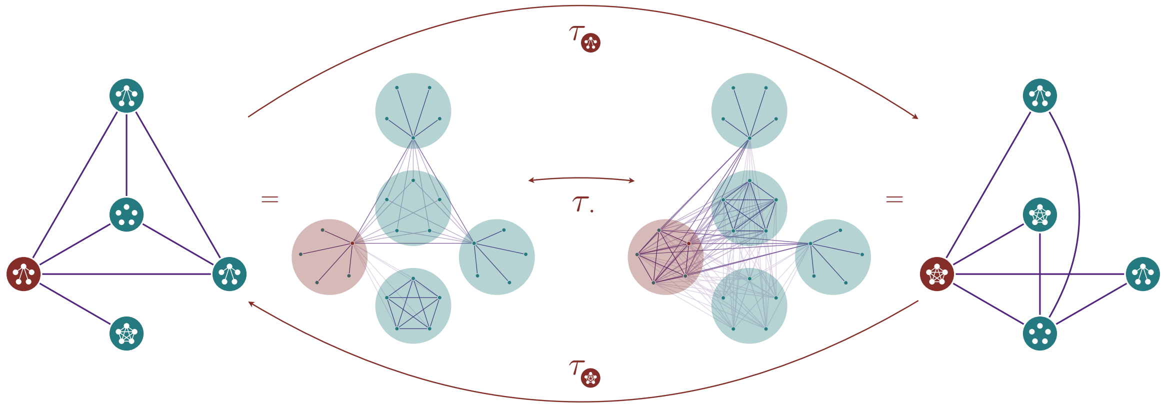
Quantum Networks

Dissertation zur Erlangung des Grades eines Doktors der Naturwissenschaften
(Dr. rer. nat.) am Fachbereich Physik der Freien Universität Berlin



vorgelegt von

Frederik Hahn

Berlin, 2022

Erstgutachter: Prof. Dr. Jens Eisert (Freie Universität Berlin)

Zweitgutachter: Prof. Dr. Felix von Oppen (Freie Universität Berlin)

Datum der Disputation: 26.06.2023

Preface

In this dissertation, I present some of the results I have obtained in the course of my doctoral research. I will not only present the results themselves, but also give a (hopefully) easy-to-follow introduction to the general ideas and methods commonly used in the study of quantum communication and quantum networks.

Our communication has become more digital, and not just because of the COVID-19 pandemic. When we talk and write to each other today, we immediately know who we are talking to. Though today's social networks do not require us to use our legal names, we know that at least intelligence services have more than a vague idea who is hiding behind pseudonyms. Even one of the most popular encryption of emails is only called PGP –short for pretty good privacy. This privacy is not complete: Although the text is encrypted, it is always exposed who is communicating with whom. It is precisely this metadata that is of greatest financial interest. Is privacy a thing of the past?

While this thesis does not attempt to answer that question, it does aim to shed light on how communication protocols based on quantum mechanics could change the way we communicate. With the vision of a future quantum internet in mind, we can think about the distribution and manipulation of entanglement, more secure encryption protocols, and even anonymous encryption.

Frederik Hahn
Berlin, 2022

Contents

Appendix **119**

Author publications

List of the author's journal publications and arXiv preprints

[HPE19] F. Hahn, A. Pappa, and J. Eisert. 'Quantum network routing and local complementation'. en. *npj Quantum Information* 5.1 (2019), p. 76. DOI: 10.1038/s41534-019-0191-6.

[HJP20] F. Hahn, J. de Jong, and A. Pappa. 'Anonymous Quantum Conference Key Agreement'. en. *PRX Quantum* 1.2 (2020), p. 020325. DOI: 10.1103/PRXQuantum.1.020325.

[Tha+21] C. Thalacker, F. Hahn, J. de Jong, A. Pappa, and S. Barz. 'Anonymous and secret communication in quantum networks'. *New Journal of Physics* 23.8 (2021), p. 083026. DOI: 10.1088/1367-2630/ac1808.

[Wal+22a] J. Wallnöfer, F. Hahn, M. Gündoğan, J. S. Sidhu, F. Wiesner, N. Walk, J. Eisert, and J. Wolters. 'Simulating quantum repeater strategies for multiple satellites'. en. *Communications Physics* 5.1 (2022), p. 169. DOI: 10.1038/s42005-022-00945-9.

[Hah+22] F. Hahn, A. Dahlberg, J. Eisert, and A. Pappa. 'Limitations of nearest-neighbor quantum networks'. *Physical Review A: Atomic, Molecular, and Optical Physics* 106.1 (2022), p. L010401. DOI: 10.1103/PhysRevA.106.L010401.

[Gra+22] F. Grasselli, G. Murta, J. de Jong, F. Hahn, D. Bruß, H. Kampermann, and A. Pappa. 'Secure Anonymous Conferencing in Quantum Networks'. en. *PRX Quantum* 3.4 (2022), p. 040306. DOI: 10.1103/PRXQuantum.3.040306.

[Jon+22a] J. de Jong, F. Hahn, J. Eisert, N. Walk, and A. Pappa. 'Anonymous conference key agreement in linear quantum networks' (2022). DOI: 10.48550/ARXIV.2205.09169.

[Rüc+22] L. Rückle, J. Budde, J. de Jong, F. Hahn, A. Pappa, and S. Barz. 'Experimental anonymous conference key agreement using linear cluster states' (2022). DOI: 10.48550/ARXIV.2207.09487.

[Jon+22b] J. de Jong, F. Hahn, N. Tcholtchev, M. Hauswirth, and A. Pappa. 'Extracting maximal entanglement from linear cluster states' (2022). DOI: 10.48550/ARXIV.2211.16758.

Summary

Entangled quantum states are remarkably rich resources for communication and computation. Today, we are witnessing the emergence of useful quantum technologies and global efforts to build the first entangled quantum communication infrastructures –the world's first quantum networks.

In this thesis, we explore the potential of communication in such networks of entangled states by going beyond the typical bipartite point-to-point settings. Entanglement between more than two particles is called multipartite entanglement. Multipartite entangled states exhibit rich structures making them ideal for complex communication tasks.

In the first part of this thesis, we begin with an introduction in which we establish notation, present preliminary mathematics, and explain initial bipartite quantum communication protocols. We show how to use quantum teleportation to transfer the quantum state of one particle to another, how to use quantum repeaters to extend the range of entanglement, and how to use quantum key distribution to exploit entanglement for cryptography.

In the second part of this thesis, we then address quantum networks and multipartite quantum communication protocols. Here we use the mathematical abstraction of quantum graph states to theoretically explore the possibilities of real world quantum networks.

We discuss the use of graph states for routing quantum information. Graph states are multipartite entangled states of quantum particles that we can manipulate with local operations on the individual particles. With these operations, which correspond to the so-called local complementation of a mathematical graph, the graph state entanglement can be redirected such that particles that never physically interacted with each other become entangled. These graph state manipulations offer fascinating possibilities.

We present these possibilities of entanglement manipulation, but also some limitations of its use. For example, we prove that typical bottleneck communication problems cannot be solved in a large class of nearest-neighbor network topologies.

In the light of these limitations, we further investigate the manipulation of graph state entanglement at a foundational level: We derive new and easy-to-compute invariants of graph states and study the class of circle graph states.

In the third and final part of this thesis, we then explore multipartite quantum cryptography protocols with the added feature of anonymity. Exploiting the intricate features of graph state entanglement, we introduce the first protocol for anonymous quantum conference key agreement. Hopefully, quantum networks protocols like this will pave the way for a future quantum internet.

Zusammenfassung

Verschränkte Quantenzustände eignen sich hervorragend als Ressourcen für Kommunikation und Quantenrechnungen. Heute werden bereits erste nützliche Quantentechnologien entwickelt und es gibt weltweite Bestrebungen zum Aufbau der ersten auf Verschränkung basierenden Quantennetzwerke der Welt.

In dieser Dissertation untersuchen wir das Potenzial der Kommunikation mittels solcher Netzwerke von verschränkten Quantenzuständen. Dabei gehen wir über die einfachen bipartiten Punkt-zu-Punkt-Verbindungen hinaus. Die Verschränkung zwischen mehr als zwei Teilchen wird als multipartite Verschränkung bezeichnet. Multipartit verschränkte Zustände weisen vielschichtige Strukturen auf, die sie ideal für komplexe Kommunikationsaufgaben machen.

Im ersten Teil dieser Arbeit beginnen wir mit einer Einführung, in der wir die Notation festlegen, die mathematischen Grundlagen legen und erste Protokolle der bipartiten Quantenkommunikation darlegen. Wir zeigen, wie wir mit Hilfe von Quantenteleportation den Zustand eines Teilchens auf ein anderes übertragen, wie wir mit Quantenrepeatern die Reichweite von Verschränkung vergrößern und wie wir mit Hilfe von Quantenschlüsselverteilung Verschränkung für Kryptographie nutzen können.

Im zweiten Teil dieser Dissertation befassen wir uns dann mit Quantennetzwerken und multipartiten Quantenkommunikationsprotokollen. Hier verwenden wir die mathematische Abstraktion von Graphenzuständen, um die Potenziale von Quantennetzwerken in der realen Welt theoretisch zu untersuchen.

Wir diskutieren die Verwendung von Graphenzuständen für das Routing von Quanteninformation. Graphenzustände sind multipartit verschränkte Zustände von Teilchen, die wir mit lokalen Operationen auf den einzelnen Teilchen manipulieren können. Mit diesen Operationen, die der so genannten lokalen Komplementierung eines mathematischen Graphen entsprechen, kann die Verschränkung der Graphenzustände so umgelenkt werden, dass selbst Teilchen, die niemals miteinander in Kontakt gekommen sind, miteinander verschränkt werden können. Diese Graphenzustandsmanipulationen bieten faszinierende Möglichkeiten.

Wir diskutieren diese Möglichkeiten der Verschränkungsmanipulation, erklären dabei aber auch einige Einschränkungen der Verschränkungsanwendung. Wir beweisen zum Beispiel, dass typische Engpässe in Netzwerken in einer großen Klasse von Netzwerktopologien (welche nur Verbindungen zwischen nächsten Nachbarn zulassen) nicht umgangen werden können.

Vor dem Hintergrund dieser Einschränkungen untersuchen wir die Manipulation der Graphenzustandsverschränkung auf einer grundlegenden Ebene: Wir leiten neue und einfach zu berechnende Invarianten von Graphenzuständen her und untersuchen die Klasse der Kreisgraphenzustände.

Im dritten und letzten Teil dieser Dissertation untersuchen wir dann multipartite Protokolle zur Quantenkryptographie unter dem zusätzlichen Gesichtspunkt der Anonymität. Unter Verwendung der vielschichtigen Eigenschaften der Verschränkung von Graphenzuständen präsentieren wir das erste bekannte Protokoll für anonyme Schlüsselvereinbarungen für mehrere Teilnehmer. Es bleibt zu hoffen, dass Quantennetzwerkprotokolle wie dieses den Weg für ein zukünftiges Quanteninternet ebnen werden.

