlined in chapter 6. However, another concept that is also relevant to the scheme is quantum key distribution (QKD) which enables secured long-distance communication. QKD is a means of certifying the security of a cryptographic key generated between two parties (the sender is typically called *Alice* and the receiver *Bob* in literature for demonstration purposes) by utilising the properties of quantum mechanics. Since the inception of QKD by Bennett and Brassard in 1984 [11] and Ekert in 1991 [49], new protocols were proposed, e.g., B92 [50] and SARG04 [51]. In fact, the protocols mentioned above are part of one of the three families of explicit protocols, namely, the discrete-variable (DV) protocols. In DV protocols, a single-photon detector (SPD) is applied on Bob's side. The other two are called continuous-variable (CV) protocols and distributed-phase-reference protocols, which are not discussed in this thesis. For a comprehensive overview on these topics, we recommend this review paper by Scarani *et al.* [52].

In this chapter, we will focus solely on the six-state variant of the BB84 protocol [53] and its corresponding secret key fraction, which will be crucial in studying and quantifying the performance of the hybrid repeater scheme in chapter 6. In fact, we chose the six-state variant of the BB84 protocol for two reasons: (1) the six-state BB84 protocol has higher tolerance for depolarising errors compared to the conventional BB84 protocol [52], and (2) to compare the results of a homogeneous one-way repeater scheme that used the same QKD protocol [18]. The BB84 protocol and its variants are part of the DV protocols which achieves the *unconditional security* (i.e., guaranteed security without imposing any restriction on the power of the eavesdropper) by leveraging the no-cloning theorem (see section 3.1) and the indistinguishability of non-orthogonal states (see theorem 5.1.1).

Theorem 5.1.1. There can never exist a measurement device such that it can deterministically distinguish between non-orthogonal states.

Remark. This theorem implies that if an eavesdropper *Eve* interacts with the transmitted quantum states from Alice to Bob and tries to steal information from those states, she will inadvertently disturb the fidelity of the quantum states, which results in the detection by Bob. For the proof of this theorem, refer to chapter 5 of the textbook by Djordjevic [31].

5.2. SIX-STATE VARIANT OF BB84

The six-state variant of the BB84 protocol is basically the original four-state BB84 protocol with an extra basis. In the original BB84 scheme, only 2 pairs of antipodal points on the Bloch sphere are utilised, i.e., the points along the $\pm x$ and $\pm y$ directions. The essence of the original protocol consists of Alice sending a qubit prepared in one of the two bases to Bob, who then measures the received qubit in either the X and Y basis in a uniformly random fashion. This implies that Alice and Bob will on average use the same basis 50% of the time and therefore they would have to discard half of the qubits before the extraction of the secret key.

In the six-state protocol, the extra pair of antipodal points along the $\pm z$ axis of the Bloch sphere are also utilised, and therefore there are in total six distinct states which Alice can prepare her qubits in. When Bob receives the qubit, he can then randomly choose between X, Y, or Z basis to measure it in, which results in a reduced probability of them sharing the same basis. Now, Alice and Bob on average use the same basis only $\approx 33.3\%$ of the time and they would have to discard $2/3$ of the qubits before the extraction of the secret key.

Despite the higher proportion of discarded qubits, the six-state BB84 protocol has higher symmetry compared to the original scheme, which results in significantly reduced the number of degrees of freedom in problems related to eavesdropping. In this section, however, we will only be reviewing the protocol and not the eavesdropping strategies. For further reading in the security of the protocol against various eavesdropping strategies of the six-state BB84 protocol, we suggest this paper by Bechmann-Pasquinucci and Gisin [53].

The illustration of the six-state BB84 protocol with detailed step-by-step descriptions is shown in table 5.1, which assumes no leakage of information during the transmission, e.g., due to an eavesdropper or an error-prone communication channel. Unfortunately, the assumption that no eavesdroppers or errors during the transmission of qubits between Alice and Bob as shown in table 5.1 is too idealistic. Such undisturbed transmission of qubits is almost impossible to achieve in practice as it is extremely difficult to isolate qubits from external interactions with the environment and for the time required in practical applications. To ensure security, the protocol must be resilient against eavesdroppers, i.e., detect the presence of an eavesdropper and correct for any erroneous transmitted bits.

The BB84 protocol detects the presence of an eavesdropper if there is at least one mismatch during the comparison of measured bits between Alice and Bob. After the sifting step, Alice and Bob performs *parameter estimation* where they compute an error

rate with the measured values that they shared with each other. If the number of mismatches exceeds a certain threshold, Alice and Bob abort the protocol and retry from the beginning. Else, Alice and Bob proceed to perform *error correction* and *privacy amplification* to the resulting bit string (sifted key), and they share the *secure key* [25].

The qubit error rates, or QBER, is crucial in determining the secret key fraction and the secret key rate, which we will discuss in the following section.

For qubit no.	1	2	3	4	5	6	7	8	9	10	11	12	…
	Alice chooses randomly one of the basis: X-, Y- or Z-basis. Suppose she chooses												
Alice's basis	X	X	Z	Y	Y	X	Z	Y	Z	X	Z	Y	…
	and measures												
Alice's value	$+1$	-1	-1	$+1$	$+1$	-1	$+1$	-1	-1	$+1$	-1	$+1$	…
	Alice's qubit is then in the												
Qubit state	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+i\rangle$	$\|+i\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-i\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+i\rangle$	…
	Bob measures the prepared qubits sent by Alice to Bob, who chooses randomly one of the basis: X-, Y- or Z-basis. Suppose he chooses												
Bob's basis	Z	Y	Z	Z	X	X	Y	X	Z	Z	Y	Y	…
	and measures												
Bob's value	$+1$	$+1$	-1	-1	$+1$	-1	-1	$+1$	-1	-1	-1	$+1$	…
	Alice and Bob publicly compare via a secure classical communication channel which basis was used in each of the measurements. They, however, do not reveal the measured value. Then, they choose a subset of bits where they chose the same basis. This procedure is called *sifting*.												
Same basis?	$\neq$	$\neq$	$=$	$\neq$	$\neq$	$=$	$\neq$	$\neq$	$=$	$\neq$	$\neq$	$=$	…
	Their measured values must agree at qubits where they share the same chosen basis to measure in. As a control, they publicly compare via a secure classical communication channel every second of the measured values that shared the same basis:												
Control-value Alice			-1						-1				…
Bob			-1						-1				…
	100% agreement in comparison of the control values indicates that most probably there was no leakage of information during the transmission between Alice and Bob. The remaining measured values with shared basis are then used as *joint*, *secret*, and *random*												
bitstring						$\mathbf{-1}$						$\mathbf{+1}$	…

Table 5.1: Six-state BB84 protocol assuming no eavesdroppers or errors. Adapted and modified from [27].

5.3. SECRET KEY FRACTION

As mentioned in section 5.1, determining the secret key fraction of a QKD protocol is imperative in quantifying its performance given some quantum repeater scheme. The secret key fraction can be seen together commonly with the *raw key rate*, forming the *secret key rate* or SKR, and it can be written generally as a product below [52]:

$$SKR = f \cdot R_{\text{raw}}, \tag{5.1}$$

where f is the secret key fraction and R_{raw} is the raw key rate. Recall from section 5.2 that after the sifting procedure (which leaves them with n bits out of N transmitted bits), Alice and Bob performs classical post-processing where they perform error correction and privacy amplification. The errors could be caused by either an imperfect quantum communication channel or the presence of an eavesdropper Eve. After the error correction step, the resulting key is called the *corrected key*. In the step where Alice and Bob remove correlation associated with Eve, which is called privacy amplification, they are left with m bits out of n bits. The corresponding key is the *secure key*. In the asymptotic limit of the raw key size, i.e., $N \to \infty$ where N is the raw key size, the secret key fraction is expressed as [52]:

$$f = \frac{m}{n}, \tag{5.2}$$

which represents the essence of QKD since it is the quantity which must be explicitly derived in the proofs for security. In finitely long keys, the secret key fraction deviates from these expression above due to the parameter estimation being performed on a finite number of samples, which results in statistical fluctuations. We focus on the asymptotic case in this thesis since it is a useful way to quantify the performance of a QKD protocol. It should be, however, noted that error corrections in finite cases are actually not negligible [52].

In the context of the presence of an eavesdropper, the secret key fraction can also be expressed as [52]:

$$f = \max(I(A:B) - I_E, 0), \tag{5.3}$$

where $I(A:B) = 1 - h(Q)$[1] is the mutual information between Alice's and Bob's raw keys with $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ being the binary entropy and Q denoting the QBER. I_E is the information that Eve has about Alice or Bob's raw key. We can see that if $I(A:B) < I_E$, then Eve has more information Alice's bitstring than Bob does, and therefore the QKD protocol must be aborted and no secret key can be obtained. This is reflected in the *max* function in eq. (5.3).

Now, we present the explicit expression of I_E in the six-state BB84 protocol, assuming a depolarising channel, i.e., qubit errors in the X, Y, and Z basis are all equally probable [52]:

$$I_E = Q + (1-Q)h\left(\frac{1-3Q/2}{1-Q}\right). \tag{5.4}$$

For the detailed derivation of eq. (5.4), refer to the appendix of the paper by Scarani *et al.* [52]. With this, the secret key fraction then becomes:

$$f = \max(1 - h(Q) - Q - (1-Q)h\left(\frac{1-3Q/2}{1-Q}\right), 0). \tag{5.5}$$

Solving for eq. (5.5) yields $Q_{\text{threshold}} \approx 12.61\%$ when f reaches 0, which implies that at QBER higher than $\approx 12.61\%$, the QKD protocol is compromised by Eve having too much information and has to be aborted. For quantifying the performance of the hybrid one-way quantum repeater network in the following chapter, we will be using the secret key fraction as shown in eq. (5.5).

[1] It was assumed that the bit values of Alice and Bob are both equally probable. See [52]

6

HYBRID ONE-WAY QUANTUM REPEATER CHAIN

The results in this chapter as well as appendices cited in this chapter were obtained using code written in MATLAB [54] and the source code can be found in the following public GitHub repository: `github.com/bernwo/Master-Thesis-Code`.

6.1. SEQUENTIAL SCHEDULING

In homogeneous one-way quantum repeater schemes (i.e., quantum repeater chain consisting of only one type of station) such as the one found in [18], the operational errors are unaccounted for because of the noisy Bell state measurement during the encoding of the message qubit into a tree cluster state, whose root qubit is unprotected against errors. To account for the operational errors, we introduce an additional QECC acting as the outer code while the tree code acts as the inner code. The outer code considered here is the $[\![5,1,3]\!]$ code, which is outlined and explained in detail in previous sections. Inevitably, the introduction of an outer code results in a repeater network which consists of 2 types of stations: a *hybrid one-way quantum repeater chain*. The overview of such a network using a sequential scheduling is shown in fig. 6.1 and its detailed scheduling is shown in fig. 6.2.

