Robustness of Quantum Networks for Resource Distribution

by
ABHISHEK SADHU

A thesis submitted to the Jawaharlal Nehru University
In Partial Fulfilment of the Requirements for the
Degree of
DOCTOR OF PHILOSOPHY

Jawaharlal Nehru University,
Delhi, India

Raman Research Institute,
Bangalore, India

Advisor: Prof. Shiv Sethi (RRI)
Co-advisor: Dr. Siddhartha Das (IIIT-H)

2024

Author's declaration

I, hereby, declare that this thesis is composed independently by me at Raman Research Institute, Bangalore, India, under the supervision of Prof. Shiv Sethi and Dr. Siddhartha Das (IIIT-H). The subject matter presented has not been previously formed the basis of the award of any degree, diploma, associateship, fellowship or another similar title in any other university. I also declare that I have run it through the DrillBit plagiarism software.

Prof. Shiv Sethi
Raman Research Institute
Bangalore - 560080, India

Abhishek Sadhu

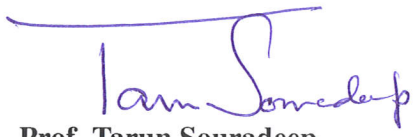
Abhishek Sadhu
Raman Research Institute
Bangalore - 560080, India

Dr. Siddhartha Das
International Institute of Information
Technology,
Hyderabad, Telangana - 500032, India

Certificate

This is to certify that the thesis entitled "Robustness of quantum networks for resource distribution" submitted by Abhishek Sadhu for the award of the degree of doctor of philosophy of Jawaharlal Nehru University is his original work. This has not been published or submitted to any other University for any other Degree or Diploma.

Prof. Shiv Sethi
(Thesis Supervisor)
Raman Research Institute
Bangalore - 560080, India



Prof. Tarun Souradeep
(Center Chairperson)
Director
Raman Research Institute
Bangalore - 560080, India

Dr. Siddhartha Das
(Thesis Co-supervisor)
International Institute of Information Technology,
Hyderabad, Telangana - 500032, India

List of Publications

Articles published in journals/unpublished eprints:

[1] "Testing of quantum nonlocal correlations under constrianed free will and imperfect detectors",
Abhishek Sadhu and Siddhartha Das,
Physical Review A, **2023**, 107(1), 012212.

[2] "Practical limitations on robustness and scalability of quantum Internet",
Abhishek Sadhu, Meghana Ayyala Somayajula, Karol Horodecki and Siddhartha Das,
arXiv:2308.12739v2 [quant-ph], **2023**.

Prof. Shiv Sethi
Raman Research Institute
Bangalore - 560080, India

Abhishek Sadhu
Raman Research Institute
Bangalore - 560080, India

Dr. Siddhartha Das
International Institute of Information Technology,
Hyderabad, Telangana - 500032, India

I would like to dedicate this thesis to my beloved parents.

For my late father, who inspired me to always follow my heart,

and my mom, who never stopped believing in me.

"When it looks impossible, look deeper. And then fight like you can win."

– Rost, Horizon Forbidden West.

ACKNOWLEDGEMENTS

First and foremost, I would like to convey my gratitude and respect to my supervisor Prof. Shiv Sethi, for all his encouragement, continuous support, and guidance, which enabled me to complete my PhD happily. I would like to thank my co-supervisor Dr. Siddhartha Das for his guidance and immense knowledge that helped me in my research and writing of this dissertation. I am very grateful to him for sharing his insightful thoughts on several problems related to this thesis. He gave me time to think about ideas and problems to work on, the freedom to pursue them at my own pace, and provided the necessary feedback and constructive criticism. I would like to thank the CSTAR and CQST groups at IIIT-Hyderabad for the insightful discussions and hospitality during my visits.

Besides my advisor and co-advisor, I am grateful to my thesis advisory committee members, Prof. Biman Nath and Prof. Saptarishi Chaudhuri for their support and constructive feedback on my research. I would like to thank Prof. Sadiq Rangwala and the SAAC members for their encouragement and support during my PhD journey.

I would like to thank my collaborators Prof. Karol Horodecki and Meghana Ayyala Somayajula for insightful discussions on the projects from which I learned a lot. I would like to thank Prof. Antonio Acín, Dr. Stefan Bäuml, Dr. Máté Farkas, Carlos Pascual and the whole Quantum Information Theory group at ICFO Barcelona for insightful discussions

and their hospitality during my visit. I would like to thank Prof. Alok Kumar Pan, Dr. Souradeep Sasmal, Dr. Som Kanjilal, Lewis Wooltorton, Akash Kundu, Arnab Ghorui, and Swati Choudhary for insightful discussions. Also, I would like to thank Keval Jain for discussions on coding-related aspects.

I acknowledge the support received from the Computer Section, RRI, for providing facilities related to computation and networking. I have benefitted from the vast volume of the digital repository, online resources, and massive collection of print version books maintained by the Library section, RRI.

I would like to thank the Secretary, A&A (Mrs. Mahima) and the Administrative Block, RRI, for the timely processing of official documents and other essential tasks. I am obliged for the fellowship grant, travel allowance, accommodation facility, etc., provided by RRI during my PhD tenure.

I am indebted to my parents and family members for their constant support and unwavering belief in me. My wholehearted love and good wishes go to all my friends for all the fun, memories, and happiness.

Abhishek Sadhu **February 27, 2024**
Raman Research Institute
Bangalore - 560080, India

CONTENTS

SYNOPSIS

A major breakthrough in science in the last century has been the development of quantum theory to explain physical phenomena on a microscopic scale and explore its advantage in different information-processing tasks. In the last few years, several practical communication and computing protocols have been introduced that provide the “quantum advantage" over classical technology. Recent efforts have been made to build a quantum internet, which is a network of users using quantum technologies for different information processing tasks [3–6]. This thesis aims to present fundamental and practical limitations on building a quantum internet. We introduce different figures of merit for assessing the robustness and present the limitations of different network topologies for current and futuristic quantum internet implementations. These investigations will serve as benchmarks for experimentalists to compare various components and make optimal choices in the architecture, quantum systems, and channels used in the network. We divide the thesis broadly into three parts. In the first part of the thesis, we introduce a graphical analysis of networks [2]. Then, in the second part, we present practical limitations on different quantum network architectures designed for implementing different information processing tasks [2]. In the third part, we consider a special bipartite network where the end users have constrained free will and present limitations on testing quantum nonlocal

correlations using such a network with the use of imperfect detectors [1].

Graph theoretic analysis of networks

In this part of the thesis, we consider a framework for representing networks as undirected weighted graphs. We let the edge weight e_{ij} for the edge connecting the nodes v_i and v_j of the graph take the value $-\log_2 p_{ij}$, where p_{ij} is the success probability of transmitting a resource from node v_i to v_j. For a particular information processing task, let p_* be the critical success probability below which the task fails; we introduce an effective weight $w_*(e_{ij})$ of an edge e_{ij} for such a task as $-\log_2 p_{ij}$ if $p_{ij} \geq p_*$ and ∞ otherwise. The edge weights and the effective weights are path-dependent and additive across the connecting edges. It is desirable for users of the network to select paths with minimum weight for maximum success. We adapt the concepts of adjacency matrix in terms of the edge weights and introduce task-dependent effective adjacency matrix and effective success matrix. The elements of the effective success matrix provide the highest probability with which a resource can be shared between the nodes of the network. We present the critical success probability p_* for implementing different information processing tasks using a linear quantum network.

In analysing networks as graphs, observing their robustness for different information-processing tasks is important. For this, we introduce different robustness measures for networks. The first robustness measure we introduce is link sparsity, (Υ), which is a measure of the fraction of nodes in the network that are not active or are damaged by an adversary. Next, considering networks with the same link sparsity, we define the connection strength of nodes (ζ) and the total connection strength (Γ). Using these definitions, we define the sparsity index (Ξ) as a measure of the robustness of a network. It is desirable for a network to have low values of link sparsity and high values of sparsity index. We then present the robustness parameters for different star and mesh network topologies. Furthermore, certain network nodes are crucial for a network's proper functioning. We call such nodes as the critical nodes of the network. If we remove some of the critical

nodes, the graph's other nodes can get disconnected. We introduce a measure for a node's critical coefficient (ν). The critical nodes of the network are those nodes with high values of (ν).

We then provide algorithms for performing different network tasks. The first algorithm provides the shortest path between a pair of nodes for our framework. Secondly, we provide an algorithm to construct a network for sharing resources between two parties each having multiple nodes. Third, we provide an algorithm to optimize the flow of resources at a node having multiple input and output channels. Finally, we provide an algorithm based on calculating ν to identify the critical nodes of a given network.

Practical Limitations on quantum networks

Quantum network architectures have potential applications in diverse fields like computing, defence, etc. In this section, we consider quantum networks performing different information processing tasks and present the bottlenecks for such networks. We first consider a linear repeater-relay network and provide practical limitations on the state parameter and the number of nodes in the network for performing device-independent secret key distillation between the end nodes of the network. This provides a practical limitation on the structure of such networks for performing secure communication. We also consider the similar network structure and provide limitations on the number of relay stations between the end users and the success probability for (a) performing teleportation protocol, (b) performing the Bell-CHSH inequality violation experiment and (c) for the shared state being entangled. This provides a practical limitation on the robustness of the linear repeater-relay network for performing different information processing tasks.

Next, we consider the task of distributing entangled states between two geographically far-off cities. For this, we introduce a hybrid satellite-fiber network model. The model has a global scale satellite network connecting different ground stations and a local scale network connecting different localities to the ground stations. Furthermore, we consider the scenario where the ground stations have quantum memory and multiple input and out-

put channels. In such a scenario, we present an algorithm for the distribution of resources from the input channels to the output channels. For this hybrid satellite-fiber network, we present the average entanglement yield ξ_{avg} for currently available and futuristic experimental architectures.

The different quantum processors in the current Noisy Intermediate-Scale Quantum era are physically implemented using different technologies. The processors by Google, Rigetti and IBM use superconducting architecture, while those by Honeywell and IonQ use a trapped ion-based architecture. We present these processors as graphical networks and present their robustness measures. Furthermore, we introduce a futuristic 1024 qubit network model for quantum processors and present their robustness. We then consider two futuristic tasks (a) connecting all major airports of the world via a mesh quantum network and (b) connecting the Pentagon to the major nuclear power plants in the United States via a star quantum network. We present practical limitations for implementing these network structures.

Testing quantum nonlocal correlations under constrained free will and imperfect detectors

In this part of the thesis, we consider a special network consisting of two nodes representing two parties that share a bipartite quantum state ρ_{AB}. In such a scenario, two central assumptions in testing the standard locally realistic hidden variable (LRHV) theories are that (a) the two parties have free will in choosing the measurement settings, and (b) the parties have perfect detectors at the measurement devices. We investigate the effect of relaxing these two assumptions in testing the LRHV theories. We begin by considering that there exists some hidden variable λ belonging to some hidden variable space Λ. The probability distribution of the outputs conditioned on the inputs can then be expressed as

$$p(ab|xy) = \sum_{\lambda\in\Lambda} p(ab|xy\lambda)p(\lambda|xy) \tag{1}$$

The hidden variable λ can provide an explanation of the observed experimental statistics. An adversary can bias the choice of the measurement settings in the λ scale according to

$$p(xy) = \sum_{\lambda \in \Lambda} p(xy|\lambda)p(\lambda) \tag{2}$$

and trick Alice and Bob into thinking they are choosing the measurement settings with equal probability. We consider the simplest situation where each party chooses between two measurement settings and provide a cheating strategy of an adversary [1].

The measurement independence assumption requires that λ does not contain any information about the choice of measurement settings. This assumption can be expressed as $p(\lambda|xy) = p(\lambda)$ or equivalently $p(xy|\lambda) = p(xy)$, where x and y are the measurement settings of Alice and Bob. In standard literature, the relaxation of measurement independence, which we call measurement dependence, has been quantified via two approaches. The first approach involves bounding $p(xy|\lambda)$ in the range $[l, h]$ [7, 8]. The second approach involves using a distance measure to quantify the measurement dependence [9, 10]. We consider the first approach in quantifying measurement dependence, i.e., $l \leq p(xy|\lambda) \leq h$ and obtain allowed values of l to ensure nonlocality for different interesting quantum behaviours [1]. At first, we consider the behaviour that violates the AMP tilted Bell inequality [11] and provides close to 2 bits of randomness. We observe that such behaviours are always local with measurement dependence. Next, for the behaviour that maximally violates the Bell-CHSH inequality [12], we require $l > 0.2023$. Next, we consider the behaviour that provides 1.6806 bits of global randomness and show that for such a behaviour, we require $l > 0$.

We next consider the distance measure approach to quantify measurement dependence. In this approach, following [9, 10], we define the measure of measurement dependence for Alice and Bob as

$$M_1 = \max\left\{ \int d\lambda |p(\lambda|x_1, y_1) - p(\lambda|x_2, y_1)|, \int d\lambda |p(\lambda|x_1, y_2) - p(\lambda|x_2, y_2)| \right\}, \tag{3}$$

and

$$M_2 = \max\left\{ \int d\lambda |p(\lambda|x_1, y_1) - p(\lambda|x_1, y_2)|, \int d\lambda |p(\lambda|x_2, y_1) - p(\lambda|x_2, y_2)| \right\}. \tag{4}$$

We show [1] that the AMP tilted Bell expression $I_\alpha^\beta := \beta\langle x_1\rangle + \alpha\langle x_1y_1\rangle + \alpha\langle x_1y_2\rangle + \langle x_2y_1\rangle - \langle x_2y_2\rangle$ in the presence of locality and relaxed measurement independence is bounded by

$$I_\alpha^\beta \leq \beta + 2\alpha + \min\Big\{\alpha(M_1 + \min\{M_1, M_2\}) + M_2, 2\Big\}. \tag{5}$$

Using the modified upper bound on the AMP tilted Bell inequality from Eq. (5), we present bounds on M_1 and M_2 to ensure that quantum nonlocal behaviours remain nonlocal with measurement independence relaxed for Alice, Bob and both.

We next deviate from the conventional approach of assuming perfect detectors; we present a framework to determine the threshold values of the detector parameters that are robust enough to certify the nonlocality of quantum nonlocal behaviours [1]. For this, we adapt the approach discussed in [13] to model imperfect detectors as a sequential application of a perfectly working inner box followed by a lossy outer box. We deviate from the approach in [13] by considering an inner box containing a quantum source generating bipartite quantum states whose behaviour is nonlocal under constrained free will but assuming that detectors are perfect. An outer box introduces the detector imperfections (dark counts and no detection events). The quantum nonlocal behaviours generated in the inner box get mapped to the outer box behaviour with the detector imperfection parameters, dark count probability δ and detector efficiency η. The outer box behaviour then undergoes an LRHV test, based on which we present the threshold detector parameters. We present the critical detector parameters η and δ that make the detectors robust for testing of different quantum nonlocal behaviours.

Outlook

In this thesis, we consider a framework for representing networks as undirected weighted graphs and observing their robustness for different information processing tasks. This framework is potentially useful in designing any network structure for performing information processing tasks. We then provide practical limitations on (a) implementing quantum networks suited for sharing entanglement between two far-off cities, (b) design-

ing quantum processor networks and (c) testing the nonlocality of quantum nonlocal behaviours in a bipartite network with imperfect detectors and constrained free-will. These limitations would provide a benchmark for experimentalists to compare different components to be used in the network so that optimal choices in the architecture and quantum systems and channels to be used in the network can be made.

Supervisor: Prof. Shiv Sethi
Raman Research Institute
Bangalore - 560080, India

Abhishek Sadhu
Raman Research Institute
Bangalore - 560080, India

Co-supervisor: Dr. Siddhartha Das
International Institute of Information Technology,
Hyderabad, Telangana - 500032, India

LIST OF FIGURES

LIST OF ALGORITHMS

CHAPTER 1

INTRODUCTION

"The most beautiful experience we can have is the mysterious. It is the fundamental emotion that stands at the cradle of true art and true science."

— Albert Einstein

1.1 Motivation and Overview

Figure 1.1: The quantum Internet - an interconnected network of users enabled to perform desired quantum information processing and computing tasks among them. Some of the tasks that are envisioned to be possible in full-fledged quantum Internet are enabling remote end users to access quantum computers over the cloud [14], secure communication [15–27], and cryptographic tasks against adversaries of varying degree [6, 28–35].

The development of the Internet has been one of the key technological developments of the twentieth century. While digital computing has been the definitive technology of the twentieth century, it is anticipated that quantum technology will be for the 21st century. Among others, the most promising prospect of such technology is the development of quantum key distribution, which provides unconditional security for generating secure, random bits among trusted end users against an eavesdropper limited by the laws of quantum theory.

Today we are already starting to see elementary realizations of essential quantum technologies like quantum communication, quantum key distribution [36], and quantum computing [37–39]. With further technological advancement, as the technologies become increasingly accessible, there will be a demand for networking them, and it is anticipated that the sharing of quantum resources between end users of a network will become a

pressing issue.

If we look at the historical development of today's Internet, the first demonstrations of digital computer networks were point-to-point communication networks. Since then, rapid technological development has resulted in today's Internet, which allows arbitrary world-wide networking across ad hoc networks consisting of an arbitrarily large number of end users in a decentralised plug-and-play manner. As with digital computing, it is foreseeable that there will be a demand for a quantum Internet [40–42] (see Fig. 1.1), enabling a wide range of quantum information-processing tasks between any number of users over ad hoc networks.

Today's Internet is a technology stack, such as Transmission Control Protocol (TCP)/ Internet Protocol (IP), having different levels of abstraction of digital information [43]. At the bottom layer, digital data is communicated across a physical medium. Above this, data is decomposed into packets. These packets are then transmitted over networks. TCP guarantees data integrity, Quality of Service (QoS), and packet routing between source and destination. Finally, raw data is reconstructed from the data packets the end user receives. The packets of data transmitted over the quantum Internet will be quantum states, and the TCP will enable the transmission of these states between end nodes and ensure quality control.

The TCP layer offers a virtual software interface to the remote digital assets, enabling high-level services such as File Transfer Protocol (FTP), multimedia streaming, remote computation, cloud storage and many others. The end user is unaware of the underlying network protocols. The FTP and cloud storage enable end users to store data on far-off data centres and mount them as if they were local. A similar concept holds for online streaming services like Netflix and HBO, where remotely stored multi-media files behave like a local copy. It is foreseeable that there may be a demand for such services over the quantum Internet.

In a quantum network, the successful functioning of an elementary link is dependent on the properties of the packets of data (the quantum states), such as purity, fidelity with a target state, amount of nonlocality, and others, none of which are applicable to classical

digital data processing. As in the classical case, a primary objective is to find optimal strategies for routing data packets between end nodes. However, the success of the strategy will depend on the properties of the data packets (such as singlet fraction) being above a critical threshold defined by the information processing task that the end nodes intend to perform. Also, quantum resources (such as state, measurement operation, etc...) being noisy [6, 36, 44–47], imperfect [1, 34, 48–50] and fragile [51–54], limits the realization of quantum networks for practical purposes thereby making it necessary to analyse the scalability of networks for performing various information processing tasks.

The routing strategies do not guarantee on-demand access to network bandwidth. In networks with limited bandwidth, there can be congestion during high traffic, and some end nodes may have to wait their turn. For this, some networks may require at least some nodes to have quantum memories, which will allow the buffering of quantum packets for a sufficiently long duration while they wait for network resources. The required lifetime of the quantum states in the memory will have to be greater than the network congestion time.

The physical realization of the quantum Internet will likely follow a task-oriented approach. The underlying network structure at any implementation stage is expected to provide loose coupling [55], meaning that the end users can perform information processing tasks without knowing the underlying implementation details. The loose coupling reduces the inter-dependencies between multiple tasks performed over the quantum Internet and motivates analysing the practical limitations involved in implementing different tasks over the quantum Internet.

As the size of the quantum networks increases, a possible reason that can compromise the proper functioning of the network is the random breakdown of nodes and edges [56] either due to hardware failure or from a strategic point of view, with adversaries attacking the network [57–59]. Such failures can possibly prevent some active nodes from connecting to the rest of the network, leading to a partition or even a destroyed system. To observe the extreme effect of the random breakdown of nodes and edges, consider the k-complete graph and tree graph. In a k-complete graph with point-to-point links between every

pair of nodes, there are alternate paths between the surviving nodes if some nodes and edges fail. In a tree graph, the breakdown of a single node or edge may disconnect the network, making certain routes impossible. Somewhere in between the two extremes is a mesh network, which is relatively robust against the random failure of nodes and edges but is susceptible to conspiratorial attacks, which target the most important nodes. Consequently, it is important to analyse the robustness of networks, i.e., their ability to withstand structural failures.

Having analysed the robustness of a given network, an important question remains: How can we improve the network's robustness? A possible first approach would be to identify and ensure the proper functioning of the critical nodes of the network. These nodes play an important role in ensuring the operational effectiveness of the network. By prioritizing the proper functioning of the critical nodes, we can significantly reduce the network's vulnerability to disruptions in the face of adversarial attacks or random failures.

Looking at specific tasks that can be performed over the quantum Internet, we note that the sharing of quantum nonlocal correlations [60–67] among the nodes of a network is a primitive for tasks such as the generation and certification of randomness and secret key in a device-independent way [28, 68–73]. Quantum systems that violate local realistic hidden variable (LRHV) inequalities [74] are said to have quantum nonlocal correlations. The LRHV inequalities, also called Bell-type inequalities, are based on two physical assumptions: (a) the existence of local realism and (b) the no-signalling criterion [75] (see, e.g., [74] and references therein). Such inequalities were first obtained by J.S. Bell [76] to show that the statistical predictions of quantum mechanics cannot be explained by local realistic hidden variable (LRHV) theories.

It is known that the experimental verification of Bell's inequality requires additional assumptions which could lead to incurring loopholes such as locality loophole [77], freedom-of-choice (measurement independence or free will) loophole [78, 79], fair-sampling loophole (detection loophole) [78, 80]. In recent major breakthroughs [63, 64, 81, 82], incompatibility of quantum mechanics with LRHV theories has been demonstrated by considerably loophole-free experiments showing violation of Bell's inequality by quantum states

with quantum nonlocal correlations.

The assumption of free will was first relaxed in [9] using a distance-measure-based quantification of the measurement dependence. It was shown that the Bell-CHSH inequality can be violated by sacrificing equal free will for both parties. This result was extended to the scenario of parties having different amounts of free will in [10] and for one of the parties in [83]. In an alternate approach, measurement dependence was quantified in [7,8] by bounding the probability of choosing the measurement settings to be in a given range. Following this approach, tests for nonlocality have been constructed [7, 84]. These inequalities have been applied to randomness amplification protocols [84,85]. However, the consideration of imperfect detectors in the implication of these measurement-dependent LRHV inequalities is still lacking, as the above-mentioned works assumed perfect detection while allowing for relaxation in measurement dependence. A possible first approach would be to analyze limitations on sharing nonlocality among neighbouring nodes when an adversary biases the choice of measurement settings and the detection units of the two parties.

1.2 Organization of the thesis

Chapter 2 is devoted to the basic knowledge of quantum states, channels and measurement. We discuss definitions of quantum state, separable and entangled states, isotropic and Werner states, as well as quantum channels, quantum instruments and measurement channels. We also present a brief introduction to graph theory relevant to the content of the thesis.

In **Chapter 3**, we analyze the robustness and scalability of the quantum Internet using graph (network) theoretic tools. Specifically, we present a graph theoretic framework for networks performing various tasks in Sec. 3.1 and present conditions for no percolation in a lattice network for a class of tasks. In Sec. 3.2, we present figures of merit to compare the robustness of network topologies and observe them for different networks in Sec. 3.2.1. Noting different quantum processor architectures as instances of quantum

networks, we compare the figures of merit of different currently available and futuristic quantum processors in Sec. 3.3. In Sec. 3.2.2, we present measures to identify the critical nodes in a given network. In Sec. 3.4, we present algorithms that are primitives for implementing different information-processing tasks using the quantum Internet. The content of this chapter is based on [2].

In **Chapter 4**, we analyze limitations on the potential use of the quantum Internet for real-world applications. Specifically, we present the critical success probability of elementary links and critical length scales for various tasks over a repeater-based network in Sec. 4.1. In Sec. 4.2, we present limitations on the scalability of networks for quantum communication, assuming some hypothetical scheme can improve the transmission of channels connecting the nodes of the network. We present limitations on using isotropic states in networks for device-independent secret key distillation in Sec. 4.3. Considering a repeater-based network, we present an upper bound on the number of elementary links between the end nodes such that the shared state remains entangled and is useful for different information-processing tasks. We present practical bottlenecks in the distribution of entangled states between far-off cities using a satellite-based network in Sec. 4.4. Looking at possible tasks that can be performed over the quantum Internet in the future, we present practical bottlenecks on some of the tasks in Sec. 4.5. The content of this chapter is based on [2].

In **Chapter 5**, we analyze the limitations of sharing nonlocality between two neighbouring nodes when an adversary biases the choice of measurement settings and the detection units of the two nodes. Specifically, we introduce the framework of locality and measurement dependence, a constraint limiting the user's free will in Section 5.1. We present a model where an adversary tricks the user into thinking they have freedom of choice for the measurement. Section 5.2 compares two approaches to quantify the measurement dependence. We determine the critical values of the measurement-dependence parameters necessary for the certification of nonlocality when free will is relaxed and compare them with the amount of violation obtained for the Bell-CHSH inequality, tilted Hardy relations and the tilted Bell inequalities. In Section 5.3, We determine the threshold values of the detector parameters, namely inefficiency and dark count probability, such that the

detectors are robust enough to certify nonlocality in the presence of constrained free will. In Section 5.4, we introduce a new set of LRHV inequalities adapted from the AMP tilted Bell inequality using distance-measures-based measurement dependence quantities. We use these inequalities to observe the effect of relaxing the free will assumption for either party on certifying quantum nonlocal correlations. The content of this chapter is based on [1].

Finally, in **Chapter 6**, we conclude the thesis by summarising all results provided in the thesis along with presenting possible future directions of research.

CHAPTER 2

PRELIMINARY

"If I have seen further, it is by standing
on the shoulders of Giants."

— Sir Isaac Newton

This chapter briefly introduces some of the background information needed for the thesis. In Sec. 2.1, we present definitions of quantum states, channels, and measurements. In Sec. 2.2, we briefly introduce basic definitions and concepts of graph theory that relate to the contents of the thesis.

2.1 Quantum states, channels, and measurement

The mathematical formulation of quantum mechanics was initiated by von Neumann [86, 87] and Dirac [88], who presented an axiomatic approach to quantum theory. The axiomatic approach is advantageous for theoretical work as the physical systems' pertinent details are unimportant. This approach has proved to be quite fruitful in quantum information processing and has become the standard approach to these topics [89–92]. Please refer to [89–92] for more details on the topics presented in this section.

The mathematical structure of quantum mechanics is based on the Hilbert space, an inner product space (vector space with inner product) that is complete. In this thesis, we consider only finite-dimensional complex Hilbert spaces. The theory of linear algebra and matrix analysis is sufficient for our purposes.

2.1.1 Quantum states

Every quantum system, say A, has an associated Hilbert space $\mathcal{H}_A$ of (finite) dimension d_A. We call a quantum system having $d \geq 2$ and belonging to Hilbert space $\mathbb{C}^d$ as a qudit. Qudits with $d = 2$ are called qubits. The state of a quantum system is represented by a linear positive semi-definite operator having a unit trace called the density operator.

Definition 1. *(Quantum state) The state of a quantum system A is represented by the density operator ρ_A defined on $\mathcal{H}_A$ and satisfies the conditions: (i) $\rho_A \geq 0$, (ii) $\rho_A = \rho_A^\dagger$, (iii) $\mathrm{Tr}[\rho_A] = 1$. The set of density operators of A is denoted by $\mathcal{D}(\mathcal{H}_A)$.*

A pure state is a rank-one density operator given by $\rho_A := |\psi\rangle\langle\psi|_A$ where $|\psi\rangle_A \in \mathcal{H}_A$ are

unit-norm vectors in the Hilbert space. Every pure-state vector has the form

$$|\psi\rangle_A = \sum_{k=0}^{d-1} \alpha_k \, |k\rangle_A, \tag{2.1}$$

where $\alpha_k \in \mathbb{C}$ and follows the normalisation condition $\sum_{k=0}^{d-1} |\alpha_k|^2 = 1$.

Every density operator ρ_A can be decomposed as a convex combination of pure states

$$\rho_A = \sum_x p_x |\psi_x\rangle\langle\psi_x|_A \tag{2.2}$$

where $p_x \in [0, 1]$, $\sum_x p_x = 1$, and $\{|\psi_x\rangle\}_x$ is the set of state vectors.

We denote the density operator of a composite system AB as $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$; $\mathrm{Tr}_B[\rho_{AB}] = \rho_A \in \mathcal{D}(\mathcal{H}_A)$ is the reduced state of A.

Definition 2. *(Fidelity [93]) The fidelity between the states ρ and σ is defined as*

$$F(\rho, \sigma) := \left(\mathrm{Tr}\left[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}} \right] \right)^2 \tag{2.3}$$

Fidelity between two states quantifies the overlap between the states. We note that $F(\rho, \sigma) = 0$ iff ρ and σ have support on orthogonal subspaces while $F(\rho, \sigma) = 1$ iff $\rho = \sigma$. The fidelity between ρ and a pure state σ is given by

$$F(\rho, |\sigma\rangle\langle\sigma|) = \langle\sigma|\rho|\sigma\rangle = \mathrm{Tr}[\rho\sigma]. \tag{2.4}$$

The fidelity is multiplicative meaning,

$$F(\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2) = F(\rho_1, \sigma_1) F(\rho_2, \sigma_2) \tag{2.5}$$

Definition 3. *(Separable and entangled states) The state of a composite system AB denoted by $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$ is called separable if it can be expressed as in the form of*

$$\rho_{AB} = \sum_x p_x \, \rho_A^x \otimes \rho_B^x, \tag{2.6}$$

where $\{\rho_A^x\}_x$ *and* $\{\rho_B^x\}_x$ *are sets of pure states,* $p_x \in [0,1]$ *and* $\sum_x p_x = 1$. *States that cannot be expressed in the form of Eq. (2.6) are said to be entangled.*

A maximally entangled state of bipartite system AB is defined as $\Psi_{AB}^+ := |\Psi^+\rangle\langle\Psi^+|_{AB}$ where

$$|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle_{AB}, \tag{2.7}$$

$d = \min\{|A|, |B|\}$ is the Schmidt-rank of the state Ψ_{AB}^+, and $\{|i\rangle\}_{i=0}^{d-1}$ forms an orthonormal set of vectors (kets).

We next discuss two classes of states called isotropic states and Werner states that will be used later in the thesis.

An isotropic state [94] $\rho_{AB}^I(p,d)$ is $U \otimes U^*$ invariant for an arbitrary unitary U. For $p \in [0,1]$, such a state can be written as

$$\rho_{AB}^I(p,d) := p\Psi_{AB}^+ + (1-p)\frac{\mathbb{1}_{AB} - \Psi_{AB}^+}{d^2-1} \tag{2.8}$$

where Ψ_{AB}^+ is a maximally entangled state of Schmidt rank d. An Isotropic state $\rho_{AB}^I(p,d)$ written as in Eq. (2.8)[1] is separable iff $p \in [0, 1/d]$.

A Werner state [95] $\rho_{AB}^W(p,d)$ is $U \otimes U$ invariant for an arbitrary unitary U. For $p \in [0,1]$, such a state can be written as

$$\rho_{AB}^W(p,d) := p\frac{2}{d(d+1)}\Pi_{AB}^+ + (1-p)\frac{2}{d(d-1)}\Pi_{AB}^- \tag{2.10}$$

where $\Pi_{AB}^\pm := (\mathbb{I} \pm F_{AB})/2$ are the projections onto the symmetric and anti-symmetric sub-spaces of $\mathcal{H}_A$ and $\mathcal{H}_B$. $F_{AB} = \sum_{ij} |i\rangle\langle j|_A \otimes |j\rangle\langle i|_B$ is the SWAP operator on A and B. A

[1] We can also express isotropic states (Eq. (2.8)) as

$$\rho_{AB}^I\Big(p(\lambda), d\Big) = \lambda\Psi_{AB}^+ + (1-\lambda)\frac{\mathbb{1}_{AB}}{d^2} \tag{2.9}$$

for $p(\lambda) = [\lambda(d^2-1)+1]/d^2$ and $\lambda \in [-1/(d^2-1), 1]$. We note that $\lambda^n \geq 0$ for all even $n \in \mathbb{N}$. For our purposes in this thesis, we will be restricting $\rho_{AB}^I\Big(p(\lambda), d\Big)$ to the case $\lambda \in [0,1]$ without loss of generality. We call λ as the visibility of the state $\rho_{AB}^I\Big(p(\lambda), d\Big)$.

Werner state $\rho_{AB}^{W}(p,d)$ written as in Eq. (2.10) is separable iff $p \in [1/2, 1]$.

Another important type of state is the classical-quantum state, which we define next.

Definition 4. *(Classical-quantum state) The density operator corresponding to a classical quantum state ρ_{XA} can be expressed as*

$$\rho_{XA} = \sum_x p_x |x\rangle\langle x|_x \otimes \rho_A^x, \tag{2.11}$$

where $\{\rho_A^x\}_x$ is a set of quantum states. If A is prepared in a state from the set $\{\rho_A^x\}_x$ according to the probability distribution p_x, then the information of x is stored in the classical register X. A classical register X is represented by a set of orthogonal quantum states $\{|x\rangle\langle x|_X\}_x$ defined on the Hilbert space $\mathcal{H}_X$.

2.1.2 Bipartite Entanglement

A fundamental question of interest is to check if a given state is separable or entangled. For two-qubit states, an entanglement measure is the concurrence [96], which is defined as

$$C(\rho_{AB}) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}, \tag{2.12}$$

where $\lambda_1, \lambda_2, \lambda_3,$ and λ_4 are the eigen-values in descending order of the Hermitian matrix $\mathcal{R} = \sqrt{\sqrt{\rho}\tilde{\rho}\sqrt{\rho}}$ with $\tilde{\rho} = (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)$ being the spin-flipped state of ρ.

For the two-qubit systems, we have a maximally entangled state as

$$|\Psi^+\rangle_{AB} := \frac{1}{\sqrt{2}}\Big(|00\rangle_{AB} + |11\rangle_{AB}\Big). \tag{2.13}$$

If we perform σ_z^A on the subsystem A of the state $|\Psi^+\rangle_{AB}$, we obtain the state $|\Psi^-\rangle_{AB} := \frac{1}{\sqrt{2}}\Big(|00\rangle_{AB} - |11\rangle_{AB}\Big)$. Similarly, on performing σ_x^A and σ_y^A on the subsystem A of the composite system $|\Psi^+\rangle_{AB}$, we obtain $|\Phi^+\rangle_{AB} := \frac{1}{\sqrt{2}}\Big(|01\rangle_{AB} + |10\rangle_{AB}\Big)$ and $|\Phi^-\rangle_{AB} := \frac{1}{\sqrt{2}}\Big(|01\rangle_{AB} - |10\rangle_{AB}\Big)$. The states $|\Psi^\pm\rangle_{AB}$ and $|\Phi^\pm\rangle_{AB}$ are known as the Bell states. The Bell states have

concurrence of one and form an orthonormal basis, called the Bell basis, for a two-qubit space.

2.1.3 Quantum Channels

We define a quantum channel as follows.

Definition 5. *(Quantum channel) A quantum channel* $\mathcal{M}_{A\to B} : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_B)$ *is a completely positive, and trace-preserving map acting on the space* $\mathcal{D}(\mathcal{H}_A)$ *of operators belonging to the Hilbert space* $\mathcal{H}_A$ *of the quantum system A. For the input state* $\rho_A \in \mathcal{D}(\mathcal{H}_A)$*, the output state is given by* $\mathcal{M}_{A\to B}(\rho_A) \in \mathcal{D}(\mathcal{H}_B)$*.*

A map $\mathcal{M}_{A\to B} : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_B)$ is a linear, trace-preserving, and completely positive if it has the following Choi-Kraus decomposition [97, 98]:

$$\mathcal{M}_{A\to B}(\rho_A) = \sum_{i=1}^{r-1} \mathcal{K}_i \rho_A \mathcal{K}_i^\dagger \;\; \forall \rho_A \in \mathcal{D}(\mathcal{H}_A) \tag{2.14}$$

where $\mathcal{K}_i \in \mathcal{D}(\mathcal{H}_A, \mathcal{H}_A)$ and $\sum_{i=1}^{r-1} \mathcal{K}_i^\dagger \mathcal{K}_i = \mathbb{1}_A$ with r need not be larger than $\dim(\mathcal{H}_A)$ $\dim(\mathcal{H}_B)$.

The Choi-Kraus decomposition presented in Eq. (2.14) may be interpreted in two ways (see Fig. 2.1). For the first interpretation, consider a quantum state represented by a density operator ρ and measurements $\{O_j\}_j$ are being performed on the state. The probability of obtaining outcome j from the measurement is given by $p_j = \mathrm{Tr}[O_j^\dagger O_j \rho]$ and we have the post-measurement state as $(O_j \rho O_j^\dagger)/p_j$. In a black-box scenario, if an adversary measures the system and does not inform us of the measurement outcomes, we have the resulting ensemble as $\{p_j, (O_j \rho O_j^\dagger)/p_j\}_j$. The density operator corresponding to this ensemble is $\sum_k O_j \rho O_j^\dagger$, which is equivalent to the evolution of ρ via a quantum channel with the measurement operators as the Kraus operators.

For the second interpretation, consider a joint system in a state $\rho_A \otimes |0\rangle\langle 0|_E$. Let the system evolve according to some unitary U_{AE}. After the evolution, let us only have access to the system A, whose state is given by $\sigma_A = \mathrm{Tr}_E[U_{AE}(\rho_A \otimes |0\rangle\langle 0|_E)U_{AE}^\dagger]$. This evolution is

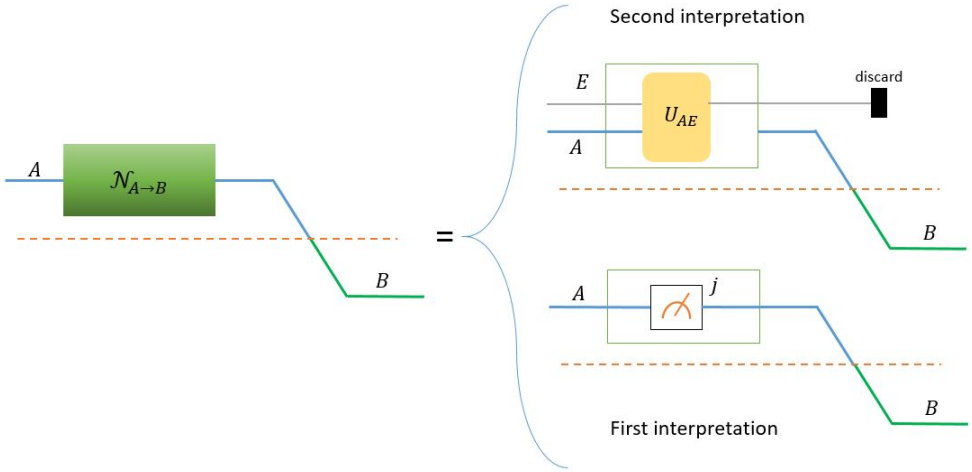


Figure 2.1: In this figure, we depict a quantum channel $\mathcal{M}_{A\to B}$ taking a quantum system A to a quantum system B. We can interpret the noise in the quantum channel as (a) the loss in knowledge of a measurement outcome and (b) due to the unitary interaction with an environment to which we do not have access.

equivalent to that of a completely positive, trace-preserving map having Kraus operators $\{O_j \equiv (\mathbb{1}_A \otimes \langle i|_E) U_{AE} (\mathbb{1}_A \otimes |i\rangle_E)\}_j$ (see [90] for details).