Resumen

Los estados cuánticos entrelazados son recursos extraordinariamente ricos para la comunicación y la computación. A día de hoy, presenciamos la aparición de tecnologías cuánticas útiles y esfuerzos mundiales para construir las primeras infraestructuras de comunicación cuántica entrelazada: las primeras redes cuánticas del mundo.

En esta tesis, exploramos el potencial de la comunicación con redes de estados cuánticos entrelazados yendo más allá de las configuraciones bipartitas punto-a-punto habituales. El entrelazamiento entre más de dos partículas se denomina entrelazamiento multipartito. Los estados entrelazados multipartitos presentan estructuras ricas que los hacen ideales para manejar tareas complejas de comunicación.

En la primera parte de esta tesis, comenzamos con una introducción en la que establecemos la notación, presentamos las matemáticas preliminares y explicamos los protocolos iniciales de comunicación cuántica bipartita. Mostramos cómo utilizar la teleportación cuántica para transferir el estado cuántico de una partícula a otra, cómo utilizar repetidores cuánticos para ampliar el alcance del entrelazamiento y cómo utilizar la distribución cuántica de claves para explotar el entrelazamiento para la criptografía.

En la segunda parte de esta tesis, abordamos las redes cuánticas y los protocolos de comunicación cuántica multipartita. Aquí utilizamos la abstracción matemática de los estados grafo cuánticos para explorar teóricamente las posibilidades de las redes cuánticas del mundo real.

Discutimos el uso de los estados grafo para enrutar información cuántica. Los estados grafo son estados de partículas cuánticas con entrelazamiento multipartito que podemos manipular con operaciones locales sobre las partículas individuales. Con estas operaciones, que corresponden a la llamada complementación local de un grafo matemático, se puede redirigir el entrelazamiento del estado grafo de manera que partículas que nunca han interactuado físicamente entre sí queden entrelazadas. Estas manipulaciones del estado grafo ofrecen posibilidades fascinantes.

Presentamos estas posibilidades de manipulación del entrelazamiento, pero también algunas limitaciones de su uso. Por ejemplo, demostramos que los problemas de embotellamiento habituales en comunicación no pueden resolverse en una amplia clase de topologías de red de vecino más próximo.

A la luz de estas limitaciones, investigamos más a fondo la manipulación del entrelazamiento de estados grafo a un nivel fundacional: Derivamos invariantes de estados grafo nuevos y fáciles de calcular y estudiamos la clase de estados grafo circulares.

En la tercera y última parte de esta tesis, exploramos protocolos de criptografía cuántica multipartita con la característica añadida del anonimato. Aprovechando las intrincadas características del entrelazamiento de estados grafo, presentamos el primer protocolo cuántico de acuerdo anónimo de claves de conferencia. Esperamos que protocolos de redes cuánticas como éste allanen el camino para un futuro internet cuántico.

Part I
Elements of Quantum Communication

Introduction 1

The emergence of quantum technologies is ushering in an unprecedented wave of possibilities in communication, computation, and cryptography. At the forefront of these developments is the promise of entangled quantum communication infrastructures, the precursor to a potential global quantum network, or as some envision it, even the quantum internet. However, while significant progress has been made, there are numerous research gaps and shortcomings that hinder the realization of this quantum vision, particularly in the area of multiparty quantum communication.

Currently, quantum communication is heavily focused on two-party point-to-point settings. Two-party communication is undoubtedly fundamental and has paved the way for groundbreaking protocols such as quantum key distribution and quantum teleportation. However, this perspective offers only a limited view of the full spectrum of possibilities that quantum communication offers. Real-world communication is inherently complex, often involving more than two parties and requiring versatile network configurations. To meet these communication demands, we seek to explore the untapped potential of multipartite entangled quantum states.

Entangled quantum states serve as versatile and rich resources for communication and computation. When we explore the notion of entanglement beyond two particles, we arrive at multipartite entanglement –a realm in which quantum states exhibit intricate structures and correlations that are open to exploitation. These structures, with their inherent complexity, seem ideal for solving the complex communication tasks that exist in modern communication scenarios.

This thesis aims to push the boundaries of existing knowledge by focusing on the potential of communication in networks of entangled quantum states beyond the conventional bipartite settings. It seeks to explore the emerging field of multipartite quantum communication in quantum networks, bridging the gap between current hardware limitations and the future possibilities of a fully functional quantum internet.

1.1 State of the art

Quantum communication and cryptography

As early as 1984 [BB84b] it was realized that entangled quantum systems could be used to establish keys that could in turn be used for secure information transmission. The most fascinating aspect of this idea is that its security is not based on unproven assumptions about the computational intractability of mathematical problems. Instead, it is based on fundamental laws of nature, which ultimately relate to the insight that one cannot measure the quantum state of a quantum system without disturbing it to some extent. With this seminal work, the idea of quantum key distribution (QKD) was born.

Not surprisingly, the path from the initial idea to feasible schemes for quantum cryptography has been long and winding [GT07]. Much of the theoretical work since has focused on security proofs of protocols that provide security even in the presence of noise and other imperfections. The famous first proofs [SP00; Bih+98; LC99; May01] were based on ideas of entanglement purification, firmly establishing a link between notions of security and entanglement even in prepare and measure schemes.

Since the millennium, the machinery of security proofs has matured considerably [PR22], including in particular finite resources.

Born out of the need to understand the precise role that knowledge of the detectors plays and to improve security proofs, the idea of device-independent quantum key distribution was developed [Ací+07; ARV19]. Although potentially impractical due to significantly smaller rates, this concept has the charm that no assumptions need to be made about the detectors used, and that security is based entirely on the use of classical measurement data alone, an idea based on Bell's theorem [Bel64].

Beyond quantum key distribution

Going beyond QKD, quantum conference key agreement (CKA) enables multiple parties to establish a shared secret key, using entangled quantum resources, public communication, and local operations. For an in-depth review of CKA, see Reference [Mur+20].

A typical CKA protocol involves n quantum network users sharing multipartite entangled quantum states. Although CKA could be achieved by establishing $n(n-1)$ bipartite QKD keys between n users, multipartite entanglement offers the advantage of generating the conference key for all users directly.

Such conference key generation protocols mirror quantum key distribution protocols in that they consist of three steps: the distribution of the entangled state to the users; the measurements of this state, often randomly selected, over multiple rounds; and the classical postprocessing of the resulting data.

Entanglement distribution and quantum repeaters

It quickly became clear that in the presence of realistic noise levels, quantum key distribution between arbitrary points on Earth would only be possible with the help of quantum repeaters [Bri+98; San+11] –at least if one does not want to live with the burden of having to trust any intermediate nodes.

Such repeater schemes rely on the distribution of entanglement between nodes of a larger scheme, in the original formulation followed by entanglement distillation, and finally establishing entanglement over arbitrary distances by entanglement swapping.

Recently, experimental work has caught up with the theoretical proposals in the point-to-point paradigm. At the time of revision of this thesis in the summer of 2023, quantum teleportation between non-neighboring nodes was achieved [Her+22a], heralded entanglement over fibre links between two independently trapped atoms was generated [Van+22], and the first telecom-wavelength quantum repeater based on trapped ions was experimentally realized [Kru+23].

With respect to practical implementations, today there are several commercial devices available that implement fully fletched quantum key distribution schemes that are secure at least for short distances and that do not require full quantum repeater schemes. In fact, there has been a tremendous push recently to implement quantum key distribution systems under realistic conditions over long distances and in a practical way, not least by the partners of the European Quantum Internet Alliance.

1.2 Research objective

The primary goal of this thesis is to address some fundamental questions that remain unresolved in the field of quantum communication, thus further illuminating its full potential. The scope of this work includes the study of multipartite quantum communication involving more than two end nodes, leading to the notion of quantum networks in the first place. We explore and develop new network communication protocols and anonymous applications that show an advantage over the bipartite, point-to-point domain.

Navigating this landscape of multipartite entanglement transformation, however, is not without its challenges. In particular, we encounter graph theoretic problems that are hard from the computational complexity perspective. We therefore also reach for the limits of what we can hope to achieve by transforming multipartite entanglement in quantum networks.

Quantum network routing capabilities and limitations

Our exploration begins with an overview of quantum communication and cryptography in the currently established paradigms. We revisit the essential bipartite building blocks –quantum teleportation, quantum repeaters, and quantum key distribution– and use these fundamental concepts as stepping stones into the more complex multipartite domains.

Relevant publications of the author in this context: [Wal+22a], [Wal+22b].

The core of this thesis is dedicated to the exploration of quantum networks and multipartite quantum communication protocols.

Through the lens of quantum graph states –an abstract yet powerful mathematical tool– we explore the possibilities of real-world quantum networks. These graph states, as examples of multipartite entangled states of quantum particles, can be manipulated via local operations to control the distribution of entanglement, and hence route the resources for communication, in the network.

Relevant publications of the author in this context: [HPE19], [Hah+22], [Jon+22b].

We are interested not only in how multipartite entangled resources can be transformed into different multipartite entanglement, but also in how they can optimally be transformed back into bipartite entanglement between subsets of chosen nodes. This routed entanglement can then again be used for quantum teleportation and quantum key distribution.

We explore routing of entanglement in the context of constraints and limitations and focus on bottleneck communication problems, in a broad category of nearest-neighbor network topologies.

Local complementation invariants

Relevant publication of the author in this context: [BH23].

To address the arising graph theoretic challenges, we dive deeper into the properties of graph states: An ongoing challenge is the computational inefficiency of known invariants under graph transformations called local complementations. Known invariants require knowledge of the full set of stabilizers, which grows exponentially with the with the number of qubits. We overcome this limitation by deriving new and easily computable invariants.

Anonymity in quantum networks

Relevant publications of the author in this context: [HJP20], [Tha+21], [Gra+22], [Jon+22a], [Rüc+22].

The final part of the thesis moves back into the realm of quantum cryptography –again with a focus on multipartite settings. Using the complex correlation patterns of graph state entanglement, we propose the first protocol for anonymous key agreement in quantum conferences. It is our hope that this and other explorations will contribute significantly to the realization of the dream of a quantum internet.

Towards quantum networks

In essence, this thesis is about exploring the theoretical limits of communication in quantum networks, taking on new challenges such as anonymity, and trying to pave the way for a quantum future that may redefine how we communicate and compute. Overall, with this thesis, I hope to have significantly contributed to the timely question: What, after all, can we do with quantum networks, once they become a reality?

Mathematical preliminaries 2

"[The book of nature] is written in the language of mathematics, and the characters are triangles, circles, and other geometrical figures, without which it is impossible to humanly understand a word; without which one wanders in vain through a dark labyrinth."