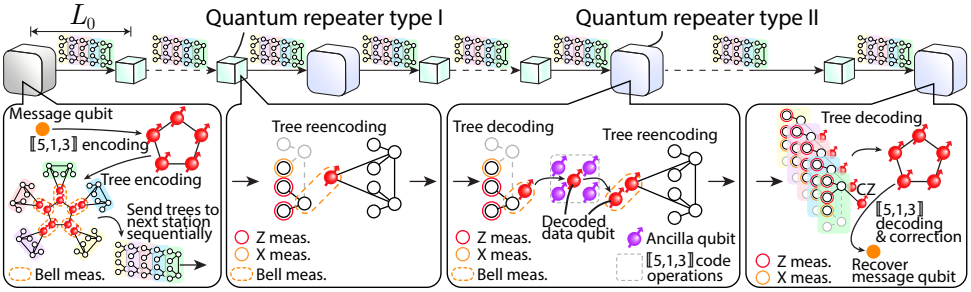


Figure 6.1: Overview of the hybrid one-way quantum repeater network with sequential scheduling containing two types of repeater stations: type I (green) and type II (blue). In the first station (greyed because no error correction is involved), a message qubit is encoded using the ⟦5,1,3⟧ code into 5 data spin qubits. Then, each of those data spin qubit is sequentially encoded into a time-bin based photonic tree cluster state via a Bell state measurement (orange dashed box) with the root spin qubit. The $\vec{t} = [2,2]$ tree is used as an example here. The encoded qubits (each encased in differently coloured boxes) are then sequentially sent along the repeater chain where the repeater stations are spaced L_0 apart from each other. Stations of type I (green) decodes the received partially lost tree, and reencodes the decoded qubit into a new tree via heralded storage (not shown, see [18]). Stations of type II (blue) decode the incoming tree at the tree level, then perform stabiliser operations (i.e., two-qubit gates and syndrome extraction on the ⟦5,1,3⟧ level) between the decoded qubit and the ancilla qubits in the station. After the stabiliser operations, the decoded qubit is reencoded back into a new tree and sent off to the next station. At the end station, the incoming 5 trees are received and decoded sequentially. Once all decoded 5 data qubits are obtained, the ⟦5,1,3⟧ code corrections are applied according to the syndromes obtained along the network and finally they are decoded back into the message qubit.

As shown in fig. 6.1, there are quantum repeaters of type I and II. Type I repeaters are primarily responsible for correcting the loss error at the tree code level (see section 4.1). The type II repeaters, on the other hand, specialise in correcting for both arbitrary single qubit error (see chapter 3) due to reencoding error and heralded loss error (see chapter 4) using the ⟦5,1,3⟧ code.

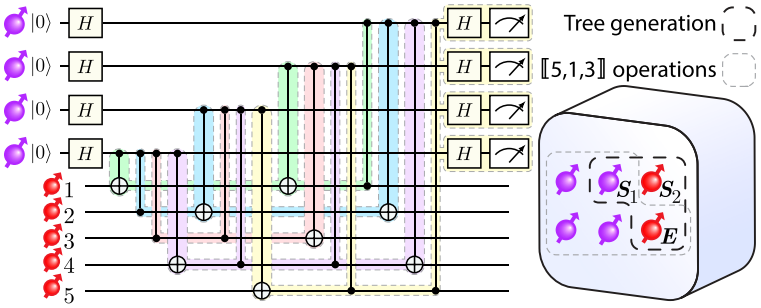


Figure 6.2: (Left) Detailed sequential scheduling with respect to the non-fault-tolerant implementation of the ⟦5,1,3⟧ code and (right) physical resources of the type II quantum repeater. The tree associated with qubit $_1$ arrives first, followed by the tree associated with qubit $_2$, and so on. Since the trees are received sequentially, the ⟦5,1,3⟧ operations are also done sequentially and in the following order: → → → → . When all five data qubits have passed through the station, the ancilla qubits are measured in parallel in the step denoted by . Three out of the six spins inside the repeater station are used for tree generation (see section 4.1.1). When a tree is generated, two of the three spins become available for other operations. In this case, the spin $_{S_1}$ can be allocated as an ancilla qubit for the ⟦5,1,3⟧ operations while the emitter spin $_E$ is used for storing the decoded data qubit $_i$ with $i \in \{1,2,3,4,5\}$. The remaining spin $_{S_2}$ is the root qubit of the new tree.

The noise in the circuit can be modelled the same way as shown previously in fig. 3.9. In fact, the input single-qubit depolarising noise experienced by the data qubits in fig. 6.2 can be described by an effective error rate of the incoming trees that travelled n links:

$$\epsilon_{\text{trans}} = 1-(1-\epsilon_r)^n, \tag{6.1}$$

where ϵ_r is the reencoding error rate at each of the links between type I stations. We say that each of the 5 data qubits at each of the type II stations is subjected to a depolarising channel $\Lambda_{(1)}(\epsilon_{\text{trans}})$ (see eq. (3.6)). We also assume that each qubit in a tree cluster state experiences the uncorrelated depolarising error at a rate of ϵ_0; we say that the qubits in the tree are subjected to the depolarising channel $\Lambda_{(1)}(\epsilon_0)$. As for the reencoding error, it was established that it is dominated by the root qubit and the first-level qubit involved in the reencoding and that the reencoding error rate does not differ significantly between different tree vectors [18]. Together with the faulty Bell state measurement[1], the reencoding error can be modelled as $\epsilon_r = 1-(1-\epsilon_0)^3$ which can be approximated as $\epsilon_r \approx 3\epsilon_0$ for when ϵ_0 is small which is consistent with what Borregaard *et al.* has found via numerical analysis that takes majority voting into account [18]. We also assume that the two-qubit gates in fig. 6.2 are subjected to the two-qubit depolarising channel as shown in eq. (3.7) at the same error rate, i.e., the noisy two-qubit gates are described by the depolarising channel $\Lambda_{(2)}(\epsilon_0)$. Since we have established the noise channels present in the quantum circuit, let us rewrite it in the channel representation (see section 3.6) as $\mathcal{C}_{\text{seq}}$, which is shown alongside with the network and circuit representations in fig. 6.3.

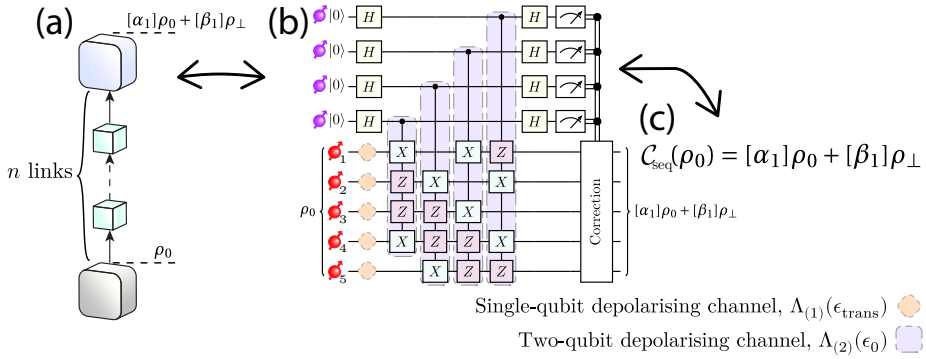


Figure 6.3: Equivalence between the (a) network, (b) circuit, and (c) channel representations. The initial input state is the perfect logical state on the $[\![5,1,3]\!]$ code level which is denoted as $\rho_0 = |\psi_L\rangle\langle\psi_L|$.

It should be noted that the $[\![5,1,3]\!]$ code correction step is not carried out locally in the interstitial type II stations between the start and end station due to the nature of the sequential scheduling protocol[2], i.e., the 5 data qubits are never in the same station simultaneously. Instead, the measured syndrome at each of the station is sent through a

[1] The two-qubit gate in the Bell state measurement is assumed to be subjected to the depolarising channel $\Lambda_{(2)}(\epsilon_0)$ (see eq. (3.7)).

[2] Despite the delayed error correction step, this is actually equivalent to the case where the correction steps are not delayed, provided that the application of correction itself does not introduce error. In practice, they do introduce non-zero error, and thus the delayed correction method is preferred.

classical channel to the end station and only then the $[\![5,1,3]\!]$ code corrections are applied to the 5 physical qubits by interpreting the received syndromes correctly. Moreover, the encoding step (i.e., at the start station) and decoding step (i.e., at the end station) introduce negligible error compared to the error introduced by the transmission through the entire repeater chain, which is why these errors are not considered. The error in the readout of the ancilla qubits is also assumed negligible compared to the error introduced by the two-qubit gates.

Owing to the $[\![5,1,3]\!]$ code acting as our additional outer code, the effective error rate is lower compared to the case without an outer code. We say that the tree code is concatenated with the $[\![5,1,3]\!]$ code. The effective (logical) error rate in the case with code concatenation, i.e., hybrid repeater chain, is described by $\epsilon_L(c) = 1 - \langle\psi_L|\,\rho_c\,|\psi_L\rangle$ where ρ_c is the resulting state after applying $\mathcal{C}_{\text{seq}}$ to ρ_0 c times. Using the recursive model function as shown in eq. (A.5), it can be approximated as $\epsilon_L(c) \approx 1 - \mathcal{F}^{c,2}_{\mathcal{C}_{\text{seq}}}[\rho_0]$. In the case *without* code concatenation, i.e., homogeneous repeater chain, the effective error rate is simply ϵ_{trans} [18]. In fig. 6.4 below, we find the comparison of the effective error rates between the hybrid and homogeneous for varying reencoding error rate ϵ_r, with fixed $n = 20$ links between consecutive type II stations. Note that for all logical error calculations in this chapter assumes that the initial state is $|\psi_L\rangle = |+_L\rangle$. We found that there is no significant difference in the resulting error rate with different initial states due to the depolarising noise model.