Let us consider a scenario where we are required to determine the evolution of a quantum state with the output consisting of both classical and quantum systems. Such a scenario may arise when Alice wants to send both classical and quantum information, and Bob uses a quantum instrument to decode both kinds of information. Such an evolution with a hybrid output is given by a quantum instrument, which we will define next.

Definition 6. *(Quantum instrument) A quantum instrument $\mathcal{I}$ is a (finite) set of completely positive, trace non-increasing maps $\{\mathcal{M}_x\}_x$ such that $\sum_x \mathcal{M}_x$ is a trace-preserving map. The action of the quantum instrument on a density operator is a quantum channel with a classical and quantum output defined as follows.*

$$\mathcal{I}(.) := \sum_x \mathcal{M}_x(.) \otimes |x\rangle\langle x|_X. \tag{2.15}$$

The quantum instrument channel defines an operation that stores outcome x in a classical register X and the corresponding output state. We next define the quantum measurement channel.

Definition 7. *(Quantum measurement channel) A quantum measurement channel $\mathcal{M}_{A'\to AX}$ is a quantum instrument whose action is defined as*

$$\mathcal{M}_{A'\to AX}(.) := \sum_x \mathcal{E}^x_{A'\to A}(.) \otimes |x\rangle\langle x|_X, \tag{2.16}$$

where each $\mathcal{E}^x_{A'\to A}$ is a completely positive, trace non-increasing map such that $\mathcal{M}_{A'\to AX}$ is a quantum channel and X is a classical register that stores the measurement outcomes.

The qubit Bell measurement channel is an example of a measurement channel, which we will define next.

Definition 8. *(Qubit Bell measurement channel) The qubit Bell measurement with success probability q is defined as*

$$\mathcal{M}_{A_1A_2\to X}(.) := q \sum_{j=1}^{4} \mathrm{Tr}[\Psi^{(j)}(.)\Psi^{(j)}]|j\rangle\langle j|_X + (1-q)\,\mathrm{Tr}[.] \otimes |\perp\rangle\langle\perp|_X, \tag{2.17}$$

where $\{\Psi^{(j)}_{A_1A_2}\}_{j=1}^4$ denotes projective measurements on the set of maximally entangled states $\{\Psi^+_{A_1A_2}, \Psi^-_{A_1A_2}, \Phi^+_{A_1A_2}, \Phi^-_{A_1A_2}\}$ and $|\perp\rangle \perp |j\rangle$.

Another example of a quantum channel used frequently is the partial trace channel, often called the partial trace. Physically, it corresponds to discarding a part of a quantum system. Given a quantum state ρ_{AB}, the partial trace over the subsystem A is a channel denoted by Tr_A and is defined as

$$\mathrm{Tr}_A(\rho_{AB}) := \sum_{j=0}^{d_A-1} (\langle j|_A \otimes \mathbb{1}_B)\rho_{AB}(|j\rangle_A \otimes \mathbb{1}_B). \tag{2.18}$$

Similarly, the partial trace over the subsystem B is a channel denoted by Tr_B and is defined as

$$\mathrm{Tr}_B(\rho_{AB}) := \sum_{j=0}^{d_B-1} (\mathbb{1}_A \otimes \langle j|_B)\rho_{AB}(\mathbb{1}_A \otimes |j\rangle_B). \tag{2.19}$$

In this thesis, we write $\rho_A \equiv \mathrm{Tr}_B(\rho_{AB})$ and $\rho_B \equiv \mathrm{Tr}_A(\rho_{AB})$ to denote states at the output of

the partial trace channels over subsystems B and A respectively.

2.2 Graph Theory

This section presents a brief introduction to graph theory relevant to what is needed for this thesis. We will be working only with undirected graphs. For a more detailed introduction, please refer [99]. We define a graph in the following way.

Definition 9. *(Graph [99]) A graph G is a triple containing a vertex set $\mathbb{V}$, an edge set $\mathbb{E}$, and a relation that associates with each edge two vertices (not necessarily distinct) called its end-points.*

We consider networks represented as graph $G(\mathbb{V}, \mathbb{E})$ classified as weighted and undirected. We denote $|\mathbb{V}|$ as N_v and $|\mathbb{E}|$ as N_e, where $|\mathbb{X}|$ denotes the size of the set $\mathbb{X}$. The vertices of the graph G are denoted as $v_i \in \mathbb{V}$ and the edges connecting the nodes $\{v_i, v_j\} \in \mathbb{V}$ as $e_{ij} \in \mathbb{E}$. A network's nodes, edges, and weights may in general, change with time (see Appendix A.7 for details).

Given a graph $G(\mathbb{V}, \mathbb{E})$, a walk from v_i to v_j denoted by $v_i \leftrightarrow v_j$ is a finite sequence $\mathbb{W} = (v_i, e_{i1}, v_1, e_{12}, v_2, ..., v_{k-1}, e_{k-1j}, v_j)$ of vertices $v_l \in \mathbb{V}$ and edges $e_{lm} \in \mathbb{E}$ such that $(v_i, v_1) \in e_{i1}$, $(v_1, v_2) \in e_{12}$,...,$(v_{k-1}, v_j) \in e_{k-1j}$. A walk between a pair of nodes has the following properties:

1. $v_i \leftrightarrow v_i \; \forall v_i \in \mathbb{V} \implies \mathbb{W} = (v_i)$.
2. From $v_i \leftrightarrow v_j$, we obtain $v_j \leftrightarrow v_i$ by reversing the walk.
3. If $v_i \leftrightarrow v_j$ and $v_j \leftrightarrow v_k$ then $v_i \leftrightarrow v_k$ is obtained by concatinating walks from v_i to v_j and v_j to v_k.

A walk between v_i and v_j where all the intermediate vertices and edges are distinct is called a path between the pair of vertices. We denote the path connecting two distant nodes v_i and v_k as $\mathcal{P}(v_i, v_k)$ having length $len(\mathcal{P})$. The shortest network path between v_i

and v_k is denoted as $dist(v_i, v_k)$. The shortest path length between the most distant nodes of a graph is called the graph's diameter.

A value $w_{ij} \in \mathbb{R}$ assigned to an edge e_{ij} of the graph is called the edge weight. The graph G together with w_{ij} is called a weighted graph. A graph where the edges do not have a direction is called an undirected graph. The edges of an undirected graph indicate a bidirectional relationship where each edge can be traversed from both directions.

For the graph $G(\mathbb{V}, \mathbb{E})$, let us partition the set of vertices $\mathbb{V}$ as

$$[v] \coloneqq \{v_j \in \mathbb{V} : v_j \leftrightarrow v\} \tag{2.20}$$

denoting the set of all vertices connected to v via a walk. Let us denote the set of edges connecting the vertices in $[v]$ as $\mathbb{E}_{[v]}$; it then follows that $\mathbb{E}_{[v]} \subseteq \mathbb{E}\ \forall v \in \mathbb{V}$. The graph $G_{sg} \coloneqq G(\mathbb{V}_{sg}, \mathbb{E}_{sg}) = ([v], \mathbb{E}_{[v]})$ is a subgraph of G. We next define a subgraph.

Definition 10. *(Subgraph [99]) A subgraph of a graph G is a graph G_{sg} such that $\mathbb{V}(G_{sg}) \subseteq \mathbb{V}(G)$ and $\mathbb{E}(G_{sg}) \subseteq \mathbb{E}(G)$ and the assignment of the end-points to edges in G_{sg} is the same as in G. We denote a subgraph G_{sg} of the graph G as $G_{sg} \subseteq G$.*

We next define a special type of graph called a tree graph that will be used later in the thesis.

Definition 11. *(Tree [99]) A graph that does not have a cycle is acyclic. A tree is a connected acyclic graph. A leaf node in a tree is a vertex of degree 1.*

We next present some properties of tree graphs,

- Every tree with at least two vertices has at least two leaf nodes.
- Deleting a leaf node from a tree with n vertices produces a tree with $n - 1$ vertices.
- For any pair of vertices $\{v_i, v_j\}$ in a tree, there is exactly one path connecting them.

Tree graph structures are often used to store and organize data in memories. We next present a particular kind of data storage structure called the max-heap data structure that will be later used in the thesis.

Definition 12. *(Max-heap data structure [100]) A max heap is a tree-based data structure that satisfies the following heap property: for any given node Y, if X is a parent of Y, X's key (the value) is greater than or equal to the key of Y.*

In Fig. 2.2, we present the tree and array representations of a max heap data structure with 9 nodes.

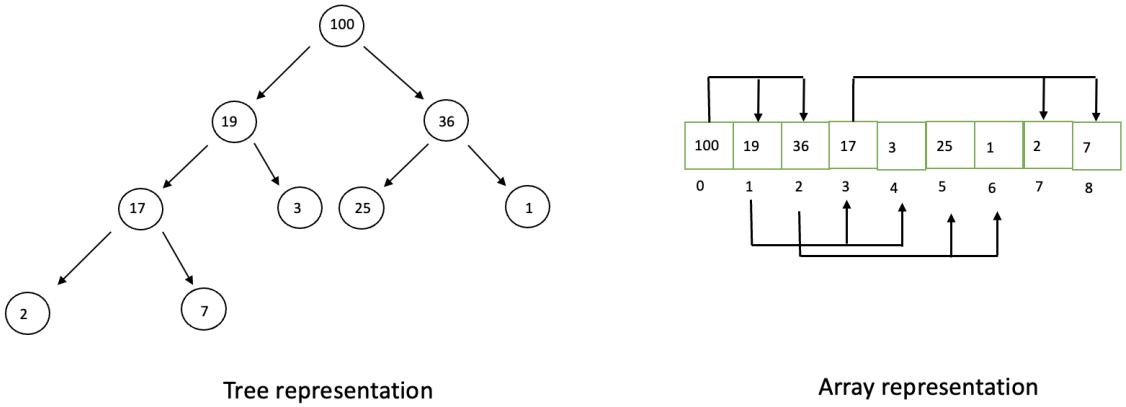


Figure 2.2: In this figure, we present the tree and array representations of a max-heap data structure with nine nodes. The tree representation shows the nodes in circles with the node values written inside them. In the array representation, the nodes are stored in continuous memory allocations (shown in green boxes numbered 0 to 9). The relation between the nodes is shown using arrows. We see that it satisfies the heap property: the value (or key) of a parent is always greater than its children.

CHAPTER 3

GRAPH THEORETIC ANALYSIS OF NETWORKS

"Graphs stand or fall by their choice of nodes and edges."

– Watts & Strogatz

This chapter is entirely based on [2], a joint work with Meghana Ayyala Somayajula, Karol Horodecki, and Siddhartha Das.

The quantum Internet [40–42] is an interconnected network of users enabled to perform desired quantum information processing [101,102] and computing tasks [103,104] among them. As the quantum Internet grows in scale spanning vast distances, ensuring its robustness against disruptions becomes important.

Random failures of nodes and communication links, whether due to physical imperfections or adversarial attacks [59], can severely hinder the network's performance, potentially isolating certain regions or even rendering it inoperable. This motivates analyzing the resilience of networks to failures, identifying critical components of the network and observing limitations on performing different tasks over the network.

Motivated by the power of abstraction of graph theory [99, 105, 106], we employ graph-theoretic quantifiers to evaluate network robustness and identify nodes that are crucial to its overall functioning. We present a graph-theoretic framework for quantum networks, presenting a theorem that outlines conditions for which there is no percolation [107–109] for a class of tasks performed over lattice networks (sufficiently large graphs). Additionally, we present algorithms for implementing different network tasks.

3.1 Graph theoretic framework of networks

Let us consider networks represented as graph $G(\mathbb{V}, \mathbb{E})$ classified as weighted and undirected. A graph is a mathematical structure that is used to define pairwise relations between objects called nodes. The set of nodes, also called vertices is denoted by $\mathbb{V}$ and $\mathbb{E}$ denotes the set of edges which are pairs of nodes of the graph that connect the vertices. We denote $|\mathbb{V}|$ as N_v and $|\mathbb{E}|$ as N_e, where $|\mathbb{X}|$ denotes the size of the set $\mathbb{X}$. The vertices of the graph G are denoted as $v_i \in \mathbb{V}$ and the edges connecting the nodes $\{v_i, v_j\} \in \mathbb{V}$ as $e_{ij} \in \mathbb{E}$. We denote the path connecting two distant nodes v_i and v_k as $\mathcal{P}(v_i, v_k)$ having length $len(\mathcal{P})$. The shortest shortest network path between v_i and v_k is denoted as $dist(v_i, v_k)$. The shortest path length between the most distant nodes of a graph is called the diameter of the graph. A value $w_{ij} \in \mathbb{R}$ assigned to an edge e_{ij} of the graph is called the edge weight. The graph G together with w_{ij} is called a weighted graph. A graph

where the edges do not have a direction is called an undirected graph. The edges of an undirected graph indicate a bidirectional relationship where each edge can be traversed from both directions.

In general, the nodes, edges, and edge weights of a network can change with time (see Appendix A.7 for details). In this work, we will deal with undirected, weighted graphs depicting networks for communication tasks among multiple users. The edges in the graph are representative of links in the corresponding network, where links between nodes are formed due to quantum channels (or gates) over which resources are being transmitted between connected nodes. We denote labelled graphs as $G(\mathbb{V}, \mathbb{E}, \mathbb{L})$ where $\mathbb{L}$ denotes the set of labels associated with the vertices and edges of the graph.

We denote the nodes of the graph that are present between the end nodes when traversing along a path from one end node to another as the virtual nodes associated with the path. While analysing the network for different tasks, it may be possible that all the virtual nodes of the network are secure and cooperate in the execution of the task. We call this the cooperating strategy. It may also be possible that some virtual nodes of the network may be compromised and are not available for the task. We call this the non-cooperating strategy. We next define the weights for the edges of a network performing different tasks.

Definition 13. *Let a network depicted by an undirected, weighted graph $G(\mathbb{V}, \mathbb{E})$, where $v_i \in \mathbb{V}$ for $i \in [N_v]$, be given by $\mathcal{N}(G(\mathbb{V}, \mathbb{E}))$. The success probability of transmitting a desirable resource χ between any two different nodes v_i, v_j (i.e., when $i \neq j$) connected with edge e_{ij} is given by p_{ij}; we assume $p_{ii} = 1$ for an edge e_{ii} connecting a node v_i with itself. The weight $\mathrm{w}(e_{ij})$ for each edge e_{ij} is given by $-\log p_{ij}$. We define an effective weight $\mathrm{w}_*(e_{ij})$ of an edge e_{ij} over which the resource χ is transmitted between v_i to v_j for a particular information processing task (*Task_**) as, for all $i, j \in [N_v]$*

$$\mathrm{w}_*(e_{ij}) := \begin{cases} -\log p_{ij} & \text{if } p_{ij} \geq p_*, \\ \infty & \text{otherwise}, \end{cases} \tag{3.1}$$

where p_* is the critical probability below which the desired information processing task Task_* fails. Since $G(\mathbb{V}, \mathbb{E})$ is undirected, we have $p_{ij} = p_{ji}$, $\mathrm{w}(e_{ij}) = \mathrm{w}(e_{ji})$, $\mathrm{w}_*(e_{ij}) =$

$\mathrm{w}_*(e_{ji})$.

Observation 1. *The weight* $\mathrm{w}(e_{ij})$ *for an edge is path-dependent and additive across connecting edges. If a resource* χ *is being transmitted between nodes* v_i *and* v_l *by traversing the virtual nodes* v_j *and* v_k *in an order* $v_i \to v_j \to v_k \to v_l$*, i.e., through a connecting path* $e_{ij} \to e_{jk} \to e_{kl}$*, then the weight* $\mathrm{w}(e_{i\to j\to k\to l}) = \mathrm{w}(e_{ij}) + \mathrm{w}(e_{jk}) + \mathrm{w}(e_{kl}) = -\log p_{ij}p_{jk}p_{kl}$*. The effective weight* $\mathrm{w}_*(e_{ij})$ *is also path-dependent. The effective weight* $\mathrm{w}_*(e_{i\to j\to k\to l}) = \mathrm{w}_*(e_{ij}) + \mathrm{w}_*(e_{jk}) + \mathrm{w}_*(e_{kl}) = -\log p_{ij}p_{jk}p_{kl}$ *if* $p_{ij}p_{jk}p_{kl} \geq p_*$*, else* $\mathrm{w}_*(e_{i\to j\to k\to l}) = \infty$*. If any of the* p_{ij}, p_{jk}, p_{kl} *is strictly less than* p_* *then* $p_{ij}p_{jk}p_{kl} < p_*$*. To maximize the success probability of transmitting the resource* χ *between any two nodes of the network, it is desirable to select the path between these two nodes that has the minimum weight.*

The critical success probability for performing Task_* over a network limits its diameter. This motivates the following definition of critically large networks for Task_*.

Definition 14 (Critically large network)**.** *We define a network* $\mathcal{N}_{crit}(G(\mathbb{V}, \mathbb{E}))$ *as critically large network for* Task_* *if*

$$\forall_{e_{ij}\in\mathbb{E}} \;\; p_{ij} \leq c, \;\; \textit{where } c \in (0, 1), \tag{3.2}$$

and it contains at least two vertices $x_0, y_0 \in \mathbb{V}$ *which are at distance*

$$dist(x_0, y_0) \geq \left\lceil \frac{\log p_*}{\log c} \right\rceil + 1, \tag{3.3}$$

where p_* *is the critical probability for successful transmission of resource* χ *(Definition 13).*

In the following proposition we show that there are at least two vertices in critically large network that cannot perform Task_* over all paths of length larger or equal to the distance between the vertices.

Proposition 1. *Assume that it is possible to perform* Task_* *between any two distinct nodes* v_i, v_j *of the network* $\mathcal{N}_{crit}(G(\mathbb{V}, \mathbb{E}))$ *if and only if nodes* v_i, v_j *can share resource* χ *over the*

network path $\mathcal{P}(v_i, v_j)$ *having success probability* $s(\mathcal{P}(v_i, v_j)) \geq p_* > 0$. *Then*

$$\exists_{n_0 \in \mathbb{N}} \, \forall_{\{v_i, v_j\} \in \mathbb{V}} \quad \Big[dist(v_i, v_j) \geq n_0 \Rightarrow \forall_{\mathcal{P}(v_i, v_j)} \; s(\mathcal{P}(v_i, v_j)) < p_* \Big]. \tag{3.4}$$

In other words, there will be at least two vertices in this network, that cannot share resource χ *by* Task_*.

Proof. We begin with an observation that the success probability of sharing a resource between vertices $\{v_i, v_j\}$ along the path $\mathcal{P}(v_i, v_j)$ is given by $s(\mathcal{P}(v_i, v_j)) := p_{ik}...p_{mj}$. The vertices v_i and v_j cannot share a resource along the path $\mathcal{P}(v_i, v_j)$ if $s(\mathcal{P}(v_i, v_j)) < p_*$.

Let us choose n_0 such that $c^{n_0} < p_*$. Consider now any two vertices v_i and v_j be such that $dist(v_i, v_j) > n_0$ (the set of such vertices is non-empty since $dist(x_0, y_0) > n_0$ by assumption in Eq. (3.3)). Then any path $\mathcal{P}(v_i, v_j)$ has length $l \geq dist(v_i, v_j)$. The success probability of sharing resource along the path $\mathcal{P}(v_i, v_j)$ is given by $s(\mathcal{P}(v_i, v_j)) = p_{ik}p_{kl}...p_{mj} \leq (\max\{p_{ik}, p_{kl}, ..., p_{mj}\})^l \leq c^l \leq c^{n_0} < p_*$. Thus for any $\{v_i, v_j\}$ at distance $\geq n_0$, there does not exist a path $\mathcal{P}(v_i, v_j)$ with $s(\mathcal{P}(v_i, v_j)) \geq p_*$. □

Consider a d-dimensional lattice $G_{lat}(\mathbb{V}, \mathbb{E})$ having $|\mathbb{V}| \to \infty$. The vertex set $\mathbb{V}$ is defined as the set of elements of $\mathbb{R}^d$ with integer coordinates. Let us denote $G_{sg}(\mathbb{V}_{sg}, \mathbb{E}_{sg})$ as a finite subgraph of $G(\mathbb{V}, \mathbb{E})$ from which the entire graph can be constructed by repetition and

$$\exists_{N_{sg} \ll |V|} : \forall_{v_j \in \mathbb{V}_{sg}} \text{degree}(v_j) \leq N_{sg}. \tag{3.5}$$

A percolation configuration $\omega_p = (\omega_{ij} : e_{ij} \in \mathbb{E})$ on the graph $G(\mathbb{V}, \mathbb{E})$ is an element of $\{0, 1\}^{|\mathbb{E}|}$. If $\omega_{ij} = 1$, the edge is called open, else closed. If a node $v_i \in \mathbb{V}$ fails, all the edges $e_{ij} \in \mathbb{E}$ connected to v_i will be disconnected and for such edges $\omega_{ij} = 0$. A configuration ω_p is a subgraph of $G(\mathbb{V}, \mathbb{E})$ with vertex set $\mathbb{V}$ and edge-set $\mathbb{E}_p := \{e_{ij} \in \mathbb{E} : \omega_{ij} = 1\}$ (cf. [107]). For performing Task_* over lattice network, we next present a theorem that describes conditions for which there is no percolation in a lattice network.

Theorem 1. *Let us consider performing* Task_* *(Definition 13) over the lattice* $G_{lat}(\mathbb{V}, \mathbb{E})$ *where each edge is open with probability* p_{ij} *and* $0 < p_* \leq p_{ij} < 1$. *Then the network arising among nodes from this task does not form a percolation configuration, i.e., a connected component of length* N_c *such that* $N_c/|\mathbb{V}| > 0$.

The above theorem follows from the facts that there are periodic repetitions of the finite subgraph $G_{sg}(\mathbb{V}_{sg}, \mathbb{E}_{sg})$ in $G_{lat}(\mathbb{V}, \mathbb{E})$ and there exists at least two subgraphs whose distance is greater than critical threshold for inter-subgraph nodes to remain connected for Task_* with some desirable probability (see Proposition 1). See also [108, Page 20] for discussion on 1-dimensional lattice and condition for percolation [110] to exist. Theorem 1 implies limitations on the scalability of quantum communication (see Observation 2) and DI-QKD (see Example 4) over networks.

Let us next define the adjacency matrix and the effective success matrix of a network in terms of the success probability of transmitting a desirable resource χ between two nodes of the network.

Definition 15. *Consider a network* $\mathcal{N}(G(\mathbb{V}, \mathbb{E}))$ *with* $|\mathbb{V}| = N_v$ *and* $\text{w}(e_{ij})_{i,j}$. *The adjacency matrix* $\mathbf{A}$ *of the network is a* $N_v \times N_v$ *matrix such that for all* $i, j \in [N_v]$ *we have*

$$[\mathbf{A}]_{ij} = \text{w}(e_{ij}), \tag{3.6}$$

and the effective adjacency matrix $\mathbf{A}_*$ *of the network is given by*

$$[\mathbf{A}_*]_{ij} = \text{w}_*(e_{ij}). \tag{3.7}$$

The effective success matrix of any network $\mathcal{N}(G(\mathbb{V}, \mathbb{E}))$ *for the transmission of a desirable resource* χ *(associated with* Task_**) between its nodes is an* $N_v \times N_v$ *matrix* $\mho_*$ *such that for all* $i, j \in [N_v]$ *we have*

$$[\mho_*]_{ij} := \begin{cases} p_{ij}^{\max} & \text{if } p_{ij}^{\max} \geq p_* \text{ for } i \neq j, \\ 0 & \text{otherwise}, \end{cases} \tag{3.8}$$

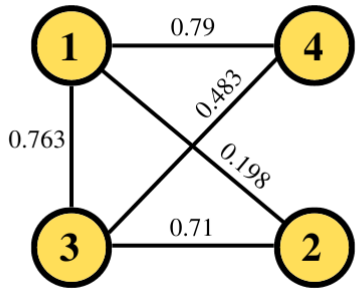


Figure 3.1: A partially connected mesh network with 4 nodes. In this network, the edge weights denote the success probability of transmitting χ between the end nodes for performing Task$_*$. It is preferable to use a cooperative strategy $v_1 \rightarrow v_3 \rightarrow v_2$ over a non-cooperative strategy $v_1 \rightarrow v_2$ as it has a higher success probability.

where $p_{ij}^{\max}$ is the maximum success probability of transmitting the desirable resource χ between nodes v_i and v_j over all possible paths between the two nodes.

The elements $[\mho_*]_{ij}$ of the success matrix provide the highest probability with which χ can be shared between the nodes v_i and v_j thus corresponds to the path having minimum cumulative effective weight. Let us consider a graph of diameter 2 as shown in Fig. 3.1. The success probability of transmitting χ between v_1 and v_2 via non-cooperative strategy over the edge e_{12} is 0.198 while that via cooperative strategy over the path $e_{1\rightarrow3\rightarrow2}$ is 0.5417. We thus observe that the success probability of transferring χ between nodes v_1 and v_2 via a non-cooperating strategy leads to a lower success probability $p_{1\rightarrow2}$ as compared to that via a cooperative strategy $p_{1\rightarrow3\rightarrow2}$.

Note 1. *Henceforth, we will be dealing with communication over networks where the success probability of transmitting resources from a node a to node c via node b is less than or equal to the multiplication of the success probability of resource transmission from a to b and b to c.*

In analysing networks represented as graphs, it is important to analyze the robustness of the network for different information-processing tasks. In recent works, the robustness

has been studied in the context of removal of network nodes [111] and has been modelled as a percolation process on networks [4, 112, 113] represented as graphs. In these studies, the vertices are considered present if the nodes connecting them are functioning normally. In the following section, taking motivations from degree centrality [114], betweenness centrality [115] and Gini index [116] of network graphs, we present figures of merit to compare the robustness of network topologies. We then compare different network topologies based on these measures.

3.2 Robustness measure for networks

Networks that have a large number of edges are more tolerant to non-functioning nodes and edges as compared to those with fewer edges. Taking motivation from the degree centrality of a graph [114], we define the link sparsity of a network to assess the performance of a network.

Definition 16. *Consider a network $\mathcal{N}(G(\mathbb{V},\mathbb{E}))$ having the effective success matrix as $\mathfrak{V}_*$. Let the total number of entries and the number of non-zero entries in $\mathfrak{V}_*$ be m and m_* respectively. The link sparsity of such a network is given by*

$$\Upsilon(\mathcal{N}) = 1 - \frac{m_*}{m}. \tag{3.9}$$

Typically it is desirable for the network to have low values of link sparsity. The networks represented as graphs can exist in different topologies and have the same number of nodes, edges and also the same weighted edge connectivity. These networks are said to be isomorphic to one another.

Definition 17. *(Graph isomorphism [99]) The graphs $G(\mathbb{V},\mathbb{E},\mathbb{L})$ and $G'(\mathbb{V}',\mathbb{E}',\mathbb{L}')$ are isomorphic iff there exists a bijective function $f : \mathbb{V} \to \mathbb{V}'$ such that:*

1. $\forall u \in \mathbb{V}, l \in \mathbb{L}, l' \in \mathbb{L}',\ l(u) = l'(f(u))$
2. $\forall u, v \in \mathbb{V},\ (u,v) \in \mathbb{E} \leftrightarrow (f(u), f(v)) \in \mathbb{E}'$

3. $\forall (u,v) \in \mathbb{E}, l \in \mathbb{L}, l' \in \mathbb{L}',\ l(u,v) = l'(f(u), f(v))$

It follows from Eq. (3.9) that isomorphic networks have the same value of link sparsity. Networks having the same value of link sparsity can differ in the distribution of edge weights. Taking motivation from the betweenness centrality of a graph [115], we define the connection strength of the nodes in the network and the total connection strength of the network.

Definition 18. *Consider a network $\mathcal{N}(G(\mathbb{V},\mathbb{E}))$ with $|\mathbb{V}| = N_v$ having the adjacency matrix and the effective success matrix as $\mathbf{A}_*$ and $\mho_*$. The connection strength of a node v_i in the network $\mathcal{N}$ is given by*

$$\zeta_i(\mathcal{N}) := \begin{cases} \left(\sum_{\substack{j \\ j\neq i}} 2^{-[\mathbf{A}_*]_{ij}}\right)/N_v & \textit{non-cooperative}, \\ \left(\sum_{\substack{j \\ j\neq i}} [\mho_*]_{ij}\right)/N_v & \textit{cooperative}. \end{cases} \tag{3.10}$$

The total connection strength of the network $\mathcal{N}$ in the (non-)cooperative strategy is obtained by adding the connection strengths of the individual nodes and is given by

$$\Gamma(\mathcal{N}) = \sum_j \zeta_j(\mathcal{N}). \tag{3.11}$$

In the following subsection, we compare the robustness measures for different network topologies.

3.2.1 Comparison of the robustness of network topologies

The topology of a network is defined as the arrangement of nodes and edges in the network. The information processing task that the network is performing decides the topology of the network. Two of the most commonly used network topologies are the star and mesh topologies.

A star network topology [117] of n nodes is a level 1 tree with 1 root node and $n-1$ leaf nodes. A star network with 8 nodes is shown in Fig. 3.2. The root node labelled 1 is the

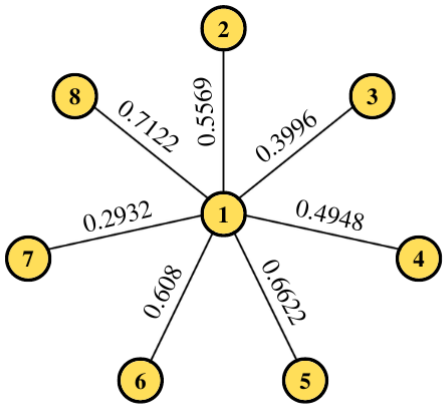
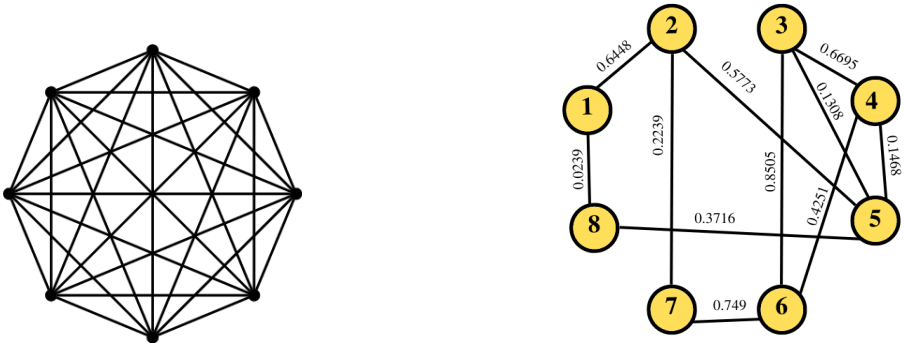


Figure 3.2: In this figure, we present a star network with 8 nodes. The node v_1 is the hub and nodes v_2 to v_8 are the outer nodes. The functioning of the hub node is critical to the functioning of the network.

hub node and acts as a junction connecting the different leaf nodes labelled 2 to 8. Among all network topologies, this network typically requires the minimum number of hops for connecting two nodes that do not share an edge between them. The working of the hub is most critical to the functioning of the star network. The failure of a leaf node or an edge connecting a leaf node to the root does not affect the rest of the network. As an example of its use, this type of network finds application as a router or a switch connecting a ground station to different locations in an entanglement distribution protocol. In such a protocol, an adversary can attack the root node to prevent the proper functioning of the network. If the root node fails to operate, all leaf nodes connected to it become disconnected.

In a mesh network topology [118], each node in the network shares an edge with one or more nodes, as can be seen from Fig. 3.3a and 3.3b. There are two types of mesh topologies depending on the number of edges connected to each node. A mesh is called fully connected if each node shares an edge with every other node of the network, as shown in Fig. 3.3a. A mesh is called partially connected if it is not fully connected, as shown in Fig. 3.3b. A mesh where each node shares an edge with only one other node of the network is called a linear network.

In a partially or fully connected mesh, the presence of multiple paths between two nodes



(a) Fully connected mesh with 8 nodes (b) A partially connected mesh with 8 nodes.

Figure 3.3: In this figure, we present (a) fully connected and (b) partially connected mesh networks with 8 nodes. In a fully connected mesh network, there are edges between every pair of nodes. The presence of multiple paths between two nodes of the mesh network makes it more robust as compared to a star network with the same number of nodes.

of the network makes it robust. As an example of its use, a mesh network can be used for a satellite-based entanglement distribution, which we discuss in detail in a later section.

Let us consider a mesh network $\mathcal{N}_m(G_m(\mathbb{V},\mathbb{E}))$ of diameter d with $|\mathbb{V}| = N_v$ and for $(v_i, v_j) \in \mathbb{E}$, $p_{ij} = p$. Let there be a non-cooperating strategy for sharing resources between the nodes of the network. For such a strategy, the rows of the adjacency matrix of the network have N_z number of zero entries where $0 \leq N_z \leq N_v - 1$. Next, let there also exist a cooperating strategy for sharing resources between the nodes of this network. For such a strategy, the node v_i of the network does not share an edge with N_z' number of nodes where $0 \leq N_z' \leq N_z \leq N_v - 1$. From the remaining nodes, there exists edges between v_i and $(N_v - N_z' - 1)/d$ number of nodes with $p_{ij} = p^j$ where $1 \leq j \leq d$. For such a network, we have the link sparsity as

$$\Upsilon(\mathcal{N}_m) := \begin{cases} (N_z + 1)/N_v & \text{non-cooperating,} \\ (N_z' + 1)/N_v & \text{cooperating.} \end{cases} \tag{3.12}$$

The connection strength of the node v_i is given by

$$\zeta_i(\mathcal{N}_m) := \begin{cases} [1 + p(N_v - N_z)]/N_v & \text{non-cooperating,} \\ [1 + \frac{p(p^d-1)(N_v-N_z'-1)}{d(p-1)}]/N_v & \text{cooperating.} \end{cases} \tag{3.13}$$

The total connection strength of the network is given by $\Gamma(\mathcal{N}_m) = N_v \times \zeta_i(\mathcal{N}_m)$. It can be seen that for this network the sparsity index $\Xi(\mathcal{N}_m)$ (see Eq. (A.7)) is the same as the connection strength of the node. This follows from the equal distribution of the weights in the network.

Next consider a star network $\mathcal{N}_s(G_s(\mathbb{V}, \mathbb{E}))$ with $|\mathbb{V}| = N_v$ and for $(v_i, v_j) \in \mathbb{E}$ we have

$$p_{ij} \coloneqq \begin{cases} p & \text{if } i = 1 \text{ and } p \geq p_*, \\ 0 & \text{otherwise.} \end{cases} \tag{3.14}$$

The link sparsity of such a network is $\Upsilon(\mathcal{N}_s) = 1 - (1/N_v)$ for the cooperative strategy and $\Upsilon(\mathcal{N}_s) = 1 - [(3N_v - 2)/N_v^2]$ for the non-cooperative strategy. The connection strength of the root node is $\zeta_i(\mathcal{N}_s) = (1 + p(N_v - 1))/N_v$, while for the leaf nodes is

$$\zeta_i(\mathcal{N}_s) \coloneqq \begin{cases} (1 + p)/N_v & \text{non-cooperative,} \\ [1 + p + p^2(N_v - 2)]/N_v & \text{cooperative.} \end{cases} \tag{3.15}$$

The sparsity index (see Eq. (A.7)) of the network is

$$\Xi(\mathcal{N}_s) \coloneqq \begin{cases} [N_v^2 + p(N_v^2 & \\ \qquad +N_V - 2)]/N_v^3 & \text{non-cooperative,} \\ [N_v^2 + p(N_v - 1)(N_v + 2) & \\ \quad +p^2(N_v - 2)(N_v - 1) & \\ \qquad (N_v + 1)]/N_v^3 & \text{cooperative.} \end{cases} \tag{3.16}$$

As another example, consider a network $\mathcal{N}(G(\mathbb{V}, \mathbb{E}))$ having $|V| = N_v$ number of nodes, and each node shares an edge with d other nodes. The effective adjacency matrix $\mathbf{A}_*$ of such a network is a circulant matrix. Let the success probability of transferring a resource

between the node 1 and the node n be given by,

$$p_{1n} \coloneqq \begin{cases} p^n & \text{if } n \leq d/2 \text{ and d = even,} \\ p^{d-n+1} & \text{if } n > d/2 \text{ and d = even,} \\ p^n & \text{if } n \leq (d+1)/2 \text{ and d = odd,} \\ p^{d-n+1} & \text{if } n > (d+1)/2 \text{ and d = odd.} \end{cases} \tag{3.17}$$

The first row of the adjacency matrix is formed by calculating the weights $w_*(e_{1n}) = -\log p_{1n}$. The k^{th} row is formed by taking the cyclic permutation of the first row with an offset equal to k. In the non-cooperative strategy, the link sparsity of the network is then given by

$$\Upsilon(\mathcal{N}) = 1 - \left(\frac{d+1}{N_v}\right), \tag{3.18}$$

and the connection strength of the node v_i is given by

$$\zeta_i(\mathcal{N}) \coloneqq \begin{cases} \frac{(1+p)(p^{(d+1)/2}-1)}{N_v(p-1)} & \text{if } d \text{ is odd,} \\ \frac{1}{N_v}\left[1 + \frac{2p(p^{d/2}-1)}{(p-1)}\right] & \text{if } d \text{ is even.} \end{cases} \tag{3.19}$$

In the following subsection, we introduce measures for identifying the critical nodes of a given network.

3.2.2 Critical nodes in a network

The critical nodes of a network are the nodes that are vital for the proper functioning of the network. Removing any of these nodes can lead to some of the other nodes in the network being disconnected. Given a network $\mathcal{N}(G)$, we proceed to define a measure for the criticality of the nodes in G. For this, at first, taking motivation from [119], we define the clustering coefficient for the nodes of a given network.

Definition 19. *For a network $\mathcal{N}(G)$, let $G_i(\mathbb{V}_i, \mathbb{E}_i)$ be a sub-graph of G formed by the neighbours of node $v_i \in \mathbb{V}$. Let $n_i = |\mathbb{V}_i|$ be the number of nodes present in G_i and $e_i = |\mathbb{E}_i|$ be the number of edges present in G_i with $p_{ij} \geq p_*$. The clustering coefficient of the node*

v_i is defined as

$$C_i = \frac{2\, e_i}{n_i(n_i - 1)}. \tag{3.20}$$

The average clustering coefficient of a network is calculated by taking the average of C_i for all the nodes of the network. We next proceed to define the average effective weight of a network using Eq. (3.1).