"Egli è scritto in lingua matematica, e i caratteri son triangoli, cerchi, ed altre figure geometriche, senza i quali mezi è impossibile a intenderne umanamente parola; senza questi è un aggirarsi vanamente per un oscuro laberinto."

—*Galileo Galilei* [Gal23]

2.1 Qubits and Hilbert spaces

Analogous to classical bits that only take the values 0 and 1 in classical information theory, one of the most fundamental building blocks of quantum information theory are two-level quantum systems called *qubits*. In quantum mechanics, any system with two degrees of freedom is considered a qubit.

In experimental implementations, qubits can be realized in various ways [Lad+10; Moo+21]. Some of the most popular ways are the use of ion traps [CZ95; Geo20], quantum dots [LD98; KL13], neutral atoms [SWM10; Hen+20], superconducting electronic circuits [NCT97; CW08] or point defects in diamond like the so-called nitrogen vacancy centres [Gru+97; Doh+13].

However, since only photons travel at the speed of light, photonic qubits are arguably the most relevant type for the purposes of quantum communication. They can take advantage of the numerous degrees of freedom that photons can access [Kok+07; Wan+20]: their polarization (*e.g.* horizontal and vertical), their arrival time (*e.g.* early or late at a given location), or their number (*e.g.* vacuum mode or arrival of a single photon).

Mathematically, the state space of qubits is described by Hilbert spaces. For multiple qubits, this state space is expanded by taking the tensor product of the individual Hilbert spaces.

Definition 2.1 (Hilbert space) *A Hilbert space $\mathscr{H}$ over the field of complex numbers $\mathbb{C}$ is a complex vector space with an inner product*

$$\langle \cdot | \cdot \rangle : \mathscr{H} \times \mathscr{H} \to \mathbb{C}, \quad (\phi, \psi) \mapsto \langle \phi | \psi \rangle \tag{2.1}$$

that is anti-linear in the first argument and linear in the second, as well as positive, i.e. $\langle \psi | \psi \rangle$ is non-negative for all ψ in $\mathscr{H}$.

Hilbert spaces are complete with respect to the canonical metric of the norm $\|\psi\| := \sqrt{\langle \psi | \psi \rangle}$ induced by the inner product. For simplicity, the

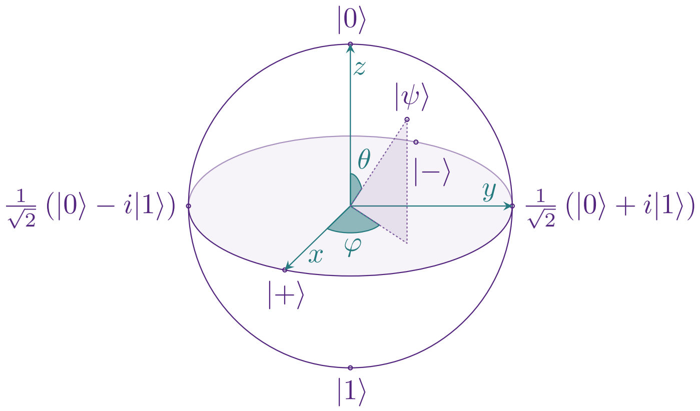

$|0\rangle$
z
$|\psi\rangle$
θ
$|-\rangle$
y
$\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$
$\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$
x
φ
$|+\rangle$
$|1\rangle$

Figure 2.1: The state space of qubits can be represented by the Bloch ball. While *pure* qubit state vectors are the extremal points on the ball's surface, mixed states are points in the ball's interior. Since $\sin^2 + \cos^2 = 1$, Equation 2.3 can be rewritten as

$$|\psi\rangle = e^{i\varphi_0} \cos \frac{\theta}{2} |0\rangle + e^{i\varphi_1} \sin \frac{\theta}{2} |1\rangle.$$

As global phases do not have any observable effect in quantum mechanics we find

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$$

with $\varphi := \varphi_1 - \varphi_0$. The *maximally mixed* state is the center of the Bloch ball.

Hilbert space of a single qubit system is typically considered as $\mathbb{C}^2$ spanned by the orthonormal basis $\{|0\rangle, |1\rangle\}$, where

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.2}$$

A qubit *state vector* can be expanded in this basis as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.3}$$

with $|\alpha|^2 + |\beta|^2 = 1$. The state space of a qubit can be represented as a ball, the *Poincaré ball* or *Bloch ball* visualized in Figure 2.1.

Denoting the basis of the dual space of $\mathbb{C}^2$, *i.e.* $\langle\cdot| : \mathbb{C}^2 \to \mathbb{C}$, as $\{\langle 0|, \langle 1|\}$, we naturally obtain the inner product of the Hilbert space as $\langle\cdot|\cdot\rangle : \mathbb{C}^2 \times \mathbb{C}^2 \to \mathbb{C}$ and $\langle\psi| = \alpha^*\langle 0| + \beta^*\langle 1|$.

Besides the standard *computational basis* $\{|0\rangle, |1\rangle\}$ of $\mathbb{C}^2$, other typical basis choices are given by the eigenvectors of the *Pauli matrices*. We will introduce them in the following (see Definition 2.3).

2.2 Hermitian, unitary and Pauli matrices

> **Definition 2.2** (Hermitian, unitary & normal matrix) *Matrices that are equal to their conjugate transpose $H^\dagger := (H^T)^*$ are called Hermitian. If their conjugate transpose is equal their inverse, $U^\dagger = U^{-1}$, they are called unitary. Matrices N that can be diagonalized by a unitary matrix are called normal.*

Every unitary matrix U can be written as a matrix exponential

$$U = e^{iH} := \sum_{k=0}^{\infty} \frac{1}{k!} (iH)^k \tag{2.4}$$

of a Hermitian matrix H. Likewise, every Hermitian matrix H defines a unitary matrix U via Equation 2.4.

Given U, we can calculate H with the matrix logarithm (see Definition 2.7).

The unitarity of the expression on the right hand side of Equation 2.4 follows from

$$\begin{aligned} UU^\dagger &= \sum_{k=0}^{\infty} \frac{(iH)^k}{k!} \sum_{l=0}^{\infty} \frac{(-iH^\dagger)^l}{l!} \\ &= \sum_{m=0}^{\infty} \sum_{l=0}^{m} \frac{(iH)^{m-l}}{(m-l)!} \frac{(-iH^\dagger)^l}{l!} \\ &= \sum_{m=0}^{\infty} \frac{1}{m!} \sum_{l=0}^{m} \binom{m}{l} (iH)^{m-l} (-iH^\dagger)^l \\ &= \sum_{m=0}^{\infty} \frac{1}{m!} (iH - iH^\dagger)^m, \end{aligned}$$

where we reordered the sum with $m := k + l$ and used the binomial theorem for commuting matrices. Since $H = H^\dagger$ the only nonzero contribution from the sum over m is $\mathbb{1}_2$ via $m = 0$.

Time dependent unitary operators of the type $U(t) := e^{-\frac{i}{\hbar}tH}$, where

Planck's constant $\hbar$ is often set to one, solve the Schrödinger equation

$$i\hbar\frac{\mathrm{d}}{\mathrm{d}t}|\psi(t)\rangle = H|\psi(t)\rangle \tag{2.5}$$

by giving the time evolution of a quantum state $|\psi(t=0)\rangle$ as

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle. \tag{2.6}$$

The Hermitian matrix that is governing the time evolution of a quantum system is also-called its *Hamiltonian* in reference to classical Hamiltonian mechanics.

For all normal operators, we can find a *spectral decomposition*.

Theorem 2.1 (Spectral decomposition) *Any normal matrix N with eigenvalues $\alpha_i \in \mathbb{C}$ and eigenvectors $\{|\psi_1\rangle, \dots, |\psi_d\rangle\}$ can be written as*

$$N = \sum_{i=1}^{d} \alpha_i |\psi_i\rangle\langle\psi_i|. \tag{2.7}$$

For Hermitian matrices, the eigenvalues in the spectral decomposition are real and for unitary matrices they have unit absolute value. This can be derived as follows.

Lemma 2.2 *The eigenvalues of unitary matrices have unit absolute value.*

Proof. Let $|\alpha\rangle$ be an eigenvector with eigenvalue α of a unitary U. Then $U|\alpha\rangle = \alpha|\alpha\rangle$ and $\langle\alpha|U^\dagger = \alpha^*\langle\alpha|$ imply

$$\langle\alpha|\alpha\rangle = \langle\alpha|U^\dagger U|\alpha\rangle = \alpha^*\alpha\langle\alpha|\alpha\rangle \tag{2.8}$$

and thus $|\alpha|^2 = \alpha^*\alpha = 1$. □

Lemma 2.3 *Hermitian matrices have real eigenvalues.*

Proof. Let $|\beta\rangle$ be an eigenvector with eigenvalue β of a Hermitian matrix H. Then $H|\beta\rangle = \beta|\beta\rangle$ and $\langle\beta|H^\dagger = \beta^*\langle\beta|$ imply

$$\beta^*\beta\langle\beta|\beta\rangle = \langle\beta|H^\dagger H|\beta\rangle = \langle\beta|H^2|\beta\rangle = \beta^2\langle\beta|\beta\rangle \tag{2.9}$$

and thus $|\beta|^2 = \beta^2$, *i.e.*, $\beta \in \mathbb{R}$. □

Lemma 2.4 *Normal matrices with real eigenvalues are Hermitian.*

Proof. Given a unitary diagonalization of a normal matrix, *i.e.*, $N = U^\dagger D U$ with D containing the eigenvalues of N on its diagonal, we find

$$N^\dagger = \left(U^\dagger D U\right)^\dagger = U^\dagger D^\dagger (U^\dagger)^\dagger = U^\dagger D U = N,$$

where the third equality holds if and only if these eigenvalues are real. □

An operator basis for the Hermitian matrices is given by the *Pauli matrices* in Definition 2.3.

Definition 2.3 (Pauli matrices) *The Pauli matrices are the unitary matrices*

$$\sigma_1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_3 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.10}$$

With $\sigma_0 := \mathbb{1}_2$ they form an orthogonal[a] *basis of the $\mathbb{C}^{2\times 2}$ Hermitian matrices.*

[a] Orthogonal with respect to the scalar product $\langle A|B\rangle := \operatorname{Tr}\left(A^\dagger B\right)$.

The Pauli matrices $\sigma_1, \sigma_2, \sigma_3$ are self inverse

$$\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = \mathbb{1}_2 \tag{2.11}$$

and fulfill the commutation relations

$$\left[\sigma_j, \sigma_k\right] := \sigma_j\sigma_k - \sigma_k\sigma_j = 2i\varepsilon_{jkl}\sigma_l \tag{2.12}$$

as well as the anticommutation relations

$$\{\sigma_j, \sigma_k\} := \sigma_j\sigma_k + \sigma_k\sigma_j = 2\delta_{jk}\mathbb{1}_2 \tag{2.13}$$

in the Einstein summation convention for index l. Here, the epsilon tensor ε_{jkl} is equal to 1 if jkl is a cyclic permutation of 123 and equal to −1 if jkl is an anticyclic permutation of 123 and zero otherwise.