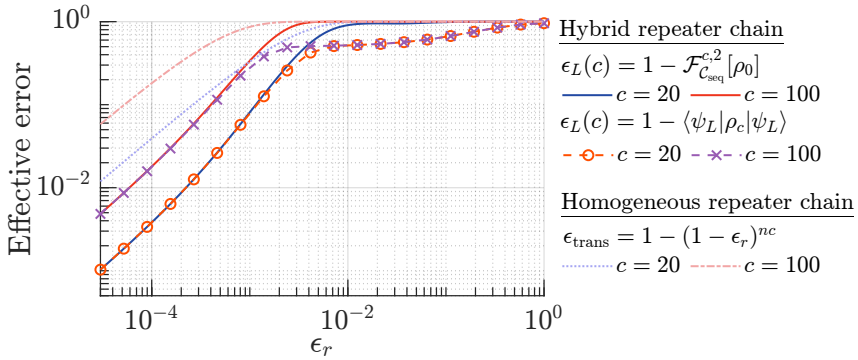


Figure 6.4: Effective error as a function of the reencoding error ϵ_r with fixed $n = 20$ links between consecutive type II stations. Results are computed for $c \in \{20, 100\}$ number of type II stations exactly (marker-ed dashed lines) and approximately using the recursive model function (solid lines). The effective error rates for the homogeneous repeater chain with corresponding $n_{\text{tot}} = nc$ are also shown for comparison (dashed lines). The initial logical state which we are using here is $|\psi_L\rangle = |+_L\rangle$.

The observations we can make from fig. 6.4 are two-fold. First, the effective output error rate for the hybrid case is significantly lower than the homogeneous case with corresponding n_{tot} for sufficiently low reencoding error rate, ϵ_r. For instance, the dashed orange line shows a significantly lower effective error rate compared to that of the dashed blue line. Therefore, we have confirmed that the hybrid repeater chain indeed offers clear advantage in terms of effective output error rate over the homogeneous repeater chain. Second, the error rates computed using the recursive model (see eq. (A.5)) are

accurate for sufficiently low ϵ_r. For example, the solid blue line and the dashed orange line overlaps almost perfectly for ϵ_r less than $\sim 10^{-3}$. We can thus say that the recursive model is a reliable method of calculating the effective error rate which saves significant computational resources for large c. A trade-off is that the recursive model does not produce accurate result at higher error rates, which remains an outstanding challenge.

Now, let us re-introduce eq. (4.1) in the context of the repeater network:

$$\eta_e = [(1-\mu+\mu R_1)^{b_0} - (\mu R_1)^{b_0}](1-\mu+\mu R_2)^{b_1}, \tag{6.2}$$

where η_e is the probability of successful transmission of the encoded qubit at the tree level between repeater stations. $R_k = 1-[1-(1-\mu)(1-\mu+\mu R_{k+2})^{b_{k+1}}]^{b_k}$ is the probability of successfully performing on indirect Z-basis measurement on a qubit in the k^{th} level and was given in eq. (4.2). Here, $\mu = 1-\eta\eta_d$ with $\eta = e^{-L_0/L_{\text{att}}}$ being the transmission probability of a single photon between repeater stations and η_d being the probability of the photon detector successfully detecting the incoming photon. As shown in fig. 6.1, L_0 is the inter-repeater distance while the quantity $L_{\text{att}} = 20$ km is the attenuation length of the optical fibre.

Recall that in chapter 4 we have established that the $[\![5,1,3]\!]$ code can correct for heralded 1- and 2-erasure errors. In the context of the hybrid repeater network as shown in fig. 6.1, the probability of two trees being completely unrecoverable (without the help of $[\![5,1,3]\!]$ erasure correction) in the same type II station is negligible compared to the probability of only one tree being completely unrecoverable. Therefore, we consider only correcting for 1-erasure errors at the $[\![5,1,3]\!]$ code level in our hybrid repeater scheme. With this, the probability of a message qubit successfully being transmitted through the entire hybrid repeater chain can be written as:

$$p_{\text{trans}}(c,i) = [\eta_e^{5n}]^{c-i} \cdot [5\eta_e^{4n}(1-\eta_e^n)]^i, \tag{6.3}$$

where n is the number of links between consecutive type II stations and c is the total number of type II stations in the entire hybrid repeater chain. Here, i denotes the occurrence of 1-erasure errors on i distinct type II stations. For example, $p_{\text{trans}}(c,0) = \eta_e^{5n_{\text{tot}}}$ is the transmission probability of the message qubit throughout the entire chain given absolutely no erasure errors occurred on the $[\![5,1,3]\!]$ code level. Here, $n_{\text{tot}} = nc$ is the total number of links throughout the entire chain. The first term in eq. (6.3), i.e., η_e^{5n}, represents the probability of the set of five trees being completely recoverable without the need for erasure correction at the $[\![5,1,3]\!]$ code level. The second term, i.e., $5\eta_e^{4n}(1-\eta_e^n)$, represents the probability of one of the five trees being completely unrecoverable at the tree code level at the following type II station.

The logical error rate associated with a single 1-erasure error occurrence, i.e., $i = 1$, for a hybrid repeater chain with $c = 1$ and $n = 20$ is shown in fig. 6.5. Since $c = i = 1$, it means that there is only 1 type II station (which is also the end station) in the hybrid chain and that the 1-erasure error happened in that same station. Despite the higher error rate of the hybrid chain compared with the homogeneous chain in fig. 6.5, the performance is actually better than that of the homogeneous chain because in the homogeneous case, the probability of the message qubit being successfully transmitted to the end station *given that a tree is lost and completely unrecoverable* is 0. In the hybrid case,

however, despite losing one out of the five trees, we can still recover the lost information through the heralded 1-erasure correction protocol as outlined in section 4.2.1.

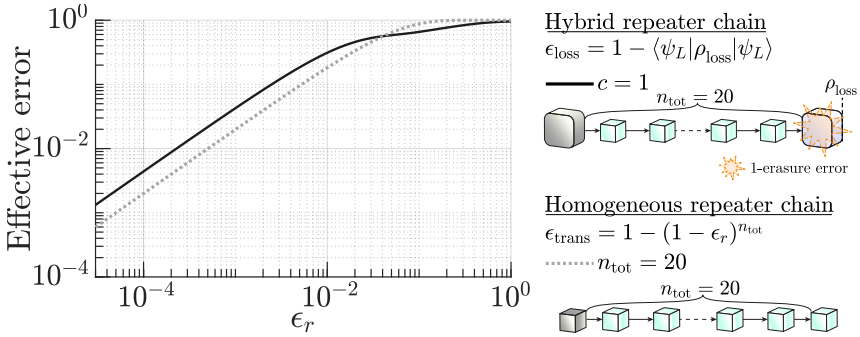


Figure 6.5: Effective error as a function of the reencoding error ϵ_r with fixed $n = 20$ links between consecutive type II stations. The effective error rates for both the hybrid and homogeneous repeater chain are shown here. A single 1-erasure error occurrence is assumed for the hybrid repeater chain. On the left, sketches of the corresponding simulated systems are shown for clarity.

Another important quantity to consider is the generation time of a tree described by the tree vector $\vec{t} = [b_0, b_1, \ldots, b_d]$, which is estimated as [18]:

$$\begin{aligned}\tau_{\text{tree}} \approx\ & b_0\Big[100 + b_1(1 + b_2(1 + \cdots b_{d-1}(1 + b_d)\cdots))\Big]\tau_{\text{ph}} \\ & + b_0\Big[3 + b_1(1 + b_2(1 + \cdots b_{d-2}(1 + b_{d-1})\cdots))\Big]\tau_{\text{ss}},\end{aligned} \tag{6.4}$$

where τ_{ph} is the emission time of a single photonic qubit while τ_{ss} is the time needed to apply a spin-spin gate, i.e., *CZ* or *CX* gate. As assumed in [18], the time to emit the first-level (i.e., b_0) photons is set to be slower by a factor of 100 to ensure low error rate in the reencoding step, hence the term $100\tau_{\text{ph}}$ in eq. (6.4). On the other hand, the term $3\tau_{\text{ss}}$ comes from the fact that 3 spin-spin gates are needed for the creation of the first-level photons.

If the six-state variant of the BB84 protocol (see section 5.2) is chosen for the QKD between the start and end station, then the secret key fraction is given by:

$$f(Q_{c,i}) = \max(1 - h(Q_{c,i}) - Q_{c,i} - (1 - Q_{c,i})h\left(\frac{1 - 3Q_{c,i}/2}{1 - Q_{c,i}}\right), 0), \tag{6.5}$$

where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy and $Q_{c,i} = 2\epsilon_{\text{eff}}(c,i)/3$ denotes the QBER of the decoded qubit at the end station[3]. This secret key fraction was also shown in eq. (5.5) in chapter 5, but is reintroduced here for the convenience of the reader. The quantity $\epsilon_{\text{eff}}(c,i)$ is the effective error rate of the received qubit at the end station given there were i 1-erasure error occurrences and c type II stations. Unfortunately, the computational resource needed to obtain the closed form expression of $\epsilon_{\text{eff}}(c,i)$ is infeasibly high. Instead, it is approximated using a combination of the *recursive model* for

[3] We assume that the decoded qubit is subjected to a single-qubit depolarising channel of error rate $\epsilon_{\text{eff}}(c,i)$, i.e., $\Lambda_{(1)}(\epsilon_{\text{eff}}(c,i))$.

the 0-erasure part of the chain (see eq. (A.5)) and *pessimistic model* for the 1-erasure occurrences (see eq. (3.14)). To do this, we first need to establish the following assumption that all possible permutations of the 1-erasure occurrence in the repeater chain corresponds to the same effective error rate. Such an example using $c = 4$ type II stations and $i = 2$ 1-erasure errors is shown in fig. 6.6 below. Then, the simplified calculation can be done as shown in the example in fig. 6.7 using a repeater chain with the same configuration. Using this simplified calculation method, the effective error rate can then be written as:

$$\epsilon_{\text{eff}}(c,i) = 1 - (1-\epsilon_L(c-i))(1-\epsilon_{\text{loss}})^i. \tag{6.6}$$

Note that we found no significant difference in the effective error rates between the different set-ups in fig. 6.6, especially in the regime where $c \gg i$. This is a suitable approximation for our calculation in the following section since it involves working in the same regime.

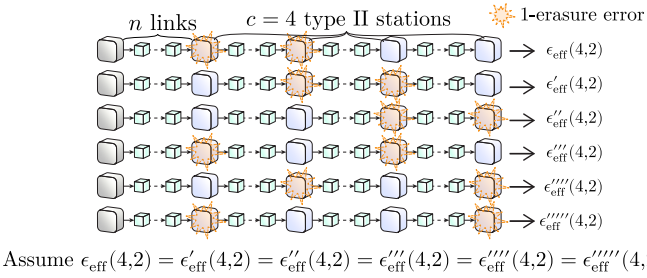


Figure 6.6: All $\binom{4}{2} = 6$ possible permutations of $i = 2$ 1-erasure occurrences in a network with $c = 4$ type II stations and their corresponding effective error rate.