Definition 20. *For a network $\mathcal{N}(G)$, the average effective weight of a network denoted by $\widetilde{\mathrm{w}}_*$ is defined as the mean of the effective weight between all the node pairs in the network and is expressed as*

$$\widetilde{\mathrm{w}}_*(G) = \frac{1}{n(n-1)} \sum_{\substack{v_i, v_j \in \mathbb{V} \\ i \neq j}} \mathrm{w}_*(e_{i \to \ldots \to j}), \tag{3.21}$$

where $\mathrm{w}_*(e_{i \to \ldots \to j})$ is the effective weight associated with the path connecting the nodes v_i and v_j.

When two nodes (v_i, v_j) are disconnected, the effective weight $\mathrm{w}_*(e_{i \to \ldots \to j})$ becomes infinite. Small values of $\widetilde{\mathrm{w}}_*(G)$ indicate that the network performs the task with high efficiency.

Taking motivation from [115], we define centrality for the nodes of a given network. Then, using definitions of centrality, average effective weight and clustering coefficient, we define the critical parameter for the nodes of a given network.

Definition 21. *For a network $\mathcal{N}(G)$, let us denote the shortest path connecting the node pairs $(v_i, v_j) \in G$ as $d_{ij} \in \mathbb{D}$. We define the centrality τ_i of the node v_i as the number of paths belonging to the set $\mathbb{D}$ in which the node v_i appears as a virtual node. The critical parameter associated with the node v_i is defined as*

$$\nu_i = \frac{\tau_i}{C_i \widetilde{w}_*(G_i)}. \tag{3.22}$$

The critical nodes of a graph have high values of ν. These nodes of the network are essential for the proper functioning of the network. If one of these nodes is removed, it

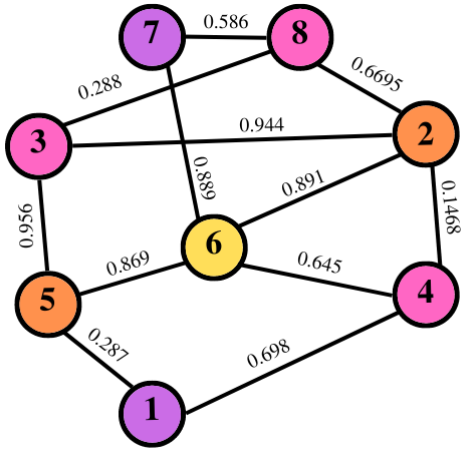


Figure 3.4: A network represented by a weighted graph with 8 nodes and 12 edges. Node v_6 (shown in yellow) is the most critical node followed by nodes v_2 and v_5 (shown in orange). These nodes are the most critical for the proper functioning of the network.

will lead to a decrease in the overall efficiency of the network. We present a heuristic algorithm in Sec. 3.4.3 to obtain the critical parameter ν_i for the node $v_i \in \mathbb{V}$ of the network $\mathcal{N}(G(\mathbb{V}, \mathbb{E}))$.

Example 1. *Let us obtain the critical nodes of the graph with* 8 *nodes shown in Fig. 3.4. We present the critical parameter for the different nodes of the network in the table below.*

node number (i)	ν_i	node number (i)	ν_i
v_1	0.1714	v_5	1.5238
v_2	1.6667	v_6	2.5714
v_3	0.7619	v_7	0.1714
v_4	0.9523	v_8	0.5714

We observe that node v_6 is the most critical followed by node v_2 and node v_5. We label these nodes as the critical nodes of the network.

The following section compares the robustness of different currently available quantum processor networks.

Name	Layout	Fidelity	Qubits	T_1
Sycamore (Google) [39]	square lattice	96.9% (RO) 99.85% (1Q) 99.64% (2Q)	54	15 μs
Eagle (IBM) [37, 120]	heavy hexagonal	99.96% (RO) 99.99% (1Q) 99.94% (2Q)	127	95.57 μs
Aspen-M-2 (Rigetti) [38]	octagonal	97.7% (RO) 99.8% (1Q) 90% (2Q)	80	30.9 μs

Table 3.1: The performance details of different quantum processors. In the above table, the second column provides the arrangement of the qubits in the processor. The third column provides the 1 qubit (1Q), 2 qubits (2Q), and the readout (RO) fidelity of the processors. The fourth column provides the total number of qubits in the processor, and the fifth column provides the thermal relaxation time (T_1) of the qubits of the processor.

3.3 Robustness of Quantum Processors

The currently available quantum processors (QPUs) use different technologies to implement the physical processor. The processors of IonQ and Honeywell utilize a trapped ion-based architecture, while IBM, Rigetti, and Google have a superconducting architecture. The superconducting architecture requires physical links between qubits that are to be entangled, while the trapped ion-based architecture does not have any topological constraint. In this section, we model the different quantum processor architectures as graphical networks (see Table 3.1) and present the robustness measures (defined in Sec. 3.2) for such networks.

We consider different qubit quantum processor network architectures in square, heavy-hexagonal and octagonal layouts. The link sparsities of each unit cell[1] for these different

[1]Unit cell is the smallest group of processor qubits which has the overall symmetry of the processor, and from which the entire processor can be constructed by repetition.

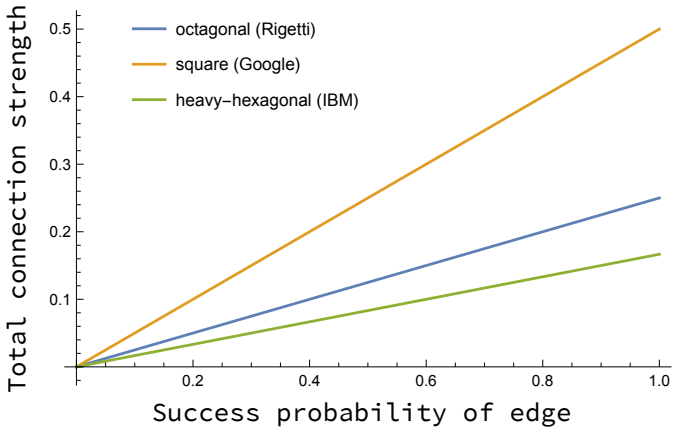


Figure 3.5: In this figure, we consider three processor designs by (a) Rigetti [38] (octagonal lattice), (b) Google [39] (square lattice), and (c) IBM [37, 120] (heavy-hexagonal lattice) as quantum networks and plot the connection strength of the nodes (see Eq. (3.10)) as a function of success probability of edge. It is assumed that the network have uniform distribution of edge success probability. (Color online)

network layouts are given by

$$\Upsilon(N) := \begin{cases} 1 - (\frac{16}{64}) \approx 0.75 & \text{octagonal,} \\ 1 - (\frac{8}{16}) \approx 0.5 & \text{square,} \\ 1 - (\frac{24}{144}) \approx 0.833 & \text{heavy hexagonal.} \end{cases} \tag{3.23}$$

We observe that the square structure has the lowest link sparsity, followed by octagonal and heavy hexagonal structures. Next, let the edges present in these network layouts have success probability p.

The connection strength of the i^{th} node in the unit cell of octagonal, heavy hexagonal and square network for a non-cooperative strategy is given by

$$\Gamma(\mathcal{N}) := \begin{cases} p/4 & \text{octagonal,} \\ p/2 & \text{square,} \\ p/6 & \text{heavy hexagonal.} \end{cases} \tag{3.24}$$

We plot in Fig. 3.5 the connection strength of the i^{th} node for different values of the success probability of edge. We observe that the connection strength for a given success

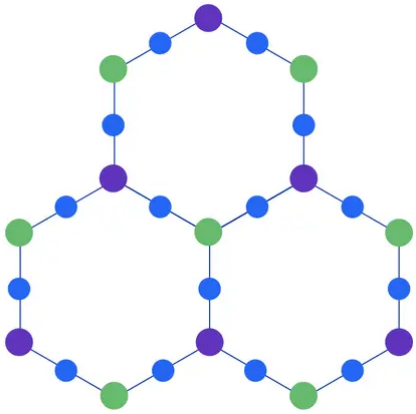


Figure 3.6: A slice of a quantum processor model based on heavy-hexagonal structure discussed in [121]. The link sparsity of the unit cells in the network is 0.833, and the critical nodes of the network slice are shown in green and violet.

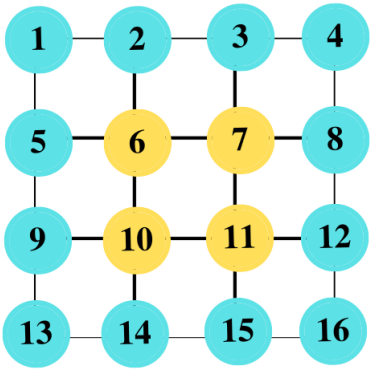


Figure 3.7: A 4×4 slice of a 1024 node quantum processor architecture based on square structure. The total network layout is represented as a 32×32 lattice. The link sparsity of the network is 0.9962, and the critical nodes of the network slice are shown in yellow.

probability of edge is highest for square networks, followed by octagonal and heavy-hexagonal networks.

We propose a 1024-node square lattice-based quantum processor network architecture represented as a 32×32 lattice. We show in Fig. 3.7 a 4×4 slice of the lattice as a representation of the entire quantum processor. The link sparsity of the 1024 node square network is 0.9962. The nodes shown in yellow in Fig. 3.7 are identified as critical nodes. We observe in Fig. 3.7 that there are three types of nodes in the network based on the number of edges that are connected to the node. We call a node a corner node, edge node, and inner node if it shares an edge with two, three, and four other nodes, respectively. The

connection strength of these three types of nodes is given by

$$\zeta_i(\mathcal{N}) := \begin{cases} p/256 & \text{inner node,} \\ 3p/1024 & \text{boundary node,} \\ p/512 & \text{corner node.} \end{cases} \tag{3.25}$$

In the following section, we present algorithms for implementing different network-related tasks.

3.4 Algorithms

In Sec. 3.4.1, we provide an algorithm to find the shortest path between a pair of end nodes. We then provide an algorithm in Sec. 3.4.2 to constrict a network architecture for sharing resources between two parties, each having multiple nodes. Then in Sec. 3.4.3, we provide an algorithm to obtain the critical parameter for the nodes of a given network. In Sec. 3.4.4, we provide an algorithm to optimize the flow of resources at a node having multiple input and output channels.

3.4.1 Shortest path between a pair of nodes

For performing Task$_*$ with maximum success probability, it is desirable to transmit resource χ between any two nodes via the shortest network path connecting them. Recent works have considered different network topologies [122–124] and limitations on current and near-term hardware [125–127] for routing resources over quantum networks. For a given network $\mathcal{N}$ represented as a graph G, we consider here the task of finding the path between two given nodes in G that have the lowest effective weight for routing resources between them [122]. We call a path connecting two nodes in the network and having the lowest effective weight as the shortest path between them. Finding the shortest path between two nodes of a network is important as longer paths are more vulnerable to node and edge failures. To find the shortest path between two nodes, we use Dijkstra's algo-

rithm [128, 129] suited to our network framework. In Algorithm 1, the shortest spanning tree is generated with the source node as the root node. Then the nodes in the tree are stored in one set and the other set stores the nodes that are not yet included in the tree. In every step of the algorithm, a node is obtained that is not included in the second set defined above and has a minimum distance from the source. To obtain the shortest path

Algorithm 1 Obtaining the shortest spanning tree with source node as root

```
1:  function SpanTree(G, S, target)
2:      Initialize:
        pq ← empty min priority queue
        dist ← ∅
        pred ← ∅
3:      for every node in G do
4:          if node = S then
5:              pq[node] ← 0
6:          else
7:              pq[node] ← infinite
8:      for every node and minDist in pq do
9:          dist[node] ← minDist
10:         if node = target then
11:             break
12:         for every neigh of node do
13:             if neigh ∈ pq then
14:                 score ← dist[node] + G[node, neigh][weight]
15:                 if score < pq[neigh] then
16:                     pq[neigh] ← score
17:                     pred[neigh] ← node
        return dist, pred
```

between any two nodes of a given graph, we apply Algorithm 2. Algorithm 2 returns a path only *iff* the weight associated with the network path between the source and target nodes is at most equal to the critical weight $w_{crit}(= -\log p_*)$, p_* being the critical success probability for $Task_*$.

Example 2. *Let us consider a weighted graph with* 8 *nodes as shown in Fig. 3.8. A physical interpretation can be to consider the transfer of quantum states from node* v_i *to node* v_j *via quantum channels denoted by the edges. The edge weight between the nodes* v_i *and* v_j *is given by* $-\log p_{ij}$ *where* p_{ij} *is the success probability of sharing the resource between these two nodes. The shortest path connecting the nodes would then provide the*

Algorithm 2 Obtaining the shortest network path between the source and target nodes in a graph for end nodes to perform Task_* by sharing χ.

Initialize:
    $source \leftarrow$ starting node
    target $\leftarrow$ target node
    flag $\leftarrow 0$
    $p_* \leftarrow$ success probability for $Task_*$
G $\leftarrow$ the given graph
[dist, pred] $\leftarrow$ DIJKSTRA(G, source, target)
end $\leftarrow$ target
path $\leftarrow$ [end]
while (end $\neq$ source) AND (flag $\leq -\log p_*$) **do**
    end = pred[end]
    now = path[end]
    path.append(end)
    next = path[end]
    flag $\leftarrow$ flag + weight(G.edge(next,now))
if path[end] = source **then**
    disp(path)
else
    disp(disconnected nodes)

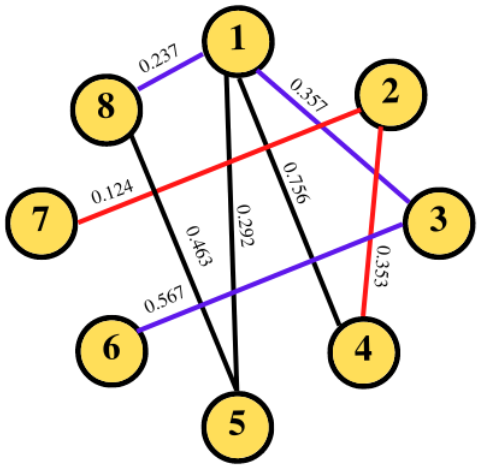


Figure 3.8: A network represented by a weighted graph with 8 nodes. Multiple pairs of nodes can share resources using this network. As an example, nodes $(8, 6)$ can share resource via the path $8 \leftrightarrow 1 \leftrightarrow 3 \leftrightarrow 6$ (shown in blue), then nodes $(7, 4)$ can share resource via the path $7 \leftrightarrow 2 \leftrightarrow 4$ (shown in red). (Color online)

highest success probability for the task. If we consider the source as node v_8 and the target as node v_6, then the algorithm returns the shortest path as $v_8 \leftrightarrow v_1 \leftrightarrow v_3 \leftrightarrow v_6$. It may be desirable for another node say v_7 to share a resource with node v_4 using the same network. The node v_7 and v_4 can share resources via the path $v_7 \leftrightarrow v_2 \leftrightarrow v_4$ without involving the virtual nodes in the shortest path between (v_8, v_6). We observe that multiple pairs of nodes can share resources using this network.

In the following subsection, we present an algorithm to construct a network for sharing resources between two parties each having multiple nodes.

3.4.2 Network Construction

Let two parties Alice (denoted by A) and Bob (denoted by B) require to share a resource using a mesh network. We assume that A and B have n_A and n_B number of nodes respectively. We introduce Algorithm 3 to obtain the structure of the mesh that ensures there exist distinct paths between nodes of A and B. In Algorithm 3, we impose the constraints that (a) at a time all nodes of A shall be connected to distinct nodes of B via the shortest available path with unique virtual nodes and (b) there exists a path between every nodes of A and B.

Algorithm 3 Network construction algorithm

```
1:  function NETWORK(n_A, n_B)
2:      Initialize:
        count ← n_A + n_B
        g ← complete graph (no. of nodes: count)
        g[weight] ← mesh edge weights
        wt ← local edge weights
3:      for every node v_i of A do
4:          add g.node(v_i)
5:          add g.edge(v_i, g[node=count], weight = wt[count])
6:          count ← count - 1
7:      for every node v_j of B do
8:          add g.node(v_j)
9:          add g.edge(v_i, g[node=count], weight = wt[count])
10:         count ← count - 1
        return g
```

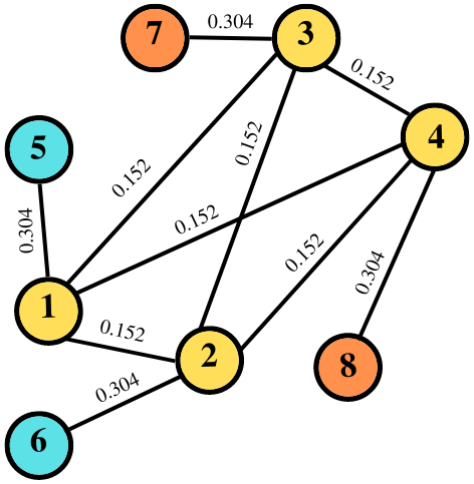


Figure 3.9: A 4 node network (shown in yellow) constructed using Algorithm 3 for connecting the hubs A and B. The hubs A and B each have two nodes and are shown in orange and blue respectively. (Color online)

Example 3. *Consider two geographically separated companies A and B requiring to connect to each other via a mesh network. We call the headquarters of the companies as hubs. In Fig. 3.9 we show the hubs of A and B in blue and orange respectively. Using Algorithm 3 we obtain the network topology for which there exists distinct paths for possible pairs of* (a_i, b_j) *where* $a_i \in A$ *and* $b_j \in B$.

3.4.3 Critical nodes in a network

The critical nodes of the network are essential for the proper functioning of the network. If one of these nodes is removed, it will lead to a decrease in the overall performance efficiency of the network. We present heuristic Algorithm 4 to obtain the critical parameter ν_i for the network node $v_i \in \mathbb{V}$ of the network $\mathcal{N}(G(\mathbb{V}, \mathbb{E}))$ using Eq. (3.22).

Algorithm 4 Finding the critical parameter ν_i for node $v_i \in \mathbb{V}$ of the network $\mathcal{N}(G(\mathbb{V}, \mathbb{E}))$

```
G ← the given graph
for every node in G do
    C_i ← clustering coeff using Eq. (3.20)
    w̄_*(G) ← avg cost using Eq. (3.21)
    τ_i ← centrality of the node
    ν_i ← τ_i / C_i w̄_*(G)
    critPar[node] ← ν_i
```

In the following subsection, we present an algorithm for optimizing resource flow at a node with multiple input and output channels.

3.4.4 Resource allocation at a node

The ground stations in the satellite-based network presented in Sec. 4.4 share an entanglement buffer [130] to store the incoming quantum states from the satellite network. The stored states are later distributed via different output channels to neighbouring nodes based on traffic requests. We present Algorithm 5 for the optimal flow of states at a node with multiple input (producer(thread)) and output channels (consumer(thread)). Algorithm 5 is the standard producer-consumer model in networking where the procedures CONSUMER threads[2] are the instances of the output channels that extract quantum states from the buffer, while the PRODUCER are the instances for the input channels that inputs quantum states to the buffer.

Algorithm 5 Resource allocation at a node

```
Initialize:
    buffSize ← size of quantum memory
    buffer ← ∅
procedure PRODUCER(thread)
    while state incoming AND empty memory slot do
        gain access to memory
        insert state into empty memory slot
        update other memory slots as per task
        release memory access
procedure CONSUMER(thread)
    while memory is not empty do
        gain access to memory
        acquire state from the memory
        update other memory slots as per task
        release memory access
create and start all producer threads
create and start all consumer threads
```

[2]Thread is a sequential execution of tasks in a process.

3.5 Discussion

In this chapter, we take a graph theoretic (and information-theoretic-) approach to analyse the robustness of the quantum Internet. We have provided measures for comparing the robustness and identifying the critical nodes of different network topologies.

Identifying quantum processors as real-world mesh networks, we compared the robustness measures for the quantum processor architectures by Google, IBM, and Rigetti. With the vision of having a 1024-qubit quantum processor in the future, we extend the 54-qubit layout by Google to include 1024 qubits and observe the robustness of such a network.

Considering performing some desirable information processing tasks over lattice networks, we present a theorem specifying conditions that lead to the absence of percolation. As implications of the theorem, we highlight the constraints on network scalability and limitations of current technology for performing quantum communication and implementing DI-QKD protocols in the next chapter.

Overall, the assessment presented in this chapter can be used to assess network robustness, identify the critical components of a network, and perform different underlying network tasks.

CHAPTER 4

LIMITATIONS ON QUANTUM NETWORKS

"Probable impossibilities are to be preferred to improbable possibilities."

-Aristotle

This chapter is entirely based on [2], a joint work with Meghana Ayyala Somayajula, Karol Horodecki, and Siddhartha Das.

In classical computing, there is a strong motivation to use delegated computation [14] in the form of cloud computing [131] as it is less resource extensive on the individual user. Now, given that there is no full clarity regarding the path along which quantum computing will develop, delegated quantum computing [132–134] is a vision ahead [135]. This vision has been supported by efforts to provide access to quantum processors [136] over the Internet. The recent developments in the field of secure and high-speed global communication networks only increase the scope for early adoption of delegated quantum computing.

A method for perfectly secure communication between a receiver and a sender requires sharing cryptographic keys between the parties [137]. The secret keys can be shared between the receiver and the sender using quantum key distribution (QKD) protocols. For these protocols, the transmission of quantum states from one party to another is an important step. However, the transmission of quantum states from a sender to a receiver via a lossy channel inevitably degrades the state being transmitted. The overlap of the shared state with the intended state typically decreases monotonically with the length of the channel. Unlike a classical signal, for quantum states this loss cannot be reduced using amplifiers since the measurement will disturb the system [138] and also quantum states cannot be cloned [139]. The degradation of the quantum states when transmitted over a quantum channel places limitations on the distance over which there can be secure communication [6]. This limitation may be overcome by using entanglement-based QKD protocols [28, 140] along with quantum repeaters [48, 141, 142].

For the implementation of a quantum network that enables delegated quantum computing and other information processing tasks, it is important to have a realistic assessment of limitations involved in performing primitive tasks such as secure communication, sharing of entanglement, and nonlocal correlations among the end nodes. This is the central theme of this chapter. In particular, we analyse the critical success probability of elementary links, critical length scales for various tasks, and scalability limitations for quantum communication networks.

4.1 Limitations on repeater networks

In this section, we present the critical success probability of the elementary links for implementing different information processing tasks. Extending to a linear repeater-based network, we present the critical time and length scales for implementing different information processing tasks.

4.1.1 Critical success probability for repeater networks

Consider a network $\mathcal{N}(G(\mathbb{V},\mathbb{E}))$ for performing a particular information processing task denoted by the symbol Task_*. As examples, we let the Task_* be sharing of entanglement, or implementing teleportation protocol between the nodes $\{v_i, v_j\} \in \mathbb{V}$. Let v_i, v_j share an isotropic state given by

$$\rho^I_{ij}(p,d) = p_{ij}\Psi^+_{ij} + (1-p_{ij})\frac{\mathbb{1}_{ij} - \Psi^+_{ij}}{d^2-1}, \tag{4.1}$$

via a qudit depolarising channel (cf. [6, 47]). Let performing Task_* require nodes v_i and v_j to share Ψ^+_{ij} with critical success probability p_*. We note that the state $\rho^I_{ij}(p,d)$ become separable for $p_{ij} < 1/d$, this implies a critical success probability $p^{\text{ent}}_* \geq 1/d$. The singlet fraction of $\rho^I_{ij}(p,d)$ is given by $f_{ij} = p_{ij}$. The maximum achievable teleportation fidelity of a bipartite $d \times d$ system in the standard teleportation scheme is given by $F = \frac{f_{ij}d+1}{d+1}$ [143]. The maximum fidelity achievable classically is given by $F_{cl} = \frac{2}{d+1}$ [143]. Thus the shared state between v_i and v_j is useful for quantum teleportation if $f_{ij} > 1/d$. The critical success probability p^{tel}_* for performing teleportation protocol over $\mathcal{N}(G(\mathbb{V},\mathbb{E}))$ is $p^{\text{tel}}_* > 1/d$.

4.1.2 Critical time and length scales for repeater networks

Consider an entanglement swapping-based repeater network. Let there be two sources S_1 and S_2 producing dual-rail encoded entangled pairs (for details see Appendix A.1) in the state Ψ^+ with probability η_s and with probability $1-\eta_s$ produces a vacuum state. The

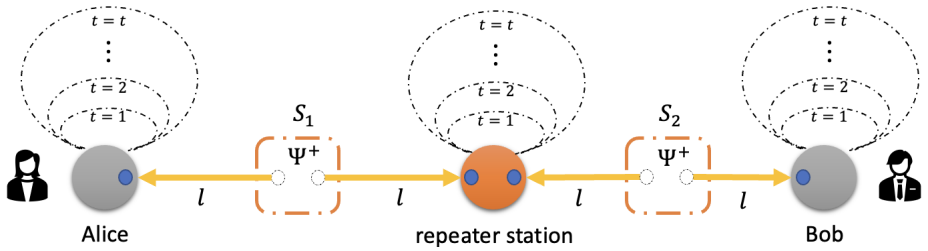


Figure 4.1: In this figure, we present an entanglement swapping-based repeater network. There are sources $S_1(S_2)$ producing state Ψ^+ and sending it to a repeater station and Alice (Bob) via optical fibers of length l (shown in yellow). The qubits are stored in quantum memories at the repeater station and the stations of Alice and Bob for t time steps (shown as self-loops). The repeater station performs standard Bell measurement on its share of qubits.

source S_1 sends one qubit from its entangled pair to Alice and the other to the repeater station via optical fibers of length l. Similarly, S_2 sends one qubit from its entangled pair to Bob and the other to the repeater station via optical fibers of length l (see Fig. 4.1). Let the qubits be stored in quantum memories at the repeater station and the stations of Alice and Bob for time t. We model the evolution of the qubits through the fiber and at the quantum memory as a qubit erasure channel (see Sec. A.4.2) with channel parameter $\eta_e = \mathrm{e}^{-(\alpha l+\beta t)}$, where α and β are respectively the properties of the fiber and the quantum memory. The repeater station performs a standard Bell measurement on its share of qubits with success probability q. After the repeater station has performed the standard Bell measurement, Alice and Bob share the state Ψ^+ with probability $q\,\eta_s^2\,\mathrm{e}^{-2(\alpha l+\beta t)}$ (cf. [6, Eq. (64)]). Let Alice and Bob require to perform Task_* (Definition 13) using their shared state. Furthermore, let performing Task_* require Alice and Bob to share Ψ^+ with critical success probability p_*. We then require

$$q\,\eta_s^2\,\mathrm{e}^{-2(\alpha l+\beta t)} > p_*. \tag{4.2}$$

We observe that Eq. (4.2) bounds the length of the optical fibers and the time till which the qubits can be stored in the quantum memories. This motivates the definition of the critical length of the fibers l_c and the critical storage time at the nodes t_c above which the shared state becomes useless for information processing tasks. These two critical parameters are

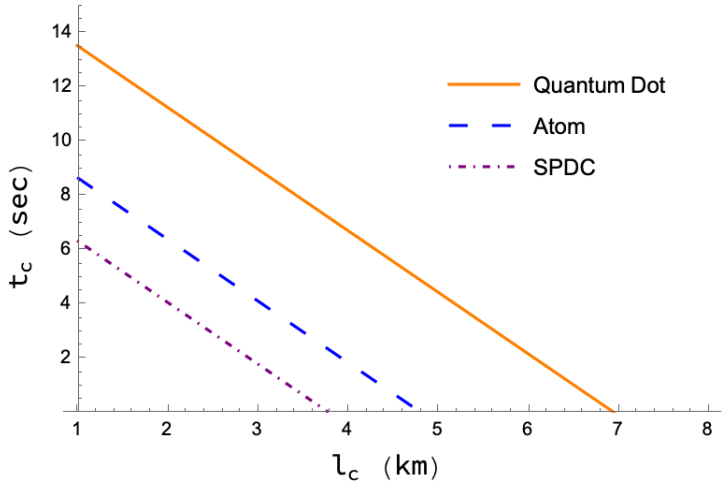


Figure 4.2: In this figure, we consider a repeater-based network and plot the critical storage time t_{cr} as a function of critical fiber length l_{cr} for different qubit architectures. The single photon architectures have efficiencies (a) $\eta_s = 0.97$ (Quantum Dots [144]) (b) $\eta_s = 0.88$ (Atoms [145]) and (c) $\eta_s = 0.84$ (SPDC [146]). We set $p_* = 0.5$, $q = 1$, $\alpha = 1/22$ km^{-1} and $\beta = 1/50$ sec^{-1}.

related via the expression

$$\alpha\, l_c + \beta\, t_c < \frac{1}{2} \ln\left(\frac{q\,\eta_s^2}{p_*}\right). \tag{4.3}$$

We plot in Fig. 4.2 the critical fibre length l_c and the critical storage time t_c for different qubit architectures and set $p_* = 0.5$ for some desired Task$_*$.

Let us introduce a finite number of repeater stations between the two end nodes, each performing standard Bell measurements on its share of qubits. The network is useful for Task$_*$ when

$$q^r\, \eta_s^{r+1}\, \mathrm{e}^{-2r(\alpha l+\beta t)} > p_*, \tag{4.4}$$

where r denotes the number of repeater stations between the end nodes. Let l_{cr} and t_{cr} denote the critical length of the fiber and the critical storage time of the quantum memory. These two critical parameters are then related via the expression

$$\alpha\, l_{cr} + \beta\, t_{cr} < \frac{1}{2r} \ln\left(\frac{q^r \eta_s^{r+1}}{p_*}\right). \tag{4.5}$$

We plot in Fig. 4.3 the critical fiber length l_{cr} and the critical storage time t_{cr} such that Eq. (4.5) holds for different values of r. The bounds on l_{cr} and t_{cr} for other values of r not

shown in Fig. 4.3 can be obtained from Eq. (4.5). We observe that for a given information processing task, increasing the number of repeater stations allows shorter fiber lengths and quantum memory storage times.

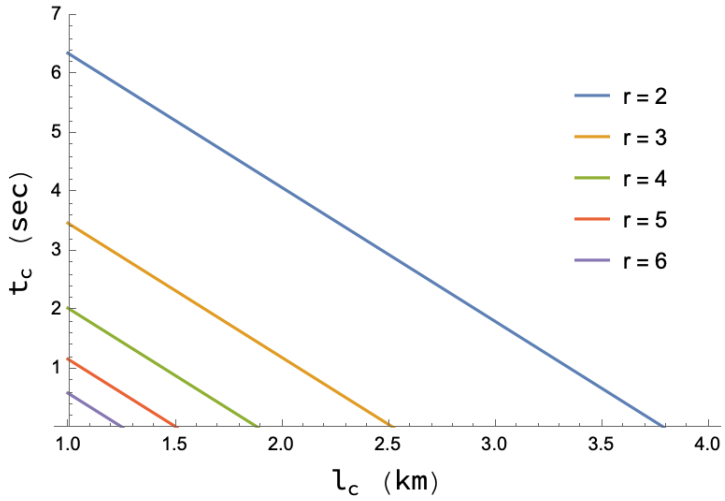


Figure 4.3: In this figure, we consider a repeater-based network and plot the critical storage time t_{cr} as a function of critical fiber length l_{cr} for the different numbers of repeater stations. We set $p_* = 0.5$, $\alpha = 1/22$ km^{-1}, $\beta = 1/50$ sec^{-1}, $q = 1$ and $\eta = 0.999$.

We note that the optimal rate of two-way assisted quantum communication or entanglement transmission (i.e., in an informal way, it is the maximum number of ebits per use of the channel in the asymptotic limit of the number of uses of the channel) over an erasure channel, also called LOCC (local operations and classical communication)-assisted quantum capacity of an erasure channel, is given by $\eta_e \log_2 d$ [147], where $1 - \eta_e$ is the erasing probability and d is the dimension of the input Hilbert space. Two-way assisted quantum and private capacities for erasure channel coincide [148, 149] (see [150] for strong-converse capacity). Two-way assisted private and quantum capacities for a qubit erasure channel is η_e [148, 149].

In the following section, we present limitations on the scalability of networks for quantum communication tasks assuming some hypothetical scheme can improve the transmittance of quantum channels connecting the nodes of the network.

4.2 Limitations on quantum network topologies

Let us consider an equilateral triangle-mesh network having the set of nodes as $\mathbb{V}$ (see Fig. 4.4(a) for $n = 3$). The nodes of the triangle network are connected by qubit erasure channels having transmittance $\eta = \mathrm{e}^{-(\alpha l+\beta t)}$, where l denotes the distance between the nodes and t is the time it takes for some resource χ to pass through the channel. In this section, we assume perfect measurements for the sake of simplicity. Consideration of imperfect measurements will only increase the critical probability p_* for the transmission of quantum resources over an edge between the nodes. This would imply that quantum network topologies and architecture with imperfect measurement devices will be more limited (constrained) than the network with perfect measurement devices.

Let us introduce a repeater scheme in the form of a star network (see Fig. 4.4(b) for $n = 3$) to effectively mitigate the losses due to transmission. The star network has virtual channels connecting the repeater node v_R to the node $v_i \in \mathbb{V}$. The transmittance of the virtual channels $\eta_R = \eta^{1/\sqrt{3}}$ is greater than η.

We now consider the transmittance of channels connecting pairs of nodes with a hypothetical scheme in a network that would lead to the following assumption.

Assumption 1. *Let us assume there exist repeater-based quantum communication or quantum key distribution schemes that can mitigate the loss due to transmittance of a quantum channel such that the rate of communication (ebits or private bits per channel use [6]) is effectively of the order*

$$\eta_R = \eta^{1/f} \tag{4.6}$$

in some regime (distance)[1]*, where η is the transmittance of the channel and for some $f \geq 1$ (cf. [32, 151–153]).*

To illustrate Assumption 1, let us consider a regular polygon network with n nodes having vertex set $\mathbb{V}$ and edge set $\mathbb{E}$ as shown in Fig. 4.4(a). For $e_{ij} \in \mathbb{E}$ the nodes $\{v_i, v_j\}$ are

[1] This need not be true for any length/distance in general and may hold only in certain distance regimes or sections.

connected by erasure channels having transmittance $\eta = e^{-\alpha l}$, where l is the distance between the nodes. Let us introduce a repeater scheme in the form of a star network as shown in Fig. 4.4(b) having the vertex set $\mathbb{V}_s := \mathbb{V} \cup \{v_R\}$ where v_R denotes the repeater node and the edge set is denoted by $\mathbb{E}_s$. For $e_{kR} \in \mathbb{E}_s$ the channel connecting nodes $\{v_k, v_R\} \in \mathbb{V}_s$ have transmittance $\eta_R = e^{-\alpha l/2\sin(\pi/n)}$, where $n = |\mathbb{V}|$. Comparing with Eq. (4.6) we observe that the star network provides an advantage of $f = 2\sin(\pi/n)$ over a repeater-less scheme for $n < 6$. For the triangle network discussed previously, we have $f = \sqrt{3}$. There may be other repeater-based schemes which uses entanglement distillation and error-correction techniques to further mitigate the transmission loss and enhance the rate of communication between end nodes.

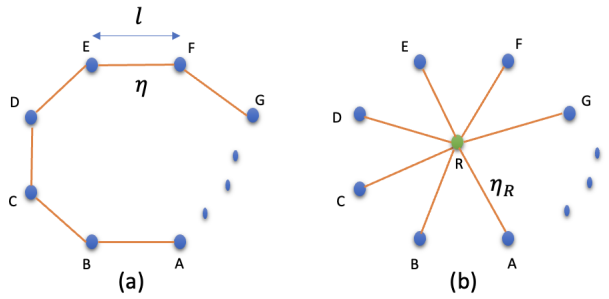


Figure 4.4: In this figure, we show (a) repeater-less regular polygon network with n nodes and (b) star-repeater network with n nodes.

In Eq. (4.6), the case of $f = 1$ has been shown in [6] for measurement-device-independent quantum key distribution (see [149, 150] for quantum key distribution over point-to-point channel) and the case of $f = 2$ has been shown in [32, 151–154] for twin-field quantum key distribution and asynchronous measurement-device-independent quantum key distribution [155, 156]. In Fig. 4.5, we set $\beta = 0$ and plot the variation of η_R as a function of the channel length l for different values of f.

Consider the task of sending ebits or private bits over the qubit erasure channel at a rate greater than p_*. To successfully perform the task, the critical length l_c and the critical time t_c are related via the expression

$$\alpha l_c + \beta t_c \leq -f \ln p_*. \tag{4.7}$$

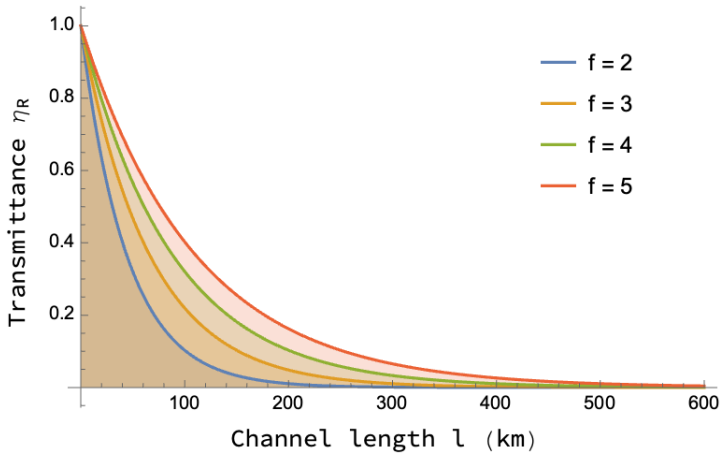


Figure 4.5: In this figure, we plot the variation of η_R as a function of the channel length l (km) (setting $\beta = 0$) for different values of f.

We see from Eq. (4.7) that using repeaters provides $f-$fold advantage over repeater-less networks. We plot in Fig. 4.6 the critical length l_c and critical time t_c for sending ebits or private bits over the channel at a rate $p_* = 0.5$ for different values of f. In the plot, we have set $\alpha = 1/22$ km^{-1}, and $\beta = 1/10$ s^{-1}.

We next consider performing quantum communication over a lattice network with fiber-based elementary links and present limitations on its scalability.

Observation 2. *Let us require to perform* Task$_*$ *over the lattice* $G_{lat}(\mathbb{V}, \mathbb{E})$ *having open edges with probability* p_{ij} *and* $0 < p_* \leq p_{ij} < 1$. *It follows from Theorem 1 that for any vertex* $v \in \mathbb{V}$, *the set of vertices connected to it via a network path is finite. This implies* G_{lat} *has a finite diameter. We may assume the elementary link formed by edge* $e_{ij} \in \mathbb{E}$ *connecting nodes* $\{v_i, v_j\} \in \mathbb{V}$ *to be optical fibers of length L having attenuation factor of* $\alpha_{dB/km} = 0.22$ *dB/km. The fibers having transmittance* $\eta = \mathrm{e}^{-\alpha L}$ *where* $\alpha = 0.051$*/km.*[2] *Let there be some repeater-based scheme that increases the transmittance from* η *to* $\eta^{1/f}$ *(see Assumption 1). Assuming that performing* Task$_*$ *by the nodes* $\{v_i, v_j\}$ *requires transmittance of at least* $\epsilon(= 0.5)$ *bounds the length of the fiber to* $L \leq (f/\alpha)\ln(1/\epsilon) \approx 27$ *km for* $f = 2$. *If there are* $r = 10$ *elementary links each of length* $L = 27$ *km between two nodes separated by a distance* $l = rL = 270$ *km, then performing* Task$_*$ *requires* $f \geq rL\alpha/\ln(1/\epsilon) \approx 20$.