The Einstein summation convention is a shorthand for efficiently writing sums, *e.g.*,

$$\varepsilon_{jkl}\sigma_l := \varepsilon_{jk1}\sigma_1 + \varepsilon_{jk2}\sigma_2 + \varepsilon_{jk3}\sigma_3.$$

The matrices $\sigma_1, \sigma_2, \sigma_3$ are often referred to as $\sigma_x, \sigma_y, \sigma_z$ or simply called X, Y, Z due to the position of their eigenvectors on the surface of the Bloch ball shown in Figure 2.1.

The computational basis $\{|0\rangle, |1\rangle\}$ spans the eigenspace of σ_3 with eigenvalues +1, −1. With the same eigenvalues we find

$$\left\{|+\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), |-\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right\} \tag{2.14}$$

as an eigenbasis induced by σ_1 and

$$\left\{|+i\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle + i|1\rangle\right), |-i\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle - i|1\rangle\right)\right\} \tag{2.15}$$

as an eigenbasis induced by σ_2.

It is often useful to switch between bases. For this reason, the Hadamard matrix is another important unitary Hermitian matrix.

Definition 2.4 (Hadamard matrix) *The Hadamard matrix is defined as*

$$H := \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}. \tag{2.16}$$

Conjugation with the Hadamard matrix maps the Pauli X basis to the Z basis and vice versa while the Y basis is just flipped by a phase, *i.e.*,

$$H\sigma_1H^\dagger = \sigma_3, \quad H\sigma_2H^\dagger = -\sigma_2, \quad H\sigma_3H^\dagger = \sigma_1. \tag{2.17}$$

Likewise, another essential unitary is the single qubit phase matrix.

Definition 2.5 (Phase matrix) *The phase matrix is defined as*

$$S := \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{2.18}$$

Conjugation with the phase matrix S, leaves the Pauli Z basis invariant and maps the X basis to the Y basis as well as Y to $-X$, *i.e.*,

$$S\sigma_1 S^\dagger = \sigma_2, \quad S\sigma_2 S^\dagger = -\sigma_1, \quad S\sigma_3 S^\dagger = \sigma_3. \tag{2.19}$$

In the context of matrices acting on quantum states, the matrices are often referred to as *quantum gates* or simply *gates* acting on the respective qubits.

2.3 Matrix functions

We now introduce a few functions from functional analysis that are useful for the manipulation of the frequently arising matrices in quantum information processing.

A first important notion is that of matrix powers and matrix exponentials of square matrices. Integer powers of matrices are easy to understand. As a generalization of powers for real numbers, we simply write

$$A^n := \underbrace{A \cdot A \cdot \ \ldots \ \cdot A}_{\times n} \tag{2.20}$$

for each square matrix A. Using Theorem 2.1 it is even easy to generalize the notion of powers for normal matrices further.

Definition 2.6 (Powers of normal matrices) *For any normal matrix $N = \sum_{i=1}^d \alpha_i |\psi_i\rangle\langle\psi_i|$ and arbitrary exponent $x \in \mathbb{C}$ we define*

$$N^x := \sum_{i=1}^d \alpha_i^x |\psi_i\rangle\langle\psi_i|. \tag{2.21}$$

Using power series expansions of more complicated functions, we can also extend these functions into the domain for normal matrices. We will exemplify this with the matrix exponential and the matrix logarithm.

Definition 2.7 (Matrix exponential, matrix logarithm) *For any normal matrix $N = \sum_{i=1}^d \alpha_i |\psi_i\rangle\langle\psi_i|$ we define its exponential as the power series*

$$e^N := \sum_{k=0}^\infty \frac{1}{k!} N^k = \sum_{i=1}^d e^{\alpha_i} |\psi_i\rangle\langle\psi_i|. \tag{2.22}$$

Likewise, we define the logarithm of N as the power series

$$\ln(N) := \sum_{k=1}^{\infty}(-1)^{k+1}\frac{(N-\mathbb{1}_d)^k}{k} = \sum_{i=1}^{d}\ln(\alpha_i)\,|\psi_i\rangle\langle\psi_i|. \qquad (2.23)$$

For N close to the identity in trace norm (*cf.* Definition 2.10), *i.e.* for $\|N-\mathbb{1}\|<1$ we find

$$e^{\ln(N)} = N.$$

It is important to note that matrix exponentials behave analogously to number exponentials with respect to their algebraic rules only if they commute: For two normal matrices N, M, one might expect that the product of their exponentials commutes and that $e^N e^M$ equals e^{N+M}. However, this is only true if $[N, M] := NM - MN = 0$. More generally, we find the so-called *Baker–Campbell–Hausdorff formula* [Bak05; Cam96; Hau06].

Theorem 2.5 (Baker–Campbell–Hausdorff [Bak05; Cam96; Hau06]) *The solution to the equation $e^L = e^M e^N$ is given by the expansion of L in nested commutators of N and M as*

$$L = M + N + \frac{1}{2}[M,N] + \frac{1}{12}([M,[M,N]] - [N,[M,N]]) \qquad (2.24)$$

$$\pm \textit{ higher order nested commutators}, \qquad (2.25)$$

where the higher order terms are of the type $[M,[\cdots[M,[M,N]]\cdots]$.

If M, N commute, the Baker–Campbell–Hausdorff formula reduces to $L = M + N$. Importantly, if M, N commute with their commutator $[N, M]$, it reduces to $L = M + N + \frac{1}{2}[M,N]$.

Matrices arising in quantum information processing frequently have the property of positive (semi-) definiteness.

Equivalently, one could define A to be positive semi-definite if $\langle\psi|A|\psi\rangle \geq 0$ for all $|\psi\rangle$ in $\mathscr{H}$ and positive definite if $\langle\psi|A|\psi\rangle > 0$.

Definition 2.8 (Positive definite, positive semi-definite matrix) *Matrices A are called positive semi-definite if there exist matrices B such that $A = B^\dagger B$. If such a matrix B is additionally invertible, then A is called positive definite.*

The positivity or positive semi-definiteness of a given matrix A are often denoted as $A > 0$ or $A \geq 0$, respectively.

Hermitian matrices are positive definite if their eigenvalues are positive and positive semi-definite if their eigenvalues are nonnegative. Given a spectral decomposition of a Hermitian matrix $A = \sum_m m|m\rangle\langle m|$, it is straightforward to calculate $B = \sqrt{A} = \sum_m \sqrt{m}|m\rangle\langle m|$ if the eigenvalues are nonnegative.

It is possible to decompose square matrices into the product of a unitary rotation and a positive semi-definite matrix by the *polar decomposition*.

Theorem 2.6 (Polar decomposition [NC10]) *For any square matrix A there exists a unitary matrix U such that*

$$A = U\sqrt{A^\dagger A} = \sqrt{AA^\dagger}U. \qquad (2.26)$$

If A is invertible it follows that U is unique.

The polar decomposition is intimately related to a further decomposition called the *singular value decomposition*.

Theorem 2.7 (Singular value decomposition [NC10]) *For any matrix A there exist two unitary matrices U and V such that*

$$A = UDV^\dagger \tag{2.27}$$

with a (rectangular) diagonal matrix D. Its diagonal elements are non-negative and called the singular values of A.

It is straightforward to see that with the singular value decomposition of a square matrix $A = UDV^\dagger$ one can determine the polar decomposition as $U_{\text{polar}} = UV^\dagger$ and $\sqrt{A^\dagger A} = VDV^\dagger$, $\sqrt{AA^\dagger} = UDU^\dagger$, respectively.

Another frequently used matrix function in quantum information theory is the trace of a matrix. The Pauli matrices introduced in Definition 2.3 are *traceless*, *i.e.*, their trace equals zero.

Definition 2.9 (Trace) *The trace of a matrix A is the sum of its diagonal,*

$$\operatorname{Tr}(A) := \sum_i (A)_{ii}. \tag{2.28}$$

Since the elementwise addition in Equation 2.28 is linear, the trace is a linear function, *i.e.*, $\operatorname{Tr}(A+B) = \operatorname{Tr}(A) + \operatorname{Tr}(B)$ for two matrices A, B and $\operatorname{Tr}(aA) = a\operatorname{Tr}(A)$ for matrices A and complex valued scalar factors a, since the elementwise addition is linear. A second important property of the trace is that is cyclic

$$\operatorname{Tr}(AB) = \operatorname{Tr}(BA). \tag{2.29}$$

The cyclicity of the trace implies that the trace of a matrix A is invariant under conjugation with unitary matrices U, *i.e.*,

$$\operatorname{Tr}(UAU^\dagger) = \operatorname{Tr}(AU^\dagger U) = \operatorname{Tr}(A). \tag{2.30}$$

For evaluating the trace of the product of a matrix A and the ket-bra matrix derived from a unit vector $|\psi\rangle$ on the same Hilbert space, we find

$$\operatorname{Tr}(A|\psi\rangle\langle\psi|) = \sum_i \langle i|A|\psi\rangle\langle\psi|i\rangle = \langle\psi|A|\psi\rangle, \tag{2.31}$$

where we used the *Gram–Schmidt procedure* [Sch07; NC10] to extend $|\psi\rangle$ to an orthonormal basis $|i\rangle$.

The trace induces a norm for matrices. This trace norm is later used to define the trace distance, which is a common measure on the space of quantum density matrices (see Definition 2.16).

Definition 2.10 (Trace norm) *We denote the trace norm of a matrix by*

$$\|A\| := \operatorname{Tr}\left(\sqrt{AA^\dagger}\right). \tag{2.32}$$

A matrix' trace norm is equal to the sum of its singular values (see Theorem 2.7).

After we have defined the tensor product (see Definition 2.11) in the following section we will define a related operation, the *partial trace* (see Definition 2.21).

2.4 Composite quantum systems

While systems of multiple qubits are harder to visualize than single qubit systems, we can mathematically describe their state spaces with the help of tensor products.