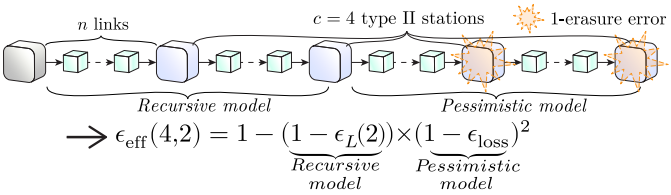


Figure 6.7: Example calculation of $\epsilon_{\text{eff}}(4,2)$ using a combination of recursive and pessimistic model. The recursive model is used on the section without erasure errors, while the pessimistic model is used on the section with 1-erasure errors.

6.1.1. SECRET KEY RATE AND COST FUNCTION

With preliminaries established in the previous section, the secret key rate can then be written as:

$$SKR = T^{-1} \cdot \sum_{i=0}^{c} \left(\binom{c}{i} \cdot f(Q_{c,i}) \cdot p_{\text{trans}}(c,i) \right), \tag{6.7}$$

where $T = 5\tau_{\text{tree}} + 16\tau_{\text{ss}} + \tau_{\text{meas}}$ is the total processing time of each repeater station for one logical qubit. τ_{meas} is the time needed to read out an ancilla qubit but since the

readouts are done in parallel, we do not need to multiply this term. The emitter is considered to be strongly coupled with a single-sided cavity and the readout time by photon scattering of the cavity is assumed to be negligible compared to the tree generation time [18] and two-qubit gate operations, i.e., $5\tau_{\text{tree}} + 16\tau_{\text{ss}} \gg \tau_{\text{meas}}$. Therefore, we can approximate $\tau_{\text{meas}} \approx 0$. In addition, owing to the assumption made in fig. 6.6, we can group the secret key fraction terms together with a binomial coefficient as prefactor, i.e., $\binom{c}{i} \cdot f(Q_{c,i})$. Note that for the purpose of saving on computational resources, we capped the sum at $c = 20$ for our secret key rate calculation. This is a good approximation since higher terms have negligible contributions to the secret key rate.

Then, we propose the following (dimensionless) cost function, denoted by C, related to the resources used by the network chain which we will seek to minimise:

$$C = SKR^{-1} \cdot \frac{mL_{\text{att}}}{\tau_{\text{ph}} L_{\text{tot}}}, \tag{6.8}$$

where $m = s_I^3 m_I + s_{II}^3 m_{II}$ is the weighted sum of the stations in the network and $L_{\text{tot}} = L_0 n_{\text{tot}}$ is the total distance between the start and end station. Here, $m_I = (n-1)c$ refers to the total number of type I stations while $m_{II} = c$ refers to the total number of type II stations. For a given L_{tot}, we can calculate the number of links between consecutive type II stations as $n = L_{\text{tot}}/(L_0 c)$. However, it should be noted that L_0 should be chosen such that the resulting n is a (positive) integer. The weights $s_I = 3$ and $s_{II} = 6$ refer to the number of spins used by a type I and type II station, respectively. To capture the essence of the increasing difficulty of maintaining a low noise system with increasing number of qubits, we raised the weights to a power of 3. The choice of the power of 3, however, is arbitrary.

The parameters which we minimise C with respect to are the inter-repeater distance L_0, number of type II stations c, and tree vector $\vec{t} = [b_0, b_1, \ldots, b_d]$ with the following constraints: minimum inter-repeater distance $L_0 \geq 1$ km, maximum photon number $N = \sum_{i=0}^{d} \prod_{j=0}^{i} b_j$ in a given tree vector $N_{\max} = 300$ and fixed depth of the tree $d = 2$. Additionally, we impose that the first-level of the tree has exactly 4 photons, i.e., $b_0 = 4$. This is because we have found that most of the time tree vectors with $b_0 = 4$ give the optimum result, and the rest of the time they still give near-optimum result. Mathematically, we can write the minimisation of C as:

$$C_{\min} = \min_{L_0,\, c,\, \vec{t}} C, \text{ subject to: } L_0 \geq 1 \text{ km}, \; c \geq 1, \; \vec{t} \in \{\mathbb{Z}_{>0}^{d+1} | b_0 = 4 \text{ and } d = 2 \text{ and } N \leq N_{\max}\}, \tag{6.9}$$

where $\mathbb{Z}_{>0} = \{1, 2, \ldots\}$ is the set of positive integers. The value of the rest of the parameters is fixed and shown in table 6.1. With these, the result of the numerical optimisation for fixed values of ϵ_r and L_{tot} is shown in fig. 6.8. The quantities associated with the minimised cost function are each labelled with a prime, e.g., SKR', L_0', etc, and they are shown in fig. 6.9. For comparison, the secret key rate of a homogeneous repeater chain[4] is also included in fig. 6.8.

[4] The expression of the cost function and secret key rate of the homogeneous repeater chain are found in [18].

[5] 100 ns is the within the typical timescale of a two-qubit gate in diamond defects based architectures [55–57], which is the architecture we are assuming in our analysis.

Quantity		Value
Spin-spin gate time, τ_{ss}	◊	100 ns[5]
Single photon emission time, τ_{ph}	◊	1 ns
Spin readout time, τ_{meas}		≈ 0
Optical fibre's attenuation length, L_{att}	◊	20 km
Photon detector's efficiency, η_d	◊	0.95

Table 6.1: Values of the quantities used in the minimisation of the cost function shown in eq. (6.8). The symbol ◊ denotes that the values were also used in [18].

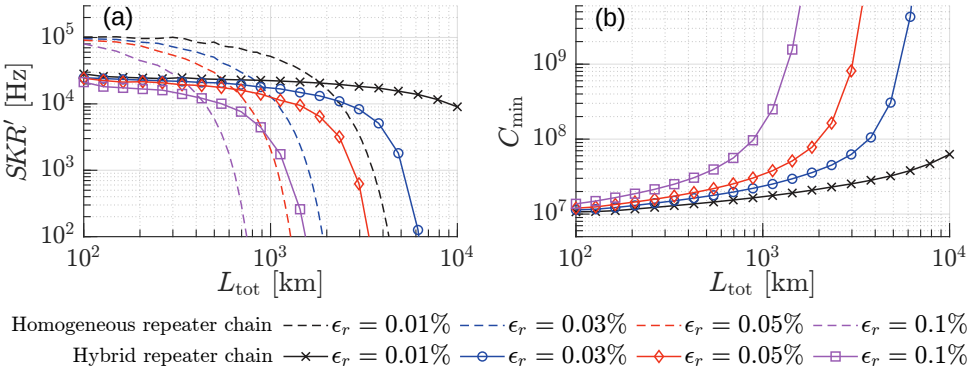


Figure 6.8: (a) The secret key rate SKR', corresponding to the (b) minimised cost function C_{min} as a function of the distance L_{tot}. For comparison, the secret key rates of a homogeneous repeater chain (see footnote 4) are also included and they are indicated by dashed lines.

From fig. 6.8, we see that as the total distance L_{tot} increases, the secret key rate of the network drops. This is because the reencoding error rate ϵ_r generally increases as more stations are needed. Despite this, the secret key rate for the hybrid repeater chain (solid lines with marker) surpasses that of the homogeneous repeater chain (dashed lines) for long enough distances L_{tot}. At short distances, however, the secret key rate of the homogeneous network protocol still wins owing to the long processing time of each station in the hybrid network protocol, i.e., generating five trees sequentially instead of just one. Nevertheless, the improvement that code concatenation offers is significant: the distance for which the secret key rate is still viable is extended over several times. For instance, the secret key rate for $\epsilon_r = 0.03\%$ (blue line) is $\sim$8.3 kHz at a distance of $\sim$3000 km by using the hybrid network protocol, while for the homogeneous network protocol, the distance for which the secret key rate is about the same is only $\sim$1100 km. For $\epsilon_r = 0.1\%$ (purple line), we also see an extension in the total distance while maintain relatively high secret key rates. This is promising since we have shown that the one-way repeater chain can be made to tolerate higher error rates via code concatenation.

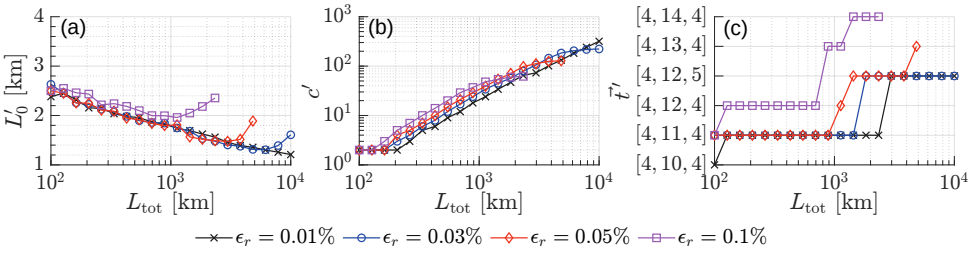


Figure 6.9: (a) The corresponding inter-repeater distance L_0', (b) number of type II stations c', and (c) tree vector $\vec{t}'$ to the minimised cost function shown in fig. 6.8.

In fig. 6.9, we find that the optimal inter-repeater distance ranges from ~1 km to ~3 km. However, for $\epsilon_r = 0.05\%$ and $\epsilon_r = 0.1\%$, they reach their limit before 10^4 km because their secret key rates go to 0 at this distance. We also see that as L_{tot} increases, there tends to be more number of type II stations to counter the increasing error rates. The rest of the parameters associated with the minimised cost function can be found in appendix B. Additionally, we show a variant of the secret key rate and cost function results *without* considering for erasure correction on the $[\![5,1,3]\!]$ code level in appendix C.