[2]Note that $\alpha = \alpha_{dB/km}\frac{\ln(10)}{10}$.

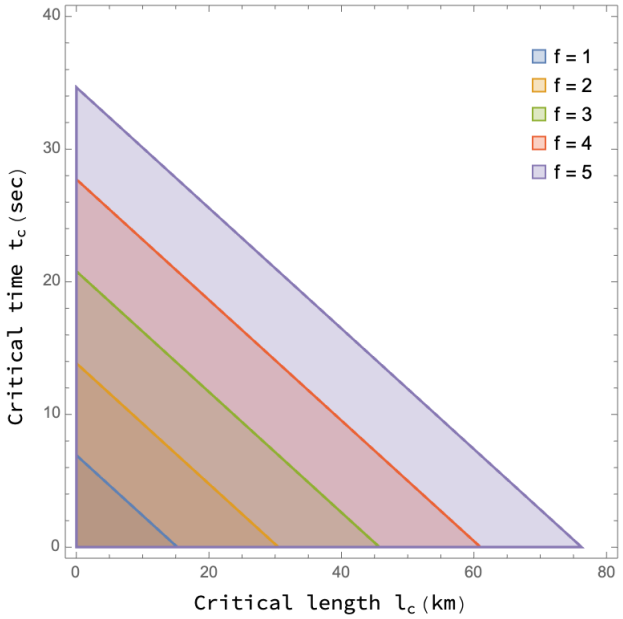


Figure 4.6: In this figure, we plot the critical length l_c (km) and critical time t_c (sec) for sending ebits or private bits over the channel at a rate of $p_* = 0.5$ for different values of f. We have considered $\alpha = 1/22$ km^{-1} and $\beta = 1/10$ sec^{-1}.

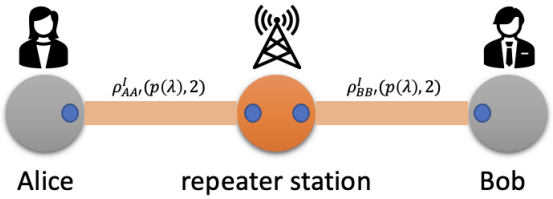
In the following example, we present limitations on the scalability of DI-QKD networks assuming there exists some scheme that can mitigate loss due to transmittance over a quantum channel.

Example 4. *Let us consider the task of connecting end nodes separated by the continental scale of (order of* 1000 *km) distance. To enable such a task, let there be a repeater-based network with* $t = 10$ *elementary links connecting two virtual nodes separated by metropolitan distances (order of* 100 *km). Each elementary link has two sources say* S_i *and* S_j *producing dual-rail encoded entangled pairs (for details see Appendix A.1) in the state* Ψ^+. *The sources* S_i *and* S_j *send one qubit from its entangled pair to the nearest virtual node and the other to the repeater station via optical fibers of length* $l = 25$ *km having attenuation factor* $\alpha = 0.02$ *km*$^{-1}$. *Let the qubits evolve through the fiber as a qubit erasure channel (see Sec. A.4.2) with channel parameter* $\eta_e = \mathrm{e}^{-(\alpha l/f)}$, *where we assume that some technique allow us to increase the transmissivity of optical fiber by factor* $1/f$ *for* $f > 1$. *After passing through the optical fiber, the qubits are stored in identical quantum memories at the repeater station, the virtual nodes, and the end nodes for* $n = 2$ *time steps. We model the evolution of the qubits in the quantum memory as depolarising*

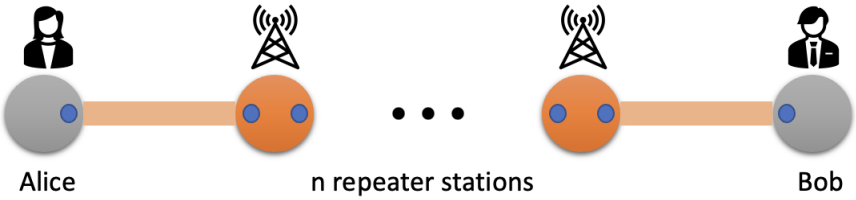
channel (see Sec. A.4.1) having channel parameter $p = 0.01$. *Assuming the repeater station performs perfect standard Bell measurement on its share of qubits, the singlet fidelity of the state shared by Alice and Bob is given by* $\eta_d^2\, e^{-2\alpha l t/f}$. *The state shared by the end nodes is useful for CHSH-based DI-QKD protocols if* $\eta_d^2\, e^{-2\alpha l t/f} \geq 0.7445$ *which requires* $f \geq 38$.

Observation 2 and Example 4 illustrate how far is current technology from designing quantum networks for performing quantum communication and implementing DI-QKD protocols.

4.3 Limitations on network architecture with repeaters



(a) Alice and Bob each send halves of isotropic state of visibility λ to a repeater station which performs standard Bell measurement on the received qubits with a success probability q. After the Bell measurement, Alice and Bob share an isotropic state of visibility $q\lambda^2$.



(b) Alice and Bob with n repeater stations in between them. After the repeater stations have performed standard Bell measurement, Alice and Bob share isotropic state of visibility $q^n\lambda^{n+1}$.

Figure 4.7: In this figure, we present a repeater-based network to share isotropic states between Alice and Bob. The shared state is then used to perform DI-QKD protocols. The blue circles in the figure depict qubits. We assume all the repeater stations are equidistant and identical.

Let us consider the task of sharing secret key between two distant parties over a repeater-based network. The parties say Alice and Bob each have identical two-qubit isotropic

states (see Eq. 2.8) $\rho^I_{AA'}(p(\lambda),2)$ and $\rho^I_{BB'}(p(\lambda),2)$ given by

$$\rho^I_{AA'}(p(\lambda),2) = \lambda \Psi^+_{AB} + (1-\lambda)\frac{\mathbb{1}_{AB}}{4}. \tag{4.8}$$

with $\lambda \in [0,1]$ and $\rho^I_{BB'}(p(\lambda),2) = \rho^I_{AA'}(p(\lambda),2)$. Alice and Bob send halves of their isotropic states to a repeater station. The repeater station performs a standard Bell measurement on the halves of the isotropic states with success probability q (see Fig. 4.7a). The action of the noisy standard Bell measurement is described by Eq. (A.5) (see Appendix A.2 for details). With the error correction possible post-Bell measurement, from a single use of the repeater Alice and Bob share the two-qubit isotropic state

$$\rho^I_{AB}(p(q\lambda^2),2) = q\lambda^2 \ \Psi^+_{AB} + \frac{1}{4}(1-q\lambda^2)\mathbb{1}_{AB} \tag{4.9}$$

of visibility λ^2 and q being the success probability of performing the successful standard Bell measurement by the repeater station. The state $\rho^I_{AB}(p(q\lambda^2),2)$ is separable if $\lambda \leq 1/\sqrt{3q}$. All two-qubit states are entanglement distillable if and only if they are entangled [157]. All entanglement distillable states have non-zero rates for secret-key distillation [158]. Alice and Bob can use the shared state $\rho^I_{AB}(p(q\lambda^2),2)$ to perform a DI-QKD protocol based on the tilted CHSH inequality [11] or the modified standard CHSH inequality [159]. It was shown in [160] that for such protocols, the device-independent secret key distillation rate is zero when the visibility $q\lambda^2$ of isotropic state $\rho^I_{AB}(p(q\lambda^2),2)$ is below the critical threshold

$$\gamma^\theta_{\text{crit}} = \frac{\gamma^\theta_L + 1}{3 - \gamma^\theta_L}, \tag{4.10}$$

where $\gamma^\theta_L = 1/(\cos\theta + \sin\theta)$ and $\theta \in (0, \pi/2)$. The standard CHSH-based DI-QKD protocols use settings with $\theta = \pi/4$, which gives $\gamma^{\pi/4}_{\text{crit}} \approx 0.7445$. The DI-QKD rate is known to be non-zero for $q\lambda^2 \geq 0.858$ [29]. For n repeater stations in between them (see Fig. 4.7b), Alice and Bob share the two-qubit isotropic state

$$\rho^I_{AB}(p(q^n\lambda^{n+1}),2) = q^n\lambda^{n+1} \ \Psi^+_{AB} + (1-q^n\lambda^{n+1})\frac{\mathbb{1}_{AB}}{4} \tag{4.11}$$

of visibility $q^n\lambda^{n+1}$, where q appears as it the success probability of performing a standard Bell measurement by the individual repeater stations. We call such linear links of repeaters with standard Bell measurement (possibly noisy) performed at relay stations as standard linear DI key repeater chains. In the following proposition, we present limitations on the use of isotropic states for distilling secret keys via DI-QKD protocols.

Proposition 2. *Consider a standard linear DI key repeater chain with n relay (intermediate) stations between two end nodes. The successive nodes v_i and v_j of the repeater chain share a two-qubit isotropic state $\rho^I_{ij}(p(\lambda^2), 2)$ and the relay stations perform standard Bell measurement with success probability q. The end nodes of such a network cannot perform CHSH-based DI-QKD protocols for*

$$\lambda \in \left(0, (\gamma^\theta_{crit}/q^n)^{1/(n+1)}\right). \tag{4.12}$$

Proof. The end nodes of the standard linear DI key repeater chain can use the shared state $\rho^I_{AB}(p(q^n\lambda^{n+1}), 2)$ to perform a DI-QKD protocol based on the tilted CHSH inequality [11] or the modified standard CHSH inequality [159]. The device-independent secret key rate for such protocols becomes zero for $q^n\lambda^{n+1} \in (0, \gamma^\theta_{\text{crit}})$. This limits λ to the range

$$\lambda \in \left(0, (\gamma^\theta_{\text{crit}}/q^n)^{1/(n+1)}\right) \tag{4.13}$$

when no secret key can be distilled. □

The following observation is direct consequence of the above proposition and the fact that family of two-qubit isotropic states $\rho^I_{ij}(p(\lambda), 2)$ is known to have zero DI-QKD rate for $\lambda \in (0, \gamma^\theta_{\text{crit}})$, where $q = 1$ is safely assumed without any ramification for the observation below.

Observation 3. *There exist quantum states with non-zero DI-QKD rates that are not useful as standard DI key repeaters. For example, for a family isotropic states $\rho^I_{ij}(p(\lambda), 2)$ with $\lambda \in \left(\gamma^\theta_{crit}, (\gamma^\theta_{crit}/q^n)^{1/(n+1)}\right)$ the DI key rate is nonzero but the standard DI key repeater rate is zero.*

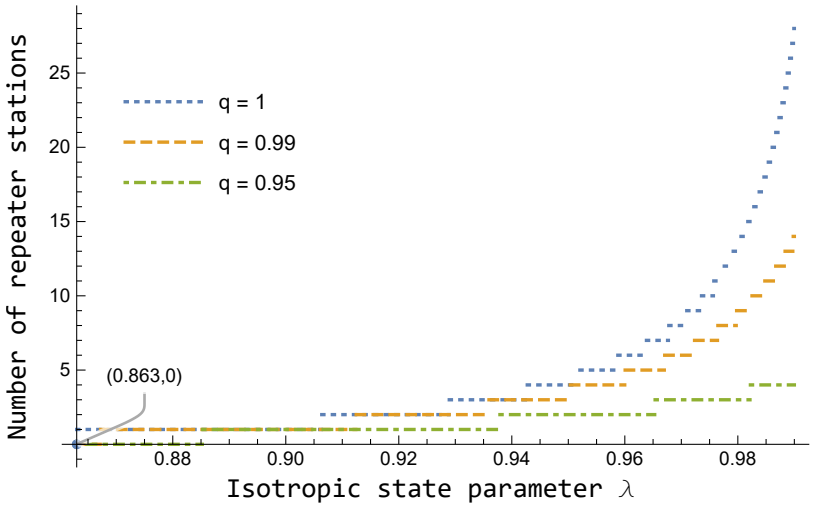


Figure 4.8: In this figure, we plot the allowed number of relay stations for performing a DI-QKD protocol with non-zero key rates by Alice and Bob as a function of the isotropic state parameter λ for different success probability of standard Bell measurement when the critical threshold from Eq. (4.10) is $\gamma^{\theta}_{\text{crit}} = 0.7445$.

For non-zero key rates from tilted CHSH inequality-based and the modified standard CHSH inequality-based DI-QKD protocols we require

$$n < \left\lfloor \frac{\log(\lambda/\gamma^{\theta}_{\text{crit}})}{\log(1/(q\lambda))} \right\rfloor, \tag{4.14}$$

where $\lfloor . \rfloor$ denotes the floor function and q is the probability of success for the perfect, standard Bell measurement at each relay (repeater) station. For values of n below the above threshold, we will have a positive secure key rate. We plot in Fig. 4.8, the dependence of n on λ for performing CHSH-based DI-QKD protocol with non-zero key rate for different success probability of standard Bell measurement. In the plot, we have set $\gamma^{\theta}_{\text{crit}}$ to be 0.7445. In Fig. 4.8, we observe that the neighbouring nodes of a repeater chain network sharing a two-qubit isotropic state $\rho^{I}_{AB}(p(\lambda^2), 2)$ with high values of λ allow a large number of repeater stations between the end nodes for performing a DI-QKD protocol with non-zero key rates. In the bipartite scenario with two binary inputs and two binary outputs, there is a region where the device is nonlocal but has zero key [161]. Results similar to Proposition 2 and Eq. (4.14) would apply to such a scenario if considered appropriately.

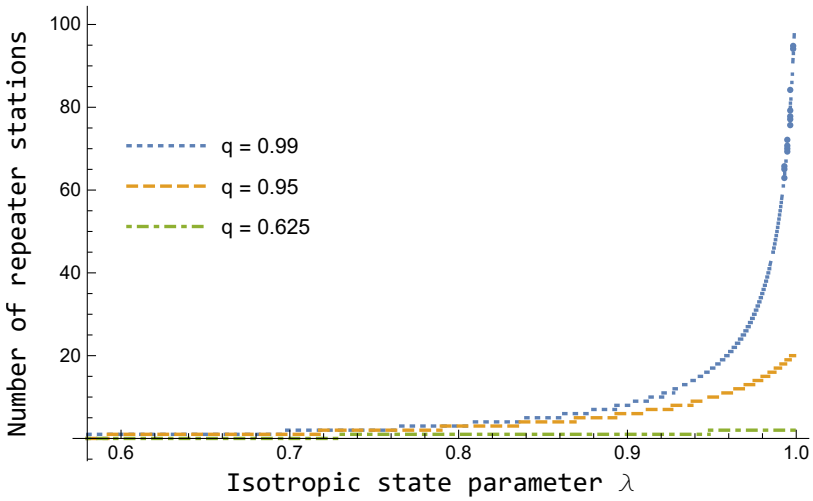


Figure 4.9: In this figure, we plot the maximum allowed number of relay stations between the end nodes as a function of λ, considering values of $q \in \{0.625, 0.95, 0.99\}$ such that the end nodes can implement a teleportation protocol.

In the following propositions, we present the bound on the number of virtual nodes in the network such that the state $\rho^I_{AB}(p(q^n\lambda^{n+1}), 2)$ (a) is useful for teleportation, (b) can violate the Bell-CHSH inequality and (c) is entangled.

Proposition 3. *The state $\rho^I_{AB}(p(q^n\lambda^{n+1}), 2)$ can be used to perform teleportation protocol when*

$$n < \left\lfloor \frac{\log(3\lambda)}{\log(1/(q\lambda))} \right\rfloor. \tag{4.15}$$

Proof. Let us have u_k as the eigenvalues of the matrix $T^\dagger T$ where the T matrix is formed by the elements $t_{nm} = \mathrm{Tr}[\rho^I_{AB}(p(q^n\lambda^{n+1}), 2)\, \sigma_n \otimes \sigma_m]$ where σ_j denotes the Pauli matrices. We then define the quantity $N(\rho_{AB}) = \sum_{k=1}^{3} \sqrt{u_k}$. The state $\rho^I_{AB}(p(q^n\lambda^{n+1}), 2)$ is useful for teleportation for values of $N(\rho_{AB})$ greater than 1 [162]. This then implies $n < \left\lfloor \frac{\log(3\lambda)}{\log(1/(q\lambda))} \right\rfloor$. □

We plot in Fig. 4.9 the maximum number of repeater stations that can be allowed for a given value of λ and setting $q \in \{0.625$ [163]$, 0.95, 0.99\}$ to implement a teleportation protocol successfully.

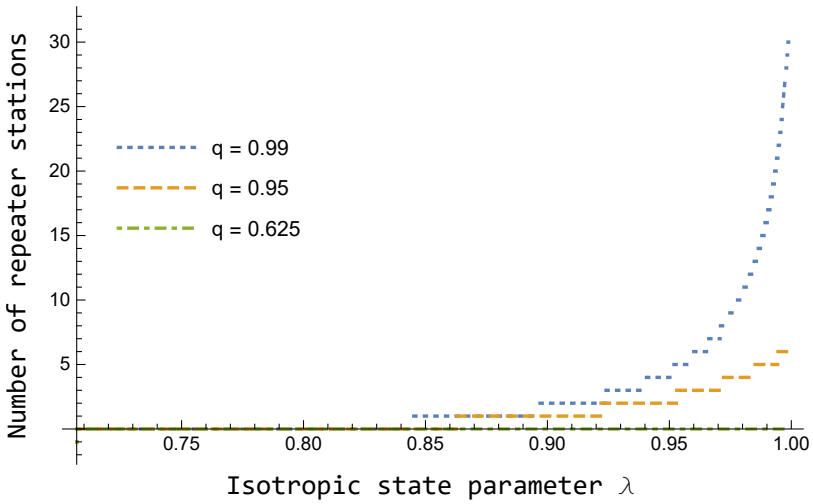


Figure 4.10: In this figure, we plot the maximum allowed number of relay stations between the end nodes as a function of λ, considering values of $q \in \{0.625, 0.95, 0.99\}$ such that the end nodes can perform Bell-CHSH violation experiment.

Proposition 4. *The state* $\rho^I_{AB}(p(q^n\lambda^{n+1}), 2)$ *can violate the Bell-CHSH inequality when*

$$n < \lfloor \frac{\log(\sqrt{2}\lambda)}{\log(1/(q\lambda))} \rfloor. \tag{4.16}$$

Proof. Let us have u_i, u_j be the two largest eigenvalues of the matrix $T^\dagger T$ where the T matrix is formed by the elements $t_{nm} = \mathrm{Tr}[\rho^I_{AB}(p(q^n\lambda^{n+1}), 2)\ \sigma_n \otimes \sigma_m]$ where σ_j denotes the Pauli matrices. We then define the quantity $M(\rho_{AB}) = u_i + u_j$. The state $\rho^I_{AB}(p(q^n\lambda^{n+1}), 2)$ is Bell-CHSH nonlocal for values of $M(\rho_{AB})$ greater than 1 [164]. This then implies $n < \lfloor \frac{\log(\sqrt{2}\lambda)}{\log(1/(q\lambda))} \rfloor$. □

We plot in Fig. 4.10 the maximum number of repeater stations that can be allowed for a given value of λ and setting $q \in \{0.625$ [163], $0.95, 0.99\}$ such that the state shared by the end nodes can violate the Bell-CHSH inequality.

Proposition 5. *The state* $\rho^I_{AB}(p(q^n\lambda^{n+1}), 2)$ *remains entangled when*

$$n < \left\lfloor \frac{\log(\lambda/(\frac{2}{\sqrt{3}} - 1))}{\log(1/(q\lambda))} \right\rfloor. \tag{4.17}$$

Proof. The concurrence of the state $\rho^I_{AB}(p(q^n\lambda^{n+1}), 2)$ is given by $\max\{0, \lambda^e_1 - \lambda^e_2 - \lambda^e_3 - \lambda^e_3\}$ [96] where the λ^e_s are the eigenvalues of $\rho^I_{AB}(p(q^n\lambda^{n+1}), 2)(\rho^I_{AB}(p(q^n\lambda^{n+1}), 2))_f$ in descend-

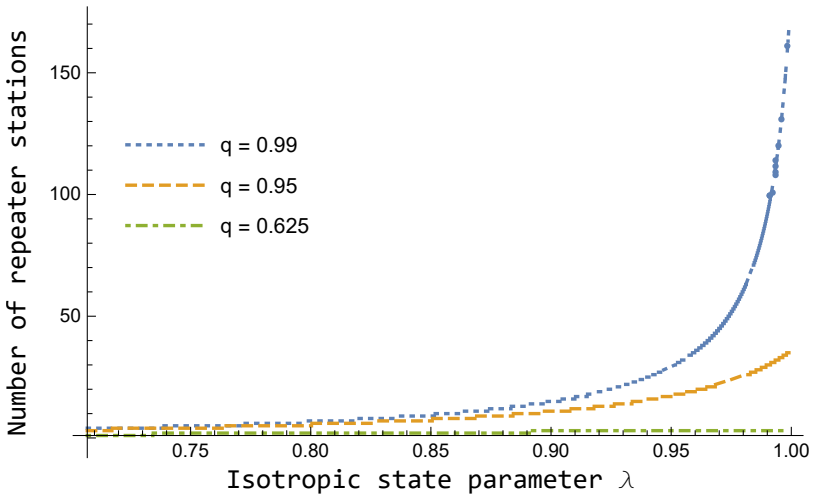


Figure 4.11: In this figure, we plot the maximum allowed number of relay stations between the end nodes as a function of λ, considering values of $q \in \{0.625, 0.95, 0.99\}$ such that the end nodes share an entangled state.

ing order. The spin flipped density matrix is given by $(\rho^{I}_{AB}(p(q^n\lambda^{n+1}), 2))_f = (\sigma_y \otimes \sigma_y)\rho^{I*}_{AB}(p(q^n\lambda^{n+1}), 2)(\sigma_y \otimes \sigma_y)$. The state is entangled when the concurrence is greater than zero. This requires $n < \left\lfloor \frac{\log(\lambda/(\frac{2}{\sqrt{3}}-1))}{\log(1/(q\lambda))} \right\rfloor$. □

We plot in Fig. 4.11 We plot in Fig. 4.10 the maximum number of repeater stations that can be allowed for a given value of λ and setting $q \in \{0.625, 0.95, 0.99\}$ such that the end nodes can share an entangled state.

It is observed that the number of allowed repeater stations in the network depends on the information processing task that the network is executing. The number of allowed repeater stations increases with the increase in λ.

The repeater network discussed in this section can be generalised to a network structure with multiple pairs of end nodes. It is observed that the number of allowed repeater stations in the network depends on the information processing task that the network is executing. The number of allowed repeater stations increases with the increase in λ. Furthermore, the success probability of the information processing task decreases with an increase in the number of allowed repeater stations. The repeater network discussed in this section can be generalised to a network structure with multiple pairs of end nodes.

4.4 Entanglement distribution between cities

Consider a satellite-based network for sharing entangled pairs between two far-off cities. Let such a network be a two-layered model consisting of a global scale and a local scale. On a global scale, there are multiple ground stations located across different cities. Such ground stations are interconnected via a satellite network. Two ground stations share an entangled state using the network via the shortest network path between them (see Sec. 3.4.1 for an illustration of shortest network-path finding algorithm).

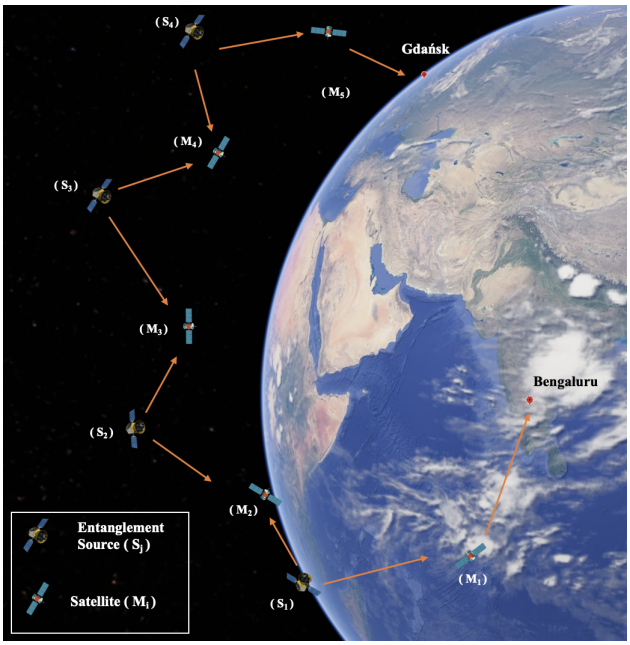
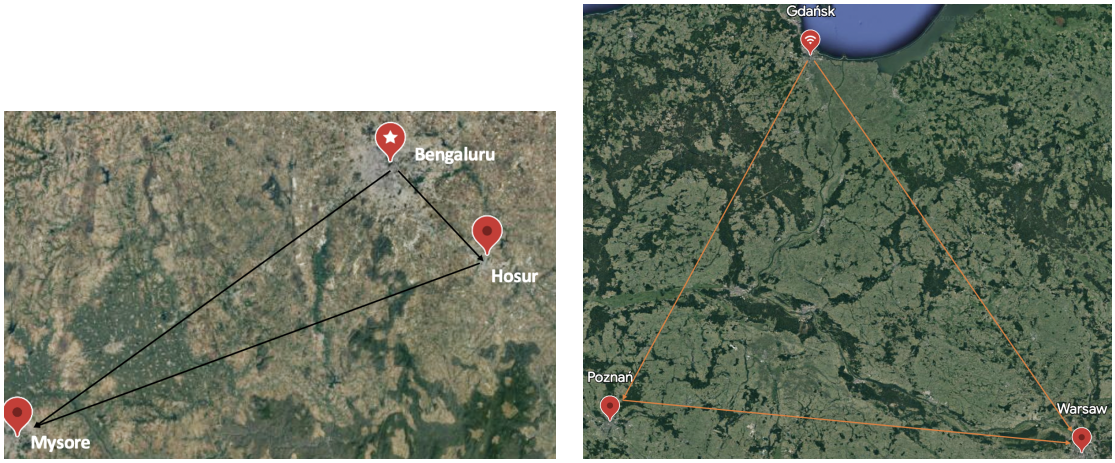


Figure 4.12: In this figure, we present the shortest network path between the ground stations at Bengaluru and Gdańsk via the global satellite network. The entangled sources are marked as S_i and the satellite stations are marked as M_i. The shortest path has 6 entangled sources and 5 satellite stations. The image was created using the Google Earth software [165].

As an example, we show in Fig. 4.12 the shortest path connecting the ISTRAC ground station located at Bengaluru to the ground station at Gdańsk via the global satellite network. On the local scale, different localities (end nodes) are connected to their nearest ground station via optical fibers. We show in Fig. 4.13 the local scale network for the ground station located at Bengaluru and Gdańsk. The ground station at Bengaluru is connected to the localities of Hosur and Mysore. The ground station at Gdańsk is connected to the

localities of Poznań and Warsaw.



(a) Bengaluru ground station (b) Gdańsk ground station

Figure 4.13: In this figure, we present the local scale network architectures at (a) Bengaluru and (b) Gdańsk for sharing entangled pairs across nearby localities. The ground stations are connected to multiple localities via optical fibers (shown in black and orange lines). The images were created using Google Earth software [165].

In the satellite network, there are sources (S_j) producing entangled photonic qubit pairs in the state Ψ^+. The source then sends the photons belonging to a pair to different neighbouring satellites via a quantum channel as shown in Fig. 4.12. We model the quantum channel between the ground station and the satellite at the limits of the atmosphere as a qubit thermal channel (see Sec. A.4.3 and Sec. A.5) and that between two satellites as an erasure channel (see Sec. A.4.2) having erasure parameter η_e. The erasure channel parameter is assumed to be identical throughout the network. The satellite stations M_j outside the limits of the atmosphere perform standard Bell measurement with success probability q on their share of the qubits that they received from their neighbouring source stations. The satellites at the boundary of the atmosphere transmit their share of qubit via the atmospheric channel to the ground stations (which we call local servers). The ground stations on receiving the state store it in a quantum memory. In the quantum memory, the state evolves via a depolarising channel (see Sec. A.4.1). The local servers distribute the quantum states to different localities (which we call clients) on request using optical fibers as can be seen in Fig. 4.13.

In future, it may be that India and Poland establish communication links that share each

halves of the entangled pairs between a designated hub in each country so that they can perform desired quantum tasks in collaboration. Let us assume that the Indian Space Research Organization (ISRO) headquarter[3] at Bengaluru would like to perform delegated quantum computing [132–135, 166] by securely accessing the IBM Quantum Hub at Poznań [167]. For this, the ISRO headquarter can share entangled system with the IBM Quantum Hub via the shortest route in the satellite-based network. For an illustration, let the shortest network path between the ground stations at Bengaluru and Gdańsk have 5 satellites and 4 entangled photon sources as shown in Fig. 4.12. The entanglement yield of the network is given by

$$\xi_{\text{avg}} = q^3 \, \eta_t^G (\eta_e^2)^3, \tag{4.18}$$

where η_t^G is obtained from Eq. (A.25) and takes into account the local weather conditions at Bengaluru and Gdańsk. In the general network with n satellite-to-satellite links between the two ground stations, the average entanglement yield is given by

$$\xi_{\text{avg}} = \eta_t^G (\eta_e^2)^{n-1} q^{n-1}. \tag{4.19}$$

The ground stations store the incoming qubits in different quantum memory slots and serve the receiving traffic[4] requests from different local clients following queuing discipline (see Algorithm 5 for details of the incoming and outgoing traffic threads[5]). The total number of memory slots available in the quantum memory is fixed. The evolution of the stored qubits in the quantum memory is modelled via a depolarising channel with channel parameter p. We model the quantum memory as a max-heap data structure (see Definition 12) with the key as the fidelity of the stored quantum state. If the fidelity of any quantum state stored in the memory drops below a pre-defined critical value, η_{crit}, that state is deleted from the memory. The value of η_{crit} is determined by the task or the protocol that the end parties may be interested in performing using their shared entangled state.

[3] As we were finalizing the paper [2], we learnt that ISRO was successful in soft landing of its spacecraft **Chandrayaan-3** (Vikram lander and Pragyan rover) on the Moon's south polar region on 23-08-2023 at 18:03 IST.

[4] Traffic is the flow of photons between the nodes of the network for enabling the network to perform a specific information processing task.

[5] Thread is a sequential execution of tasks in a process.

On receiving a connection request from a single local client, the ground station transmits the latest qubit that it has received as outward traffic. Now when the ground station receives traffic requests from multiple local clients, there is the problem of optimizing the traffic flow[6]. For such a flow problem, we introduce the following modified fair queuing algorithm.

Let us define $t_p^{(i)}$ as the time to process the i^{th} quantum state in the memory, $t_i^{(i)}$ as the starting time for the transmission from the memory and $t_f^{(i)}$ as the time when the state has been transmitted from the memory. We then have,

$$t_f^{(i)} = t_i^{(i)} + t_p^{(i)}. \tag{4.20}$$

Now, there is a possibility that the state has arrived at the memory before or after the processing of $i-1$ states in this heap. In the latter case, the state arrives at an empty heap memory and is transmitted immediately if there is a traffic request. In the other case, it swims through the heap depending on its fidelity and is stored in the memory. Let us denote $t_r^{(i)}$ as the time required for the node to swim up to the root node from its current position in the heap. Then we have,

$$t_f^{(i)} = \max\left(t_f^{(i-1)}, t_r^{(i)}\right) + t_p^{(i)}, \tag{4.21}$$

where $t_f^{(i-1)}$ is the time required for processing $(i-1)^{\text{th}}$ quantum state. If there are multiple flows, the clock advances by one tick when all the active flows receive one state following the qubit-by-qubit round-robin basis. If the quantum state has spent s time steps in the memory then the average entanglement yield is given by

$$\xi_{\text{avg}} := \begin{cases} \eta_d^s\, \eta_t^G (\eta_e^2)^{n-1} q^{n-1} & \text{if } \eta_d^s > \eta_{\text{crit}}, \\ 0 & \text{otherwise,} \end{cases} \tag{4.22}$$

where η_d^s is obtained from Eq. (A.13) and takes into account the loss in yield per time step in the quantum memory. Let us assume the ground station at Bengaluru and Gdańsk

[6]Traffic flow is a sequence of quantum states that is sent from the ground station to the local station.

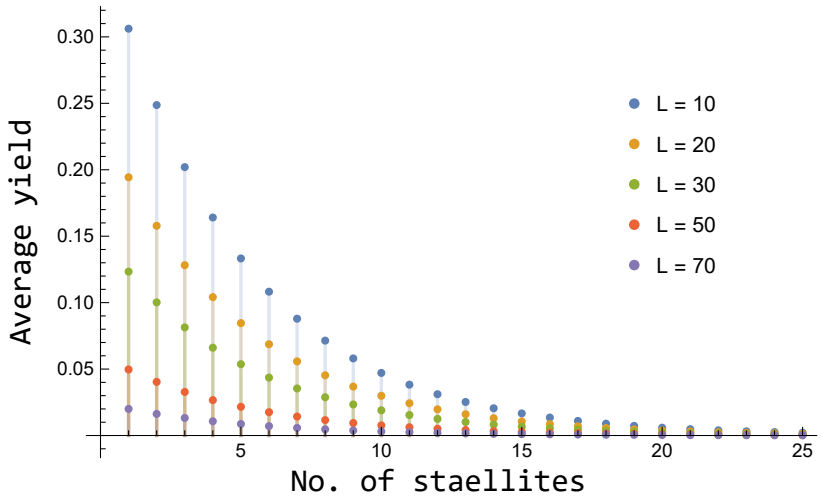


Figure 4.14: In this figure, we plot the average yield ξ_{avg} (see Eq. (4.24)) as a function of the number of satellites in the network for different values of the total optical fiber length $L = l_B + l_M$ (shown figure inset). We set $\eta_s = 0.9, s = 1, p = 0.1, \eta_e = 0.95, \eta_g = 0.5, \kappa_g = 0.5, \alpha = 1/22$ km^{-1}, and $q = 1$.

transmits the state via identical fibers to the ISRO headquarter and Poznań, respectively. Considering the fiber losses at the two ground stations given by $e^{-\alpha l_B}$ and $e^{-\alpha l_M}$, the sources producing the state Ψ^+ with probability η_s, and assuming that the quantum state has spent s time steps in the memory, the average entanglement yield is given by

$$\xi_{\text{avg}} = \eta_d^s \, \eta_t^G (\eta_e^2)^{n-1} (\eta_s)^{n-1} e^{-\alpha(l_B+l_M)} q^{n-1}, \tag{4.23}$$

where l_B and l_M are the lengths of the fibers from ISRO headquarter and Poznań to the Bengaluru and Gdańsk ground stations respectively. Inserting η_d^s from Eq. (A.13) and η_t^G from Eq. (A.25), we have the yield given by

$$\begin{aligned} \xi_{\text{avg}} \quad &= e^{-\alpha(l_B+l_M)} \left(\eta_e^2\right)^{n-1} \eta_s^{n-1} q^{n-1} \\ &\left[(1-p)^{2s} - \frac{1}{4}(p-2)p\left((s-1)(1-p)^{2(s-1)} + 1\right)\right] \\ &\left[\kappa_g(\kappa_g - 1)(\eta_g - 1)^2 + \frac{1}{2}(1+\eta_g^2)\right] \end{aligned} \tag{4.24}$$

where η_g, κ_g take into account the local weather condition at Bengaluru and Gdańsk and s is the number of applications of depolarising channel in the quantum memory. We plot in Fig. 4.14, the average entanglement yield ξ_{avg} of the two end nodes connected by the

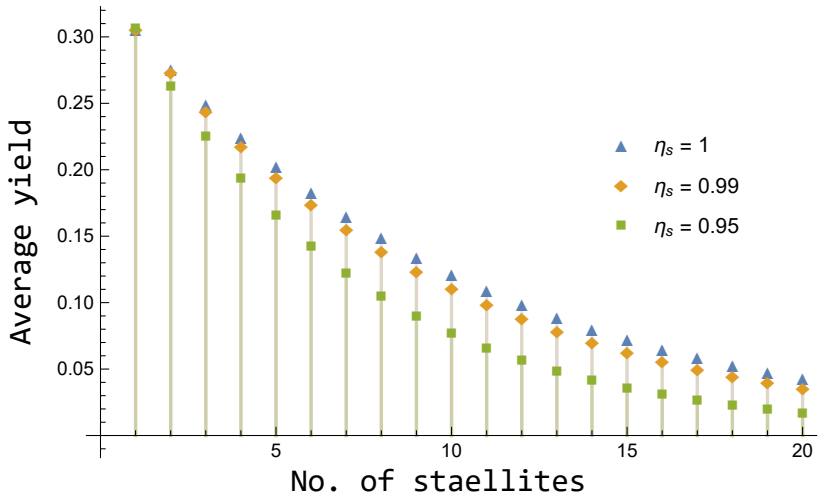


Figure 4.15: In this figure, we plot the average yield ξ_{avg} (see Eq. (4.24)) as a function of the number of satellites in the network for single photon source architectures. The single photon source architectures have the source efficiencies (a) $\eta_s = 0.95$ (b) $\eta_s = 0.99$ and (b) $\eta_s = 1$. For this, we set $L = l_B + l_M = 10$ km, $s = 1, p = 0.95, \eta_e = 0.95, \eta_g = 0.5, \kappa_g = 0.5, \alpha = 1/22$ km^{-1}, and $q = 1$.

network as a function of the number of satellite-to-satellite links n between their nearest ground stations for different values of the total optical fiber length $L = (l_B + l_M)$. We observe that for a fixed value of L, ξ_{avg} decreases with an increase in n. Also, for a fixed value of n, ξ_{avg} decreases with increase in L. Furthermore, we plot in Fig. 4.15 and A.5 the variation in ξ_{avg} as a function of n for different values of η_s. We observe that for a given η_s, ξ_{avg} decreases with increase in n. Also, we observe that Quantum dot-based, atom-based, and SPDC-based entangled photon sources are best suited for the entanglement distribution network. Finally, we plot in Fig. 4.16, the variation in ξ_{avg} as a function of n for different values of q. We observe that for a given q, ξ_{avg} decreases with increase in n. Also, ξ_{avg} decreases with a decrease in q.

Our methods in general apply to sharing multipartite entangled states among different ground stations distributed at different geographical locations across the globe. To observe this, note that if certain users of the network share bipartite entangled states, then such states can be used to distill multipartite entangled states with the use of ancilla and entanglement swapping protocols [6, 168, 169].