Definition 2.11 (Tensor product) *For a $k \times l$-matrix $A \in \mathbb{C}^{k\times l}$ and an $m \times n$-matrix $B \in \mathbb{C}^{m\times n}$, we define $A \otimes B$ to be the $km \times ln$-matrix*

$$\begin{pmatrix} (A)_{1,1}(B)_{1,1} & \cdots & (A)_{1,1}(B)_{1,n} & \cdots & (B)_{1,1}(A)_{1,l} & \cdots & (A)_{1,l}(B)_{1,n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ (A)_{1,1}(B)_{m,1} & \cdots & (A)_{1,1}(B)_{m,n} & \cdots & (A)_{1,l}(B)_{m,1} & \cdots & (A)_{1,l}(B)_{m,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ (B)_{1,1}(A)_{k,1} & \cdots & (A)_{k,1}(B)_{1,n} & \cdots & (B)_{1,1}(A)_{k,l} & \cdots & (B)_{1,n}(A)_{k,l} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ (A)_{k,1}(B)_{m,1} & \cdots & (A)_{k,1}(B)_{m,n} & \cdots & (B)_{m,1}(A)_{k,l} & \cdots & (A)_{k,l}(B)_{m,n} \end{pmatrix}. \tag{2.33}$$

It is common to write $|0 \cdots 0\rangle$ for tensor products of the type

$$|0\rangle \otimes |0\rangle \otimes |0\rangle \otimes \ldots \otimes |0\rangle. \tag{2.34}$$

Generalizing Equation 2.3 we can write vectors $|\psi\rangle$ in $(\mathbb{C}^2)^{\otimes n}$ as

$$|\psi\rangle = \alpha_{0\cdots0}|0\cdots0\rangle + \ldots + \alpha_{1\cdots1}|1\cdots1\rangle = \sum_{b\in\{0,1\}^{\times n}} \alpha_b|b\rangle \tag{2.35}$$

with $\langle\psi|\psi\rangle = \sum |\alpha_b|^2 = 1$. The summation in Equation 2.35 is over all binary strings $(b_1, b_2, \ldots, b_n) \in \{0,1\}^{\times n}$ of length n. Vectors of this type represent any pure state of a system of n qubits.

The Schmidt decomposition follows from the singular value decomposition $U\Sigma V^\dagger$ of a matrix constructed from the tensor product of basis vectors of $\mathcal{H}_A$ and $\mathcal{H}_B$. Here, U and V are unitary matrices and Σ is a (rectangular) diagonal matrix with nonnegative entries α_i.

Theorem 2.8 (Schmidt decomposition [Sch07]) *Any pure state vector $|\psi_{AB}\rangle$ in the tensor product of two Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ has a Schmidt decomposition*

$$|\psi_{AB}\rangle = \sum_i \alpha_i |\psi_A^i\rangle \otimes |\psi_B^i\rangle, \tag{2.36}$$

where $|\psi^i_{A/B}\rangle$ are orthonormal vectors in the respective Hilbert spaces $\mathcal{H}_{A/B}$ and $\langle\psi_{AB}|\psi_{AB}\rangle = \sum \alpha_i^2 = 1$ with $\alpha_i > 0$. [a]

[a] The nonnegative real numbers α_i are known as the Schmidt-coefficients.

The Schmidt decomposition is essential when regarding reduced and purified density matrices (*cf.* Definition 2.15, 2.22, 2.23).

2.5 Density matrices

In classical probability theory, it is common to denote the outcomes of a p-biased coin toss by 0 for heads and 1 for tails, or vice versa. For such a random classical bit, we can denote the probability of having 0 as p and that of having 1 as $1 - p$ with the constraint $0 \leq p \leq 1$. That is, the state space of a probabilistic classical bit is a line segment of length one.

While in quantum mechanics probabilities are omnipresent, the best quantum analog of classical probability distributions are not quantum states as defined in Equation 2.3 but *density matrices*.

Even if a large quantum system –maybe even the whole universe– can be described by a pure state as a state vector, this is not necessarily true for its subsystems. In general a subsystem of a quantum system in a pure state cannot be described as a pure state. Simple examples of this are maximally entangled *Bell states* [Bel64] or *EPR pairs* [EPR35a].

The initial work of Einstein, Podolsky and Rosen [EPR35a] was concerned with measurements of position and momentum. The use of spin-$\frac{1}{2}$ degrees of freedom to illustrate the Einstein-Podolsky-Rosen paradox goes back to Bohm [Boh51].

Definition 2.12 (Bell basis) *The Bell state basis is given by the four states*

$$|\phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{2.37}$$

$$|\phi^-\rangle := \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \tag{2.38}$$

$$|\psi^+\rangle := \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \tag{2.39}$$

$$|\psi^-\rangle := \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{2.40}$$

The reduced states of Bell states are only representable as *density matrices* and not as state vectors, since equating Equations 2.45 and 2.46 leads to a contradiction when solving for α and β. Tracing out any of the qubits leaves the other in the so-called maximally mixed state.

The states in the Bell basis can be transformed into each other by local Pauli operations, *e.g.* we have

$$|\phi^-\rangle = (\sigma_3 \otimes \mathbb{1}_2)\,|\phi^+\rangle = (\mathbb{1}_2 \otimes \sigma_3)\,|\phi^+\rangle, \tag{2.41}$$

$$|\psi^+\rangle = (\sigma_1 \otimes \mathbb{1}_2)\,|\phi^+\rangle = (\mathbb{1}_2 \otimes \sigma_1)\,|\phi^+\rangle, \tag{2.42}$$

$$|\psi^-\rangle = (\sigma_3 \otimes \mathbb{1}_2)\,|\psi^+\rangle = (\sigma_3 \otimes \sigma_1)\,|\phi^+\rangle. \tag{2.43}$$

The reduced states of Bell states are only representable as *density matrices* and not as state vectors. We can define these density matrices as follows.

Definition 2.13 (Density matrix) *Positive semi-definite matrices of unit trace*

$$\rho := \begin{pmatrix} p & a-bi \\ a+bi & 1-p \end{pmatrix} \in \mathbb{C}^{2\times 2} \tag{2.44}$$

are called density matrices and describe arbitrary quantum states of a qubit.

Since density matrices are Hermitian, we can infer from Equation 2.9 that their diagonal elements are real.

The *pure* state density matrix $|\psi\rangle\langle\psi|$ for the state in Equation 2.3 is given by

$$|\alpha|^2|0\rangle\langle 0| + \alpha\beta^*|0\rangle\langle 1| + \alpha^*\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1| = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix} \tag{2.45}$$

and that of the *maximally mixed* state is proportional to the identity

$$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{2.46}$$

With $\alpha = \cos\frac{\theta}{2}$ and $\beta = e^{i\varphi}\sin\frac{\theta}{2}$ we can also write $|\psi\rangle\langle\psi|$ as

$$\begin{pmatrix} \cos^2\frac{\theta}{2} & e^{-i\varphi}\cos\frac{\theta}{2}\sin\frac{\theta}{2} \\ e^{i\varphi}\cos\frac{\theta}{2}\sin\frac{\theta}{2} & \sin^2\frac{\theta}{2} \end{pmatrix}. \tag{2.47}$$

The concepts of purity and maximally mixedness are not only valid for qubits, that is for quantum systems of the dimension $d = 2$, but can be easily generalized to arbitrary dimensions.

For the pure single qubit state defined by Equation 2.45 above, it is easy to see that $|\psi\rangle\langle\psi|^2 = |\psi\rangle\langle\psi|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi|$ and

$$\mathrm{Tr}\,(|\psi\rangle\langle\psi|) = |\alpha|^2 + |\beta|^2 = 1.$$

Definition 2.14 (Purity, pure, mixed) *The purity of a quantum state is defined as* $\mathrm{Tr}\left(\rho^2\right)$*, where* ρ *denotes the density matrix of the state. Quantum states of dimension* d *with purity one are called pure. All other quantum states are called mixed, and those with purity* $\frac{1}{d}$ *are called maximally mixed.*

In particular, quantum systems with n qubits can be interpreted as a quantum system of the dimension $d = 2^n$. For these composite quantum systems of several qubits we can generalize the qubit density matrices from Definition 2.13 to multiple-qubit density matrices in Definition 2.15.

The density matrix formalism was systematically introduced in 1927 by John von Neumann in his seminal work [Neu27] (article in German).

Definition 2.15 (Densitiy matrix for n qubits [Neu27]) *Positive semi-definite matrices of unit trace acting on the Hilbert space* $(\mathbb{C}^2)^{\otimes n}$ *are called density matrices and describe arbitrary quantum states of* n *qubits.*

The density matrix of $|\phi\rangle^+$ introduced in Equation 2.37 is *e.g.* given by

$$|\phi^+\rangle\langle\phi^+| = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}. \tag{2.48}$$

It has trace $\frac{1}{2} + \frac{1}{2} = 1$ and is positive semi-definite with eigenvalues $0, 0, 0, 1$.

Measures for density matrices

In the space of density matrices we can use the trace norm (see Definition 2.10) to define the trace distance between and the fidelity of two density matrices [NC10].

Definition 2.16 (Trace distance) *For two density matrices* ρ_1, ρ_2 *we define their trace distance to be proportional to the trace norm of their difference, i.e.,*

$$D\left(\rho_1, \rho_2\right) := \frac{1}{2}\|\rho_1 - \rho_2\| = \frac{1}{2}\,\mathrm{Tr}\left(\sqrt{\left(\rho_1 - \rho_2\right)^2}\right) = \frac{1}{2}\sum_i |r_i|\,, \tag{2.49}$$

where r_i *are the eigenvalues of the resulting Hermitian matrix* $\rho_1 - \rho_2$.

The trace distance of two density matrices $D\left(\rho_1, \rho_2\right)$ has an operational interpretation. It is the maximum probability with which a measurement of a quantum system with density matrix ρ_1 can be distinguished from one with density matrix ρ_2.

The second equality in Equation 2.50 holds because density matrices are Hermitian and thus $\sqrt{\rho} = \sqrt{\rho}^\dagger$.

Definition 2.17 (Fidelity) *The fidelity of two density matrices* ρ_1, ρ_2 *is*

$$F\left(\rho_1, \rho_2\right) := \mathrm{Tr}\left(\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}}\right) = \|\sqrt{\rho_1}\sqrt{\rho_2}\|. \tag{2.50}$$

Both the trace distance and the fidelity have values between zero and one and both are symmetric, *i.e.*,

$$D(\rho_1, \rho_2) = D(\rho_2, \rho_1), \tag{2.51}$$

$$F(\rho_1, \rho_2) = F(\rho_2, \rho_1). \tag{2.52}$$

The fidelity equals one when $\rho_1 = \rho_2$, whereas the trace distance between a density matrix and itself is zero.

More generally, the fidelity can be used to bound the trace distance by the inequality [NC10]

$$1 - F(\rho_1, \rho_2) \leqslant D(\rho_1, \rho_2) \leqslant \sqrt{1 - (F(\rho_1, \rho_2))^2}. \tag{2.53}$$

A further similarity is that both the trace distance and the fidelity are invariant under unitary transformations in the sense that

$$D\left(U\rho_1 U^\dagger, U\rho_2 U^\dagger\right) = D(\rho_1, \rho_2), \tag{2.54}$$

$$F\left(U\rho_1 U^\dagger, U\rho_2 U^\dagger\right) = F(\rho_1, \rho_2). \tag{2.55}$$

2.6 Measurements

Having introduced density matrices as the most general representation of quantum systems, we can now turn to the mathematical description of measurements of quantum systems.