6.2. PARALLEL SCHEDULING

In the previous section, we have seen how introducing the $[\![5,1,3]\!]$ code as an outer code to the one-way quantum repeater protocol with the tree code as the inner code offers significant boost in the secret key rate. However, due to the nature of the sequential scheduling protocol, it is impractical to implement the flagged variant of the $[\![5,1,3]\!]$

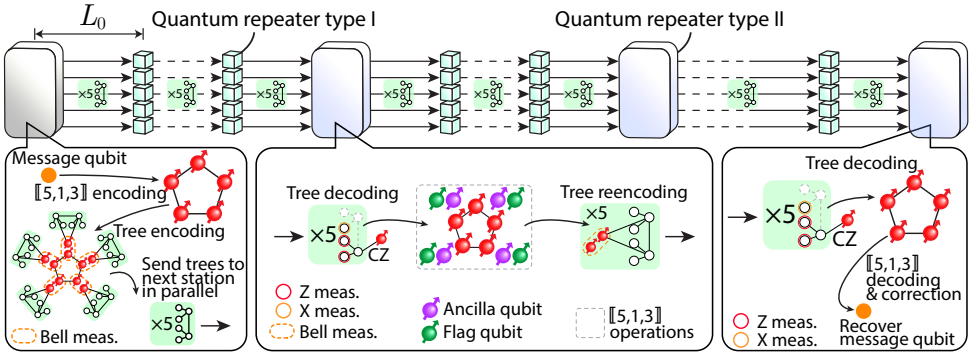


Figure 6.10: Overview of the hybrid one-way quantum repeater network with parallel scheduling containing two types of repeater stations: type I (green) and type II (blue). The steps performed in the first station and in the type I stations are exactly as described in the sequential scheduling scheme in fig. 6.1, except the five trees are now generated and sent to the next station *in parallel*. In the type II stations, which are capable of decoding the received trees in parallel, performs the fault-tolerant implementation of the $[\![5,1,3]\!]$ code on the decoded data qubits via 4 ancilla and 4 flag qubits. After the stabiliser operations, the qubits are reencoded back into five trees and sent off to the next station in parallel. At the end station, the same steps as in any type II stations are applied, but with an additional step where the logical qubit is decoded back into the original message qubit.

code which offers fault-tolerance (see section 3.4.1). In the fault-tolerant protocol via flag qubits, the operations often require that all data qubits are readily available simultaneously, which is not the case in the sequential scheduling case. Fortunately, this adversity can be circumvented by considering a *parallel scheduling* scheme instead of a sequential one. An illustration of a network that uses the parallel scheduling scheme is shown in fig. 6.10 and its physical resources needed are shown in fig. 6.11.

An obvious observation that one could immediately make from fig. 6.10 is that the parallel scheduling scheme uses significantly more resources than in the sequential scheduling scheme, i.e., the number of type I stations has increased by five-fold and the number of spins per type II stations has also increased. In spite of this, we will see in the following section that this boosts performance of the secret key rate even further than that of sequential scheduling scheme. The reason is two-fold: (1) the tree generation can now be performed in parallel, resulting in reduced processing time of each station, and (2) the flagged variant of the $[\![5,1,3]\!]$ code offers significant reduction in the logical error rate.

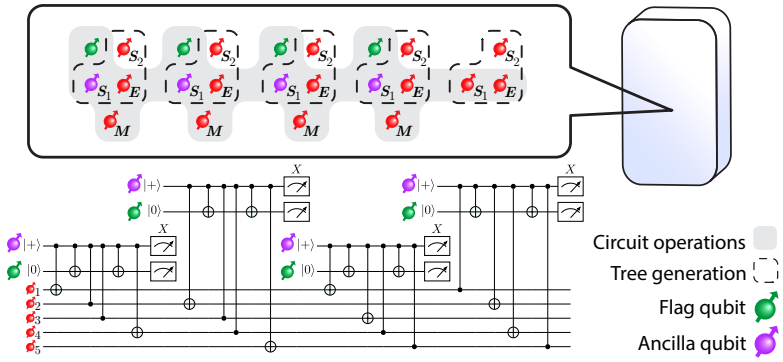


Figure 6.11: (Top) The physical resources of the type II quantum repeater in a parallel scheduling scheme and (bottom) the corresponding fault-tolerant circuit that is performed in a type II station. There are five sets of tree generating spins, each enclosed in a dashed black box. In four of the five sets, a spin is allocated as the ancilla qubit and 2 extra qubits are needed: 1 as the flag qubit and 1 as an auxiliary memory spin M for performing teleported CX gates (see fig. 6.12). The remaining set does not need any extra qubits since only 4 sets of ancilla-flag pairs are needed in the fault-tolerant $[\![5,1,3]\!]$ code. The spins involved in the circuit operations are enclosed in a grey box. Note that this is just an illustration and does not imply the actual physical layout of the spins.

In principle, the $[\![5,1,3]\!]$ code level corrections can be done locally at each of the type II stations after the syndrome extraction. However, as mentioned previously it is better to send all the syndromes to the end station where it interprets them and applies all the corrections in one go. This reduces the error rate because the application of the corrections (i.e., single-qubit gates) would in practice induce error on the qubits, even though we are making theoretical assumptions about single-qubit gates being error-free in this thesis.

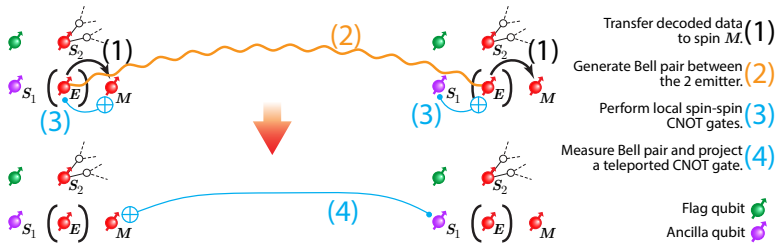


Figure 6.12: Procedure for performing a teleported CX gate between an ancilla qubit (control) and a data qubit (target) by generating a Bell pair between two emitters and performing destructive measurement on the Bell pair.

In fig. 6.12, the teleported CX gate involves freeing up the emitters by transferring the decoded data qubit onto an auxiliary memory spin M. Only then a Bell pair can be generated between the two emitters for the projection of a teleported CX gate. The reason for the need of a teleported two-qubit gate is that the data qubits and ancilla qubits are now physically further apart from each other, making a local CX/CZ gate infeasible. The teleported CX gate can be easily transformed into a CZ gate by applications of single-qubit Hadamard gates on the target qubit. Note that the generation of the Bell pair in fig. 6.12 is heralded via photon detection, and therefore this CX gate is loss tolerant. We assume the time taken to herald such a Bell pair is negligible compared to the tree generation time.

Since the teleported gate is necessary, the two-qubit gates between the data qubits and ancilla qubits on the $[\![5,1,3]\!]$ code level now has a different depolarising error rate. Namely, the two-qubit gates between the data qubits and ancilla qubits are now subjected to $\Lambda_{(2)}(1-(1-\epsilon_0)^5)$ since we assume that at least 5 two-qubit gate operations are needed to effectively perform a teleported two-qubit gate. For small ϵ_0, it can be approximated as $\Lambda_{(2)}(5\epsilon_0)$. The error rate for the two-qubit gate between the ancilla and flag qubits, however, remains the same, i.e., $\Lambda_{(2)}(\epsilon_0)$. With the noisy channels established, we can represent it in the channel representation as $\mathcal{C}_{\text{par}}$ just as we have done so for the sequential scheduling scheme in the previous section.

By utilising the fault-tolerant implementation of the $[\![5,1,3]\!]$ code in the parallel scheme, the resulting effective error rate should be lower than that of the non-fault-tolerant implementation. In fact, this is found to be true in fig. 6.13. The improvement in the effective error rate is significant, especially when the correction is done multiple times and the reencoding error is low enough. For the error rate associated with a single 1-erasure error occurrence ϵ_{loss}, we assume it is exactly the same as shown for the sequential scheduling scheme in section 6.1. In theory, there should be some improvement to this error rate via flag qubits. However, we found that the maximum number of 1-erasure occurrences that a hybrid repeater chain could tolerate before the secret key rate goes to 0 is negligible compared to the total number of type II stations. Therefore, it is safe to make such an assumption to save on computational resources.

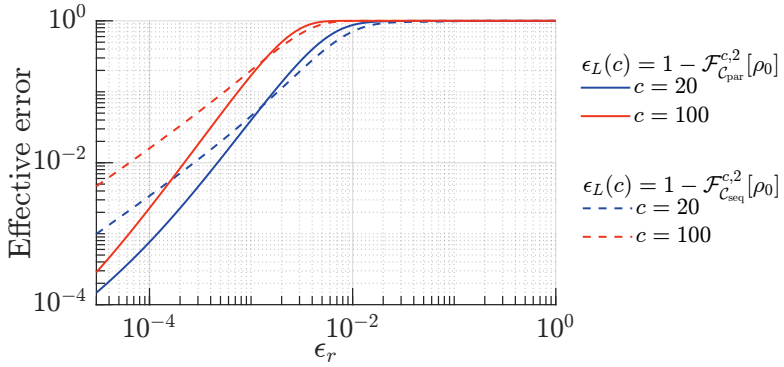


Figure 6.13: Effective error of the hybrid repeater chain as a function of the reencoding error ϵ_r with fixed $n = 10$ links between consecutive type II stations. The effective error rates (calculated using the recursive model) for both the sequential and parallel scheduling scheme are shown here.

6.2.1. SECRET KEY RATE AND COST FUNCTION

The expression of the secret key rate for the parallel scheduling scheme is still the same as that of eq. (6.5), but the total processing time of each repeater station has now become $T = \tau_{\text{tree}} + 104\tau_{\text{ss}} + 5\tau_{\text{meas}}$ for one logical qubit[6]. The expression for the cost function is also the same as that of eq. (6.8), but now we take a different weighted sum of the number of different types of stations. Namely, it is now $m = 5s_I^3 m_I + s_{II}^3 m_{II}$ with $s_I = 3$ and $s_{II} = 23$ being the number of spins used by a type I and type II station, respectively. Since two-qubit gates are not performed between parallel type I stations, we just multiply s_I^3 by 5. With this, we then numerically optimise the cost function with the same constraints as set in eq. (6.9) while using the same values for the constants as tabulated in table 6.1. The results of the minimised cost function C_{min} and the corresponding secret key rate SKR' are shown in fig. 6.14. In fig. 6.15, we find the rest of the quantities associated with the minimised cost function, i.e., L_0', c', and $\vec{t}'$.

By comparing figs. 6.8 and 6.14, we see that there is a substantial boost in the secret key rate by using the parallel scheduling scheme instead of the sequential one, especially for lower total distance L_{tot}. This is because as mentioned in the previous section, we are no longer limited by the need for sequential tree generation. The boost is also contributed by the fact that we are using the flagged variant of the $[\![5,1,3]\!]$ code as the outer code. For instance, we see that now for $\epsilon_r = 0.1\%$ (purple line), the secret key rate for the hybrid repeater chain is ~ 10 kHz at $\sim 10^3$ km, while for its homogeneous counterpart, the secret key rate at the same total distance is less than 1 Hz. This is again promising since we have shown that the hybrid repeater chain can withstand higher error rates via flag qubits, paving the way for experimentally feasible hybrid one-way repeater networks.