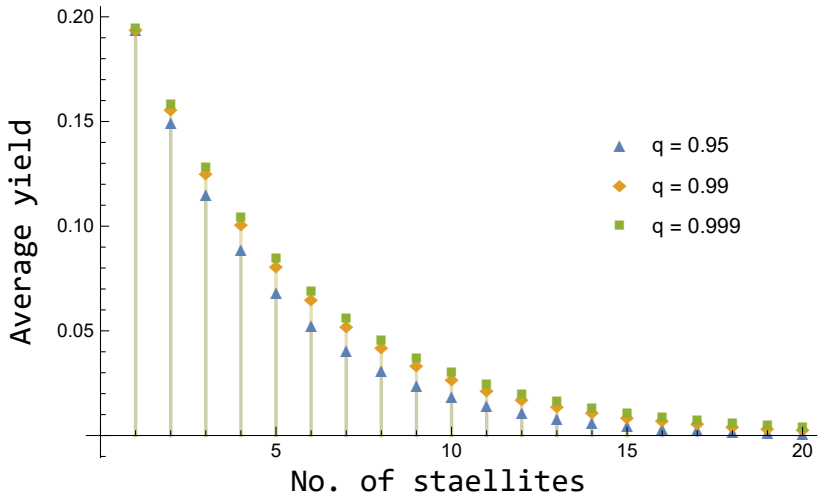


Figure 4.16: In this figure, we plot the average yield ξ_{avg} (see Eq. (4.24)) as a function of the number of satellites in the network for different values of the success probability of the standard Bell measurement denoted by q (shown figure inset). We set $\eta_s = 0.9, s = 1, p = 0.1, \eta_e = 0.95, \eta_g = 0.5, \kappa_g = 0.5, \alpha = 1/22$ km^{-1}, $L = l_B + l_M = 20$ km.

4.5 Network propositions

Let us first consider a network connecting all the major airports in the world. We say that two airports are connected if there exists at least one commercial airline currently operating between them. We consider a network consisting of 3463 airports all over the globe forming the nodes of the network and 25482 edges or airline routes between these airports [170]. For such a network, we observe that the longest route is between Singapore, Changi International Airport, and New York John F. Kennedy International Airport, in the United States, with a distance of approximately 15331 km. The average distance between the airports in the network is approximately 1952 km. We propose a quantum network with airports as nodes and the connections between the airports as edges. We define the edge weight of the edge connecting the nodes $\{v_i, v_j\}$ of the network as

$$\mathrm{w}(e_{ij}) := \begin{cases} \mathrm{e}^{-L_{ij}/22} & \text{if } L_{ij} < 50 \text{ km} \\ 0.8 & \text{if } L_{ij} \geq 50 \text{ km} \end{cases} \tag{4.25}$$

where L_{ij} is the distance between two airports denoted by nodes v_i and v_j. The link sparsity of such a network is 0.99575, and the total connection strength is given by 0.99787. We observe that the most critical airports present in this network are Istanbul International Airport, Dubai International Airport, Anchorage Ted Stevens in Alaska, Beijing Capital International Airport, Chicago O'Hare International Airport, and Los Angeles International Airport.

Let the airports of the network require to securely communicate with each other. The sharing of entangled states among the airports is a primitive for secure communication among them. Let us assume all these airports are located at the same altitude. Let the ground stations located at the airports share an entangled state using a global satellite-based mesh quantum network as described in Sec. 4.4. The ground stations connect to the satellite network via the atmospheric channel modelled as a qubit thermal channel. The satellites of the network are interconnected via a qubit erasure channel. For two airports a_1 and a_2 requiring to connect, the average entanglement yield is given by

$$\begin{aligned} \xi_{\text{avg}} &= \eta_t^a (\eta_e^2)^{n-1} q^{n-1} \\ &= q^{n-1} \left(\eta_e^2\right)^{\left\lfloor \frac{L}{L_0} \right\rfloor - 1} \left[\kappa_g (\kappa_g - 1)(\eta_g - 1)^2 + \frac{1}{2}(1 + \eta_g^2) \right], \end{aligned} \tag{4.26}$$

where L denotes the distance between a_1 and a_2 and q is the success probability of the standard Bell measurement at the satellite stations. L_0 denotes the distance between the nodes of the satellite network. We assume identical atmospheric conditions at a_1 and a_2 and set $\eta_e = 0.95, \eta_g = 0.5$, $\kappa_g = 0.5$ and $q = 1$. With these choices of parameters, we present in Fig. 4.18 the average yield as a function of the distance between the nodes of the satellite network for different values of L. Furthermore, we plot in Fig. 4.17, the variation in the average yield ξ_{avg} as a function of the distance between the virtual nodes for different values of q. For this we set $\eta_e = 0.95$, $\eta_g = 0.5$, $\kappa_g = 0.5$ and $L = 4000$ km. The entanglement yield between the airports for different channel parameters not considered in this section can be obtained from Eq. (4.26).

The quantum Internet can be used for secure communication between a central agency

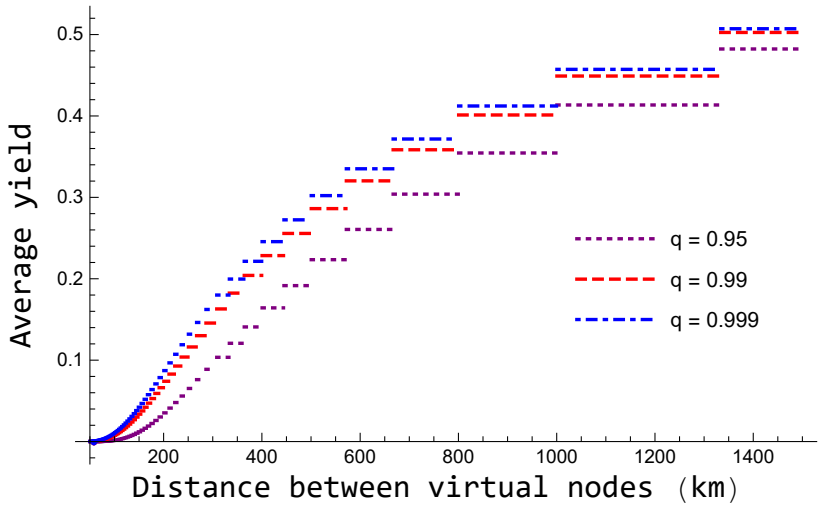


Figure 4.17: In this figure, we plot the average yield ξ_{avg} (see Eq. (4.26)) as a function of the distance between the virtual nodes (L_0) for different values of q. For this, we set $\eta_e = 0.95, \eta_g = 0.5, \kappa_g = 0.5$ and $L = 4000$ km.

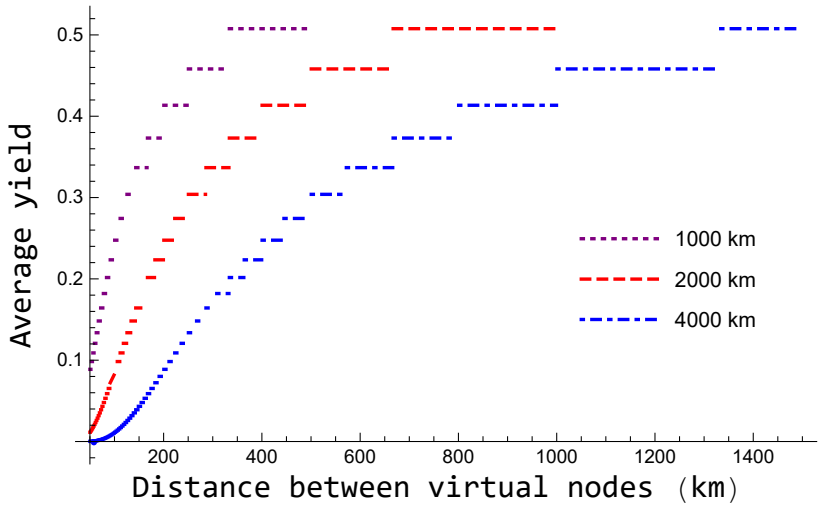


Figure 4.18: In this figure, we plot the average yield ξ_{avg} (see Eq. (4.26)) as a function of the distance between the virtual nodes for different lengths between the airports. For this, we set $\eta_e = 0.95, \eta_g = 0.5, \kappa_g = 0.5, q = 1$.

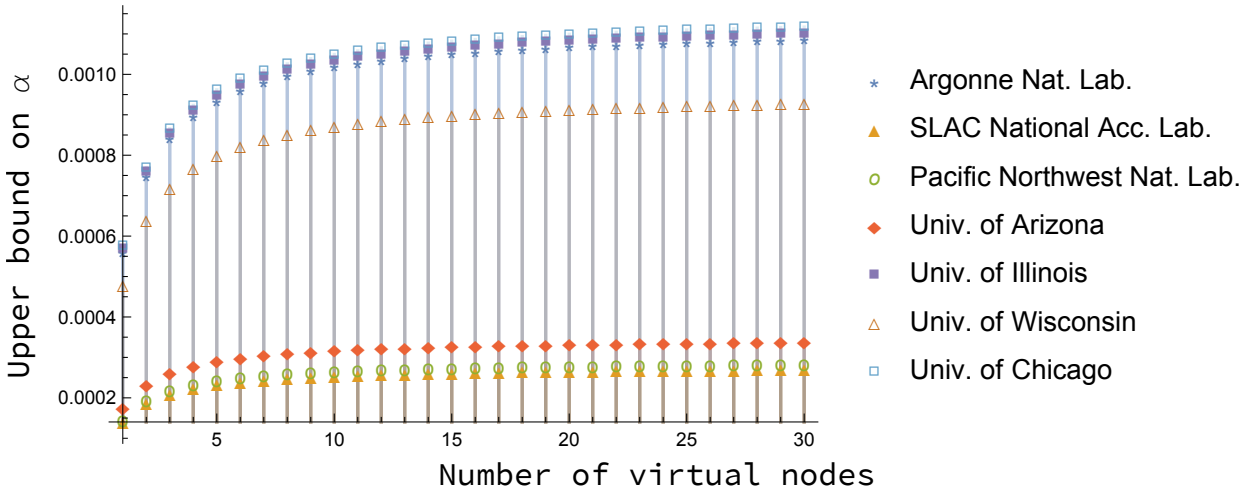


Figure 4.19: The upper bound on the channel parameter α for sharing entanglement between the U.S. Department of Energy (DoE) at Washington D.C. and some other labs [171] involved in The National Quantum Initiative (NQI). In this network, the DoE is the hub node while the labs are at the outer nodes. The edge connecting the hub to an outer node represents a repeater relay network. In this plot we set $q = 1$.

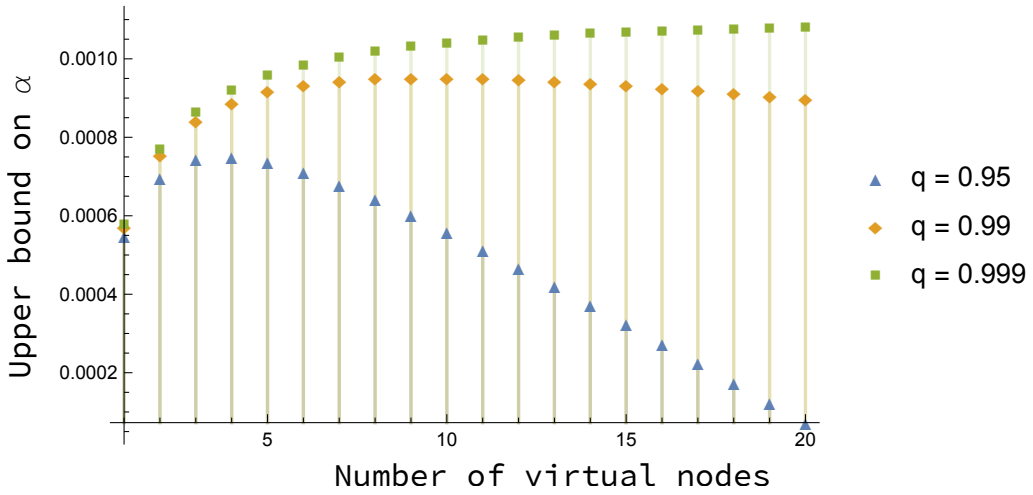


Figure 4.20: The upper bound on the channel parameter α for sharing entanglement between the U.S. Department of Energy (DoE) at Washington D.C. and the University of Chicago ($L = 952$ km) involved in The National Quantum Initiative (NQI) for different values of success probability of standard Bell measurement. In this network, the DoE is the hub node while the labs are at the outer nodes. The edge connecting the hub to an outer node represents a repeater relay network.

and end parties. It may be desirable here for the central agency to prevent direct communication between the end parties. As an example, consider the U.S. Department of Energy (DoE) in Washington D.C. require to securely communicate by sharing entangled states with the major labs [171] that are involved in The National Quantum Initiative (NQI) using the Star network. The DoE is at the hub node of such a network and the different labs are the leaf nodes. For each edge of the network, let there be independent fiber-based repeater chain networks (described in Sec. 4.3.) Let each edge present in the network have a success probability $p = \mathrm{e}^{-\alpha L/n}$ where α is the channel loss parameter, L is the total distance between the DoE and the lab, and n is the number of virtual nodes. Using the fact that isotropic state of visibility $q^n\lambda^{n+1}$ is entangled for $q^n\lambda^{n+1} > 1/3$, we obtain the upper bound on α as

$$\alpha < \frac{\log(3q^n)}{L(1+\frac{1}{n})}. \tag{4.27}$$

For different labs, we plot in Fig. 4.19 the upper bound on α for different values of n. In the figure, we have considered some of the major labs, which can be extended to all other labs involved in the NQI. Furthermore, in Fig. 4.20, we plot the upper bound on α for different values of n and q (see inset). For this figure we consider sharing entanglement between the U.S. Department of Energy (DoE) at Washington D.C. and the University of Chicago ($L = 952$ km).

4.6 Discussion

We envision that the implementation of the quantum Internet will follow a task-oriented approach. The underlying network structure at any stage of implementation is expected to provide loose coupling, meaning end users can perform information processing tasks without requiring to know the details of implementation, thereby reducing dependencies between different tasks. This requires assessing the practical limitations for implementing different tasks.

The network structure of the quantum Internet is determined by the information processing tasks that are implemented using it. Looking at the elementary link level, we have

obtained bounds on the critical success probability for performing different tasks. Extending to a more general repeater-based network, we have obtained a trade-off between the channel length and the time interval for which the states can be stored at the nodes such that the shared state is useful for different tasks.

Considering performing some desirable information processing tasks over lattice networks, in the previous chapter we have presented a theorem specifying conditions that lead to the absence of percolation. As implications of the theorem, we have highlighted the constraints on network scalability and limitations of current technology for performing quantum communication and implementing DI-QKD protocols.

Looking at the specific details of implementation, considering repeater-based networks, we have provided the range of isotropic state visibility and an upper bound on the number of repeater nodes for distilling secret keys at non-zero rates via DI-QKD protocols. We have considered practical parameters like atmospheric conditions and imperfect devices in obtaining bottlenecks for implementing a satellite-based model distributing resources between far-off places. For such a network we have presented algorithms for implementing certain underlying network-related tasks such as obtaining the network layout, obtaining the network routing path and allocating resources at the network nodes. Overall, the assessment presented in this chapter may be useful in benchmarking the critical parameters involved in realizing the quantum Internet.

CHAPTER 5

QUANTUM NONLOCALITY, FREE WILL AND IMPERFECT DETECTORS

"Not only is the Universe stranger than we think,
it is stranger than we can think."

— Werner Heisenberg

This chapter is entirely based on [1], a joint work with Siddhartha Das.

In a seminal work, J.S. Bell [76] showed that the statistical predictions of quantum mechanics cannot be explained by local realistic hidden variable (LRHV) theories. The LRHV inequalities, also called Bell-type inequalities, are based on the physical assumptions of (a) the existence of local realism and (b) no-signalling criterion [75] (see e.g., [74] and references therein). The quantum systems that violate LRHV inequalities [74] are said to have quantum nonlocal correlations.

The experimental violation of the LRHV inequalities by physical systems requires additional assumptions leading to loopholes. The free will assumption[1] in the Bell-type inequality states that the parties (users) can choose the measurement settings freely or, use uncorrelated random number generators. Also, the detectors used in experiments are never perfect and there is always a possibility of over-counting (observing dark counting [172]) and under-counting (inefficient detection [172]) the number of particles that are incident on it.

The main focus of this chapter is to study the implications of imperfect detectors and constrained free will on the test of quantum nonlocal correlations. We adapt the approach discussed in [13] to model imperfect detectors for the Bell experiment as a sequential application of a perfectly working inner box followed by a lossy outer box. The inner box contains a quantum source whose behavior is nonlocal under constrained free will, i.e., violates certain measurement-dependent LRHV inequality. The outer box separately introduces detector inefficiency and dark counts for each party. Using this model, we determine the threshold values of the detector parameters that make detectors robust for testing of quantum nonlocality under constrained free will (e.g., see Fig. 5.3 with details in Section 5.3). Next for the scenario of perfect detectors, we compare the implications two different approaches presented in [7] and [9] to quantify measurement dependence (a) by bounding the probability of choosing the measurement settings x (for Alice's side) and y (for Bob's side) conditioned on a hidden variable λ to be in the range $[l, 1-3l]$ [7] and (b) by using a distance measure M to quantify measurement settings distinguishability [9].

[1] It should be noted that the free will assumption mentioned in this chapter is also called measurement independence. This assumption relates to the possible correlations between the choice of measurement settings for the two parties, which can affect the observed experimental statistics.

This comparison is made in the 2 (party) - 2 (measurement settings per party) - 2 (outcome per measurement) scenario and their effects on the certification of the nonlocality. We also introduce a new set of measurement-dependent LRHV (MDL) inequalities by introducing distance-based measurement-dependent quantity in adapted AMP tilted Bell inequality [11] and discuss implications and trade-off between measurement dependence parameters and tilted parameters for the certification of quantum nonlocal correlations.

5.1 Adverserial role in choice of measurement settings

We consider the Bell scenario where two parties, Alice and Bob, share a bipartite quantum state ρ_{AB}. Each party can choose to perform one of two available measurements, i.e., $|\mathcal{X}| = 2 = |\mathcal{Y}|$. We attribute POVM $\{\Lambda_a^x\}_x$ to Alice and $\{\Lambda_b^y\}_y$ to Bob. Each of these measurements can have two outcomes. We denote measurement outcomes for Alice and Bob by a and b, respectively. The statistics of the measurement outcomes in the experiment can then be described by the probability distribution $\mathbf{P} = \{p(ab|xy)\}$, which is also termed behavior. In this framework, there exists a hidden variable λ belonging to some hidden-variable space, Λ. The probability distribution of the outputs conditioned on the inputs can then be expressed as

$$p(ab|xy) = \sum_{\lambda\in\Lambda} p(ab|xy\lambda)p(\lambda|xy). \tag{5.1}$$

The hidden variable λ (distribution according to $p(\lambda)$) can provide an explanation of the observed experimental (measurement) statistics. In each experiment run, a fixed λ exists that describes the outcome of the experimental trial following the distribution $p(ab|xy\lambda)$. After multiple experimental runs, the output statistics are described by sampling from the distribution $p(\lambda|xy)$.

In an adversarial scenario, Alice and Bob can believe they choose all the settings with equal probability, i.e., $p(xy) = 1/4$ for each pair (x, y), while an adversary biases their choice in the scale λ. The adversary can distribute the settings chosen by Alice and Bob

Probability distributions of Eve

Joint Setting	Distribution 1 (λ_1)	Distribution 2 (λ_2)
$p(0,0\|\lambda)$	$\cos^2(\phi_{s_1})$	$\cos^2(\phi_{s_2})$
$p(0,1\|\lambda)$	$\sin^2(\theta_{s_1})\sin^2(\phi_{s_1})$	$\sin^2(\theta_{s_2})\sin^2(\phi_{s_2})$
$p(1,0\|\lambda)$	$\cos^2(\delta_{s_1})\cos^2(\theta_{s_1})\sin^2(\phi_{s_1})$	$\cos^2(\delta_{s_2})\cos^2(\theta_{s_2})\sin^2(\phi_{s_2})$
$p(1,1\|\lambda)$	$\sin^2(\delta_{s_1})\cos^2(\theta_{s_1})\sin^2(\phi_{s_1})$	$\sin^2(\delta_{s_2})\cos^2(\theta_{s_2})\sin^2(\phi_{s_2})$

Table 5.1: Probability distribution for choice of settings by Alice and Bob based on the hidden variable λ. An adversary can use this distribution and, by suitably choosing the parameters of the table, trick Alice and Bob into thinking they have free will in choosing the measurement settings.

according to

$$p(xy) = \sum_{\lambda\in\Lambda} p(xy|\lambda)p(\lambda). \tag{5.2}$$

In Eq. (5.2), let λ take two values, λ_1 and λ_2, whose probability distributions are given as $p(\lambda_1) = \sin^2(\theta_\lambda)$ and $p(\lambda_2) = \cos^2(\theta_\lambda)$, respectively. In the simplest scenario, x and y can each take values 0 or 1, and there are four possible ways in which the measurement settings can be chosen by Alice and Bob, i.e., $(x,y) \in \{(0,0),(0,1),(1,0),(1,1)\}$.

Let the probability of choosing the measurement setting (x,y) conditioned on the hidden variable be distributed according to Table 5.1. To observe the effect of the conditional probability distribution for choice of x and y from Table 5.1 on $p(xy)$, consider the following examples:

(i) For the case of $\theta_{s_2} = 0.6847$, $\phi_{s_2} = 1.2491$, $\phi_{s_1} = 0.8861$, $\delta_{s_2} = 1.2491$, $\theta_\lambda = 0.785398$, $\theta_{s_1} = 0.50413$, and $\delta_{s_1} = 0.175353$. It can be seen that this choice of parameters set $p(xy) = 0.25\ \forall\ (x,y)$.

(ii) For the case of $\theta_{s_2} = 0.5796$, $\phi_{s_2} = 1.2491$, $\phi_{s_1} = 0.6847$, $\delta_{s_2} = 0.75$, $\theta_\lambda = 0.57964$, $\theta_{s_1} = 0.793732$, and $\delta_{s_1} = 1.06395$. It can be seen that this choice of parameters set $p(xy) = 0.25\ \forall\ (x,y)$.

The above examples show that by properly choosing parameters in Table 5.1, the adversary can trick Alice and Bob into thinking they have free will in choosing the measurement

setting. In the scenario where Alice and Bob choose between the measurement settings with unequal probabilities, i.e., $p(xy) \neq 1/4$ for each pair (x,y), the adversary can adjust the parameters of Table 5.1 accordingly. In the presence of a bias in the choice of measurement settings in the λ scale, which Alice and Bob are unaware of, the following constraints [173] can be imposed on the conditional joint probability distribution:

a. The signal locality, i.e., no-signalling, assumption imposes the factorisability constraint on the conditional joint probability distribution,

$$p(ab|xy\lambda) = p(a|x\lambda)\, p(b|y\lambda). \tag{5.3}$$

b. The measurement independence, i.e., freedom-of-choice or free will, assumption requires that λ does not contain any information about x and y which is equivalent to stating

$$p(\lambda|xy) = p(\lambda) \quad \text{or equivalently,} \quad p(xy|\lambda) = p(xy). \tag{5.4}$$

5.2 Quantifying measurement dependence

In this section, we first review two different approaches considered in [7,84] and [9,10,83] to quantify the measurement dependence. We then compare these two approaches and observe their effects on the tests of quantum nonlocal behaviors.

Review of MDL inequalities from prior works

We review the approach discussed in [7, 8] to quantify measurement dependence by bounding the probability of choice of measurement settings conditioned on a hidden variable to be in a specific range (Section 5.2). Then we review the approach discussed in [9, 10, 83] to quantify measurement dependence using a distance measure (Section 5.2).

Bound on the probability of choosing the measurement settings

In the works [7, 8], we observe that the probability of Alice and Bob choosing measurement settings x and y conditioned on λ can be bounded as

$$l \leq p(xy|\lambda) \leq h, \tag{5.5}$$

where $0 \leq l \leq p(xy|\lambda) \leq h \leq 1$. If Alice and Bob each choose from two possible measurement settings, then $l = h = 0.25$ corresponds to the complete measurement independence; other values of l and h represent bias in the choice of measurement settings.

In the 2 (user) - 2 (measurement settings per user) - 2 (outcome per measurement) scenario with $a, b \in \{+, -\}$ and $x, y \in \{0, 1\}$, it was shown in [7, 8] that all the measurement dependent local correlations satisfy the PRBLG MDL inequality

$$lp(++00) - h(p(+-01) + p(-+10) + p(++11)) \leq 0. \tag{5.6}$$

A two-dimensional slice in the non-signalling space is shown in Fig. 5.1 (figure from [7]). The quantum set is bounded by the green line in the figure, and the set of non-signalling correlations lies within the black triangle.

In Fig. 5.1, the red dotted line corresponds to Eq. (5.6) with $h = 1-3l$. If we set $h = 1-3l$, the PRBLG MDL inequality tilts from the Bell-CHSH inequality ($l = 0.25$) to the non-signalling border ($l = 0$). For $h = 1 - 3l$, Eq. (5.6) is expressed as

$$lp(++00) - (1 - 3l)\Big[p(+-01) + p(-+10) + p(++11)\Big] \leq 0. \tag{5.7}$$

We note that if Alice and Bob believe they have complete measurement dependence, i.e., $p(xy) = 0.25\ \forall(x, y)$, then Eq. (5.7) reduces to

$$lp(++|00) - (1 - 3l)\Big[p(+-|01) + p(-+|10) + p(++|11)\Big] \leq 0. \tag{5.8}$$

It follows from [84] that invoking the PRBLG MDL inequality (5.7) in the tilted Hardy

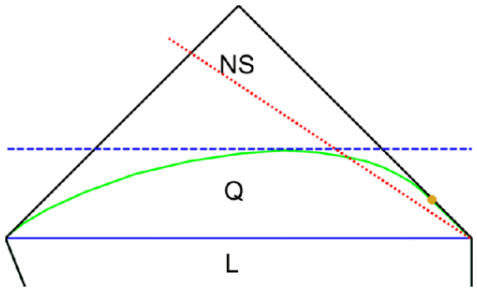


Figure 5.1: A two-dimensional slice of the no-signalling space with the MDL correlations discussed in [7]. The blue line encloses the set of Bell-CHSH local correlations. The green line encloses the quantum set. The black triangle encloses the no-signalling distributions. For the case of $h = 1 - 3l$, the inequality (5.6) shifts from the Bell-CHSH boundary to the no-signalling boundary via the red dotted line.

test [84], we obtain the ZRLH MDL inequality. The ZRLH MDL inequality is expressed as

$$\begin{aligned} &l[p(++|00) + wp(--|00) - \max\{0, w\}] \\ &-(1-3l)[p(+-|01) + p(-+|10) + p(++|11)] \leq 0, \end{aligned} \tag{5.9}$$

where w is the tilting parameter taking real numbers in the range, $w \in (-0.25, 1)$. We call the quantum behaviors that violate Eqs. (5.8) and (5.9) as quantum nonlocal in the presence of measurement dependence.

Distance measure to quantify measurement distinguishability

We discussed in Section 5.1 that the experimental statistics described by the joint probability distribution $p(ab|xy)$ can be explained by $\lambda \in \Lambda$ in the following form,

$$p(ab|xy) = \int \mathrm{d}\lambda p(ab|xy\lambda)p(\lambda|xy). \tag{5.10}$$

The assumption of the measurement independence constrains the probability distribution of measurement settings via

$$p(\lambda|xy) = p(\lambda). \tag{5.11}$$

Eq. (5.11) implies that no extra information about λ can be obtained from the knowledge of x and y. This is equivalent to saying

$$p(xy|\lambda) = \frac{p(\lambda|xy)p(xy)}{p(\lambda)} = p(xy). \tag{5.12}$$

Eq. (5.12) implies that Alice and Bob have complete freedom in choosing the measurement settings x and y respectively. If $x \in U \equiv \{x_1, x_2\}$ and $y \in V \equiv \{y_1, y_2\}$, measurement dependence implies $p(\lambda|x_1, y_1) \neq p(\lambda|x_2, y_2)$. Distinguishability between $p(\lambda|x_1, y_1)$ and $p(\lambda|x_2, y_2)$ can be quantified using a distance measure defined in [9],

$$M = \int \mathrm{d}\lambda |p(\lambda|x_1, y_1) - p(\lambda|x_2, y_2)|. \tag{5.13}$$

We can express the probability to successfully distinguish $p(\lambda|x_1, y_1)$ and $p(\lambda|x_2, y_2)$ based on the knowledge of λ as

$$F = \frac{1}{2}\left(1 + \frac{M}{2}\right). \tag{5.14}$$

When $M = 0$, we have $F = \frac{1}{2}$, which suggests that no additional information about the hidden variable λ can be obtained from knowing the choice of measurement settings.

This observation is consistent with the maximum free will that Alice and Bob have while choosing the measurement settings. Whereas for $M = 2$, we have $F = 1$, which suggests that the complete information about the hidden variable λ can be obtained from knowing the choice of the measurement settings. This observation is consistent with no free will for Alice and Bob while choosing the measurement settings.

The local degrees of measurement dependence for Alice and Bob as introduced in [9] is given by

$$M_1 \equiv \max\left\{\int \mathrm{d}\lambda |p(\lambda|x_1, y_1) - p(\lambda|x_2, y_1)|, \int \mathrm{d}\lambda |p(\lambda|x_1, y_2) - p(\lambda|x_2, y_2)|\right\}, \tag{5.15}$$

$$M_2 \equiv \max\left\{\int \mathrm{d}\lambda |p(\lambda|x_1, y_1) - p(\lambda|x_1, y_2)|, \int \mathrm{d}\lambda |p(\lambda|x_2, y_1) - p(\lambda|x_2, y_2)|\right\}, \tag{5.16}$$

M_1 quantifies the measurement dependence for Alice's settings keeping Bob's settings

$$\begin{aligned}
&\langle x_1\rangle = \cos(2\phi); && \langle x_2\rangle = 0;\\
&\langle y_1\rangle = \cos(2\phi)\cos(\mu); && \langle y_2\rangle = \cos(2\phi)\cos(\mu);\\
&\langle x_1, y_1\rangle = \cos(\mu); && \langle x_1, y_2\rangle = \cos(\mu);\\
&\langle x_2, y_1\rangle = \sin(2\phi)\sin(\mu); && \langle x_2, y_2\rangle = -\sin(2\phi)\sin(\mu).
\end{aligned}$$

Table 5.2: The table presents the expectation values of operators from [11] that violate the AMP tilted Bell inequality given in Eq. (5.34). The parameter $\mu := \tan^{-1}(\sin(2\phi)/\alpha)$ where ϕ is the state parameter and α is the tilting parameter in Eq. (5.34) as defined in [11].

fixed, and similarly the other way round for M_2. The above parameters will be useful in deriving the bounds on the AMP tilted Bell inequalities [11] in Section 5.4.

Comparison and discussion on implications of different measurement-dependent LRHV inequalities

In this section, we check for the allowed values of measurement dependence parameter l to ensure nonlocality of quantum behaviors that are used to obtain randomness. Consider the quantum behavior in Table 5.2 that violates the AMP tilted Bell inequality (5.34). In the limit of $\alpha \to \infty$, close to two bits of randomness can be obtained from such a behavior by violating the AMP tilted Bell inequality [11]. For the quantum behavior in Table 5.2, the PRBLG MDL inequality (5.8) reduces to

$$l \leq \frac{3\alpha t + \alpha\cos(2\phi)t - 2\sqrt{2}\alpha\sin^2(\phi) + \sqrt{2}(\cos(4\phi) - 1)}{10\alpha t + 4\alpha\cos(2\phi)\left(t + \sqrt{2}\right) - 2\sqrt{2}\left(\alpha + 3\sin^2(2\phi)\right)} \tag{5.17}$$

where $t = \sqrt{-\frac{\cos(4\phi)}{\alpha^2} + \frac{1}{\alpha^2} + 2}$. In the limit of $\alpha \to \infty$, from Eq. (5.17) we have $l \leq 0.25$. We see that in the limit of $\alpha \to \infty$ the quantum behavior in Table 5.2 does not violate any PRBLG MDL inequality. For $\alpha = 1$ (which is equivalent to Bell-CHSH inequality) and $\phi = \frac{\pi}{4}$ (the maximum violation of the Bell-CHSH inequality,) we see from Eq. (5.17) that the quantum behavior in Table 5.2 violates the family of PRBLG MDL inequalities for $l > 0.2023$.

We observe in Fig. 5.2 that for a fixed value of α, the range of the allowed values of ϕ from Table 5.2 that violates the PRBLG MDL inequality given by Eq. (5.8) increases

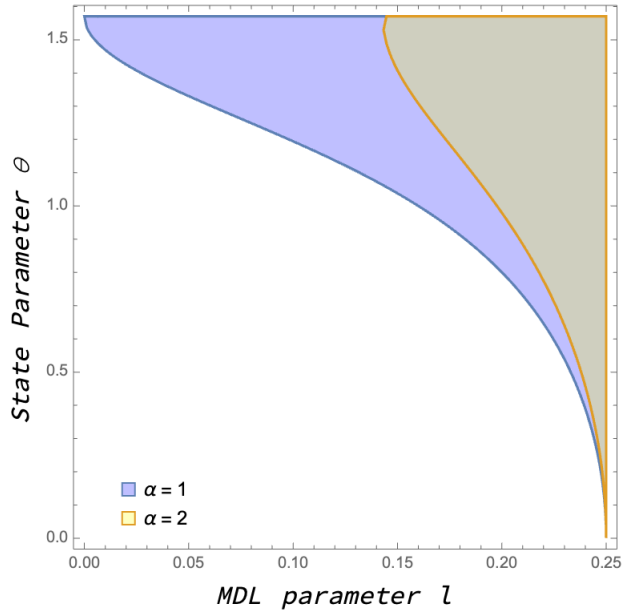


Figure 5.2: For $\alpha \in \{1, 2\}$, we plot the range of the state parameter ϕ from Table 5.2 ($\phi = \frac{1}{2}\sin^{-1}(\alpha \tan \mu)$) that violates the PRBLG MDL inequality (given by Eq. (5.8)) for different values of the measurement dependence parameter l.

with the increase in l. Also as α increases, for a particular value of l, there is a decrease in the range of the allowed values of ϕ from Table 5.2 that violates the AMP tilted Bell inequality. It was shown in [84] that the state $\rho_g = |\psi_g\rangle\langle\psi_g|$ (5.18) and measurement settings $\{A_0^g, A_1^g, B_0^g, B_1^g\}$ can be used to obtain close to 1.6806 bits of global randomness (at $\theta \approx 1.13557$), where

$$|\psi_g\rangle = \cos\left(\frac{\theta}{2}\right)|00\rangle - \sin\left(\frac{\theta}{2}\right)|11\rangle, \tag{5.18}$$

$$A_0^g = B_0^g = \frac{-\sqrt{2}\sin(\theta)\sqrt{\sin(\theta)}}{(2-\sin(\theta))\sqrt{\sin(\theta)+1}}\sigma_x + \frac{-(\sin(\theta)+2)\sqrt{1-\sin(\theta)}}{(2-\sin(\theta))\sqrt{\sin(\theta)+1}}\sigma_z, \tag{5.19}$$

$$A_1^g = B_1^g = \frac{\sqrt{2}\sqrt{\sin(\theta)}}{\sqrt{\sin(\theta)+1}}\sigma_x - \frac{\sqrt{1-\sin(\theta)}}{\sqrt{\sin(\theta)+1}}\sigma_z, \tag{5.20}$$

such that $\theta = \sin^{-1}(3 - \sqrt{4w+5})$ and A_x^g, B_y^g for $x, y \in \{0, 1\}$ denote measurement settings for Alice and Bob, respectively.

Observation 4. *Let us consider the quantum behavior given by the state ρ_g and measurement settings $\{A_0^g, A_1^g, B_0^g, B_1^g\}$. For such behavior, the PRBLG MDL inequality given by Eq. (5.8) reduces to*

$$\frac{2l}{(\xi-1)^2}\left(31\xi + w\left(4\xi-34\right)-69\right) + \frac{2l(\xi-5)\sqrt{\xi-2}}{\sqrt{4-\xi}(\xi-1)}\sqrt{-4w+6\xi-13} - \frac{2(1-3l)}{1-\xi}\left(8w-10\xi+\frac{\sqrt{\xi-2}\sin\left(2\sin^{-1}\left(3-\xi\right)\right)}{\sqrt{4-\xi}}+22\right)\leq 0, \tag{5.21}$$

where $\xi = \sqrt{4w+5}$. On inspection we see that for all $w \in (-0.25, 1)$, Eq. (5.21) reduces to $l \leq 0$. The quantum behavior specified by the state ρ_g and measurement settings $\{A_0^g, A_1^g, B_0^g, B_1^g\}$ is nonlocal for $l > 0$.

For the given quantum behavior, the ZRLH MDL inequality (5.9) reduces to

$$\frac{1}{2\left(\xi-1\right)}\left(2l\left(-4w+7\xi-15\right)+\frac{\left(1-3l\right)\sqrt{\xi-2}\sin\left(2\sin^{-1}\left(3-\xi\right)\right)}{\sqrt{4-\xi}} +8w-10\xi+22\right)-l\max(0,w)\leq 0. \tag{5.22}$$

On inspection we see that for all $w \in (-0.25, 1)$, Eq. (5.22) reduces to $l \leq 0$.

That is, the quantum behavior given by state ρ_g and measurement settings $\{A_0^g, A_1^g, B_0^g, B_1^g\}$ violates both PRBLG and ZRLH MDL inequalities, and its quantum nonlocality can be certified for all possible $l > 0$.

5.3 Imperfect detector and constrained free will

We model the detection units of Alice and Bob using a two-box approach following [13]. There is an inner box containing a quantum source generating bipartite quantum states whose behavior is nonlocal under constrained free will but assuming that detectors are perfect. Nonlocality of the quantum behavior in the inner box is tested by violation of a given MDL inequality. The output of the inner box is quantum nonlocal behavior that violates a given MDL inequality. An outer box introduces the detector imperfections, namely

the detection inefficiency and dark counts. The quantum nonlocal behavior obtained from the inner box gets mapped at the outer box to the output behavior with detector imperfection parameters. The output behavior then undergoes an LRHV test, based on which we are able to determine threshold values of detection inefficiency and dark counts such that the given quantum nonlocal behavior can still be certified to be nonlocal with imperfect detectors. A deviation from a two-box approach in [13] is the introduction of the measurement dependence assumption to the working of the inner box. Alice and Bob have access only to the input settings and the outputs of the outer box. We assume that either party (Alice and Bob) has access to two identical detectors that can distinguish between the orthogonal outputs.

The measurement outcomes for the inner box are labelled as a^{id} and b^{id} respectively. We note that a^{id} and b^{id} can each take values from the set $\{+,-\}$. Introducing non-unit detection efficiency, $0 \leq \eta \leq 1$, and non-zero dark count probability, $0 \leq \delta \leq 1$ in the outer box, the ideal two-outcome scenario becomes a 4-outcome scenario with the addition of no-detection event Φ, and the dark-count event χ. These events are defined in the following way:

Φ : One particle is sent to the party and none of the two detectors of that party click.

χ : One particle is sent to the party and both the detectors of the party click.