Projective measurements

An *observable* is given by any Hermitian operator on the Hilbert space associated with the observed quantum system. The measurement of an observable disturbs the original state by projecting it into a eigenbasis state which depends on the result of the measurement. Mathematically, we define the *projective measurement* or *von-Neumann measurement* of observables in quantum systems as follows.

Definition 2.18 (Projective measurement) *Let $H = H^\dagger$ be an observable on the Hilbert space of a d-dimensional quantum system. The spectral decomposition $H = \sum_m mP_m$ –with eigenspace projectors $P_m := |m\rangle\langle m|$ given by the eigenvectors $H|m\rangle = m|m\rangle$– defines the projective measurement of H on a quantum system with state vector $|\psi\rangle$ as follows. The d possible measurement outcomes correspond to the eigenvalues of H. Every possible measurement result m occurs with probability*

$$\Pr(m) = \langle\psi|P_m|\psi\rangle \tag{2.56}$$

and the quantum system is projected into the state

$$|\psi_m\rangle := \frac{P_m|\psi\rangle}{\sqrt{\Pr(m)}} \tag{2.57}$$

The spectral decompositon for all normal matrices is given by Theorem 2.1.

after measurement.

Note that not all quantum measurements are repeatable in the same way as projective measurements are. A more general definition of quantum measurements is given by the POVMs in Definition 2.20.

Performing a projective measurement multiple times does not change the state further. After one projective measurement of a state $|\psi\rangle$ with outcome m, the post measurement state is described by $|\psi_m\rangle$ in Equation 2.57. The state is not changed by applying the projector P_m for a second time. For a repeated measurement we obtain outcome m with unit probability, since $\langle\psi_m|P_m|\psi_m\rangle = 1$. Inductively each further measurement yields the result m again while the quantum system remains in the state $|\psi_m\rangle$.

Definition 2.19 (Projective Pauli measurements) *We define operators $P_{j,\pm}$ to project into the eigenbases of the Pauli matrices (cf. Definition 2.3). Since $P^2 = P$ for projectors, we can use Equation 2.11 to define for $j \in \{0,1,2,3\}$*

$$P_{j,\pm} := \frac{\mathbb{1}_2 \pm \sigma_j}{2}, \tag{2.58}$$

that is, we have $P_{1,\pm} = |\pm\rangle\langle\pm|$, $P_{2,\pm} = |\pm i\rangle\langle\pm i|$ and $P_{3,\pm} = |\frac{1\mp1}{2}\rangle\langle\frac{1\mp1}{2}|$.

While the *relative phase* in Equation 2.3 does not impact the measurement probabilities in the computational basis, it is relevant for the measurement of other observables, *e.g.* measuring σ_1 for $\alpha|0\rangle \pm \beta|1\rangle$ yields

$$\begin{aligned}\Pr(+) &= \frac{1}{2}\left(|\alpha|^2 + |\beta|^2 \pm \alpha\beta^* \pm \alpha^*\beta\right)\\ &= \frac{1}{2}(\alpha \pm \beta)(\alpha^* \pm \beta^*).\end{aligned}$$

If we measure the qubit state described by Equation 2.3 in the computational basis, *i.e.*, if we measure the observable $\sigma_3 = P_{3,+} - P_{3,-} = |0\rangle\langle 0| - |1\rangle\langle 1|$, the outcome will be -1 with probability $|\alpha|^2$ and $+1$ with probability $|\beta|^2$. The normalization of the qubit state vector ensures that the probabilities for obtaining each possible measurement result add up to one. Since it has no influence on the measurement probabilities, the *global phase* of a state vector has no physical meaning.

For measurements of multiple qubits, we can either measure the qubits independently or we can measure a joint property of the qubits by projecting them onto an entangled basis of the system. If, *e.g.*, we want to measure the two qubit Bell pair $|\phi\rangle^+$ introduced in Equation 2.37 we could measure both qubits independently in the computational basis with projectors $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ or we could jointly measure both qubits simultaneously in the entangled Bell state basis with projectors $\{|\phi^+\rangle\langle\phi^+|, |\phi^-\rangle\langle\phi^-|, |\psi^+\rangle\langle\psi^+|, |\psi^-\rangle\langle\psi^-|\}$. Following the projective measurement description in the former case, a measurement of one of the qubits will project the state for the quantum system into $|00\rangle$ or $|11\rangle$ with equal probability of $\frac{1}{2}$. In the latter case, however, the joint measurement of both qubits in the Bell basis deterministically returns the measurement outcome ϕ^+ with unit probability since the Bells states are orthogonal.

POVM measurements

Not all quantum measurements are repeatable in the same way as the projective measurements introduced in Definition 2.18 are. A more general definition of quantum measurements is given by the POVMs in Definition 2.20.

The acronym POVM stands for positive operator-valued measure.

Definition 2.20 (POVM [NC10]) *A POVM measurement on a quantum system with density matrix ρ is given by a collection of positive semi-definite Hermitian operators $E_i^\dagger E_i \geq 0$ that is indexed by the possible measurement outcomes i and that sums to the identity, that is, $\sum_i E_i^\dagger E_i = \mathbb{1}$.*

The probability of obtaining outcome i is given by[a]

$$\Pr(i) = \mathrm{Tr}(E_i^\dagger E_i \rho), \tag{2.59}$$

while the postmeasurement state can be described by the density matrix

$$\frac{1}{\Pr(i)} E_i \rho E_i^\dagger. \tag{2.60}$$

[a] The probabilities $\Pr(i)$ are nonnegative since all $E_i^\dagger E_i$ are positive semi-definite and add up to one since the set $\{E_i^\dagger E_i\}_i$ sums to the identity.

A POVM induced by the spectral decomposition of a Hermitian matrix

$$A = \sum_i a_i E_i^\dagger E_i \tag{2.61}$$

with $E_i^\dagger E_i := |\psi_i\rangle\langle\psi_i|$ is equivalent to the projective measurement of A as introduced in Definition 2.18. In particular, the set of possible measurement outcomes is given by the spectrum of A.

2.7 Reduced states

The Schmidt decomposition of Equation 2.36 is particularly useful when examining the *reduced states* of quantum systems. When we are interested in the measurement statistics of a subsystem A of a composite system on A and some environment B, it is sufficient to investigate the density matrix describing subsystem A. In fact the expectation value of an operator U_A that only acts on $\mathcal{H}_A$ and trivially on the environment is described by

$$\begin{aligned}
\langle\psi_{AB}|U_A \otimes \mathbb{1}_B|\psi_{AB}\rangle &= \sum_{i,j} \alpha_i \alpha_j^* \left(\langle\psi_A^j| \otimes \langle\psi_B^j|\right) U_A \otimes \mathbb{1}_B \left(|\psi_A^i\rangle \otimes |\psi_B^i\rangle\right) \\
&= \sum_{i,j} \alpha_i \alpha_j^* \langle\psi_A^j|U_A|\psi_A^i\rangle \delta_{ij} \\
&= \sum_i |\alpha_i|^2 \langle\psi_A^j|U_A|\psi_A^i\rangle,
\end{aligned}$$

where the first equality is the Schmidt decomposition, the second equality is its orthonormal basis property and the third equality is obtained by simplifying the j summation with the Kronecker delta. The last expression is also equal to $\mathrm{Tr}(\rho_A U_A)$ with

$$\rho_A := \mathrm{Tr}_B(|\psi_{AB}\rangle\langle\psi_{AB}|) = \sum_i |\alpha_i|^2 |\psi_A^i\rangle\langle\psi_A^i|. \tag{2.62}$$

The trace function that is indexed by some quantum (sub) system B is called the partial trace Tr_B. We define it as follows.

Definition 2.21 (Partial trace) *Let ρ_{AB} be a matrix acting on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ of two quantum systems A and B. The partial trace of ρ_{AB} with respect to $\mathcal{H}_B$ is denoted by $\mathrm{Tr}_B(\rho_{AB})$, acts on $\mathcal{H}_A$ and is implicitly defined by the trace equality for matrices A acting on the Hilbert space $\mathcal{H}_A$*

$$\mathrm{Tr}\left(\mathrm{Tr}_B(\rho_{AB})A\right) = \mathrm{Tr}\left(\rho_{AB}(A \otimes \mathbb{1}_B)\right). \tag{2.63}$$

With an orthonormal basis $\{|i\rangle_B\}$ of $\mathcal{H}_B$, we can use

$$\langle\phi|_A \operatorname{Tr}_B(\rho_{AB})|\psi\rangle_A = \sum_i \left(\left(\langle\phi|_A \otimes \langle i|_B\right) \rho_{AB} \left(|\psi\rangle_A \otimes |i\rangle_B\right)\right) \tag{2.64}$$

to calculate the matrix elements of $\operatorname{Tr}_B(\rho_{AB})$.

Motivated by the observation of Equation 2.62, we define reduced density matrices using the partial trace.

Definition 2.22 (Reduced density matrix) *The reduced density matrix ρ_A of a composite quantum system ρ_{AB} is given by $\rho_A := \operatorname{Tr}_B(\rho_{AB})$.*

As alluded to at the beginning of the section, the reason for considering reduced density matrices is that the reduced density matrix provides the correct measurement statistics for measurements on the subsystem when we only have access to that subsystem. Using the definitions above, we will show why this is indeed true.

In Subsection 2.6 we gave an introduction to the measurement formalism. Specifically, given a set of POVM measurement operators $\{E_i^\dagger E_i\}_i$ on a quantum system with density matrix ρ_{AB} (see Definition 2.20), one can calculate the probability of outcome i as

$$\Pr(i) = \operatorname{Tr}\left(E_i^\dagger E_i \rho_{AB}\right) = \operatorname{Tr}\left((F_i^\dagger F_i \otimes \mathbb{1}_B)\rho_{AB}\right), \tag{2.65}$$

where we note that a measurement that acts only on the subsystem A acts trivially on the subsystem B and is therefore necessarily of the type $E_i^\dagger E_i = F_i^\dagger F_i \otimes \mathbb{1}_B$.

Since the trace is cyclic, Equation 2.63 and Equation 2.65 now imply

$$\Pr(i) = \operatorname{Tr}\left(\rho_{AB}(F_i^\dagger F_i \otimes \mathbb{1}_B)\right) = \operatorname{Tr}\left(\operatorname{Tr}_B(\rho_{AB})F_i^\dagger F_i\right) = \operatorname{Tr}\left(\rho_A F_i^\dagger F_i\right) \tag{2.66}$$

meaning that probabilities of measurement outcomes are indistinguishable between measuring $\{E_i^\dagger E_i\}_i = \{F_i^\dagger F_i \otimes \mathbb{1}_B\}_i$ on ρ_{AB} and measuring $\{F_i^\dagger F_i\}_i$ on $\rho_A := \operatorname{Tr}_B(\rho_{AB})$.