In fig. 6.15, we find the optimal distances are generally lower than those found in

[6] We assume the worst case scenario in terms of number of readouts and gates needed. The first four τ_{meas} comes from the sequential readout of the ancilla-flag pairs in the flagged circuit, while the last τ_{meas} represents the parallel readout of the ancilla qubits in the unflagged circuit. Time for a teleported gate is assumed to be $3\tau_{\text{ss}}$, so there would be $6 \cdot 16 + 8 = 104$ two-qubit gates if both the flagged and unflagged circuit are performed in full.

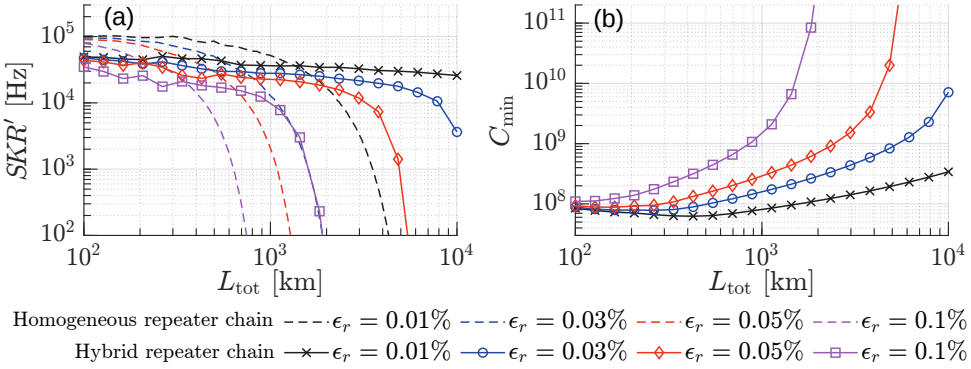


Figure 6.14: (a) The secret key rate SKR', corresponding to the (b) minimised cost function $C_{\min}$ as a function of the distance L_{tot}. For comparison, the secret key rates of a homogeneous repeater chain (see footnote 4) are also included and they are indicated by dashed lines.

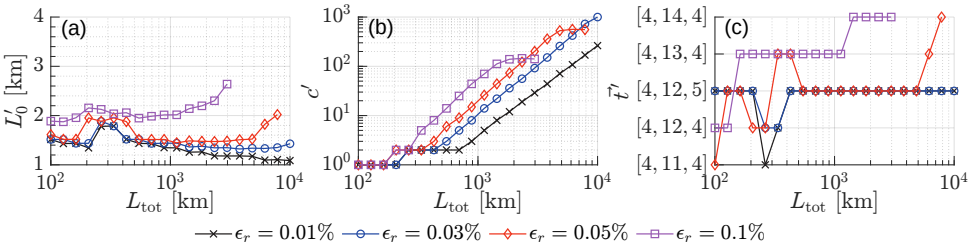


Figure 6.15: (a) The corresponding inter-repeater distance L'_0, (b) number of type II stations c', and (c) tree vector $\vec{t}'$ to the minimised cost function shown in fig. 6.14.

the sequential scheduling scheme (see fig. 6.9). This is because due to the better error correction capabilities of the flagged variant of the $[\![5,1,3]\!]$ code, our numerical optimisation found that it is desirable to place more stations in between the start and end station, which also translates to more type II stations. At $L_{\text{tot}} = 10^3$ km, the number of type II stations needed is ~ 60 for $\epsilon_r = 0.1\%$, which is a reasonable number if one is considering building such a network.

Just as for the sequential scheduling scheme, the rest of the parameters associated with the minimised cost function for the parallel scheduling scheme can be found in appendix B. The secret key rate and cost function results *without* considering for erasure correction on the $[\![5,1,3]\!]$ code level is also shown in appendix C.

7

CONCLUSION AND OUTLOOK

7.1. CONCLUSION

We have shown how the non-fault-tolerant $[\![5,1,3]\!]$ code can be used to correct for arbitrary single-qubit error and how it can be made fault-tolerant by introducing additional *flag* qubits to catch and correct for correlated errors in chapter 3. We have also introduced a novel method of extrapolating the fidelity of some initial state after applying the same *noisy* quantum error correction procedure c times by using the recursive model function (see section 3.6). This method yields the fidelity to great accuracy, provided that the error rate is sufficiently low. In the same chapter, we also showed the single-qubit and two-qubit depolarising channel, which we used to model the noise in the hybrid repeater chain in chapter 6.

In chapter 4, we have demonstrated explicitly that the $[\![5,1,3]\!]$ code can be extended to become a quantum erasure correcting code which can correct for up to 2 erasure errors provided that they are heralded owing to theorem 4.2.1. As far as we are aware, such demonstration using the $[\![5,1,3]\!]$ code to correct for heralded erasure errors has never been carried out before in both the theoretical and experimental aspects at the time of writing. As preliminaries to the hybrid quantum repeater chain scheme, the tree cluster state was revisited in chapter 4 and the basics of quantum key distribution and the six-state variant BB84 protocol were revisited in chapter 5.

Finally, we revealed the novel hybrid one-way quantum repeater scheme in chapter 6 which uses the $[\![5,1,3]\!]$ code as the outer code and the tree code as the inner code. We proposed two methods of scheduling the hybrid repeater chain and discussed their required physical resources in detail. The two schemes are the *sequential* and *parallel* scheduling scheme. In the sequential scheduling scheme, we found that it is impractical to implement the network with the flagged variant of the $[\![5,1,3]\!]$ code, and therefore we settled on its non-fault-tolerant variant. Despite this, it still achieved *higher* secret key rates than that of the homogeneous repeater chain, provided that the total distance L_{tot} between the start and end station is large enough.

The secret key rate is further improved by using the parallel scheduling scheme since the delays associated with the sequential scheme are now removed. In addition, we con-

sidered the flagged variant of the $[\![5,1,3]\!]$ code in this scheduling scheme, which lowered the error rate in the network significantly, resulting in a higher secret key rate even when compared to the hybrid repeater chain with sequential scheme. However, there is a resource-performance trade-off between the sequential and parallel scheduling scheme. In the parallel scheduling scheme, we proposed that it requires considerably more physical resources (i.e., memory spins and emitters to generate, decode, and encode trees in parallel).

All in all, we can conclude that code concatenation is beneficial in a setting involving one-way repeater networks and we hope that the hybrid one-way quantum repeater architecture proposed in this thesis forms the stepping stone towards other even more robust novel architectures.

7.2. OUTLOOK

7.2.1. OUTSTANDING CHALLENGES

In the previous section, we have concluded that the hybrid one-way quantum repeater network is superior compared to its homogeneous counterpart in terms of raw performance. However, there are outstanding challenges present in the physical implementation of the hybrid quantum repeater network. First, the error rates of the two-qubit gates used to study the hybrid repeater chain's performance are relatively low, i.e., $0.003\% \sim 0.03\%$, which is difficult to achieve experimentally. Furthermore, in the parallel scheme that we proposed, there are 5 separate cavities present, which we wish to apply controlled gates between each other via teleported gates. This poses a problem because the emitters need to be in resonance with each other and with the cavity to efficiently carry out the teleported gates. The question of how to tune multiple emitter's frequencies is an unresolved one. This becomes daunting when one realises not only do we need to calibrate 5 emitters in one station, but we also need to calibrate the emitters in the other stations.

Moreover, the flagged variant of the $[\![5,1,3]\!]$ code works relatively slowly, i.e., it involves performing readouts of the flag-ancilla qubit pair sequentially (see section 3.4.1). In experiments with high qubit rest error rates, i.e., high decoherence, this is not negligible. In the work by Reichardt [21], it was shown that it is possible to parallelise this procedure to some degree and the number of flag qubits needed can be reduced by sharing a flag qubit with multiple stabiliser measurements. Though this poses another problem of orienting the spins in the type II station properly since a flag qubit needs to be shared between multiple data qubits. Without the parallelised readout scheme, we can simply assign one local flag qubit per emitter which is what we have assumed in our scheme.

7.2.2. FUTURE IMPROVEMENTS AND EXTENSIONS

A trivial step to take to improve the secret key rate as shown in figs. 6.8 and 6.14 is to calculate the logical error rates exactly instead of using the recursive model function. This is because as seen in fig. 6.4, the recursive model function's accuracy is limited in the regime of higher error rates. In theory, this should boost the secret key rate considerably. Furthermore, since we have seen how the parallel scheduling scheme can tolerate high error rates in fig. 6.14, one can try to slowly increase the reencoding error rate beyond

0.1% and study what is the threshold such that we still have viable secret key rates at reasonable total distances.

As seen in fig. 6.5, the error rate corresponding to the 1-erasure case is relatively high. This problem could be ameliorated by immediately applying another set of $[\![5,1,3]\!]$ quantum error correction after the initial quantum erasure correction. The reason for this is that after the initial quantum erasure correction, there is likely a remaining 1-qubit error present in the 5 data qubits, which can be caught by another round of quantum error correction. However, including this extra step would result in a different total processing time of each station, which we will leave as future work.

As for the recursive model function, it could be possible that a better version can be derived as opposed to what we currently have in this thesis. In appendix A, we showed the derivation of the second order recursive model function that depends on correcting the orthogonal state 2 times. One possible improvement in this regard is that instead of applying the correction on the orthogonal state 2 times, one could apply it instead on the full state and use the corresponding information one could extract from this.

Since the time-bin encoding is considered in our hybrid one-way quantum repeater architecture, one could leverage its ability to realise states with dimensions beyond 2, i.e., qudits, and thus result in a higher secret key rate [58]. The BB84 protocol considered in our thesis can also be extended to use qudits of arbitrary dimensions and it has been shown that a qutrit-based six-state BB84 protocol offers a higher yield of secret key rates while having the same error tolerance as the qubit-based protocol [59]. However, employing qudits in the hybrid repeater chain means one would have to use a qudit-based inner and outer codes, the choice of which remains to be explored.

Other possible extensions to the hybrid repeater chain is the usage of a different quantum error correcting code as the outer code instead of the $[\![5,1,3]\!]$ code. For example, one could consider the $[\![12,2,3]\!]$ colour code that is constructed from two Steane $[\![7,1,3]\!]$ code blocks, which is fault-tolerant as it can correct for correlated errors without the need for any extra qubits [21]. However, with bigger codes comes more physical qubits per logical qubit, which means that there is a trade-off where more resources are needed in the repeater network to ensure parallelised operations. Codes with higher distances could also be interesting to study since they can correct for even more erasure errors according to theorem 4.2.1, which in theory should result in higher secret key rates.

REFERENCES

[1] J. P. Dowling and G. J. Milburn, *Quantum technology: the second quantum revolution,* Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences **361**, 1655 (2003).