We label the measurement outcomes for Alice and Bob obtained from the outer box as a^{ob} and b^{ob} respectively. We note that a^{ob} and b^{ob} can each take values from the set $\{+,-,\Phi,\chi\}$. Furthermore, we assume that Alice and Bob's detection units have identical values for η and δ. The conditional probability of observing the outcome t^{ob} from the outer box conditioned on observing t^{id} in the ideal scale is given by $p(t^{ob}|t^{id})$ with $t^{ob} \in \{a^{ob}, b^{ob}\}$ and $t^{id} \in \{a^{id}, b^{id}\}$. The observed joint probabilities can then be expressed as [13]

$$p(a^{ob}b^{ob}|xy) = \sum_{a^{id},b^{id}} p(a^{ob}|a^{id})p(b^{ob}|b^{id})p(a^{id}b^{id}|xy). \tag{5.23}$$

We relax the free will assumption in the inner box by introducing the hidden variable

$\lambda \in \Lambda$. Considering this assumption, $p(a^{id}b^{id}|xy)$ is expressed as

$$p(a^{id}b^{id}|xy) = \sum_{\lambda\in\Lambda} p(a^{id}b^{id}|xy\lambda)p(\lambda|xy). \tag{5.24}$$

The hidden variable, λ (distributed according to $p(\lambda)$) provides an explanation of the observed experimental statistics of the inner box. The distribution of settings that are chosen by Alice and Bob depends on λ via the following relation,

$$p(xy) = \sum_{\lambda\in\Lambda} p(xy|\lambda)p(\lambda). \tag{5.25}$$

If we impose the locality condition from Eq. (5.3) on the experimental statistics of the inner box, we arrive at the following factorisability constraint,

$$p(a^{id}b^{id}|xy\lambda) = p(a^{id}|x\lambda)p(b^{id}|y\lambda). \tag{5.26}$$

Also, if we impose the measurement independence assumption from Eq. (5.4), we arrive at the following constraint,

$$p(xy|\lambda) = p(xy) \text{ or equivalently, } p(\lambda|xy) = p(\lambda). \tag{5.27}$$

The output statistics of the outer box for imperfect detectors can depend on the output of the inner box in the following four ways [13]:

i) No particle is detected on either of the detectors and no dark count detection event takes place. We can then write the following:

$$p(a^{ob}|a^{id}) = (1-\eta)(1-\delta)^2. \tag{5.28}$$

ii) No particle is detected by the detector that should have detected it and a dark count takes place in the other detector. We can then write the following:

$$p(a^{ob}|a^{id}) = (1-\eta)(1-\delta)\delta. \tag{5.29}$$

iii) Either the particle is detected by one of the detectors and a dark count takes place in the other detector or the particle is not detected and dark counts take place in both the detectors. We can then write the following:

$$\begin{aligned} p(a^{ob}|a^{id}) &= \eta\delta + (1-\eta)\delta^2 \\ &= \delta[1-(1-\eta)(1-\delta)]. \end{aligned} \tag{5.30}$$

iv) Either the particle is detected and no dark count takes place or the particle is not detected and a dark count takes place in the detector in which the particle should have been registered. We can then write the following:

$$\begin{aligned} p(a^{ob}|a^{id}) &= \eta(1-\delta) + (1-\eta)\delta(1-\delta) \\ &= (1-\delta)[1-(1-\eta)(1-\delta)]. \end{aligned} \tag{5.31}$$

The quantum nonlocal behavior obtained from the inner box after getting mapped to the output behavior with detector imperfection parameters remains nonlocal if the behavior obtained from the outer box violates the inequality [13]

$$p(++|00) + p(++|01) + p(++|10) - p(++|11) - p_A(+|0) - p_B(+|0) \leq 0, \tag{5.32}$$

where $p_A(o|s)$ and $p_B(o|s)$ are the probabilities of Alice and Bob to obtain the outcome o on measuring s.

At first, let us assume there is a quantum source in the inner box that is generating a bipartite quantum state whose behavior $\{p(a^{id}, b^{id}|xy)\}$ violates the PRBLG MDL inequality given by Eq. (5.8) assuming that detectors are perfect. The quantum behavior $\{p(a^{id}, b^{id}|xy)\}$ obtained from the inner box gets mapped at the outer box to the behavior $\{p(a^{ob}, b^{ob}|xy)\}$ with the introduction of the detector inefficiency η and dark count probability δ. The behavior $\{p(a^{ob}, b^{ob}|xy)\}$ is then inserted in Eq. (5.32) to obtain the critical detector parameters using Algorithm 6. For a fixed value of δ we obtain the minimum value of η that violates Eq. (5.32) using Algorithm 6. We abbreviate the left-hand side as

LHS.

Algorithm 6 Critical detector parameters: PRBLG MDL inequality

Initialize:
  $l \leftarrow$ parameter of Eq. (5.8)
for δ in range (0, 1) **do**
  for η in range (0, 1) **do**
    $P(a^{id}, b^{id}|xy) \leftarrow$ inner box quantum behavior
    $P(a^{ob}, b^{ob}|xy) \leftarrow f(P(a^{id}, b^{id}|xy), \delta, \eta)$
    obj $\leftarrow$ LHS of Eq. (5.32) for $P(a^{ob}, b^{ob}|xy)$
    MDL $\leftarrow$ LHS of Eq. (5.8) for $P(a^{id}, b^{id}|xy)$
    maximize: obj
    such that: MDL > 0
    opt $\leftarrow$ max value of obj
    if opt > 0 **then**
      print: δ, η
      Break

We plot the critical values of η and δ obtained using Algorithm 6 in Fig. 5.3.

Observation 5. *From Fig. 5.3, we see that the minimum value of η for a given δ takes the highest value for $l = 0$ and decreases as l increases. For a fixed value of l, the minimum value of η increases monotonically with the increase in dark count probability. We note that for $\delta = 0$, we have $\eta \approx 0.667$ for all the values of l.*

We next assume there is a quantum source in the inner box that is generating a bipartite quantum state whose behavior $\{p(a^{id}, b^{id}|xy)\}$ violates the ZRLH MDL inequality given by Eq. (5.9) assuming that detectors are perfect. The quantum behavior $\{p(a^{id}, b^{id}|xy)\}$ obtained from the inner box gets mapped at the outer box to the behavior $\{p(a^{ob}, b^{ob}|xy)\}$ with the introduction of the detector inefficiency η and dark count probability δ. The behavior $\{p(a^{ob}, b^{ob}|xy)\}$ is then inserted in Eq. (5.32) to obtain the critical detector parameters using Algorithm 7. For a fixed value of δ we obtain the minimum value of η that violates Eq. (5.32) using Algorithm 7. We abbreviate the left-hand side as LHS.

Algorithm 7 Critical detector parameters: ZRLH MDL inequality

Initialize:
  $w \leftarrow$ parameter of Eq. (5.9)
  $l \leftarrow$ parameter of Eq. (5.9)
for δ in range (0, 1) **do**
  for η in range (0, 1) **do**
    $P(a^{id}, b^{id}|xy) \leftarrow$ inner box quantum behavior
    $P(a^{ob}, b^{ob}|xy) \leftarrow f(P(a^{id}, b^{id}|xy), \delta, \eta)$
    obj $\leftarrow$ LHS of Eq. (5.32)
    MDL $\leftarrow$ LHS of Eq. (5.9)
    maximize: obj
    such that: MDL > 0.
    opt $\leftarrow$ max value of obj
    if opt > 0 **then**
      print: δ, η
      Break

We plot in Fig. 5.3, the critical values of η and δ from Algorithm 7 for $w = 0$.

Observation 6. *The ZRLH MDL inequality given by Eq.* (5.9) *and the PRBLG MDL inequality given by Eq.* (5.8) *reduce to the same inequality for* $l = 0$ *and is independent of* w*. For* $l = 0$*, Eqs.* (5.9) *and* (5.8) *cannot be violated* [2]*. For* $w = 0$*, Eqs.* (5.9) *and* (5.8) *reduce to the same inequality, and their violation can happen only when* $l > 0$ [3]*. For the case* $w = 0$*, we observe the same dependence for the threshold detector parameters as seen from Fig. 5.3. We observe from Fig. 5.3 that for a fixed value of* l*, the minimum*

[2] For $l = 0$, Eqs. (5.9) and (5.8) reduces to the inequality

$$-[p(+-|01) + p(-+|10) + p(++|11)] \leq 0$$

that is independent of w. The probabilities are always non-negative, and hence the above inequality can never be violated

[3] For $w = 0$, violation of Eqs. (5.9) and (5.8) requires

$$l > \frac{p(+-|01) + p(-+|10) + p(++|11)}{p(++|00) + 3[p(+-|01) + p(-+|10) + p(++|11)]},$$

i.e., $l > 0$ necessarily.

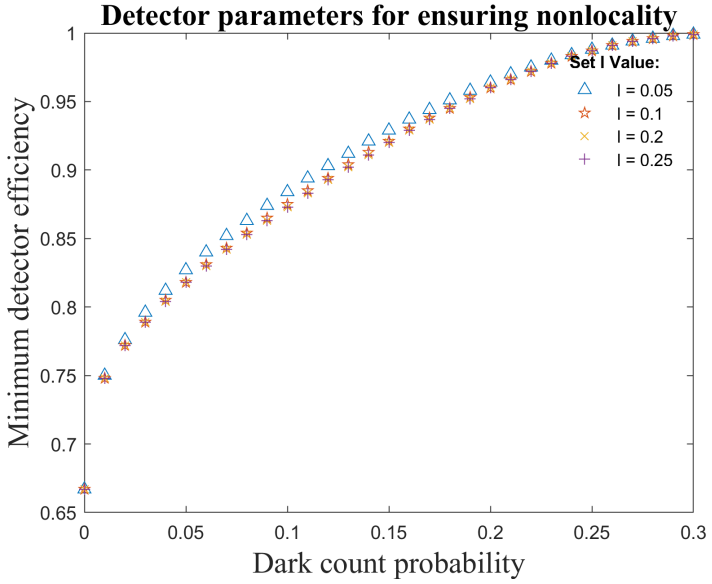


Figure 5.3: In this figure we plot the minimum detection efficiency η as a function of the dark count probability δ obtained using Algorithm 6. For each pair of (η, δ) in this figure, there exists a quantum behavior $\{p(a^{id}, b^{id}|xy)\}$ that violates Eq. (5.8). From such a behavior, $\{p(a^{ob}, b^{ob}|xy)\}$ is obtained by using the values of the pair (η, δ). The behavior $\{p(a^{ob}, b^{ob}|xy)\}$ violates Eq. (5.32). See Section 5.3.

detection efficiency increases monotonically with the dark count probability.

We comment here that using Algorithm 7, one can calculate the detector requirements for other values of (w, l) not mentioned in this section. Next, we consider the state ρ_g and measurement settings $\{A_0^g, A_1^g, B_0^g, B_1^g\}$ with $\theta \approx 1.13557$. This choice of state and measurement settings was shown to ensure 1.6806 bits of global randomness in [84].

Observation 7. *Consider the quantum source in the inner box generates bipartite quantum state ρ_g. Let Alice and Bob choose the measurement settings $\{A_0^g, A_1^g, B_0^g, B_1^g\}$, with $\theta \approx 1.13557$. With this choice of state and measurement settings, we obtain the quantum behavior $\{p(a^{id}, b^{id}|xy)\}$ assuming that the detectors are perfect. The output behavior $\{p(a^{ob}, b^{ob}|xy)\}$ obtained from the outer box is evaluated using Eq. (5.23). The behavior $\{p(a^{ob}, b^{ob}|xy)\}$ is nonlocal if we have a violation of the inequality*

$$\delta\eta[\delta(9.50424\delta - 4\delta^2 - 9.00848) + 4.25636] + \eta^2[\delta(2\delta^3 - 5.50424\delta^2 + 5.82473\delta - 3.13675) + 0.816258] + 2\delta(\delta - 1)(\delta^2 - \delta + 1) - 0.752119\eta \leq 0. \quad (5.33)$$

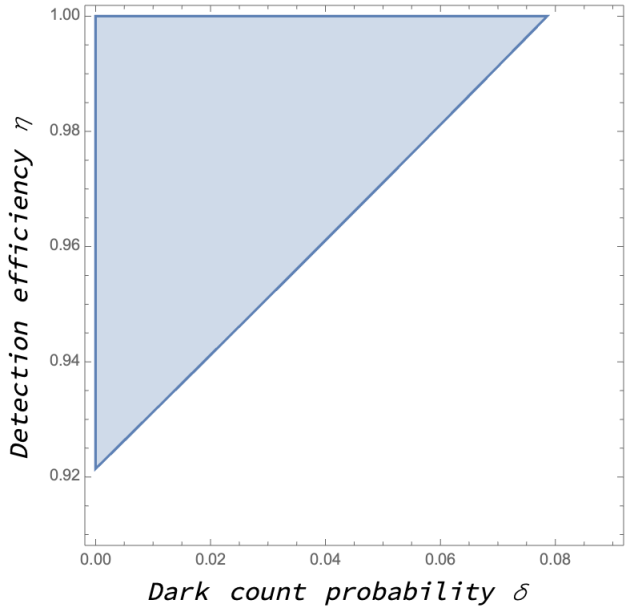


Figure 5.4: In this figure we plot the detector parameters η and δ for which the behavior $\{p(a^{ob}, b^{ob}|xy)\}$ produced in the outer box is quantum nonlocal when the quantum behavior $\{p(a^{id}, b^{id}|xy)\}$ is produced in the inner box using the state ρ_g and measurement settings $\{A_0^g, A_1^g, B_0^g, B_1^g\}$ for $\theta \approx 1.13557$.

The allowed values of the pair (η, δ) for which $p(a^{ob}, b^{ob}|xy)$ is quantum nonlocal shown in Fig. 5.4. In Fig. 5.4 we observe that for $\delta = 0$ the minimum detection efficiency $\eta_{crit} \approx 0.92$ is required to ensure $p(a^{ob}, b^{ob}|xy)$ is quantum nonlocal. We also observe that η_{crit} increases monotonically with increase in δ.

5.4 The Tilted Bell inequality

The AMP tilted Bell inequality is given as [11]

$$I_\alpha^\beta := \beta\langle x_1\rangle + \alpha\langle x_1 y_1\rangle + \alpha\langle x_1 y_2\rangle + \langle x_2 y_1\rangle - \langle x_2 y_2\rangle \leq \beta + 2\alpha. \tag{5.34}$$

It plays an important role in (a) demonstrating the inequivalence between the amount of certified randomness and the amount of nonlocality [11], (b) self-testing of all bipartite pure entangled states [174], (c) protocol for device-independent quantum random number generation with sublinear amount of quantum communication [175], (d) unbounded randomness certification from a single pair of entangled qubits with sequential measure-

ments [176].

Modified local bound for the AMP tilted Bell inequality

We consider the AMP tilted-Bell inequality introduced in [11] and given by,

$$I_\alpha^\beta = \beta\langle x_1\rangle + \alpha\langle x_1y_1\rangle + \alpha\langle x_1y_2\rangle + \langle x_2y_1\rangle - \langle x_2y_2\rangle \tag{5.35}$$

The determinism assumption states that the measurement outcomes are deterministic functions of the choice of settings and the hidden variable λ, i.e., $a = A(x,\lambda)$ and $b = B(x,\lambda)$ with $p(a|x\lambda) = \delta_{a,A(x,\lambda)}$ and $p(b|y\lambda) = \delta_{b,B(y,\lambda)}$. If we assume that the choice of the measurement settings on the side of Alice and Bob can depend on some hidden variable, λ, the correlations of Alice and Bob can be expressed as

$$\langle xy\rangle = \int \mathrm{d}\lambda p(\lambda|x,y)A(x,\lambda)B(y,\lambda). \tag{5.36}$$

The correlation function of Alice can also be written as

$$\langle x\rangle = \int \mathrm{d}\lambda p(\lambda|x)A(x,\lambda). \tag{5.37}$$

Applying Eq. (5.36) and Eq. (5.37) to Eq. (5.35) we have

$$\begin{aligned} I_\alpha^\beta \quad &= \beta\int \mathrm{d}\lambda p(\lambda|x_1)A(x_1,\lambda) + \alpha\int \mathrm{d}\lambda p(\lambda|x_1,y_1)A(x_1,\lambda)B(y_1,\lambda) \\ &+ \alpha\int \mathrm{d}\lambda p(\lambda|x_1,y_2)A(x_1,\lambda)B(y_2,\lambda) + \int \mathrm{d}\lambda p(\lambda|x_2,y_1)A(x_2,\lambda)B(y_1,\lambda) \\ &- \int \mathrm{d}\lambda p(\lambda|x_2,y_2)A(x_2,\lambda)B(y_2,\lambda). \end{aligned} \tag{5.38}$$

Adding and subtracting the terms

$$\alpha\int \mathrm{d}\lambda p(\lambda|x_1,y_2)A(x_1,\lambda)B(y_1,\lambda) \text{ and}$$
$$\int \mathrm{d}\lambda p(\lambda|x_2,y_2)A(x_2,\lambda)B(y_1,\lambda)$$

to Eq. (5.38) we obtain

$$\begin{aligned} I_\alpha^\beta \quad &= \beta \int \mathrm{d}\lambda p(\lambda|x_1)A(x_1,\lambda) + \alpha \int \mathrm{d}\lambda A(x_1,\lambda)B(y_1,\lambda)\Big[p(\lambda|x_1,y_1) - p(\lambda|x_1,y_2)\Big] \\ &+ \int \mathrm{d}\lambda A(x_2,\lambda)B(y_1,\lambda)\Big[p(\lambda|x_2,y_1) - p(\lambda|x_2,y_2)\Big] \\ &+ \alpha \int \mathrm{d}\lambda p(\lambda|x_1,y_2)\Big[A(x_1,\lambda)B(y_2,\lambda) + A(x_1,\lambda)B(y_1,\lambda)\Big] \\ &- \int \mathrm{d}\lambda p(\lambda|x_2,y_2)\Big[A(x_2,\lambda)B(y_2,\lambda) - A(x_2,\lambda)B(y_1,\lambda)\Big]. \end{aligned} \tag{5.39}$$

We observe that Eq. (5.39) is bounded by $I_\alpha^\beta \leq \max[T_1] + \max[T_2] + \max[T_3]$. We also note that as $p(\lambda|x_1)$ is a normalised probability distribution, $\int \mathrm{d}\lambda p(\lambda|x_1) = 1$. This implies that the maximum value of the quantity $\beta \int \mathrm{d}\lambda p(\lambda|x_1)A(x_1,\lambda)$ is given by β when $A(x_1,\lambda)$ is set to 1. With these observations, T_1 can be simplified as

$$\begin{aligned} T_1 = \quad & \beta \int \mathrm{d}\lambda p(\lambda|x_1)A(x_1,\lambda) \\ & +\alpha \int \mathrm{d}\lambda A(x_1,\lambda)B(y_1,\lambda)\Big[p(\lambda|x_1,y_1) - p(\lambda|x_1,y_2)\Big] \leq \beta + \alpha M_2. \end{aligned} \tag{5.40}$$

where we have set $B(y_1,\lambda) = 1$. To evaluate the maximum value of T_2 we set $A(x_2,\lambda) = 1$ and obtain

$$T_2 = \int \mathrm{d}\lambda A(x_2,\lambda)B(y_1,\lambda)\Big[p(\lambda|x_2,y_1) - p(\lambda|x_2,y_2)\Big] \leq M_2. \tag{5.41}$$

We evaluate T_3 as follows,

$$\begin{aligned} T_3 \quad &= \alpha \int \mathrm{d}\lambda p(\lambda|x_1,y_2)\Big[A(x_1,\lambda)B(y_2,\lambda) + A(x_1,\lambda)B(y_1,\lambda)\Big] \\ &- \int \mathrm{d}\lambda p(\lambda|x_2,y_2)\Big[A(x_2,\lambda)B(y_2,\lambda) - A(x_2,\lambda)B(y_1,\lambda)\Big] \\ &= \int \mathrm{d}\lambda A(x_1,\lambda)B(y_2,\lambda)\Big[\alpha p(\lambda|x_1,y_2) - p(\lambda|x_2,y_2)\frac{A(x_2,\lambda)}{A(x_1,\lambda)}\Big] \\ &+ \int \mathrm{d}\lambda A(x_1,\lambda)B(y_1,\lambda)\Big[\alpha p(\lambda|x_1,y_2) + p(\lambda|x_2,y_2)\frac{A(x_2,\lambda)}{A(x_1,\lambda)}\Big]. \end{aligned} \tag{5.42}$$

To get the maximum value of T_3, we set the values of $A(x_1,\lambda), B(y_1,\lambda), A(x_1,\lambda), B(y_2,\lambda)$ to one. This then implies,

$$T_3 = \int \mathrm{d}\lambda\Big[\alpha p(\lambda|x_1,y_2) - p(\lambda|x_2,y_2)\Big] + \int \mathrm{d}\lambda\Big[\alpha p(\lambda|x_1,y_2) + p(\lambda|x_2,y_2)\Big]. \tag{5.43}$$

We evaluate the first term of the Eq. (5.43) as

$$\begin{aligned}
& \int \mathrm{d}\lambda\Big[\alpha p(\lambda|x_1,y_2) - p(\lambda|x_2,y_2)\Big] \\
= & \int \mathrm{d}\lambda\Big[\alpha p(\lambda|x_1,y_2) - \alpha p(\lambda|x_2,y_2) + \alpha p(\lambda|x_2,y_2) - p(\lambda|x_2,y_2)\Big] && (5.44)\\
= & \int \mathrm{d}\lambda\Big[\alpha\Big(p(\lambda|x_1,y_2) - p(\lambda|x_2,y_2)\Big) + (\alpha-1)p(\lambda|x_2,y_2)\Big] && (5.45)\\
= & \ \alpha \int \mathrm{d}\lambda\Big[p(\lambda|x_1,y_2) - p(\lambda|x_2,y_2)\Big] + (\alpha-1)\int \mathrm{d}\lambda p(\lambda|x_2,y_2). && (5.46)
\end{aligned}$$

In Eq. (5.46) we note that

$$\alpha \int \mathrm{d}\lambda\Big(p(\lambda|x_1,y_2) - p(\lambda|x_2,y_2)\Big) \leq \alpha M_1.$$

We note that as $p(\lambda|x_2,y_2)$ is a normalised probability distribution, $\int \mathrm{d}\lambda p(\lambda|x_2,y_2) = 1$. This then implies

$$\int \mathrm{d}\lambda\Big[\alpha p(\lambda|x_1,y_2) - p(\lambda|x_2,y_2)\Big] \leq \alpha M_1 + \alpha - 1, \tag{5.47}$$

which on simplification reduces to

$$\int \mathrm{d}\lambda\Big[\alpha p(\lambda|x_1,y_2) - p(\lambda|x_2,y_2)\Big] \leq \alpha(M_1+1) - 1. \tag{5.48}$$

We proceed in the same way for the second term in Eq. (5.43) as follows,

$$\begin{aligned} & \int \mathrm{d}\lambda \Big[\alpha p(\lambda|x_1, y_2) + p(\lambda|x_2, y_2)\Big] \\ = & \int \mathrm{d}\lambda \Big[\alpha p(\lambda|x_1, y_2) + \alpha p(\lambda|x_2, y_2) - \alpha p(\lambda|x_2, y_2) + p(\lambda|x_2, y_2)\Big] && (5.49) \\ = & \int \mathrm{d}\lambda \alpha \Big[p(\lambda|x_1, y_2) + p(\lambda|x_2, y_2)\Big] - (\alpha - 1) \int \mathrm{d}\lambda p(\lambda|x_2, y_2) && (5.50) \\ = & \alpha \int \mathrm{d}\lambda \Big[p(\lambda|x_1, y_2) + p(\lambda|x_2, y_2)\Big] + (1 - \alpha) \int \mathrm{d}\lambda p(\lambda|x_2, y_2). && (5.51) \end{aligned}$$

We note that as $p(\lambda|x_1, y_2)$, $p(\lambda|x_2, y_2)$ are normalised probability distributions, $\int \mathrm{d}\lambda p(\lambda|x_1, y_2) = 1$ and $\int \mathrm{d}\lambda p(\lambda|x_2, y_2) = 1$. This then implies

$$\int \mathrm{d}\lambda \Big[\alpha p(\lambda|x_1, y_2) + p(\lambda|x_2, y_2)\Big] = \alpha + 1. \tag{5.52}$$

If we insert Eq. (5.48) and Eq. (5.52) in Eq. (5.43), we obtain

$$T_3 \leq \alpha(M_1 + 2). \tag{5.53}$$

Now combining Eq. (5.40), Eq. (5.41) and Eq. (5.53), we have the bound on I_α^β as

$$\begin{aligned} I_\alpha^\beta & \leq T_1 + T_2 + T_3 && (5.54) \\ & \leq \beta + \alpha M_2 + M_2 + \alpha(M_1 + 2) && (5.55) \\ & \leq \beta + 2\alpha + \alpha M_1 + (\alpha + 1)M_2 && (5.56) \\ & \leq \beta + 2\alpha + \alpha(M_1 + M_2) + M_2. && (5.57) \end{aligned}$$

We again start by considering Eq. (5.38) as

$$\begin{aligned} I_\alpha^\beta = \; & \beta \int \mathrm{d}\lambda p(\lambda|x_1) A(x_1, \lambda) + \alpha \int \mathrm{d}\lambda p(\lambda|x_1, y_1) A(x_1, \lambda) B(y_1, \lambda) \\ & + \alpha \int \mathrm{d}\lambda p(\lambda|x_1, y_2) A(x_1, \lambda) B(y_2, \lambda) + \int \mathrm{d}\lambda p(\lambda|x_2, y_1) A(x_2, \lambda) B(y_1, \lambda) \\ & - \int \mathrm{d}\lambda p(\lambda|x_2, y_2) A(x_2, \lambda) B(y_2, \lambda). \end{aligned} \tag{5.58}$$

Adding and subtracting the terms $\alpha \int d\lambda p(\lambda|x_2, y_1)A(x_1, \lambda)B(y_1, \lambda)$ and $\alpha \int d\lambda p(\lambda|x_2, y_2)A(x_1, \lambda)B(y_2, \lambda)$ to Eq. (5.38) we obtain

$$\begin{aligned} I_\alpha^\beta \quad &= \beta \int d\lambda p(\lambda|x_1)A(x_1, \lambda) + \alpha \int d\lambda A(x_1, \lambda)B(y_1, \lambda)\Big[p(\lambda|x_1, y_1) - p(\lambda|x_2, y_1)\Big] \\ &\quad + \alpha \int d\lambda A(x_1, \lambda)B(y_2, \lambda)\Big[p(\lambda|x_1, y_2) - p(\lambda|x_2, y_2)\Big] \\ &\quad + \int d\lambda A(x_2, \lambda)B(y_1, \lambda)\Big[p(\lambda|x_2, y_1) - \frac{B(y_2, \lambda)}{B(y_1, \lambda)}p(\lambda|x_2, y_2)\Big] \\ &\quad + \alpha \int d\lambda A(x_1, \lambda)B(y_1, \lambda)\Big[p(\lambda|x_2, y_1) + \frac{B(y_2, \lambda)}{B(y_1, \lambda)}p(\lambda|x_2, y_2)\Big]. \end{aligned} \tag{5.59}$$

We observe that Eq. (5.59) is bounded by $I_\alpha^\beta \leq \max[t_1] + \max[t_2] + \max[t_3]$. We also note that as $p(\lambda|x_1)$ is a normalised probability distribution, $\int d\lambda p(\lambda|x_1) = 1$. This implies that the maximum value of the quantity $\beta \int d\lambda p(\lambda|x_1)A(x_1, \lambda)$ then takes the value of β when $A(x_1, \lambda)$ is set to 1. With these observations, t_1 can be simplified as,

$$\begin{aligned} t_1 \quad &= \beta \int d\lambda p(\lambda|x_1)A(x_1, \lambda) \\ &\quad + \alpha \int d\lambda A(x_1, \lambda)B(y_1, \lambda)\Big[p(\lambda|x_1, y_1) - p(\lambda|x_2, y_1)\Big] \leq \beta + \alpha M_1. \end{aligned} \tag{5.60}$$

Similarly, t_2 can be simplified as

$$t_2 \quad = \alpha \int d\lambda A(x_1, \lambda)B(y_2, \lambda)\Big[p(\lambda|x_1, y_2) - p(\lambda|x_2, y_2)\Big] \leq \alpha M_1, \tag{5.61}$$

and for t_3, we have the expression

$$\begin{aligned} t_3 \quad &= \int d\lambda A(x_2, \lambda)B(y_1, \lambda)\Big[p(\lambda|x_2, y_1) - \frac{B(y_2, \lambda)}{B(y_1, \lambda)}p(\lambda|x_2, y_2)\Big] \\ &\quad + \alpha \int d\lambda A(x_1, \lambda)B(y_1, \lambda)\Big[p(\lambda|x_2, y_1) + \frac{B(y_2, \lambda)}{B(y_1, \lambda)}p(\lambda|x_2, y_2)\Big]. \end{aligned} \tag{5.62}$$

We set the values of $A(x_1, \lambda), B(y_1, \lambda), A(x_2, \lambda), B(y_2, \lambda)$ to one and obtain

$$t_3 \quad = \int d\lambda\Big[p(\lambda|x_2, y_1) - p(\lambda|x_2, y_2)\Big] + \alpha \int d\lambda\Big[p(\lambda|x_2, y_1) + p(\lambda|x_2, y_2)\Big]. \tag{5.63}$$

The first term in Eq, (5.63) is bounded by

$$\int \mathrm{d}\lambda \Big[p(\lambda|x_2, y_1) - p(\lambda|x_2, y_2) \Big] \leq M_2. \tag{5.64}$$

We note that as $p(\lambda|x_2, y_1)$ and $p(\lambda|x_2, y_2)$ are normalised probability distribution, $\int \mathrm{d}\lambda p(\lambda|x_2, y_1) = 1$ and $\int \mathrm{d}\lambda p(\lambda|x_2, y_2) = 1$. Eq. (5.63) is then expressed as

$$t_3 \leq M_2 + 2\alpha. \tag{5.65}$$

Now combining the values of t_1, t_2 and t_3, we have the bound on I_α^β as

$$\begin{aligned} I_\alpha^\beta &\leq t_1 + t_2 + t_3 && (5.66)\\ &\leq \beta + \alpha M_1 + \alpha M_1 + M_2 + 2\alpha && (5.67)\\ &\leq \beta + 2\alpha + 2\alpha M_1 + M_2. && (5.68) \end{aligned}$$

We note that the bound on I_α^β must be the minimum of Eqs. (5.57) and (5.68) and is expressed as

$$I_\alpha^\beta \leq \beta + 2\alpha + \alpha[M_1 + \min\{M_1, M_2\}] + M_2. \tag{5.69}$$

We observe that for the case of $\beta = 0$ and $\alpha = 1$,

$$I_1^0 \leq 2 + M_1 + M_2 + \min\{M_1, M_2\}, \tag{5.70}$$

which is in agreement with that obtained in [10]. We note that the maximum value that I_α^β [Eq. (5.35)] can take is $\beta + 2\alpha + 2$ (We get this bound by setting $\langle x_1 \rangle = 1$, $\langle x_1 y_1 \rangle = 1$, $\langle x_1 y_2 \rangle = 1$, $\langle x_2 y_1 \rangle = 1$, $\langle x_2 y_2 \rangle = -1$) and arrive at

$$I_\alpha^\beta \leq \beta + 2\alpha + \min\{\alpha(M_1 + \min\{M_1, M_2\}) + M_2, 2\}. \tag{5.71}$$

In the following proposition, we obtain the bound on I_α^β when the measurement independence assumption is relaxed (see Appendix 5.4 for proof).

Proposition 6. *The AMP tilted Bell expression I_α^β in the presence of locality and the*

relaxed measurement independence is bounded by

$$I_\alpha^\beta \leq \beta + 2\alpha + \min\{\alpha(M_1 + \min\{M_1, M_2\}) + M_2, 2\}, \tag{5.72}$$

where M_1 and M_2 are the measurement dependence parameters for Alice and Bob.

Comparison of one-sided and two-sided measurement dependence to ensure quantum representation

Let Alice and Bob have free will in choosing the measurement settings, then the maximum violation of I_α^β obtained by quantum nonlocal behaviors is given by [11]

$$I_\alpha^\beta \leq 2\sqrt{(1+\alpha^2)(1+\frac{\beta^2}{4})}. \tag{5.73}$$

As direct consequences of Proposition 6, we have the following corollaries.

Corollary 1. *When $M_1 = M_2 = M$, the quantum nonlocal behaviors that maximally violate Eq. (5.34) with the amount of violation given by the RHS of Eq. (5.73), remains nonlocal for*

$$M < \frac{-2\alpha - \beta + \sqrt{(1+\alpha^2)(4+\beta^2)}}{1+2\alpha}. \tag{5.74}$$

For $\alpha = 1$ and $\beta = 0$ (the Bell-CHSH inequality), Eq. (5.74) reduces to $M < \frac{2}{3}(\sqrt{2}-1) \approx 0.276$ and is consistent with the observation in [10].

Corollary 2. *When $M_1 = 0$ and $M_2 = M$, the quantum nonlocal behaviors that maximally violate Eq. (5.34) with the amount of violation given by the RHS of Eq. (5.73), remains nonlocal for*

$$M < -2\alpha - \beta + \sqrt{(1+\alpha^2)(4+\beta^2)}. \tag{5.75}$$

For $\beta = 0$ and $\alpha = 1$ (the Bell-CHSH inequality), Eq. (5.75) reduces to $M < 2(\sqrt{2}-1) \approx 0.828$ and is consistent with the observation in [10].

Corollary 3. *When $M_1 = M$ and $M_2 = 0$, the quantum nonlocal behaviors that maximally violate Eq. (5.34) with the amount of violation given by the RHS of Eq. (5.73), remains*

nonlocal for

$$M < \frac{1}{\alpha}(-2\alpha - \beta + \sqrt{(1+\alpha^2)(4+\beta^2)}). \tag{5.76}$$

For $\beta = 0$ and $\alpha = 1$ (the Bell-CHSH inequality), Eq. (5.76) reduces to $M < 2(\sqrt{2} - 1) \approx 0.828$ and is consistent with the observation in [10].

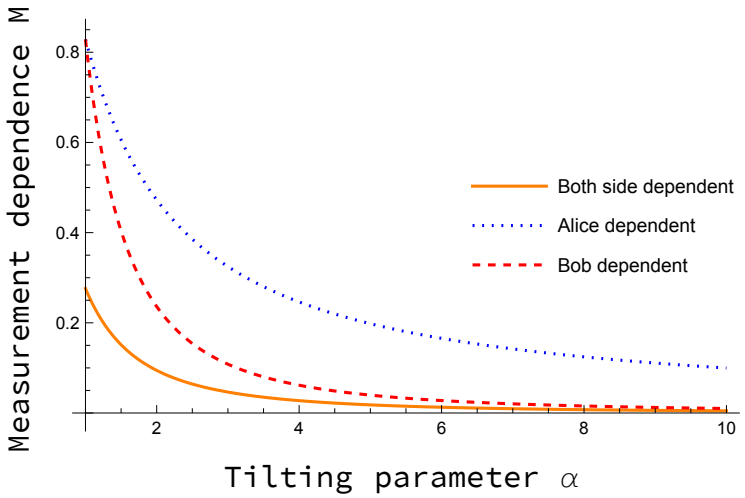


Figure 5.5: In this figure, we consider $\beta = 0$ and plot the maximum values of the measurement dependence parameter M as a function of the tilting parameter α in Eq.(5.34). The values of M and α in this figure ensure that the quantum nonlocal behaviors that maximally violate Eq. (5.34) remain nonlocal for the cases of (a) both-sided measurement dependence (in orange) (b) only Alice has measurement dependence (in dotted blue line) (c) only Bob has measurement dependence (in the dashed red line.)

In Fig. 5.5, we plot an upper bound on M as a function of α for MDL violating behaviors when $\beta = 0$ and $\alpha \geq 1$. The values of M and α from Fig. 5.5 ensure that the quantum nonlocal behaviors that maximally violate Eq. (5.34) remain nonlocal in the presence of measurement dependence.

We observe in Fig. 5.5 that for $\beta = 0$ and $\alpha \geq 1$, the introduction of one-sided measurement dependence allows for higher values of M (implying a lower degree of freedom-of-choice) as compared to introducing both-sided measurement dependence. Also, for the case of one-sided measurement dependence, Alice can have higher values of M as compared to Bob.

Bounds on the measurement dependence for testing nonlocality

We observe in Proposition 6 that in the presence of relaxed measurement dependence, the behaviors $\{p(ab|xy)\}$, that violates Eq. (5.77) are nonlocal.

$$I_\alpha^\beta \leq \beta + 2\alpha + \min\{\alpha(M_1 + \min\{M_1, M_2\}) + M_2, 2\} \tag{5.77}$$

In the following, we discuss some of the cases where Eq. (5.77) can be violated.

a. We consider a situation when both Alice and Bob have the same measurement dependence, we have $M_1 = M_2 = M$. For this case, violating Eq. (5.77) requires

$$I_\alpha^\beta > \beta + 2\alpha + \min\{(2\alpha + 1)M, 2\}. \tag{5.78}$$

If $(2\alpha+1)M \geq 2$, I_α^β reaches the no-signalling boundary. Whereas, if $(2\alpha+1)M < 2$, then Eq. (5.78) reduces to inequality

$$M < \frac{I_\alpha^\beta - \beta - 2\alpha}{2\alpha + 1}. \tag{5.79}$$

b. We consider the situation where only Bob has measurement dependence; we have $M_1 = 0, M_2 = M$. For this case, violating Eq. (5.77) requires

$$I_\alpha^\beta > \beta + 2\alpha + \min\{M, 2\}. \tag{5.80}$$

If $M = 2$, I_α^β reaches the no-signalling boundary. Whereas, if $M < 2$, then Eq. (5.80) to the inequality

$$M < I_\alpha^\beta - \beta - 2\alpha. \tag{5.81}$$

c. We consider the situation where only Alice has measurement dependence; we have $M_1 = M, M_2 = 0$. For this case, violating Eq. (5.77) requires

$$I_\alpha^\beta > \beta + 2\alpha + \min\{\alpha M, 2\}. \tag{5.82}$$

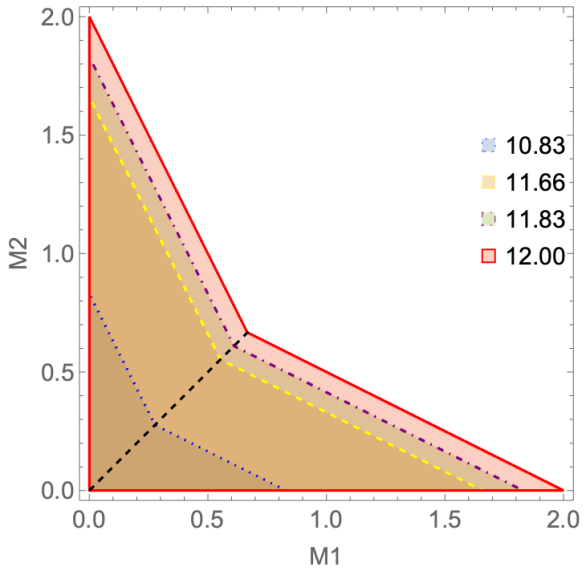


Figure 5.6: In this figure, we plot the values of the measurement dependence parameters M_1 and M_2 for which the violation of Eq. (5.34) given by $I_\alpha^\beta = I'(\alpha = 1, \beta = 8, \mathbf{P}') \in \{10.83, 11.66, 11.83, 12.00\}$ cannot be described by a deterministic MDL model. The correlations violating Eq. (5.34) with (a) $I_\alpha^\beta = 12.00$ belong to the no-signalling boundary (shown enclosed by the red line) (b) $I_\alpha^\beta = 11.66$ belong to the quantum boundary (shown enclosed by the dashed yellow line) (c) $I_\alpha^\beta = 10.83$ belong to the quantum set (shown enclosed by dotted blue line), and (d) $I_\alpha^\beta = 11.83$ belong to the no-signalling set (shown enclosed by the dot-dashed purple line). The black line in the figure denotes equal values of M_1 and M_2 in the regions (a), (b), (c), and (d).