2.8 Purifications

Conversely to reducing the size of a quantum system at hand by investigating subsystems with reduced density matrices, we can extend the size of quantum systems by constructing so-called *purifications* with an environment of the quantum system. Their name derives from the fact that it is possible to write every density matrix ρ_A of a quantum system A as the reduced density matrix of a pure state $\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$ with some environment system B.

The spectral theorem is given in the section on Hermitian, unitary and Pauli matrices as Theorem 2.1.

Since ρ_A is a density matrix, it is positive semi-definite and Hermitian –and since any Hermitian matrix can be diagonalized by the spectral theorem– we can write

$$\rho_A = \sum_i |\alpha_i|^2 |\psi_A^i\rangle\langle\psi_A^i|, \tag{2.67}$$

with nonnegative coefficients $|\alpha_i|^2$. By introducing an environment Hilbert space $\mathcal{H}_B$ –with dimension equal to the nonzero elements in $\{|\alpha_i|\}$– and an orthonormal basis of $\mathcal{H}_B$

$$\{|\psi_B^j\rangle\}_{j=1}^{|\{|\alpha_i|:\ \alpha_i\neq 0\}|} \tag{2.68}$$

we can define

$$|\psi_{AB}\rangle := \sum_j |\alpha_j||\psi_A^j\rangle \otimes |\psi_B^j\rangle. \tag{2.69}$$

Definition 2.23 (Purification) *Any density matrix of a quantum system A,*

$$\rho_A = \sum_i |\alpha_i|^2 |\psi_A^i\rangle\langle\psi_A^i|, \tag{2.70}$$

can be expressed as the reduced state of a pure state density matrix

$$\rho_{AB} = \sum_{j,k} |\alpha_j \alpha_k| |\psi_A^j\rangle\langle\psi_A^k| \otimes |\psi_B^j\rangle\langle\psi_B^k| \tag{2.71}$$

on A and an environment B, where the Hilbert space of the latter has an orthonormal basis $\{|\psi_B^j\rangle\}_{j=1}^{|\{|\alpha_i|:\ \alpha_i\neq 0\}|}$.

In summary, to purify a mixed state ρ_A, we identify basis vectors in which ρ_A is diagonal and define a purification by introducing a suitable environment system B such that we can write down a a joint state on AB which is equal to ρ_A when tracing out the environment B.

2.9 Pauli and Clifford group

The Pauli matrices introduced in Definition 2.3 form a group under matrix multiplication –the *Pauli group* $\mathcal{P}$. A product of Pauli matrices is a Pauli matrix with one of four possible scalar phases $+1, -1, +i$ or $-i$, that is,

$$\mathcal{P} := \langle\{\pm 1, \pm i\} \cdot \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}\rangle\,. \tag{2.72}$$

Taking the tensor product generalizes this definition to n qubits.

Definition 2.24 (Pauli group) *The Pauli group on n qubits is defined as*

$$\mathcal{P}_n := \langle\{\pm 1, \pm i\} \cdot \{P_1 \otimes P_2 \otimes \cdots \otimes P_n\}\rangle\,, \tag{2.73}$$

where the tensor factors P_i for $i \in \{1, \ldots, n\}$ are arbitrary Pauli matrices.

The Pauli group is a finite subgroup of order 4^{n+1} in the unitary group $\mathcal{U}(2^n)$. The normalizer of the Pauli group $\mathcal{P}_n$ in $\mathcal{U}(2^n)$ is called the *Clifford group* $\mathcal{C}_n$. As elements of the normalizer of a subgroup need to commute with the group as a set, the Pauli group is invariant under conjugation with elements from the Clifford group.

Definition 2.25 (Clifford group) *The n qubit Clifford group $\mathcal{C}_n$ is the group of unitary matrices $U \in \mathcal{U}(2^n)$ satisfying $U\mathcal{P}_nU^\dagger = \mathcal{P}_n$.*

In the context of local complementation (*cf.* Definition 4.7 in Section 4.4) we will later be interested in the *local Clifford group* $\mathscr{C}_n^l$.

Definition 2.26 (Local Clifford group) *The local Clifford $\mathscr{C}_n^l$ group is the subgroup of $\mathscr{C}_n$ that contains all n-fold tensor products of elements in $\mathscr{C}_1$.*

2.10 Separable states and entanglement

Definition 2.27 (Separability and entanglement) *A quantum state represented by a density matrix $\rho_{1,2}$ acting on the tensor product of Hilbert spaces $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ is called separable if it can be written as the convex combination*

$$\rho_{1,2} = \sum_i p_i \left(\rho_1^i \otimes \rho_2^i\right) \tag{2.74}$$

with $0 \leq p_i \leq 1$, $\sum_i p_i = 1$ and ρ_k^i denoting density matrices acting on the Hilbert spaces $\mathbb{C}^{d_k}$ for all summation indices i. Otherwise $\rho_{1,2}$ is called entangled.

It follows that a state vector $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ represents an entangled quantum system if and only if it cannot be written in the form

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle\,, \quad \text{with } |\psi_k\rangle \in \mathbb{C}^{d_k}. \tag{2.75}$$

As a simple example consider the state

$$|\varphi\rangle = \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right) \tag{2.76}$$

together with the Bell states from Definition 2.12. While $|\varphi\rangle = |+\rangle \otimes |-\rangle$ is separable, all Bell states are entangled. The latter becomes evident by considering the following. Setting any of the Bell states equal to

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle, \tag{2.77}$$

either both green coefficients would need to have absolute value 0 and both violet coefficients absolute value $\frac{1}{\sqrt{2}}$ or vice versa. But since a product is zero if and only if one of its factors vanishes, this means that at least two of $\alpha, \beta, \gamma, \delta$ are zero. This is a direct contradiction to the other coefficients having absolute value $\frac{1}{\sqrt{2}}$.

Quantum communication | 3

3.1 Quantum teleportation

Bipartite entangled states can be used to move information encoded in quantum states through spacetime. In particular, this idea leads to a simple communication protocol called *quantum teleportation*. What sounds like science fiction is just a simple quantum communication protocol that is feasible in the real world with today's technology [Urs+04] and already breaching distances of 1200 km using satellites [Li+22].

The possibility of quantum teleportation –in essence transferring the quantum state of one particle to another one– was suggested by Bennet *et al.* [Ben+93] and first implemented by Bouwmeester *et al.* [Bou+97]. A review about today's advances in quantum teleportation can be found in Reference [Pir+15].

We call the two generic participants of any two party communication protocol Alice and Bob. While Alice is the sender of quantum information, Bob is its designated recipient. Quantum teleportation simply works as follows. Alice and Bob start by sharing an entangled communication resource with each other, *e.g.*, a Bell pair $|\phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with both of them holding one of its qubits (*cf.* Figure 3.1).

Without loss of generality we describe the quantum teleportation protocol using $|\phi^+\rangle$ states. Equivalent formulations using other Bell pairs from Definition 2.12 are straightforward with local basis changes.

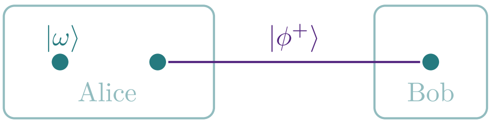


Figure 3.1: Schematic of the joint quantum systems of Alice and Bob at the beginning of the quantum teleportation protocol.

Alice can now transmit the quantum information that is encoded in an arbitrary second qubit (*cf.* Equation 2.3) $|\omega\rangle := \alpha|0\rangle+\beta|1\rangle$ she holds to Bob by jointly measuring her qubits and by only sending classical information on the measurement outcome to Bob. In the process the entanglement will be consumed, so that after the protocol is run, the resulting state is separable between the systems of Alice and Bob (*cf.* Figure 3.2).

Equivalently, Alice can entangle both of her qubits with a $CNOT$ gate and apply a Hadamard gate on her second qubit before measuring both qubits in the computational basis. The outcomes can then be used by Bob to recover $|\omega\rangle$ on his qubit.

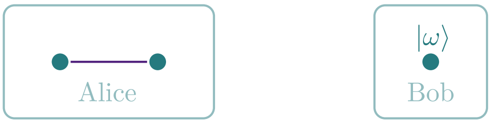


Figure 3.2: Schematic of the joint quantum systems of Alice and Bob after termination of the quantum teleportation protocol.

The joint quantum state at the beginning of the protocol is given by

$$\begin{aligned} |\omega\rangle|\phi^+\rangle &= \frac{1}{\sqrt{2}}(|\omega\rangle_A \otimes |0\rangle_A \otimes |0\rangle_B + |\omega\rangle_A \otimes |1\rangle_A \otimes |1\rangle_B) && (3.1)\\ &= \frac{1}{\sqrt{2}}(\alpha|00\rangle_A \otimes |0\rangle_B + \alpha|01\rangle_A \otimes |1\rangle_B && (3.2)\\ &\quad +\beta|10\rangle_A \otimes |0\rangle_B + \beta|11\rangle_A \otimes |1\rangle_B), && (3.3) \end{aligned}$$

where the indices refer to who can access the individual qubits.

$$
\begin{aligned}
|\phi^+\rangle|\omega\rangle &\propto \alpha|000\rangle + \alpha|110\rangle + \beta|001\rangle + \beta|111\rangle\\
|\phi^-\rangle|\omega\rangle &\propto \alpha|000\rangle - \alpha|110\rangle + \beta|001\rangle - \beta|111\rangle\\
|\psi^+\rangle|\omega\rangle &\propto \alpha|010\rangle + \alpha|100\rangle + \beta|011\rangle + \beta|101\rangle\\
|\psi^-\rangle|\omega\rangle &\propto \alpha|010\rangle - \alpha|100\rangle + \beta|011\rangle - \beta|101\rangle
\end{aligned}
$$

Alice now performs a measurement in the Bell basis on both of her qubits and sends the outcome of her measurement to Bob. Since we can rewrite

$$
\begin{aligned}
|\omega\rangle|\phi^+\rangle = \frac{1}{2}(&|\phi^+\rangle_A \otimes |\omega\rangle_B + |\phi^-\rangle_A \otimes \sigma_3|\omega\rangle_B && (3.4)\\
&+|\psi^+\rangle_A \otimes \sigma_1|\omega\rangle_B + |\psi^-\rangle_A \otimes \sigma_1\sigma_3|\omega\rangle_B), && (3.5)
\end{aligned}
$$

her measurement will project the qubit that Bob holds into one of the four states $\{|\omega\rangle, \sigma_3|\omega\rangle, \sigma_1|\omega\rangle, \sigma_1\sigma_3|\omega\rangle\}$ for the measurement outcomes $\{\phi^+, \phi^+, \psi^+, \psi^-\}$, respectively. Based on the measurement result which he receives from Alice, Bob can perform a conditional local correction operation on his qubit so that his qubit is in exactly the same quantum state $|\omega\rangle$ that Alice's second qubit was in at the beginning of the protocol. Note that all of the above was possible without either Alice or Bob knowing the amplitudes α or β at any point during the protocol.