[2] J. Simon, W. S. Bakr, R. Ma, M. E. Tai, P. M. Preiss, and M. Greiner, *Quantum simulation of antiferromagnetic spin chains in an optical lattice,* Nature **472**, 307 (2011).

[3] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,* SIAM Review **41**, 303 (1999).

[4] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, *Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance,* Nature **414**, 883 (2001).

[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum cryptography,* Reviews of Modern Physics **74**, 145 (2002).

[6] G. V. Assche, *Quantum Cryptography and Secret-Key Distillation* (Cambridge University Press, 2006).

[7] N. Gisin and R. Thew, *Quantum communication,* Nature Photonics **1**, 165 (2007).

[8] C. M. Caves, *Quantum limits on noise in linear amplifiers,* Physical Review D **26**, 1817 (1982).

[9] V. Giovannetti, S. Lloyd, and L. Maccone, *Quantum-enhanced measurements: Beating the standard quantum limit,* Science **306**, 1330 (2004).

[10] S. Wiesner, *Conjugate coding,* ACM SIGACT News **15**, 78 (1983).

[11] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing,* Theoretical Computer Science **560**, 7 (2014).

[12] S. Wehner, D. Elkouss, and R. Hanson, *Quantum internet: A vision for the road ahead,* Science **362** (2018), 10.1126/science.aam9288.

[13] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Quantum repeaters: The role of imperfect local operations in quantum communication,* Physical Review Letters **81**, 5932 (1998).

[14] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, *Optimal architectures for long distance quantum communication,* Scientific Reports **6** (2016), 10.1038/srep20463.

[15] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, *Inside quantum repeaters,* IEEE Journal of Selected Topics in Quantum Electronics **21**, 78 (2015).

[16] W. Dür and H. J. Briegel, *Entanglement purification and quantum error correction,* Reports on Progress in Physics **70**, 1381 (2007).

[17] A. M. Stephens, J. Huang, K. Nemoto, and W. J. Munro, *Hybrid-system approach to fault-tolerant quantum communication,* Physical Review A **87**, 052333 (2013).

[18] J. Borregaard, H. Pichler, T. Schröder, M. D. Lukin, P. Lodahl, and A. S. Sørensen, *One-way quantum repeater based on near-deterministic photon-emitter interfaces,* Physical Review X **10**, 021071 (2020).

[19] M. H. Abobeih, Y. Wang, J. Randall, S. J. H. Loenen, C. E. Bradley, M. Markham, D. J. Twitchen, B. M. Terhal, and T. H. Taminiau, *Fault-tolerant operation of a logical qubit in a diamond quantum processor,* (2021), arXiv:2108.01646 [quant-ph] .

[20] R. Chao and B. W. Reichardt, *Quantum error correction with only two extra qubits,* Physical Review Letters **121**, 050502 (2018).

[21] B. W. Reichardt, *Fault-tolerant quantum error correction for steane's seven-qubit color code with few or no extra qubits,* Quantum Science and Technology **6**, 015007 (2020).

[22] M. Grassl, T. Beth, and T. Pellizzari, *Codes for the quantum erasure channel,* Physical Review A **56**, 33 (1997).

[23] R. Cleve, D. Gottesman, and H.-K. Lo, *How to share a quantum secret,* Physical Review Letters **83**, 648 (1999).

[24] R. M. Gingrich, P. Kok, H. Lee, F. Vatan, and J. P. Dowling, *All linear optical quantum memory based on quantum error correction,* Physical Review Letters **91**, 217901 (2003).

[25] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2009).

[26] R. Shankar, *Principles of Quantum Mechanics* (Springer US, 1994).

[27] W. Scherer, *Mathematics of Quantum Computing* (Springer International Publishing, 2019).

[28] I. Djordjevic, *Quantum information processing, quantum computing, and quantum error correction : an engineering approach* (Academic Press, Amsterdam, 2021).

[29] P. M. Lokenath Debnath, *Introduction to Hilbert Spaces with Applications* (Elsevier Science & Techn., 2005).

[30] R. Jozsa, *Fidelity for mixed quantum states,* Journal of Modern Optics **41**, 2315 (1994).

[31] I. B. Djordjevic, *Physical-Layer Security and Quantum Key Distribution* (Springer International Publishing, 2019).

[32] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned,* Nature **299**, 802 (1982).

[33] J. Roffe, *Quantum error correction: an introductory guide,* Contemporary Physics **60**, 226 (2019).

[34] D. E. Gottesman, *Stabilizer codes and quantum error correction,* (1997), 10.7907/RZR7-DT72.

[35] J.-Y. Wu, H. Kampermann, and D. Bruß, *Group structures and representations of graph states,* Physical Review A **92**, 012322 (2015).

[36] Y. Hwang and J. Heo, *On the relation between a graph code and a graph state,* Quantum Information and Computation, 16 (3&4), pp. 237-250, March 2016 (2015), arXiv:1511.05647 [quant-ph] .

[37] M. Hein, J. Eisert, and H. J. Briegel, *Multiparty entanglement in graph states,* Physical Review A **69**, 062311 (2004).

[38] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. V. den Nest, and H. J. Briegel, *Entanglement in graph states and its applications,* (2006), arXiv:quant-ph/0602096 [quant-ph] .

[39] D. Markham and B. C. Sanders, *Graph states for quantum secret sharing,* Physical Review A **78**, 042309 (2008).

[40] C. Meignant, D. Markham, and F. Grosshans, *Distributing graph states over arbitrary quantum networks,* Physical Review A **100**, 052333 (2019).

[41] M. F. Mor Ruiz, *Towards a fault-tolerant one-way quantum repeater,* TU Delft Repository (2021).

[42] T. J. Yoder, R. Takagi, and I. L. Chuang, *Universal fault-tolerant gates on concatenated stabilizer codes,* Physical Review X **6**, 031039 (2016).

[43] G. Chartrand, *Graphs & digraphs* (CRC Press, Taylor & Francis Group, Boca Raton, 2016).

[44] K. Rosen, *Discrete mathematics and its applications* (McGraw-Hill, New York, NY, 2019).

[45] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, *Perfect quantum error correcting code,* Physical Review Letters **77**, 198 (1996).

[46] M. Varnava, D. E. Browne, and T. Rudolph, *Loss tolerance in one-way quantum computation via counterfactual error correction,* Physical Review Letters **97**, 120501 (2006).

[47] D. Buterakos, E. Barnes, and S. E. Economou, *Deterministic generation of all-photonic quantum repeaters from solid-state emitters,* Physical Review X **7**, 041023 (2017).

[48] Y. Zhan and S. Sun, *Deterministic generation of loss-tolerant photonic cluster states with a single quantum emitter,* Physical Review Letters **125**, 223601 (2020).

[49] A. K. Ekert, *Quantum cryptography based on bell's theorem,* Physical Review Letters **67**, 661 (1991).

[50] C. H. Bennett, G. Brassard, and N. D. Mermin, *Quantum cryptography without bell's theorem,* Physical Review Letters **68**, 557 (1992).

[51] A. Acín, N. Gisin, and V. Scarani, *Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks,* Physical Review A **69**, 012309 (2004).

[52] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The security of practical quantum key distribution,* Reviews of Modern Physics **81**, 1301 (2009).

[53] H. Bechmann-Pasquinucci and N. Gisin, *Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography,* Physical Review A **59**, 4238 (1999).

[54] MATLAB, *9.11.0.1809720 (R2021b) Update 1* (The MathWorks Inc., Natick, Massachusetts, 2021).

[55] G. D. Fuchs, G. Burkard, P. V. Klimov, and D. D. Awschalom, *A quantum memory intrinsic to single nitrogen–vacancy centres in diamond,* Nature Physics **7**, 789 (2011).

[56] D. Solenov, S. E. Economou, and T. L. Reinecke, *Two-qubit quantum gates for defect qubits in diamond and similar systems,* Physical Review B **88**, 161403 (2013).

[57] M. Goldman, T. Patti, D. Levonian, S. Yelin, and M. Lukin, *Optical control of a single nuclear spin in the solid state,* Physical Review Letters **124**, 153203 (2020).

[58] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, *Provably secure and high-rate quantum key distribution with time-bin qudits,* Science Advances **3** (2017), 10.1126/sciadv.1701491.

[59] G. M. Nikolopoulos and G. Alber, *Security bound of two-basis quantum-key-distribution protocols using qudits,* Physical Review A **72**, 032320 (2005).

A

SECOND ORDER RECURSIVE MODEL FUNCTION

The fidelity of an initial state ρ_0 after applying some generic channel $\mathcal{C}$ c times can be approximated using the 2$^{\text{nd}}$ order recursive model. To begin, consider the following:

$$\begin{aligned} \rho_1 = \mathcal{C}(\rho_0) &= \alpha_1\rho_0 + \beta_1\rho_\perp, \\ \rho_{\perp,1} = \mathcal{C}(\rho_\perp) &= \alpha'\rho_0 + \beta'\rho'_\perp, \\ \mathcal{C}(\rho'_\perp) &= \alpha''\rho_0. \end{aligned} \tag{A.1}$$

With eq. (A.1), we can apply $\mathcal{C}$ on ρ_0 c times:

$$\begin{aligned} \rho_1 &= \mathcal{C}(\rho_0) = [\alpha_1]\rho_0 + [\beta_1]\rho_\perp + [\delta_1]\rho'_\perp, \\ \rho_2 &= \mathcal{C}(\rho_1) = [\alpha_2]\rho_0 + [\beta_2]\rho_\perp + [\delta_2]\rho'_\perp, \\ &\vdots \\ \rho_c &= \mathcal{C}(\rho_{c-1}) = [\alpha_c]\rho_0 + [\beta_c]\rho_\perp + [\delta_c]\rho'_\perp. \end{aligned} \tag{A.2}$$

By working eq. (A.2) out, we find that:

$$\begin{aligned} \alpha_c &= \alpha_{c-1}\alpha_1 + \beta_{c-1}\alpha' + \delta_{c-1}\alpha'', \\ \beta_c &= \alpha_{c-1}\beta_1, \\ \delta_c &= \beta_{c-1}\beta'. \end{aligned} \tag{A.3}$$

Since $\beta_1 = 1-\alpha_1$ and $\beta' = 1-\alpha'$, eq. (A.3) can be rewritten in terms of α_1 and α' only:

$$\alpha_c = \alpha_{c-1}\alpha_1 + \alpha_{c-2}(1-\alpha_1)\alpha' + \alpha_{c-3}(1-\alpha_1)(1-\alpha')\alpha'', \text{ with } \alpha_i = \begin{cases} \alpha_1, & \text{if } i = 1 \\ 1, & \text{if } i = 0 \\ 0, & \text{if } i < 0 \end{cases}. \tag{A.4}$$