If $\alpha M \geq 2$, I_α^β reaches the no-signalling boundary. Whereas if $\alpha M < 2$, then Eq. (5.82) reduces to the inequality

$$M < \frac{I_\alpha^\beta - \beta - 2\alpha}{\alpha}. \tag{5.83}$$

We note that for $\alpha = 1$ and $\beta = 0$, i.e., for the Bell-CHSH inequality, the values of M_1 and M_2 that violates Eq. (5.77) are in agreement with that obtained in [10].

Consider there exists some behavior $\mathbf{P}' = \{p'(ab|xy)\}$ that violates Eq. (5.34) with the amount of violation given by $I_\alpha^\beta = I'(\alpha, \beta, \mathbf{P}')$. For $\alpha = 1, \beta = 8$, we show in Fig. 5.6 the possible values of measurement dependence parameters M_1 and M_2 for which the amount of violation of Eq. (5.34) given by I' cannot be described by a deterministic measurement dependent local model. The plots for the other combinations of (α, β) are given in Appendix 5.4.

Bounds on the measurement dependence to certify nonlocality

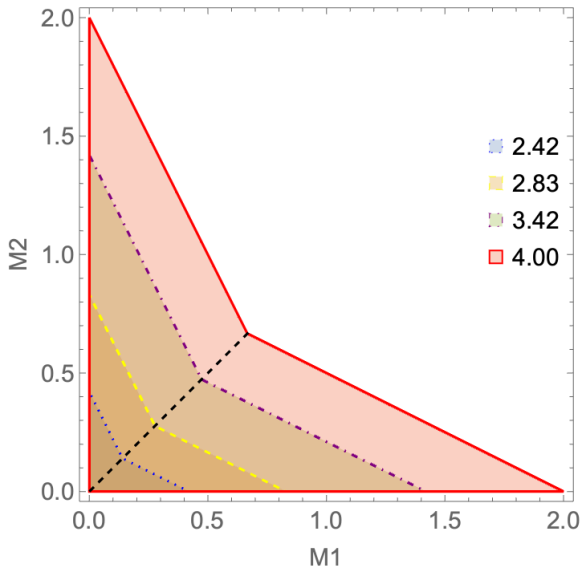


Figure 5.7: In this figure, we plot the values of the measurement dependence parameters M_1 and M_2 for which the violation of Eq. (5.34) given by $I_\alpha^\beta = I'(\alpha = 1, \beta = 0, \mathbf{P}') \in \{4.00, 3.42, 2.83, 2.42\}$ cannot be described by a deterministic MDL model. The correlations violating Eq. (5.34) with (a) $I_\alpha^\beta = 4.00$ belong to the no-signalling boundary (shown enclosed by red) (b) $I_\alpha^\beta = 2.83$ belong to the quantum boundary (shown enclosed by the dashed yellow line) (c) $I_\alpha^\beta = 2.42$ belong to the quantum set (shown enclosed by blue dotted), and (d) $I_\alpha^\beta = 3.42$ belong to the no-signalling set (shown enclosed by the dot-dashed purple line). The black line in the figure denotes equal values of M_1 and M_2 in the regions (a), (b), (c), and (d).

We observe in Proposition 6 that in the presence of relaxed measurement dependence, the behaviors $\{p(ab|xy)\}$, that violates Eq. (5.84) are nonlocal.

$$I_\alpha^\beta \leq \beta + 2\alpha + \min\{\alpha(M_1 + \min\{M_1, M_2\}) + M_2, 2\} \tag{5.84}$$

Consider there exists some behavior $\mathbf{P}' = \{p'(ab|xy)\}$ that violates Eq. (5.34) with the amount of violation given by $I_\alpha^\beta = I'(\alpha, \beta, \mathbf{P}')$. We show in Fig. 5.7 the possible values of measurement dependence parameters M_1 and M_2 for which the amount of violation of Eq. (5.34) given by I' cannot be described by a deterministic measurement dependent local model. We observe that Fig. (5.7) agrees with that obtained in [10].

5.5 Discussion

In this chapter, two different approaches in quantifying measurement dependence via parameters l and (M_1, M_2) from standard literature are presented. A bound on these parameters for certifying nonlocality of different behaviors is obtained. It is observed that the behavior certifying close to 2 bits of randomness remains measurement-dependent nonlocal only in the limit of complete measurement independence, i.e., in the limit of $l \to 0.25$. The behavior that provides 1.6806 bits of global randomness from the violation of the tilted Hardy relations is measurement-dependent nonlocal for arbitrarily small values of l.

Deviating from the conventional approach of assuming perfect detectors, we present a framework to determine the threshold values of the detector parameters that are robust enough to certify nonlocality of given quantum behaviors. This is an important step towards experimentally obtaining nonlocality in the presence of relaxed measurement independence. For an illustration, we presented the critical requirements for generating 1.6806 bits of tilted-Hardy certified global randomness. The detector parameters obtained from this study are expected to have important applications in experimentally implementing various information-processing tasks that rely on quantum nonlocality as a resource.

The modified analytical bound on the AMP tilted Bell inequality in terms of M_1 and M_2 has been obtained. Using the analytical bound, the bounds on M_1 and M_2 to ensure quantumness and nonlocality are observed. It is observed that one-sided measurement dependence is more advantageous from the point of view of the user as compared to two-sided measurement dependence. The analytical bound obtained is expected to have applications in self-testing of quantum states and other device-independent information processing protocols like randomness generation and secure communication.

CHAPTER 6

SUMMARY AND OUTLOOK

"Vivere est Cogitare."

— Marcus Tullius Cicero

6.1 Summary

The power of abstraction in graph (network) theory [99, 105] that provides a general formalism to analyze networks without getting into specific details of implementation [106], motivates the use of graph-theoretic tools in analyzing the scalability and robustness of a global scale quantum Internet. Focusing on the robustness of networks, we present figures of merit for comparing different network topologies. We also apply ideas from percolation theory [108–110] to discuss the robustness of networks formed when performing a class of information processing tasks over any lattice network (sufficiently large graph).

One might find the level of abstraction quite high. However, it is justified by the fact that we consider a system, be it a network or processor, as the one *after* any technological improvement involving repeater techniques or fault-tolerant quantum computing. No matter how they are defined, the resulting output state will never be ideal but can only be close to ideal at best. For example, in some cases of practical interests, these final states can be modelled (in the case of links) as an isotropic state: an ideal maximally entangled state mixed with the maximally mixed state (a useless noisy state) with some non-zero probability.

Considering the currently available quantum processors by Google [39], IBM [37, 120] and Rigetti [38] as real-world instances of graphical networks, we observe that the 54-qubit square topology of the Sycamore processor developed by Google [39] has the highest node connection strength and the lowest link sparsity. With the possibility of having a 1024-qubit quantum processor in the future, we extend the 54-qubit Sycamore processor layout to include 1024 qubits and present its figures of merit.

The information-processing tasks that will be implemented using the quantum Internet will determine its structure. The building blocks for the structure of any network are the elementary links connecting two nodes of the network. It is, therefore, important to assess the limitations at the elementary link scale. To do this, we present the critical success probability of the elementary links for performing some desired information processing tasks. Extending to a more general repeater-based network with memory, we present a

trade-off between the channel length and time spent at the nodes such that the state shared by the end nodes remains useful for various tasks.

There is a strong motivation to enable remote places to securely access quantum processors via the quantum Internet and perform delegated quantum computing [132–134] over the quantum Internet as it is less resource extensive on the individual user. To illustrate this, we may assume an instance where a user with limited computing resources in Bangalore requests to securely access the IBM Quantum Hub at Poznań [167] via the quantum Internet. Enabling secure access requires the sharing of entangled states among distant nodes [4, 125, 127, 177–180] along with performing secure cryptographic tasks against adversaries. We present limitations involved in implementing these tasks. In particular, we present limitations on using isotropic state [94] for distilling secret keys via DI-QKD protocols [28, 29] over the quantum Internet. We provide upper bounds on the number of elementary links between the end nodes for performing secure communication and information-processing tasks.

We show that a region of a (possibly infinite) network has a bounded size (graph theoretically bounded diameter). Namely, any two nodes can be connected by entanglement swapping to produce a device-independent key by so-called standard protocols only if the nodes are closer to each other than the critical distance d_{crit}^{DIQKD}, which is always finite. It is a consequence of the recently discovered fact that even states exhibiting quantum nonlocality may have zero device-independent key secure against quantum adversary [160]. Our result can be phrased as no-percolation for DI-QKD networks in graph-theoretic language.

Assuming some scheme can mitigate losses and improve transmittance over a quantum channel (see Assumption 1), we present limitations on the scalability of networks for performing quantum communication and implementing DI-QKD protocols. In particular, we present limitations on performing DI-QKD between two end nodes at a continental scale of distances and connected by repeater-based elementary links of metropolitan scale (see Example 4). Considering performing quantum communication over a lattice with optical fiber-based elementary links, we present limitations on its scalability (see Observation 2).

These illustrate how far the current technology is from designing quantum networks for information processing tasks.

For long-distance communication over the continental scale of (order of 1000 km) distances, the losses in transmission of optical signals over free space are significantly lower as compared to an optical fiber (see Fig. A.3), making it better suited for distributing entangled states between far-off places. In this work, we present practical bottlenecks in realising such networks (see Fig. 4.14 and 4.15). As a potential application of the satellite-based network, we present the entanglement yield (see Fig. 4.18) and figures of merit of a global mesh network having 3462 major airports across the globe as nodes and 25482 airplane routes as edges connecting the major airports in the world. For such an airport network, we present the entanglement yield considering currently available and desirable technology available in the future. Looking at short-distance communication over the regional scale (order of 100 km), we present an instance of secure communication between a central agency and end parties. It may be desirable here for the central agency to prevent direct communication between the end parties. We consider a fiber-based star network for this task and present bottlenecks in its implementation (see Fig. 4.19).

Certain underlying network tasks need to be performed to implement secure communication and share entanglement between the end nodes. We present algorithms for implementing these network tasks. An important task is constructing the network structure to connect groups of network nodes. Once we obtain the network structure, we need the network path connecting two end nodes to enable sharing of resources among them. In a general network, buffer nodes connecting multiple input and output channels may be present. The input channels may request to store resources at the buffer nodes, while the output channels may request to extract resources stored in them. A strategy is required to allocate resources to and from the buffer nodes in the network. We provide algorithms to perform these network tasks.

Focusing on the point-to-point networks, we analyze the implications of imperfect detectors and constrained free will on the test of quantum nonlocal correlations. We adapt the approach discussed in [13] to model imperfect detectors for the Bell experiment as

a sequential application of a perfectly working inner box followed by a lossy outer box. The inner box contains a quantum source whose behavior is nonlocal under constrained free will, i.e., violates certain measurement-dependent LRHV inequality. The outer box separately introduces detector inefficiency and dark counts for each party. Using this model, we determine the threshold values of the detector parameters that make detectors robust for testing of quantum nonlocality under constrained free will (e.g., see Fig. 5.3 with details in Section 5.3). Next for the scenario of perfect detectors, we compare the implications of two different approaches presented in [7] and [9] to quantify measurement dependence (a) by bounding the probability of choosing the measurement settings x (for Alice's side) and y (for Bob's side) conditioned on a hidden variable λ to be in the range $[l, 1-3l]$ [7] and (b) by using a distance measure M to quantify measurement settings distinguishability [9]. This comparison is made in the 2 (party) - 2 (measurement settings per party) - 2 (outcome per measurement) scenario and their effects on the certification of the nonlocality. We also introduce a new set of measurement-dependent LRHV (MDL) inequalities by introducing distance-based measurement-dependent quantity in adapted AMP tilted Bell inequality [11] and discuss implications and trade-off between measurement dependence parameters and tilted parameters for the certification of quantum nonlocal correlations.

6.2 Outlook

The analysis presented in this thesis opens up many prospects for future works. We discuss some of them next.

1. A possible future direction will be to analyze the practical limitations and design distributed algorithms for the simultaneous allocation of multi-party resources among the end users while providing certain guarantees, such as fair treatment for the users. A step towards that direction could be to analyze the repeater-based mesh network topology for entanglement distribution using the theory of decision processes [181] and reinforcement learning techniques [182] building on prior

works [125, 127].

2. We have analysed the limitations of sharing nonlocality between the two nodes when an adversary biases the choice of measurement setting and the detection units of the two nodes. In our analysis, we have limited ourselves to the simplest scenario of each party having two measurements, each producing one of two possible outcomes. The natural next step would be to analyze the implications of measurement dependence in multipartite Bell-type inequalities [65, 74] for the certification of multipartite nonlocality and device-independent conference keys [183–185].

3. We have compared two approaches in standard literature to quantify the adversarial role in the choice of measurement settings for Alice and Bob. The first approach involves bounding the probability of choice of measurement settings conditioned on a hidden variable to be in a specific range [7, 8] while the second approach involves quantifying the measurement dependence using a distance measure [9, 10, 83]. We have also modelled the biased detectors as a sequential application of a perfectly working inner box followed by a lossy outer box. In our model, the inner box contains a quantum source whose behaviour is nonlocal under constrained free will (violates an MD-LRHV inequality). The outer box introduces imperfections separately. A future direction would be unifying the two approaches of measurement dependence along with the model of imperfect detectors and obtaining a certifying inequality whose violation/validation would certify nonlocality in the presence of an adversary who biases the measurement settings and detection units.

4. We have observed that the behavior certifying close to 2 bits of randomness remains measurement-dependent nonlocal only in the limit of complete measurement independence, i.e., in the limit of $l \to 0.25$. The behavior that provides 1.6806 bits of global randomness from the violation of the tilted Hardy relations is measurement-dependent nonlocal for arbitrarily small values of l. An important future direction would be to explore the possibility of obtaining an inequality that provides close to two bits of global randomness (in the 2-2-2 scenario) in the limit of arbitrarily low measurement dependence.

Appendix A.

A.1 Dual rail encoding of photons

In the dual rail encoding scheme [186], the qubits are encoded using the optical modes[1] of photons. The computational basis of the photonic qubit system A encoded in the polarization modes m_1 and m_2 is given by

$$|H\rangle_A \rightarrow |1,0\rangle_{l_1,l_2},\ |V\rangle_A \rightarrow |0,1\rangle_{l_1,l_2}. \tag{A.1}$$

A pure state $|\psi\rangle_A$ of the qubit system can be expressed in such a computational basis as

$$|\psi\rangle_A = \alpha|1,0\rangle_{l_1,l_2} + \beta|0,1\rangle_{l_1,l_2} \tag{A.2}$$

$$= \alpha|H\rangle_A + \beta|V\rangle_A, \tag{A.3}$$

where $\alpha,\beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. The bipartite entangled state Ψ^+_{AB} is expressed as $\Psi^+_{AB} = |\Psi^+\rangle\langle\Psi^+|_{AB}$ where $|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|HH\rangle_{AB} + |VV\rangle_{AB})$.

[1] An optical mode of the photon is defined by the state space consisting of a superposition of number states.

A.2 Two qubit Bell measurement on isotropic states

Let there be a measurement station that performs standard Bell measurement on the halves of two-qubit isotropic states $\rho^I_{A_1A_1'}(p'(\lambda),2)$ and $\rho^I_{B_1B_1'}(p'(\lambda),2)$, where

$$\rho^I_{AB}(p'(\lambda),2) := \lambda\Psi^+_{AB} + (1-\lambda)\frac{\mathbb{1}_{AB}}{4}. \tag{A.4}$$

We call λ the visibility of the isotropic state $\rho^I_{AB}(p'(\lambda),2)$. Let the success probability of a standard Bell measurement be q. We denote the action of the noisy standard Bell measurement channel as

$$\begin{aligned}
&\mathcal{E}_{A_1'B_1'\to I_AI_A'I_BI_B'}\Big(\rho^I_{A_1A_1'}(p'(\lambda),2)\otimes\rho^I_{B_1B_1'}(p'(\lambda),2)\Big)\\
&\quad=\frac{\lambda^2 q}{4}\Big[\Psi^-_{A_1B_1}\otimes|00\rangle\langle 00|_{I_AI_B}+\Psi^+_{A_1B_1}\otimes|11\rangle\langle 11|_{I_AI_B}+\Phi^-_{A_1B_1}\otimes|22\rangle\langle 22|_{I_AI_B}\\
&\qquad\qquad+\Phi^+_{A_1B_1}\otimes|33\rangle\langle 33|_{I_AI_B}\Big]\otimes|00\rangle\langle 00|_{I_A'I_B'}\\
&\quad+(1-\lambda^2)q\frac{\mathbb{1}_{A_1B_1}}{4}\otimes\frac{1}{4}\sum_{i=0}^{3}|ii\rangle\langle ii|_{I_AI_B}\otimes|00\rangle\langle 00|_{I_A'I_B'}\\
&\quad+(1-q)\frac{\mathbb{1}_{A_1B_1}}{4}\otimes|\perp\rangle\langle\perp|_{I_AI_B}\otimes|11\rangle\langle 11|_{I_A'I_B'}.
\end{aligned}\tag{A.5}$$

The flag state $|11\rangle\langle 11|_{I_A'I_B'}$ indicates error in the standard Bell measurement with a probability $(1-q)$ and the state $\frac{\mathbb{1}_{A_1B_1}}{4}$ is left on $\mathcal{H}_{A_1B_1}$. The flag state $|00\rangle\langle 00|_{I_A'I_B'}$ indicates a successful standard Bell measurement with probability q. If error corrections are possible post-Bell measurement, then from a single use of repeater, we have the state

$$\rho^I_{AB}(p(q\lambda^2),2) = q\lambda^2\ \Psi^+_{AB} + (1-q\lambda^2)\frac{\mathbb{1}_{AB}}{4}. \tag{A.6}$$

A.3 Sparsity Index

Taking motivation from the Gini Index of network graphs [116] and using the definition of the connection strength of the nodes in a network, we define the sparsity index of the network.

Definition 22. *Consider the plot with the cumulative sum of the number of nodes in the network* $\mathcal{N}(G(\mathbb{V},\mathbb{E}))$ *along the horizontal axis and the cumulative sum of* $\zeta_i(G)$*s along the vertical axis. The sparsity index of the network* $\mathcal{N}$ *is given by*

$$\Xi(\mathcal{N}) = \frac{\textit{area enclosed by the curve and x-axis}}{\textit{area enclosed by the } 45^\circ \textit{ line}}. \tag{A.7}$$

As an example, the star network $\mathcal{N}_s(G_s(\mathbb{V},\mathbb{E}))$ (see Eq. (3.14)) with $N_v = 8$ and $p = 0.5$ have sparsity index 0.1934 for non-cooperative strategy and 0.3779 for cooperative strategy. The sparsity index $\Xi(\mathcal{N})$ of the network $\mathcal{N}$ measures the extent of inequality in the distribution of connection strength among the nodes of the network. High values of Ξ indicate a high cumulative percentage of connection strength for the cumulative fractile of the nodes. Typically, it is desirable for the network to have high values of sparsity index.

A.4 Actions of some quantum channels

A.4.1 The qubit depolarizing channel

The action of a qubit depolarizing channel [187] on the qubit density operator ρ_A is given by

$$\mathcal{D}_{A\to B}(\rho_A) = (1-p)\ \rho_B + p\ \frac{\mathbb{1}_B}{2}, \tag{A.8}$$

where $p \in [0, \frac{4}{3}]$ is the channel parameter and $\mathbb{1}_B$ is the identity operator. The effect of the channel can be defined by the following operators [188],

$$\mathcal{K}_0 = \sqrt{1-\frac{3p}{4}}\ \mathbb{1} \tag{A.9}$$

$$\text{and} \qquad \mathcal{K}_i = \frac{\sqrt{p}}{2}\ _i \text{ with } i \in \{1,2,3\}, \tag{A.10}$$

where σ_i are the Pauli matrices. The action of the depolarizing channel on each of the systems A and $\bar{A}$ is given by,

$$\begin{aligned}
&\mathcal{D}_{A\to B} \otimes \mathcal{D}_{\bar{A}\to\bar{B}}\left(\Psi^+_{A\bar{A}}\right) \\
&= \sum_{i=0}^{4}\sum_{j=0}^{4}\left(\mathcal{K}_i \otimes \mathcal{K}_j\right)\Psi^+_{A\bar{A}}\left(\mathcal{K}_i \otimes \mathcal{K}_j\right)^\dagger &\text{(A.11)}\\
&= (-1+p)^2\ \Psi^+_{B\bar{B}} + \ p\ (2-p)\ \frac{\mathbb{1}_{B\bar{B}}}{4} &\text{(A.12)}
\end{aligned}$$

Noting that $\mathbb{1}_{B\bar{B}}$ can be expressed as the sum of four maximally entangled states, we have the fidelity of the final state to the starting state as $\eta_d = 1 - \frac{3}{4}\ p\ (2-p)$. Following the approach of [127] and applying the depolarising channel n times, the final state after the evolution through the channel is

$$\rho^n_{B\bar{B}} = (\mathcal{D}_{A\to B} \otimes \mathcal{D}_{A\to B})^{\otimes n}\left(\Psi^+_{A\bar{A}}\right).$$

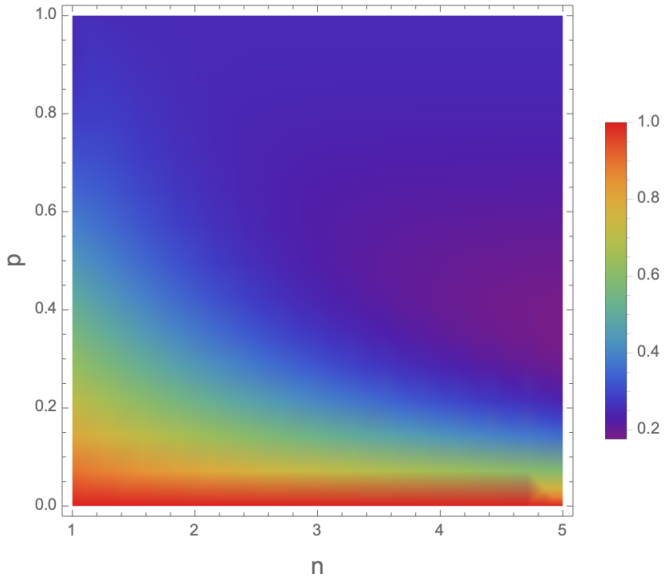


Figure A.1: In this figure, we plot the variation of η_d^n as a function of n and p.

This state $\rho^n_{B\bar{B}}$ has a fidelity with $\Psi^+_{B\bar{B}}$ given by

$$\eta_d^n = (1-p)^{2n} - \frac{1}{4}(p-2)p\left((n-1)(1-p)^{2(n-1)} + 1\right), \tag{A.13}$$

where it can be seen that $\eta_d^1 = \eta_d$. We plot in Fig. A.1 the variation of η_d^n (using Eq. (A.13)) as a function of the number of applications n of the depolarising channel and the depolarising channel parameter p.

A.4.2 The erasure channel

The action of a qubit erasure channel [189] on an input density operator ρ_A is given by

$$\mathcal{E}_{A\to B}(\rho_A) = \eta_e \rho_B + (1-\eta_e)\,\mathrm{Tr}[\rho_B]|e\rangle\langle e|_B. \tag{A.14}$$

The action of the erasure channel on the qubit system is such that it outputs the exact input state with probability η or with probability $1-\eta$ replaces it with erasure state $|e\rangle$, where $|e\rangle$ is the vacuum state. The action of the channel on the maximally entangled state $\Psi^+_{A\bar{A}}$

in the two-qubit space $A\bar{A}$ is given by

$$\mathcal{E}_{A\to B} \otimes \mathcal{E}_{\bar{A}\to\bar{B}} (\Psi^+_{A\bar{A}}) = \eta_e^2 \Psi^+_{B\bar{B}} + (1-\eta_e^2)\Psi^\perp_{B\bar{B}}, \tag{A.15}$$

where

$$\Psi^\perp_{B\bar{B}} := \frac{\eta_e}{1+\eta_e}\left(\frac{1}{2}\mathbb{1}_B \otimes |e\rangle\langle e|_{\bar{B}} + |e\rangle\langle e|_B \otimes \frac{1}{2}\mathbb{1}_{\bar{B}}\right) + \frac{1-\eta_e}{1+\eta_e}\,|e\rangle\langle e|_B \otimes |e\rangle\langle e|_{\bar{B}} \tag{A.16}$$

is a state orthogonal to $\Psi^+_{B\bar{B}}$.

Consider two sources creating pairs of entangled state Ψ^+. The first and second sources distribute the entangled pairs to node pairs (v_1, v_2) and (v_2, v_3) via erasure channels. The node v_2 then performs a Bell measurement on its share of states. Assuming error correction is possible post-measurement, the node pair (v_1, v_3) share the state Ψ^+ with probability η_e^2.

A.4.3 The qubit thermal channel

The action of a qubit thermal channel on the density operator ρ_A is given by

$$\mathcal{L}^{\eta_g, n_g}_{A\to B}(\rho_A) = \mathrm{Tr}_E[U_{\eta_g} \ (\rho_A \otimes \rho_E) \ U^\dagger_{\eta_g}], \tag{A.17}$$

where ρ_E is the density operator of the environment given by

$$\rho_E = (1-n_g)|0\rangle\langle 0|_E + n_g|1\rangle\langle 1|_E. \tag{A.18}$$

The qubit thermal channel is modelled by the interaction of a qubit system ρ_A with the environment ρ_E at a lossy beamsplitter having transmittance η_g (see Eq. (A.30)). The

evolution through the beamsplitter is via the unitary U_{η_g} expressed as

$$U_{\eta_g} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \sqrt{\eta_g} & \sqrt{1-\eta_g} & 0 \\ 0 & -\sqrt{1-\eta_g} & \sqrt{\eta_g} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{A.19}$$

The Generalised Amplitude Damping Channel (GADC) is equivalent to the qubit thermal channel up to the reparameterization $\mathcal{A}^{\eta_g,n_g}_{A\to B}(\rho_A) \equiv \mathcal{L}^{1-\eta_g,n_g}_{A\to B}(\rho_A)$ with $\eta_g \in [0,1]$ and $n_g \in [0,1]$. The effect of the thermal channel can be defined by the following Kraus operators in the standard basis

$$\widetilde{\mathcal{A}_1} = \sqrt{1-n_g}(|0\rangle\langle 0| + \sqrt{\eta_g}|1\rangle\langle 1|) \tag{A.20}$$

$$\widetilde{\mathcal{A}_2} = \sqrt{(1-\eta_g)(1-n_g)}|0\rangle\langle 1| \tag{A.21}$$

$$\widetilde{\mathcal{A}_3} = \sqrt{n_g}(\sqrt{\eta_g}|0\rangle\langle 0| + |1\rangle\langle 1|) \tag{A.22}$$

$$\widetilde{\mathcal{A}_4} = \sqrt{n_g(1-\eta_g)}|1\rangle\langle 0|. \tag{A.23}$$

The action of the thermal channel on each of the systems A and $\bar{A}$ is given by,

$$\begin{aligned} \mathcal{T}^{\eta_g,n_g}_{B\bar{B}} &:= \mathcal{L}^{\eta_g,n_g}_{A\to B} \otimes \mathcal{L}^{\eta_g,n_g}_{\bar{A}\to\bar{B}}\left(\Psi^+_{A\bar{A}}\right) \\ &= \sum_{i=0}^{4}\sum_{j=0}^{4}\left(\widetilde{\mathcal{A}_i}\otimes\widetilde{\mathcal{A}_j}\right)\left(\Psi^+_{A\bar{A}}\right)\left(\widetilde{\mathcal{A}_i}\otimes\widetilde{\mathcal{A}_j}\right)^\dagger \\ &= \eta_g\ \Psi^+_{B\bar{B}} + \ (1-\eta_g)(n_g-1)\Big(n_g(1-\eta_g)-1\Big)|00\rangle\langle 00|_{B\bar{B}} \\ &\quad + \ n_g(-1+\eta_g)\Big(n_g(-1+\eta_g)-\eta_g\Big)|11\rangle\langle 11|_{B\bar{B}} \\ &\quad + \ n_g(1-n_g)(1-\eta_g)^2\Big(|01\rangle\langle 01|_{B\bar{B}} + |10\rangle\langle 10|_{B\bar{B}}\Big). \end{aligned} \tag{A.24}$$

The state $\mathcal{T}^{\eta_g,n_g}_{B\bar{B}}$ has a fidelity with $\Psi^+_{B\bar{B}}$ given by

$$\eta_t = \frac{1}{2}(1+\eta_g^2) + n_g(n_g-1)(1-\eta_g)^2. \tag{A.25}$$

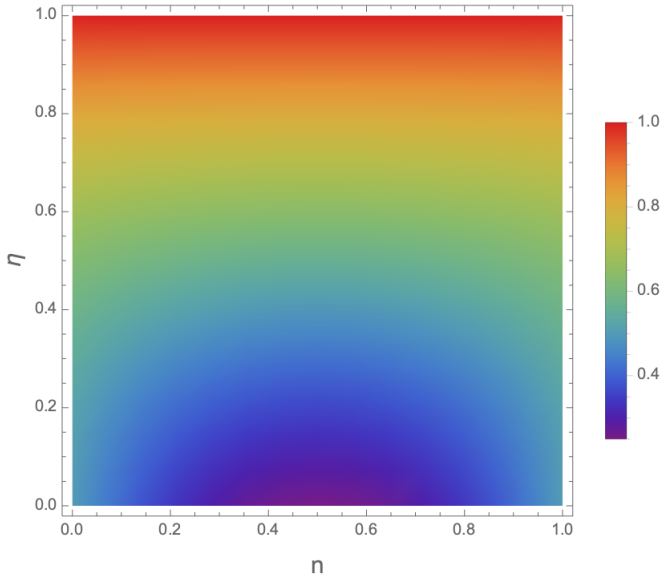


Figure A.2: In this figure, we plot the variation of η_t as a function of n_g and η_g.

We plot in Fig A.2, the variation of η_t as a function of the channel parameters η_g and n_g.

A.5 The atmospheric channel

The losses in transmitting optical signals via an optical fiber are greater than that for free space transmission. The losses are nearly negligible in the vacuum space above the earth's atmosphere. The non-birefringent nature of the atmosphere causes negligible change to the polarization state of the photons passing through it. These observations motivate the use of space and satellite technologies to establish an entanglement distribution network using such channels [36]. We observe in Fig. A.3 that the losses in the satellite-based free-space channel are much less compared to fiber-based channels for distances greater than 70 km.

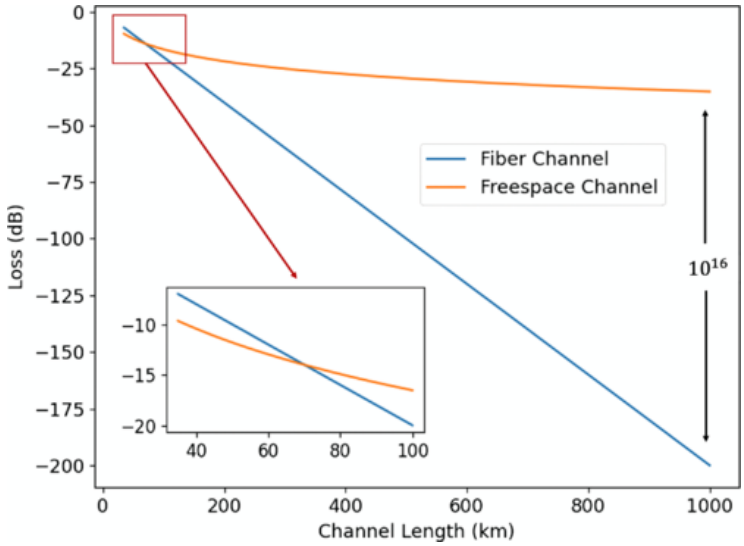


Figure A.3: The comparison of losses in fiber and free-space channels as a function of channel length as discussed and plotted in [36]. It is observed that the free-space channel is advantageous for distances over 70 km.

The network architecture should be a hybrid satellite-optical fiber based model with ground-based global nodes at different geographical locations that are connected to different local nodes at small distances via optical fibers. These global nodes will be connected to the inter-satellite network. This architecture can, in principle, be extended to deep space, allowing the possibility of sharing entanglement between nodes on Earth and the moon.

The factors affecting the transmission of optical signals between a satellite and a ground station are analyzed next. We obtain the efficiency in transmission ξ_{eff} considering losses due to (a) inefficiencies in transmitting (ξ_t) and receiving systems (ξ_r), (b) beam diffraction (ξ_d), (c) air turbulence (ξ_{at}), (d) mispointing (ξ_p) and (e) atmospheric absorption (ξ_{as}). The total transmittance is given by

$$\xi_{\text{eff}} = \xi_t \, \xi_r \, \xi_d \, \xi_{at} \, \xi_p \, \xi_{as} \, . \tag{A.26}$$

The diffraction of an optical beam depends on the beam's spatial mode, wavelength and aperture of the telescope. Assuming a Gaussian beam from the source with a waist radius of ω_0, the radius at a distance z is given by $\omega_d(z) = \omega_0 \sqrt{1 + (z/z_R)^2}$ with z_R being the Rayleigh range. If the aperture radius of the telescope is r, then the receiving efficiency is given by [36]

$$\xi_d = 1 - \exp -\frac{2r^2}{\omega_d^2}. \tag{A.27}$$

The turbulence in the atmosphere induces inhomogeneity in the refractive index, which changes the direction of the propagating beam. It was shown in [190] that large-scale turbulence causes beam deflection while small-scale turbulence induces beam broadening. At the receiver end, it was shown in [191] that the average long-term accumulation of the moving spots shows a Gaussian distribution with an equivalent spot radius of $\omega_{\text{at}}(z) = \omega_d(z) \sqrt{1 + 1.33\sigma_R^2 \Lambda^{5/6}}$, where σ_R^2 is the Rytov variance for plane wave and Λ is the Fresnel ratio of the beam at the receiver. The receiving efficiency is given by

$$\xi_{at} = 1 - \exp -\frac{2r^2}{\omega_{\text{at}}^2}. \tag{A.28}$$

Next, a high-precision and high-bandwidth acquisition, pointing and tracking (APT) system, generally consisting of coarse and fine tracking systems, is required for the satellite moving at high speed. A combination of closed-loop coarse tracking with a large field of view and fine tracking with a small field of view is generally used. The pointing error induces a spot jitter with the instantaneous spot following a Rice intensity distribution. It

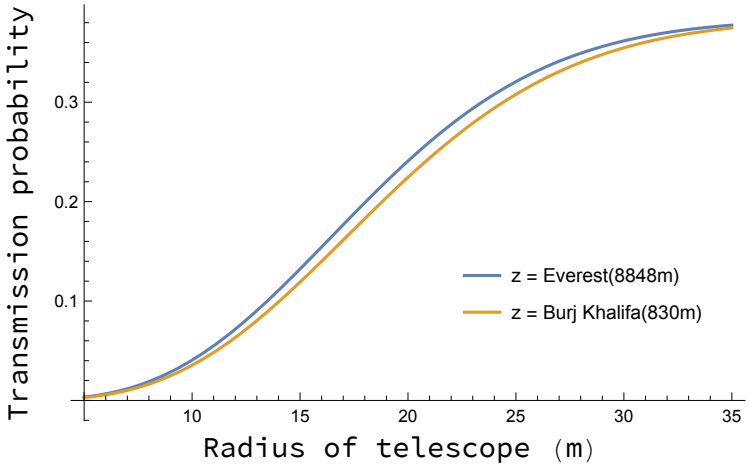


Figure A.4: In this figure, we plot the variation of the transmission probability as a function of the radius of the telescope for different receiving station altitudes. For this, we have considered a 780 nm source with $\omega_0 = 0.0021$ and quality factor 1. We have set $z_R = 17.8, \sigma_R = 0.1, \Lambda = 0.1, \xi_r = 0.99, \xi_t = 0.99, \xi_{as} = 0.5$ and $\eta = 0.95$.

was shown in [192] that the pointing efficiency is given by

$$\xi_p = 1 - \frac{\omega_{\text{at}}^2}{\omega_{\text{at}}^2 + 4\,\sigma_p^2}, \tag{A.29}$$

where σ_p is the variance of the Gaussian pointing probability distribution.

Inserting Eq. (A.27), Eq. (A.28), and Eq. (A.29) in Eq. (A.26) and imposing the condition that $\sigma_p = \eta\omega_{at}$ we obtain

$$\xi_{\text{eff}} = \frac{\eta^2\xi_{as}\xi_r\xi_t}{\eta^2 + 0.25}\left(1 - \exp\left\{-\frac{2r^2 z_R^2}{w^2(z^2 + z_R^2)}\right\}\right) \left(1 - \exp\left\{-\frac{2r^2}{w^2(1.33\Lambda^{5/6}\sigma_R^2 + 1)(\frac{z^2}{z_R^2} + 1)}\right\}\right) \tag{A.30}$$

Consider a 780 nm source with a beam waist radius ω_0 of 0.0021 m and quality factor 1. The source has a Rayleigh length $(z_R) = 17.8$ m. Let the channel have Rytov variance $(\sigma_R) = 0.1$, and the Fresnel ratio of the beam at the receiver end is $(\Lambda) = 0.1$. Let the efficiency of the receiving unit be $(\xi_r) = 0.99$, that of the transmitting source be $(\xi_t) = 0.99$. Also, let the probability of successful transmission after atmospheric absorption be $(\xi_{as}) = 0.5$. Assuming $\eta = 0.95$, we plot in Fig. A.4 the transmission probability through

the atmosphere as a function of the radius of the receiving telescope for different altitudes.

A.6 Entanglement distribution across cities

We plot in Fig. A.5 the variation of ξ_{avg} as a function of the number of satellites in the network for different currently available single photon sources.

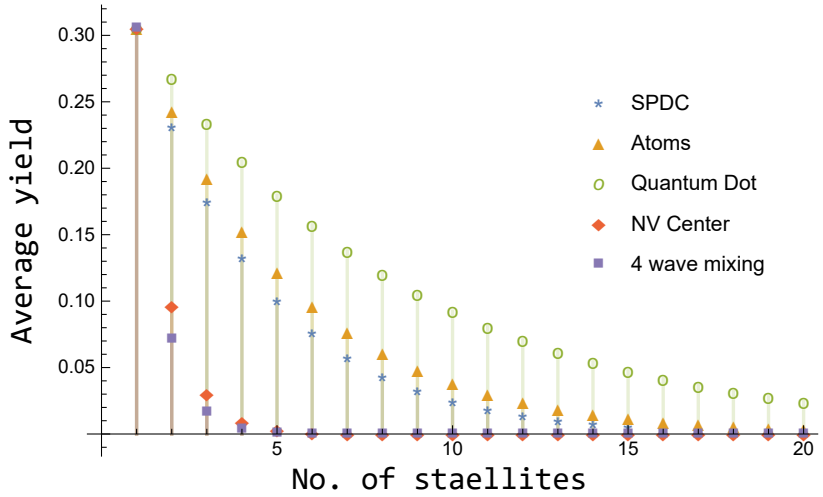


Figure A.5: In this figure, we plot the average yield ξ_{avg} (see Eq. (4.24)) as a function of the number of satellites in the network for different single photon source architectures. The single photon source architectures have the source efficiencies (a) $\eta_s = 0.84$ (SPDC [146]) (b) $\eta_s = 0.88$ (Atoms [145]) (c) $\eta_s = 0.97$ (Quantum Dots [144]) (d) $\eta_s = 0.35$ (NV Center [193]) and (e) $\eta_s = 0.26$ (4 wave mixing [194]). For this, we set $L = l_B + l_M = 10$ km, $s = 1, p = 0.1, \eta_e = 0.95, \eta_g = 0.5, \kappa_g = 0.5, \alpha = 1/22$ km^{-1}, and $q = 1$.

A.7 Analysis of time-varying quantum networks

The network parameters, i.e., the number of nodes, edges, and edge weights, may change with time. Let us denote such a time-varying network as $\mathcal{N}(G(\mathbb{V}(t), \mathbb{E}(t)))$. We say that two nodes v_i and v_j of a time-varying network are connected in the time interval $[t_1, t_2]$ if $\exists\, e_{ij} \in \mathbb{E}(t)$ with $p_{ij} \geq p_* \; \forall t \in [t_1, t_2]$. In the following example, we present the variation of link sparsity with time for the time-varying network shown in Fig. A.6.

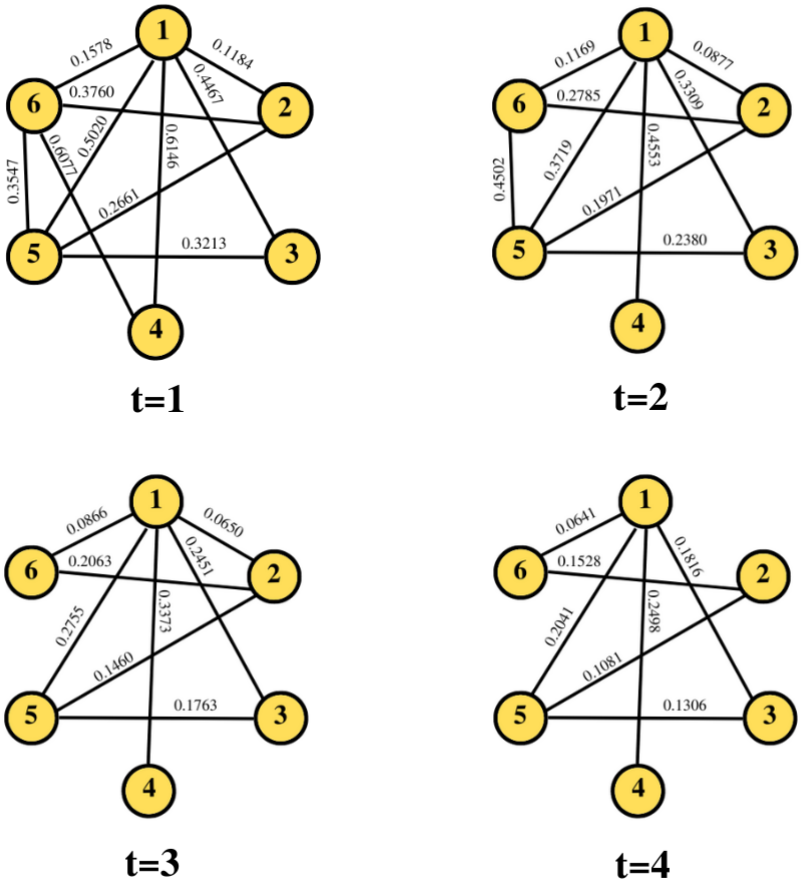


Figure A.6: We present a time varying mesh network with 6 nodes as a series of 4 static graphs. We consider the network topology at times $t \in \{1, 2, 3, 4\}$. In this network, the edges e_{ij} connecting nodes v_i and v_j denote the success probabilities p_{ij} of transferring some resource between the v_i and v_j. The success probability p_{ij} evolves in time following Eq. (A.31).

Example 5. *Consider a network* $\mathcal{N}(G(\mathbb{V}(t), \mathbb{E}(t)))$ *whose vertices and edges are evolving*

in time as shown in Fig. A.6. We assume that for $e_{ij} \in \mathbb{E}(t)$,

$$p_{ij}(t+1) := \begin{cases} w\mathrm{e}^{-kt}\ p_{ij}(t) & \textit{for } w\mathrm{e}^{-kt}\ p_{ij}(t) > p_*, \\ 0 & \textit{otherwise}, \end{cases} \tag{A.31}$$

where $w = 0.9, p_* = 0.05, k = 0.3\ sec^{-1}$ *and* $t \in [1, 4]$. *For such a network, we have the variation of the link sparsity with time as*

t (sec)	1	2	3	4
$\Upsilon(\mathcal{N})$	0.4445	0.5	0.5556	0.6112

Table A.1: Link sparsity for time-evolving graph

We observe from Table A.1 that for the network shown in Fig A.6, the link sparsity increases with time, and the network becomes less robust.

A.8 Reuse and Permissions

22 November 2023 APS Copyright Policies and Frequently Asked Questions

As the author of an APS-published article, may I include my article or a portion of my article in my thesis or dissertation?

Yes, the author has the right to use the article or a portion of the article in a thesis or dissertation without requesting permission from APS, provided the bibliographic citation and the APS copyright credit line are given on the appropriate pages.

Further information

For further information about copyright in general, please refer to the Library of Congress FAQ at https://www.copyright.gov/help/faq/

Journals published by the American Physical Society can be found at https://journals.aps.org/.

FAQ Version: December 12, 2017

Ref: https://journals.aps.org/copyrightFAQ.html

This appendix contains permission of APS to include [1] in this thesis.

BIBLIOGRAPHY

[1] Abhishek Sadhu and Siddhartha Das. Testing of quantum nonlocal correlations under constrained free will and imperfect detectors. *Physical Review A*, 107(1):012212, 2023.

[2] Abhishek Sadhu, Meghana Ayyala Somayajula, Karol Horodecki, and Siddhartha Das. Practical limitations on robustness and scalability of quantum internet. 2023. arXiv:2308.12739.

[3] Stefan Bäuml, Matthias Christandl, Karol Horodecki, and Andreas Winter. Limitations on quantum key repeaters. *Nature communications*, 6(1):6908, 2015.

[4] Siddhartha Das, Sumeet Khatri, and Jonathan P Dowling. Robust quantum network architectures and topologies for entanglement distribution. *Physical Review A*, 97(1):012335, 2018.

[5] Samuraí Brito, Askery Canabarro, Rafael Chaves, and Daniel Cavalcanti. Statistical properties of the quantum internet. *Physical Review Letters*, 124(21):210501, 2020.

[6] Siddhartha Das, Stefan Bäuml, Marek Winczewski, and Karol Horodecki. Universal Limitations on Quantum Key Distribution over a Network. *Physical Review X*, 11:041016, October 2021.

[7] Gilles Pütz, Denis Rosset, Tomer Jack Barnea, Yeong-Cherng Liang, and Nicolas Gisin. Arbitrarily small amount of measurement independence is sufficient to manifest quantum nonlocality. *Physical Review Letters*, 113(19):190402, 2014.

[8] Gilles Pütz and Nicolas Gisin. Measurement dependent locality. *New Journal of Physics*, 18(5):055006, 2016.

[9] Michael JW Hall. Local deterministic model of singlet state correlations based on relaxing measurement independence. *Physical Review Letters*, 105(25):250404, 2010.

[10] Andrew S Friedman, Alan H Guth, Michael JW Hall, David I Kaiser, and Jason Gallicchio. Relaxed Bell inequalities with arbitrary measurement dependence for each observer. *Physical Review A*, 99(1):012121, 2019.

[11] Antonio Acín, Serge Massar, and Stefano Pironio. Randomness versus nonlocality and entanglement. *Physical Review Letters*, 108(10):100402, 2012.

[12] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880, 1969.

[13] Alexander Sauer and Gernot Alber. Quantum bounds on detector efficiencies for violating bell inequalities using semidefinite programming. *Cryptography*, 4(1):2, 2020.

[14] Giovanni Di Crescenzo, Matluba Khodjaeva, Delaram Kahrobaei, and Vladimir Shpilrain. A survey on delegated computation. In *International Conference on Developments in Language Theory*, pages 33–53. Springer, 2022.

[15] Charles H. Bennett and Stephen J. Wiesner. Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69:2881–2884, Nov 1992.

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

[17] Benjamin Schumacher. Sending entanglement through noisy quantum channels. *Physical Review A*, 54:2614–2628, Oct 1996.

[18] Klaus Mattle, Harald Weinfurter, Paul G. Kwiat, and Anton Zeilinger. Dense Coding in Experimental Quantum Communication. *Physical Review Letters*, 76:4656–4659, Jun 1996.

[19] S. J. van Enk, J. I. Cirac, and P. Zoller. Ideal Quantum Communication over Noisy Channels: A Quantum Optical Implementation. *Physical Review Letters*, 78:4293–4296, Jun 1997.

[20] Sougato Bose. Quantum Communication through an Unmodulated Spin Chain. *Physical Review Letters*, 91:207901, Nov 2003.

[21] Samuel L. Braunstein and Peter van Loock. Quantum information with continuous variables. *Reviews of Modern Physics*, 77:513–577, Jun 2005.

[22] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, Kae Nemoto, W. J. Munro, and Y. Yamamoto. Hybrid Quantum Repeater Using Bright Coherent Light. *Physical Review Letters*, 96:240501, Jun 2006.

[23] Wei Zhang, Dong-Sheng Ding, Yu-Bo Sheng, Lan Zhou, Bao-Sen Shi, and Guang-Can Guo. Quantum Secure Direct Communication with Quantum Memory. *Physical Review Letters*, 118:220501, May 2017.

[24] Siddhartha Das, Stefan Bäuml, and Mark M. Wilde. Entanglement and secret-key-agreement capacities of bipartite quantum interactions and read-only memory devices. *Physical Review A*, 101:012344, January 2020.

[25] Eneet Kaur, Siddhartha Das, Mark M Wilde, and Andreas Winter. Extendibility limits the performance of quantum processors. *Physical Review Letters*, 123(7):070502, 2019.

[26] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin. Experimental demonstration of memory-enhanced quantum communication. *Nature*, 580(7801):60–64, 2020.

[27] Jian Wei Cheong, Andri Pradana, and Lock Yue Chew. Communication advantage of quantum compositions of channels from non-Markovianity. *Physical Review A*, 106:052410, Nov 2022.

[28] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661–663, Aug 1991.

[29] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

[30] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.

[31] Jonathan Barrett, Roger Colbeck, and Adrian Kent. Memory Attacks on Device-Independent Quantum Cryptography. *Physical Review Letters*, 110:010503, Jan 2013.

[32] Marco Lucamarini, Zhiliang L Yuan, James F Dynes, and Andrew J Shields. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557(7705):400–403, 2018.

[33] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. Practical device-independent quantum cryptography via entropy accumulation. *Nature communications*, 9(1):459, 2018.

[34] Siddhartha Das. Bipartite Quantum Interactions: Entangling and Information Processing Abilities. January 2019. arXiv:1901.05895.

[35] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 92:025002, May 2020.

[36] Chao-Yang Lu, Yuan Cao, Cheng-Zhi Peng, and Jian-Wei Pan. Micius quantum experiments in space. *Reviews of Modern Physics*, 94(3):035001, 2022.

[37] IBM Quantum (2022). ibm_washington. https://quantum-computing.ibm.com/services/resources, 2022.

[38] Rigetti Computing. Aspen-m-2 quantum processor. https://qcs.rigetti.com/qpus, 2020.

[39] Google Quantum AI. Quantum Computer Datasheet. https://quantumai.google/hardware/datasheet/weber.pdf, 2021.

[40] Jonathan P Dowling and Gerard J Milburn. Quantum technology: the second quantum revolution. *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 361(1809):1655–1674, 2003.

[41] H Jeff Kimble. The quantum internet. *Nature*, 453(7198):1023–1030, 2008.

[42] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412):eaam9288, 2018.

[43] Andrew S Tanenbaum. *Computer networks*. Pearson Education India, 2003.

[44] Koji Azuma, Kiyoshi Tamaki, and Hoi-Kwong Lo. All-photonic quantum repeaters. *Nature Communications*, 6(1):1–7, 2015.

[45] Sebastian Ecker, Johannes Pseiner, Jorge Piris, and Martin Bohmann. Advances in entanglement-based QKD for space applications. 2022. arXiv:2210.02229.

[46] Tonghua Liu, Shuo Cao, Sixuan Zhang, Hao Zheng, and Xiaobao Liu. Satellite-based continuous-variable quantum key distribution under the Earth's gravitational field. *Quantum Information Processing*, 21(12):397, 2022.

[47] Eneet Kaur, Karol Horodecki, and Siddhartha Das. Upper bounds on device-independent quantum key distribution rates in static and dynamic scenarios. *Physical Review Applied*, 18(5):054033, 2022.

[48] H-J Briegel, Wolfgang Dür, Juan I Cirac, and Peter Zoller. Quantum repeaters: the role of imperfect local operations in quantum communication. *Physical Review Letters*, 81(26):5932, 1998.

[49] Francesco Buscemi, Siddhartha Das, and Mark M. Wilde. Approximate reversibility in the context of entropy gain, information gain, and complete positivity. *Physical Review A*, 93:062314, June 2016.

[50] Yink Loong Len, Tuvia Gefen, Alex Retzker, and Jan Kołodyński. Quantum metrology with imperfect measurements. *Nature Communications*, 13(1):6971, 2022.

[51] Nissim Ofek, Andrei Petrenko, Reinier Heeres, Philip Reinhold, Zaki Leghtas, Brian Vlastakis, Yehan Liu, Luigi Frunzio, S. M. Girvin, L. Jiang, Mazyar Mirrahimi, M. H. Devoret, and R. J. Schoelkopf. Extending the lifetime of a quantum bit with error correction in superconducting circuits. *Nature*, 536(7617):441–445, 2016.

[52] Siddhartha Das, Sumeet Khatri, George Siopsis, and Mark M. Wilde. Fundamental limits on quantum dynamics based on entropy change. *Journal of Mathematical Physics*, 59(1), January 2018.

[53] Chenlu Wang, Xuegang Li, Huikai Xu, Zhiyuan Li, Junhua Wang, Zhen Yang, Zhenyu Mi, Xuehui Liang, Tang Su, Chuhong Yang, Guangyue Wang, Wenyan Wang, Yongchao Li, Mo Chen, Chengyao Li, Kehuan Linghu, Jiaxiu Han, Yingshan Zhang, Yulong Feng, Yu Song, Teng Ma, Jingning Zhang, Ruixia Wang, Peng

Zhao, Weiyang Liu, Guangming Xue, Yirong Jin, and Haifeng Yu. Towards practical quantum computers: Transmon qubit with a lifetime approaching 0.5 milliseconds. *npj Quantum Information*, 8(1):3, 2022.

[54] Youngseok Kim, Andrew Eddins, Sajant Anand, Ken Xuan Wei, Ewout van den Berg, Sami Rosenblatt, Hasan Nayfeh, Yantao Wu, Michael Zaletel, Kristan Temme, and Abhinav Kandala. Evidence for the utility of quantum computing before fault tolerance. *Nature*, 618(7965):500–505, 2023.

[55] Aarne Mämmelä, Jukka Riekki, and Markku Kiviranta. Loose coupling: An invisible thread in the history of technology. *IEEE Access*, 2023.

[56] Reuven Cohen, Keren Erez, Daniel Ben-Avraham, and Shlomo Havlin. Resilience of the internet to random breakdowns. *Physical Review Letters*, 85(21):4626, 2000.

[57] Reuven Cohen, Keren Erez, Daniel Ben-Avraham, and Shlomo Havlin. Breakdown of the internet under intentional attack. *Physical Review Letters*, 86(16):3682, 2001.

[58] Adilson E Motter and Ying-Cheng Lai. Cascade-based attacks on complex networks. *Physical Review E*, 66(6):065102, 2002.

[59] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 92(2):025002, 2020.

[60] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Review of Modern Physics*, 86:419–478, Apr 2014.

[61] Armin Tavakoli, Alejandro Pozas-Kerstjens, Ming-Xing Luo, and Marc-Olivier Renou. Bell nonlocality in networks. *Reports on Progress in Physics*, 85(5):056001, 2022.

[62] Alain Aspect, Jean Dalibard, and Gérard Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Physical Review Letters*, 49(25):1804, 1982.

[63] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.

[64] Marissa Giustina, Marijn A. M. Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Morgan W. Mitchell, Jörn Beyer, Thomas Gerrits, Adriana E. Lita, Lynden K. Shalm, Sae Woo Nam, Thomas Scheidl, Rupert Ursin, Bernhard Wittmann, and Anton Zeilinger. Significant-loophole-free test of bell's theorem with entangled photons. *Physical Review Letters*, 115:250401, Dec 2015.

[65] Dipankar Home, Debashis Saha, and Siddhartha Das. Multipartite Bell-type inequality by generalizing Wigner's argument. *Physical Review A*, 91:012102, Jan 2015.

[66] Ming-Xing Luo. Fully device-independent model on quantum networks. *Physical Review Research*, 4:013203, March 2022.

[67] Anders J. E. Bjerrum, Jonatan B. Brask, Jonas S. Neergaard-Nielsen, and Ulrik L. Andersen. Proposal for a long-distance nonlocality test with entanglement swapping and displacement-based measurements. *Physical Review A*, 107:052611, May 2023.

[68] Antonio Acín, Serge Massar, and Stefano Pironio. Efficient quantum key distribution secure against no-signalling eavesdroppers. *New Journal of Physics*, 8(8):126–126, August 2006.

[69] Antonio Acín and Lluis Masanes. Certified randomness in quantum physics. *Nature*, 540(7632):213–219, 2016.

[70] Eneet Kaur, Karol Horodecki, and Siddhartha Das. Upper bounds on device-independent quantum key distribution rates in static and dynamic scenarios. July 2021. arXiv:2107.06411.

[71] Ignatius W Primaatmaja, Koon Tong Goh, Ernest Y-Z Tan, John T-F Khoo, Shouvik Ghorai, and Charles C-W Lim. Security of device-independent quantum key distribution protocols: a review. 2022. arXiv:2206.04960.

[72] Víctor Zapatero, Tim van Leent, Rotem Arnon-Friedman, Wen-Zhao Liu, Qiang Zhang, Harald Weinfurter, and Marcos Curty. Advances in device-independent quantum key distribution. 2022. arXiv:2208.12842.

[73] Lewis Wooltorton, Peter Brown, and Roger Colbeck. Tight analytic bound on the trade-off between device-independent randomness and nonlocality. 2022. arXiv:2205.00124.

[74] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2):419, 2014.

[75] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777, 1935.

[76] John S Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

[77] John S Bell. *Speakable and unspeakable in quantum mechanics: Collected papers on quantum philosophy*. Cambridge University Press, 2004.

[78] John F Clauser and Michael A Horne. Experimental consequences of objective local theories. *Physical Review D*, 10(2):526, 1974.

[79] John S Bell, Abner Shimony, Michael A Horne, and John F Clauser. An exchange on local beables. *Dialectica*, 39(2):85–110, 1985.

[80] Philip M Pearle. Hidden-variable example based upon data rejection. *Physical Review D*, 2(8):1418, 1970.

[81] Lynden K Shalm, Evan Meyer-Scott, Bradley G Christensen, Peter Bierhorst, Michael A Wayne, Martin J Stevens, Thomas Gerrits, Scott Glancy, Deny R Hamel, Michael S Allman, et al. Strong loophole-free test of local realism. *Physical Review Letters*, 115(25):250402, 2015.

[82] The BIG Bell Test Collaboration. Challenging local realism with human choices. *Nature*, 557(7704):212–216, 2018.

[83] Manik Banik, MD Rajjak Gazi, Subhadipa Das, Ashutosh Rai, and Samir Kunkri. Optimal free will on one side in reproducing the singlet correlation. *Journal of Physics A: Mathematical and Theoretical*, 45(20):205301, 2012.

[84] Shuai Zhao, Ravishankar Ramanathan, Yuan Liu, and Paweł Horodecki. Tilted Hardy paradoxes for device-independent randomness extraction. May 2022. arXiv:2205.02751.

[85] Max Kessler and Rotem Arnon-Friedman. Device-independent randomness amplification and privatization. *IEEE Journal on Selected Areas in Information Theory*, 1(2):568–584, 2020.

[86] John Von Neumann. *Mathematische grundlagen der quantenmechanik*, volume 38. Springer-Verlag, 2013.

[87] John Von Neumann. *Mathematical foundations of quantum mechanics: New edition*, volume 53. Princeton university press, 2018.

[88] Paul Adrien Maurice Dirac. *The principles of quantum mechanics*. Number 27. Oxford university press, 1981.

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

[90] Mark M Wilde. *Quantum information theory*. Cambridge university press, 2013.

[91] John Watrous. *The theory of quantum information*. Cambridge university press, 2018.

[92] Alexander S Holevo. *Quantum systems, channels, information: a mathematical introduction*. Walter de Gruyter GmbH & Co KG, 2019.

[93] Armin Uhlmann. The "transition probability" in the state space of a*-algebra. *Reports on Mathematical Physics*, 9(2):273–279, 1976.

[94] Michał Horodecki and Paweł Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *Physical Review A*, 59:4206–4216, Jun 1999.

[95] Reinhard F Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Physical Review A*, 40(8):4277, 1989.

[96] William K Wootters. Entanglement of formation of an arbitrary state of two qubits. *Physical Review Letters*, 80(10):2245, 1998.

[97] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra and Its Applications*, 10(3):285–290, 1975.

[98] Karl Kraus. General state changes in quantum theory. *Annals of Physics*, 64(2):311–335, 1971.

[99] Douglas B. West. *Introduction to Graph Theory - Second edition*. Pearson, 2000.

[100] Charles Eric Leiserson, Ronald L Rivest, Thomas H Cormen, and Clifford Stein. *Introduction to Algorithms - Third edition*. MIT press Cambridge, MA, USA, 2009.

[101] Christopher Portmann and Renato Renner. Security in quantum cryptography. *Reviews of Modern Physics*, 94(2):025008, 2022.

[102] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of modern physics*, 74(1):145, 2002.

[103] Kishor Bharti, Alba Cervera-Lierta, Thi Ha Kyaw, Tobias Haug, Sumner Alperin-Lea, Abhinav Anand, Matthias Degroote, Hermanni Heimonen, Jakob S Kottmann, Tim Menke, et al. Noisy intermediate-scale quantum algorithms. *Reviews of Modern Physics*, 94(1):015004, 2022.

[104] Tameem Albash and Daniel A Lidar. Adiabatic quantum computation. *Reviews of Modern Physics*, 90(1):015002, 2018.

[105] William Thomas Tutte. *Graph theory*, volume 21. Cambridge university press, 2001.

[106] John A Barnes and Frank Harary. Graph theory in network analysis. *Social networks*, 5(2):235–244, 1983.

[107] Hugo Duminil-Copin. Introduction to Bernoulli percolation. 2018.

[108] Dietrich Stauffer and Ammon Aharony. *Introduction to percolation theory*. CRC press, 2018.

[109] S. R. Broadbent and J. M. Hammersley. Percolation processes: I. Crystals and mazes. *Mathematical Proceedings of the Cambridge Philosophical Society*, 53(3):629–641, 1957.

[110] Vincent Beffara and Vladas Sidoravicius. Percolation theory. 2005. arXiv:math/0507220.

[111] Réka Albert, Hawoong Jeong, and Albert-László Barabási. Error and attack tolerance of complex networks. *Nature*, 406(6794):378–382, 2000.

[112] Duncan S Callaway, Mark EJ Newman, Steven H Strogatz, and Duncan J Watts. Network robustness and fragility: Percolation on random graphs. *Physical Review Letters*, 85(25):5468, 2000.

[113] Arman Mohseni-Kabir, Mihir Pant, Don Towsley, Saikat Guha, and Ananthram Swami. Percolation thresholds for robust network connectivity. *Journal of Statistical Mechanics: Theory and Experiment*, 2021(1):013212, 2021.

[114] Linton C Freeman, Douglas Roeder, and Robert R Mulholland. Centrality in social networks: II. Experimental results. *Social networks*, 2(2):119–141, 1979.

[115] Linton C Freeman. A set of measures of centrality based on betweenness. *Sociometry*, pages 35–41, 1977.

[116] Corrado Gini. Variabilità e mutabilità (Variability and Mutability). *C. Cuppini, Bologna*, page 156, 1912.

[117] William Stallings. Local networks. *ACM Computing Surveys (CSUR)*, 16(1):3–41, 1984.

[118] P Green. An introduction to network architectures and protocols. *IEEE Transactions on Communications*, 28(4):413–424, 1980.

[119] Duncan J Watts and Steven H Strogatz. Collective dynamics of 'small-world'networks. *Nature*, 393(6684):440–442, 1998.

[120] Tomislav Begušić, Johnnie Gray, and Garnet Kin-Lic Chan. Fast and converged classical simulations of evidence for the utility of quantum computing before fault tolerance. 2023. arXiv:2308.05077.

[121] Paul Nation, Hanhee Paik, Andrew Cross, and Zaira Nazario. The IBM Quantum heavy hex lattice. https://research.ibm.com/blog/heavy-hex-lattice, 2021.

[122] Eddie Schoute, Laura Mancinska, Tanvirul Islam, Iordanis Kerenidis, and Stephanie Wehner. Shortcuts to quantum network routing. 2016. arXiv:1610.05238.

[123] Kaushik Chakraborty, Filip Rozpedek, Axel Dahlberg, and Stephanie Wehner. Distributed routing in a quantum internet. 2019. arXiv:1907.11630.

[124] Changhao Li, Tianyi Li, Yi-Xiang Liu, and Paola Cappellaro. Effective routing design for remote entanglement generation on quantum networks. 2020. arXiv:2001.02204.

[125] Sumeet Khatri. Policies for elementary links in a quantum network. *Quantum*, 5:537, 2021.

[126] Sumeet Khatri. On the design and analysis of near-term quantum network protocols using Markov decision processes. *AVS Quantum Science*, 4(3):030501, 09 2022.

[127] Álvaro G Iñesta, Gayane Vardoyan, Lara Scavuzzo, and Stephanie Wehner. Optimal entanglement distribution policies in homogeneous repeater chains with cutoffs. *npj Quantum Information*, 9(1):46, 2023.

[128] Edsger W Dijkstra. A note on two problems in connexion with graphs. *Numerische Mathematik*, 1(1):269–271, 1959.

[129] Rodney Van Meter, Takahiko Satoh, Thaddeus D Ladd, William J Munro, and Kae Nemoto. Path selection for quantum repeater networks. *Networking Science*, 3:82–95, 2013.

[130] Ye-Chao Liu, Otfried Gühne, and Stefan Nimmrichter. Entanglement buffers. 2023. arXiv:2312.05099.

[131] Anthony T Velte Toby J Velte and Ph D Robert Elsenpeter. *Cloud computing*. 2010.

[132] Andrew M Childs. Secure assisted quantum computation. 2001. arXiv quant-ph/0111046.

[133] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum private queries. *Physical Review Letters*, 100(23):230502, 2008.

[134] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *2009 50th annual IEEE symposium on foundations of computer science*, pages 517–526. IEEE, 2009.

[135] Joseph F Fitzsimons. Private quantum computation: an introduction to blind quantum computing and related protocols. *npj Quantum Information*, 3(1):23, 2017.

[136] Matthias Steffen, Jay M Gambetta, and Jerry M Chow. Progress, status, and prospects of superconducting qubits for quantum computing. In *2016 46th European Solid-State Device Research Conference (ESSDERC)*, pages 17–20. IEEE, 2016.

[137] C. H. Bennett and G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[138] Christopher A Fuchs and Asher Peres. Quantum-state disturbance versus information gain: Uncertainty relations for quantum information. *Physical Review A*, 53(4):2038, 1996.

[139] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[140] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without Bell's theorem. *Physical Review Letters*, 68:557–559, Feb 1992.

[141] Stefan Bäuml, Matthias Christandl, Karol Horodecki, and Andreas Winter. Limitations on quantum key repeaters. *Nature communications*, 6(1):6908, 2015.

[142] Nicolas Sangouard, Christoph Simon, Hugues De Riedmatten, and Nicolas Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Reviews of Modern Physics*, 83(1):33, 2011.

[143] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. General teleportation channel, singlet fraction, and quasidistillation. *Physical Review A*, 60:1888–1898, Sep 1999.

[144] David Press, Stephan Götzinger, Stephan Reitzenstein, Carolin Hofmann, Andreas Löffler, Martin Kamp, Alfred Forchel, and Yoshihisa Yamamoto. Photon anti-

bunching from a single quantum-dot-microcavity system in the strong coupling regime. *Physical Review Letters*, 98(11):117402, 2007.

[145] HG Barros, A Stute, TE Northup, C Russo, PO Schmidt, and R Blatt. Deterministic single-photon source from a single ion. *New Journal of Physics*, 11(10):103004, 2009.

[146] Joseph B Altepeter, Evan R Jeffrey, and Paul G Kwiat. Phase-compensated ultra-bright source of entangled photons. *Optics Express*, 13(22):8951–8959, 2005.

[147] Charles H. Bennett, David P. DiVincenzo, and John A. Smolin. Capacities of Quantum Erasure Channels. *Physical Review Letters*, 78(16):3217–3220, April 1997.

[148] K Goodenough, D Elkouss, and S Wehner. Assessing the performance of quantum repeaters for all phase-insensitive gaussian bosonic channels. *New Journal of Physics*, 18(6):063005, June 2016.

[149] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8(1):15043, 2017.

[150] Mark M. Wilde, Marco Tomamichel, and Mario Berta. Converse bounds for private communication over quantum channels. *IEEE Transactions on Information Theory*, 63(3):1792–1817, March 2017. arXiv:1602.08898.

[151] Xiang-Bin Wang, Zong-Wen Yu, and Xiao-Long Hu. Twin-field quantum key distribution with large misalignment error. *Physical Review A*, 98(6):062323, 2018.

[152] Xiongfeng Ma, Pei Zeng, and Hongyi Zhou. Phase-matching quantum key distribution. *Physical Review X*, 8(3):031043, 2018.

[153] Pei Zeng, Weijie Wu, and Xiongfeng Ma. Symmetry-protected privacy: beating the rate-distance linear bound over a noisy channel. *Physical Review Applied*, 13(6):064013, 2020.

[154] Yuan-Mei Xie, Chen-Xun Weng, Yu-Shuo Lu, Yao Fu, Yang Wang, Hua-Lei Yin, and Zeng-Bing Chen. Scalable high-rate twin-field quantum key distribution networks without constraint of probability and intensity. *Physical Review A*, 107:042603, Apr 2023.

[155] Yuan-Mei Xie, Yu-Shuo Lu, Chen-Xun Weng, Xiao-Yu Cao, Zhao-Ying Jia, Yu Bao, Yang Wang, Yao Fu, Hua-Lei Yin, and Zeng-Bing Chen. Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference. *PRX Quantum*, 3(2):020315, 2022.

[156] Lai Zhou, Jinping Lin, Yuan-Mei Xie, Yu-Shuo Lu, Yumang Jing, Hua-Lei Yin, and Zhiliang Yuan. Experimental Quantum Communication Overcomes the Rate-Loss Limit without Global Phase Tracking. *Physical Review Letters*, 130:250801, Jun 2023.

[157] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature? *Physical Review Letters*, 80(24):5239, 1998.

[158] Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim. General paradigm for distilling classical key from quantum states. *IEEE Transactions on Information Theory*, 55(4):1898–1929, 2009.

[159] René Schwonnek, Koon Tong Goh, Ignatius W Primaatmaja, Ernest Y-Z Tan, Ramona Wolf, Valerio Scarani, and Charles C-W Lim. Device-independent quantum key distribution with random key basis. *Nature Communications*, 12(1):1–8, 2021.

[160] Máté Farkas, Maria Balanzó-Juandó, Karol Łukanowski, Jan Kołodyński, and Antonio Acín. Bell nonlocality is not sufficient for the security of standard device-independent quantum key distribution protocols. *Physical Review Letters*, 127(5):050503, 2021.

[161] Marek Winczewski, Tamoghna Das, and Karol Horodecki. Limitations on a device-independent key secure against a nonsignaling adversary via squashed nonlocality. *Physical Review A*, 106:052612, Nov 2022.

[162] Ryszard Horodecki, Michał Horodecki, and Paweł Horodecki. Teleportation, Bell's inequalities and inseparability. *Physics Letters A*, 222(1-2):21–25, 1996.

[163] Matthias J Bayerbach, Simone E D'Aurelio, Peter van Loock, and Stefanie Barz. Bell-state measurement exceeding 50% success probability with linear optics. 2022. arXiv:2208.02271.

[164] Ryszard Horodecki, Pawel Horodecki, and Michal Horodecki. Violating Bell inequality by mixed spin-12 states: necessary and sufficient condition. *Physics Letters A*, 200(5):340–344, 1995.

[165] Google. Satellite network, Accessed Jul. 20, 2023. [Online].

[166] Stefanie Barz, Elham Kashefi, Anne Broadbent, Joseph F Fitzsimons, Anton Zeilinger, and Philip Walther. Demonstration of blind quantum computing. *Science*, 335(6066):303–308, 2012.

[167] Monika Maciag-Kruszewska and ibmblogs. Polish PSNC to Join IBM Quantum Network, Becoming First Hub in Central and Eastern Europe. https://www.ibm.com/blogs/southeast-europe/poland-psnc-ibm-quantum-hub/.

[168] Anton Zeilinger, Michael A. Horne, Harald Weinfurter, and Marek Żukowski. Three-Particle Entanglements from Two Entangled Pairs. *Physical Review Letters*, 78:3031–3034, Apr 1997.

[169] Sébastian de Bone, Runsheng Ouyang, Kenneth Goodenough, and David Elkouss. Protocols for creating and distilling multipartite GHZ states with Bell pairs. *IEEE Transactions on Quantum Engineering*, 1:1–10, 2020.

[170] Kelvin Lawrence. Air route data - and more!, Accessed Jan. 16, 2022. [Online].

[171] U.S. Department of Energy Office of Science. National QIS Research Centers. https://science.osti.gov/-/media/QIS/pdf/QuantumBrochure2021.pdf.

[172] Matthew D Eisaman, Jingyun Fan, Alan Migdall, and Sergey V Polyakov. Invited review article: Single-photon sources and detectors. *Review of Scientific Instruments*, 82(7):071101, 2011.

[173] Pawel Blasiak, Emmanuel M Pothos, James M Yearsley, Christoph Gallus, and Ewa Borsuk. Violations of locality and free choice are equivalent resources in Bell experiments. *Proceedings of the National Academy of Sciences*, 118(17):e2020569118, 2021.

[174] Andrea Coladangelo, Koon Tong Goh, and Valerio Scarani. All pure bipartite entangled states can be self-tested. *Nature Communications*, 8(1):1–5, 2017.

[175] Cédric Bamps, Serge Massar, and Stefano Pironio. Device-independent randomness generation with sublinear shared quantum resources. *Quantum*, 2:86, 2018.

[176] Florian J Curchod, Markus Johansson, Remigiusz Augusiak, Matty J Hoban, Peter Wittek, and Antonio Acín. Unbounded randomness certification using sequences of measurements. *Physical Review A*, 95(2):020102, 2017.

[177] Pritam Halder, Ratul Banerjee, Srijon Ghosh, Amit Kumar Pal, and Aditi Sen(De). Circulating genuine multiparty entanglement in a quantum network. *Physical Review A*, 106:032604, Sep 2022.

[178] Sumeet Khatri. On the design and analysis of near-term quantum network protocols using Markov decision processes. *AVS Quantum Science*, 4(3), 2022.

[179] Luís Bugalho, Bruno C Coutinho, Francisco A Monteiro, and Yasser Omar. Distributing multipartite entanglement over noisy quantum networks. *Quantum*, 7:920, 2023.

[180] Yuan Lee, Eric Bersin, Axel Dahlberg, Stephanie Wehner, and Dirk Englund. A quantum router architecture for high-fidelity entanglement flows in quantum networks. *npj Quantum Information*, 8(1):75, 2022.

[181] Martin L Puterman. *Markov decision processes: discrete stochastic dynamic programming*. John Wiley & Sons, 2014.

[182] Richard S Sutton and Andrew G Barto. *Reinforcement learning: An introduction*. MIT press, 2018.

[183] Jérémy Ribeiro, Gláucia Murta, and Stephanie Wehner. Fully device-independent conference key agreement. 2022. arXiv:1708.00798.

[184] Timo Holz, Hermann Kampermann, and Dagmar Bruß. Genuine multipartite bell inequality for device-independent conference key agreement. *Physical Review Research*, 2(2):023251, 2020.

[185] Karol Horodecki, Marek Winczewski, and Siddhartha Das. Fundamental limitations on the device-independent quantum conference key agreement. *Physical Review A*, 105:022604, February 2022.

[186] Emanuel Knill, Raymond Laflamme, and Gerald J Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, 2001.

[187] Charles H Bennett, David P DiVincenzo, John A Smolin, and William K Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5):3824, 1996.

[188] KM Fonseca Romero and R Lo Franco. Simple non-Markovian microscopic models for the depolarizing channel of a single qubit. *Physica Scripta*, 86(6):065004, 2012.

[189] Markus Grassl, Th Beth, and Thomas Pellizzari. Codes for the quantum erasure channel. *Physical Review A*, 56(1):33, 1997.

[190] D Vasylyev, AA Semenov, and W Vogel. Atmospheric quantum channels with weak and strong turbulence. *Physical Review Letters*, 117(9):090501, 2016.

[191] Federico Dios, Juan Antonio Rubio, Alejandro Rodríguez, and Adolfo Comerón. Scintillation and beam-wander analysis in an optical ground station-satellite uplink. *Applied Optics*, 43(19):3866–3873, 2004.

[192] Morio Toyoshima and Kenichi Araki. Far-field pattern measurement of an on-board laser transmitter by use of a space-to-ground optical link. *Applied Optics*, 37(10):1720–1730, 1998.

[193] Sebastian KH Andersen, Shailesh Kumar, and Sergey I Bozhevolnyi. Ultrabright linearly polarized photon generation from a nitrogen vacancy center in a nanocube dimer antenna. *Nano Letters*, 17(6):3889–3895, 2017.

[194] Brian J Smith, P Mahou, Offir Cohen, JS Lundeen, and IA Walmsley. Photon pair generation in birefringent optical fibers. *Optics Express*, 17(26):23589–23602, 2009.