Solving for eq. (A.4) yields us the second order recursive model function:

$$\mathcal{F}_{\mathcal{C}}^{c,2}[\rho_0] \equiv \alpha_c \equiv \frac{\zeta_0^{c+2}}{(\zeta_0-\zeta_2)(\zeta_0-\zeta_1)} + \frac{\zeta_1^{c+2}}{(\zeta_0-\zeta_1)(\zeta_2-\zeta_1)} + \frac{\zeta_2^{c+2}}{\Omega_2+\zeta_2^2+2\zeta_0\zeta_1}, \tag{A.5}$$

where ζ_k is the k^{th} root of the cubic function $\zeta^3-\Omega_1\zeta^2-\Omega_2\zeta-\Omega_3=0$. Explicitly, they are:

$$\zeta_k = \frac{1}{3}\left(\Omega_1 - \xi^k\Delta_2 - \frac{\Delta_0}{\xi^k\Delta_2}\right), \quad k\in\{0,1,2\}, \tag{A.6}$$

where $\xi=(-1+\sqrt{-3})/2$ while the polynomial coefficients and factored terms are:

$$\begin{aligned}
\Omega_1 &= \alpha_1,\\
\Omega_2 &= (1-\alpha_1)\alpha',\\
\Omega_3 &= (1-\alpha_1)(1-\alpha')\alpha'',\\
\Delta_0 &= \Omega_1^2+3\Omega_2,\\
\Delta_1 &= -2\Omega_1^3-9\Omega_1\Omega_2-27\Omega_3,\\
\Delta_2 &= \left(\frac{\Delta_1+\sqrt{\Delta_1^2-4\Delta_0^3}}{2}\right)^{1/3}.
\end{aligned} \tag{A.7}$$

As mentioned in section 3.6, we just need the quantities α_1 and α' to be able to use the first order recursion relation (see eq. (3.13)) and we have shown how to obtain them. However, to use the second order recursion relation, we also need α''. To obtain α'', we simply rearrange the expression in eq. (A.1) corresponding to $\rho_{\perp,1}$ in terms of $\rho'_\perp$:

$$\rho'_\perp = \frac{\rho_{\perp,1}-\alpha'\rho_0}{\beta'}. \tag{A.8}$$

From this, we can just calculate $\mathcal{C}(\rho'_\perp)$ numerically and obtain α'', after which we can then extrapolate the approximate fidelity for higher c using $\mathcal{F}_{\mathcal{C}}^{c,2}$.

B

PARAMETERS CORRESPONDING TO THE OPTIMISED COST FUNCTION

In this section, we present the rest of the parameters associated with the minimised cost function for the sequential scheduling scheme in section 6.1.1 and the parallel scheduling scheme in section 6.2.1.

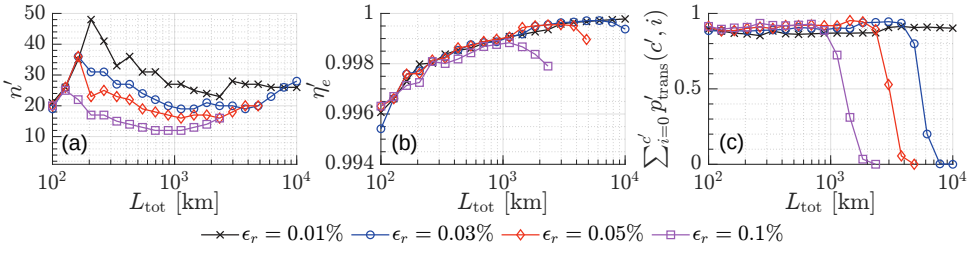


Figure B.1: The parameters corresponding to the minimised cost function for the sequential scheduling scheme in section 6.1.1. Shown here are the (a) number of links n' between two consecutive type II stations, (b) the transmission probability η'_e of a tree cluster state, and (c) the summed transmission probability of the message qubit through the repeater chain. Note that for (c), instead of summing up to c', we capped the sum at 20 since terms at higher c' have negligible contribution.

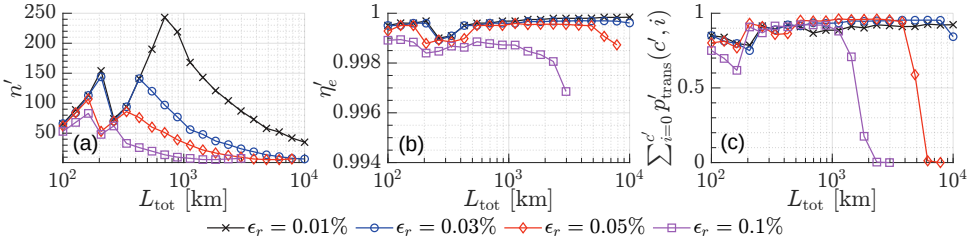


Figure B.2: The parameters corresponding to the minimised cost function for the sequential scheduling scheme in section 6.2.1. Shown here are the (a) number of links n' between two consecutive type II stations, (b) the transmission probability η'_e of a tree cluster state, and (c) the summed transmission probability of the message qubit through the repeater chain. Note that for (c), instead of summing up to c', we capped the sum at 20 since terms at higher c' have negligible contribution.

C

SECRET KEY RATES WITHOUT ERASURE CORRECTION AT THE ⟦5,1,3⟧ CODE LEVEL

In this section, we explore how not considering erasure correction at the ⟦5,1,3⟧ code level affects the secret key rate of the hybrid repeater chain. The result corresponding to the sequential scheduling scheme can be found in figs. C.1 and C.2. As for the parallel scheduling scheme, the result can be found in figs. C.3 and C.4. From these results, we see that considering the erasure correction at the ⟦5,1,3⟧ code level has significant effect on the secret key rate and thus should not be ignored.

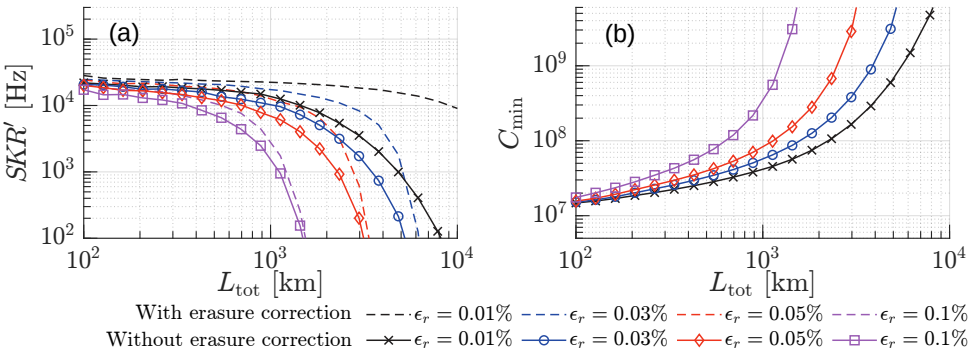


Figure C.1: (a) The secret key rate corresponding to the (b) minimised cost function of the hybrid repeater chain using the sequential scheduling scheme without considering erasure corrections at the ⟦5,1,3⟧ code level. The secret key rate from fig. 6.8 is included here (dashed lines) for comparison.

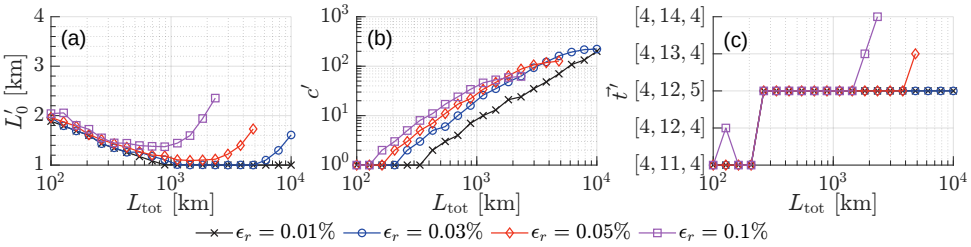


Figure C.2: (a) The corresponding inter-repeater distance L_0', (b) number of type II stations c', and (c) tree vector $\vec{t}'$ to the minimised cost function shown in fig. C.1.

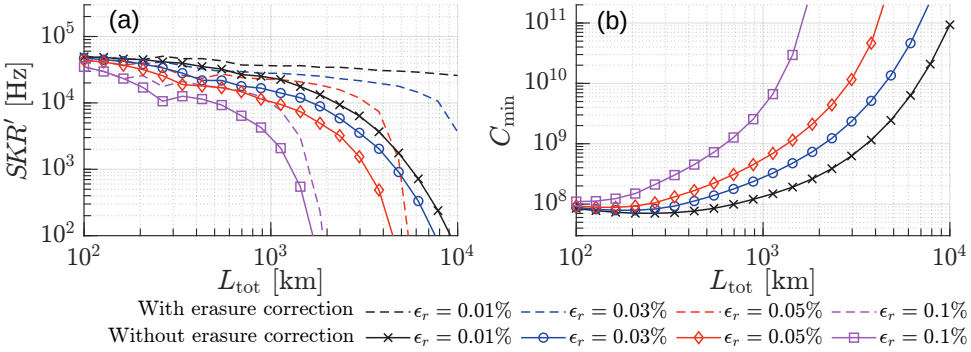


Figure C.3: (a) The secret key rate corresponding to the (b) minimised cost function of the hybrid repeater chain using the parallel scheduling scheme without considering erasure corrections at the ⟦5,1,3⟧ code level. The secret key rate from fig. 6.14 is included here (dashed lines) for comparison.

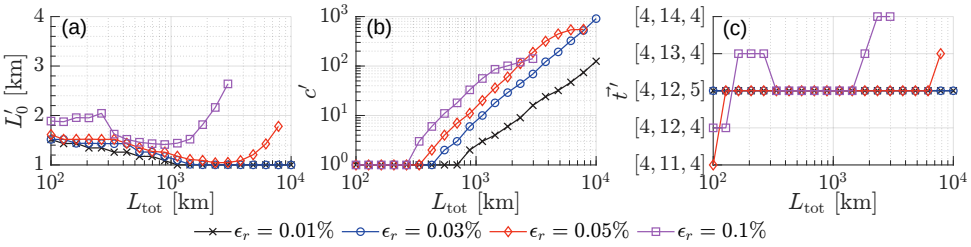


Figure C.4: (a) The corresponding inter-repeater distance L_0', (b) number of type II stations c', and (c) tree vector $\vec{t}'$ to the minimised cost function shown in fig. C.3.