While the possibility of quantum teleportation is a fascinating facet of nature, it does neither allow for the cloning of unknown quantum states nor does it allow for communication to bridge distances faster than the speed of light.

The so-called no-cloning theorem was proven by Wootters and Zurek in 1982 [WZ82].

Cloning of unknown quantum states is impossible here since Alice's second qubit has to be projected together with her first one –before Bob can recover the original state of her second qubit. At both the beginning and the end of the quantum teleportation protocol, there is only one qubit in the unknown quantum state $|\omega\rangle$.

Communication faster than the speed of light is impossible here due to the probabilistic nature of Alice's measurement. All four possible measurement outcomes appear with equal probability of $\frac{1}{4}$. This means that without receiving the classical correction information about her measurement outcome from Alice (which can only reach Bob with the speed of light), Bob does not have a better than random chance to recover the unknown quantum state $|\omega\rangle$.

3.2 Entanglement swapping, distillation and quantum repeaters

Bipartite entangled states from different sources can be merged into longer range bipartite entangled states by so-called *entanglement swapping*. However, when the entangled states are noisy, the noise is amplified for this merged entangled state. Fortunately, the entanglement of multiple noisy entangled states can be converted into a single, less noisy entangled state by a process called *entanglement distillation*.

Nested protocols of repeated entanglement swapping and entanglement distillation are called *quantum repeater* protocols. They allow for quantum communication protocols bridging larger distances than protocols without quantum repeaters.

In the following, we will briefly introduce both entanglement swapping and entanglement distillation and explain how they can be combined to form a quantum repeater.

Entanglement swapping

It is possible to create entanglement between particles that have never interacted in the past [YS92]. In particular, two bipartite entangled states shared between quantum systems A, C_1 and B, C_2 can be *swapped* into a –potentially longer range– bipartite entangled state between A, B and a second one between the auxillary systems C_1, C_2. This idea is called *entanglement swapping* and was introduced by Żukowski *et al.* in Reference [Żuk+93]. Entanglement swapping is enabled by a joint entangled basis measurement of C_1 and C_2 and classical communication. Astonishingly, this is possible even if the quantum systems A and B never interact.

After its initial proposal, entanglement swapping was first implemented by Pan *et al.* [Pan+98]. Today, successive entanglement swapping with three entangled states is feasible [Goe+08] and even a combination of entanglement swapping and quantum teleportation can be achieved. The latter was demonstrated by Hermans *et al.* [Her+22b].

We call the three generic participants an entanglement swapping protocol Alice, Bob and Charlie. While Alice and Bob want to generate entanglement without being initially entangled, Charlie is entangled to both Alice and Bob at the beginning of the protocol. Charlie wants to help Alice and Bob to generate entanglement by *"sacrificing"* his entanglement to both of them.

Entanglement swapping simply works as follows. Both Alice and Charlie as well as Charlie and Bob start by sharing an entangled communication resource with each other, *e.g.*, a Bell pair $|\phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with both of them holding one of its qubits (*cf.* Figure 3.3).

W.l.o.g. we describe the entanglement swapping protocol using $|\phi^+\rangle$ states. Equivalent formulations using other Bell pairs from Definition 2.12 are straightforward with local basis changes.

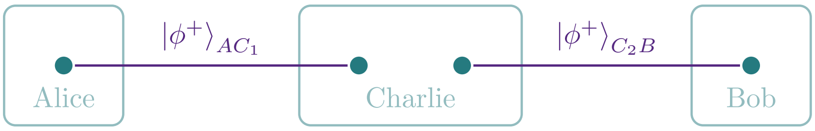


Figure 3.3: Schematic of the quantum systems A, B and C_1, C_2 of Alice, Bob and Charlie at the beginning of the entanglement swapping protocol.

Charlie can now *swap* the entanglement that he has with both Alice and Bob by jointly measuring the two qubits he holds in the Bell basis. Upon receiving the measurement outcome $\varphi \in \{\phi^+, \phi^-, \psi^+, \psi^-\}$ he only needs to send classical information on this outcome to either Alice or Bob. The recipient of the measurement outcome information will then be able to locally correct the joint state $|\varphi\rangle$ of Alice and Bob to be a ϕ^+ Bell pair. This process swaps the entanglement, in the sense that after the protocol is run, the resulting state is separable between the systems of Alice and Charlie and the systems of Bob and Charlie, whereas Alice's qubit is entangled with Bob's and both of Charlie's qubits are entangled to each other (*cf.* Figure 3.4).

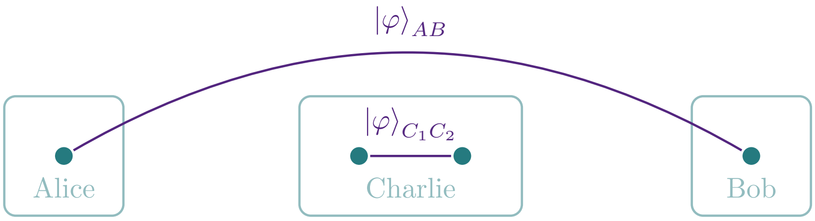


Figure 3.4: Schematic of the quantum systems A, B and C_1, C_2 of Alice, Bob and Charlie after termination of the entanglement swapping protocol.

The joint quantum state $|\phi^+\rangle|\phi^+\rangle$ at the start of the protocol is given by

$$\frac{1}{2}(|0000\rangle_{AC_1C_2B} + |0011\rangle_{AC_1C_2B} + |1100\rangle_{AC_1C_2B} + |1111\rangle_{AC_1C_2B}) \tag{3.6}$$

$$= \frac{1}{2}(|0000\rangle_{C_1C_2AB} + |0101\rangle_{C_1C_2AB} + |1010\rangle_{C_1C_2AB} + |1111\rangle_{C_1C_2AB}) \tag{3.7}$$

where the indices refer to who can access the individual qubits. For the equality of Equations 3.6 and 3.7 we have simply changed the order of the quantum systems.

Since for the tensor product of two Bell pairs of the same type we find

$$|\phi^+\rangle|\phi^+\rangle = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle) \tag{3.8}$$

$$|\phi^-\rangle|\phi^-\rangle = \frac{1}{2}(|0000\rangle - |0011\rangle - |1100\rangle + |1111\rangle) \tag{3.9}$$

$$|\psi^+\rangle|\psi^+\rangle = \frac{1}{2}(|0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle) \tag{3.10}$$

$$|\psi^-\rangle|\psi^-\rangle = \frac{1}{2}(|0101\rangle - |0110\rangle - |1001\rangle + |1010\rangle), \tag{3.11}$$

we can rewrite Equation 3.7 to state that $|\phi^+\rangle_{AC_1}|\phi^+\rangle_{C_2B}$ is equal to

$$\frac{1}{2}\big(|\phi^+\rangle|\phi^+\rangle + |\phi^-\rangle|\phi^-\rangle + |\psi^+\rangle|\psi^+\rangle + |\psi^-\rangle|\psi^-\rangle\big)_{C_1C_2AB}. \tag{3.12}$$

From Equation 3.12 it is evident that measuring the two qubits C_1 and C_2 in the Bell basis will project the qubits A and B that Alice and Bob hold into the state $|\varphi\rangle_{AB} \in \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ for the respective measurement outcome $\varphi \in \{\phi^+, \phi^+, \psi^+, \psi^-\}$ on the qubits C_1 and C_2. After receiving the measurement result from Charlie, both Alice and Bob are able to perform a a conditional local correction operation on their qubit, so that their joint quantum state is $|\phi^+\rangle$.

Even though the quantum systems A and B never interact, it is important that Alice and Bob agree beforehand on who will correct the state. In practical applications, either only one of the two receives the measurement result in order to avoid contradictory corrections –or the entangled state is measured by both Alice and Bob and the resulting correlations are corrected during a round of post processing (see Section 3.3 on quantum key distribution).

Entanglement distillation

Entanglement distillation or *entanglement purification* was first proposed by Bennett *et al.* for pure states in Reference [Ben+96a] and within the same year for mixed states in Reference [Ben+96b] with Erratum [Ben+97].

In the following we will describe the more efficient protocol for entanglement distillation introduced by Deutsch *et al.* [Deu+96]. The protocol is performed over multiple rounds. A source of noisy bipartite entangled states provides both Alice and Bob access to one qubit of each entangled state it produces. Alice and Bob seek to purify this entanglement across the rounds of the protocol.

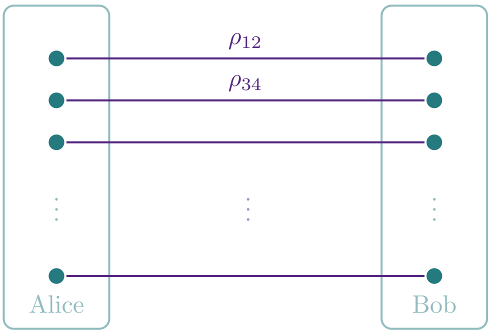


Figure 3.5: Schematic of the quantum systems of Alice and Bob at the beginning of the entanglement distillation protocol.

Alice and Bob start each round with two noisy entangled qubit pairs, which they share by each holding one of the qubits of both pairs. The first iteration of the protocol is performed on the density matrices ρ_{12} and ρ_{34} visualized in Figure 3.5.

Alice starts the protocol by performing the single-qubit Clifford unitary

$$\sqrt{-i\sigma_1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} \tag{3.13}$$

on both of her qubits, while Bob is performing the inverse operation $\sqrt{i\sigma_1}$ on each of his two qubits.

The Clifford $\sqrt{-i\sigma_1}$ permutes the Pauli matrices as $(\sigma_1, \sigma_2, \sigma_3) \mapsto (\sigma_1, \sigma_3, -\sigma_2)$ and $\sqrt{i\sigma_1}$ as $(\sigma_1, \sigma_2, \sigma_3) \mapsto (\sigma_1, -\sigma_3, \sigma_2)$.

In the next step, Alice and Bob each perform a coordinated controlled-NOT gate on their two qubits –*i.e.* both Alice and Bob choose the same pair for their control qubit– and measure the target qubit in the computational basis. In Figure 3.5, the control pair is ρ_{12} and the target pair is ρ_{34}.

A conditional σ_3 gate or controlled-NOT gate on two qubits acts as

$$\underset{i \to j}{\text{CNOT}} \, |i\rangle \otimes |j\rangle = |i\rangle \otimes |i \oplus j\rangle,$$

where i is the control and j the target qubit. It can be represented by the matrix

$$\underset{1 \to 2}{\text{CNOT}} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

If their measurement outcomes coincide, Alice and Bob keep only the control pair for the next round of the purification protocol and repeat the procedure with both this pair and the next pair that is provided by the source. If their measurement outcomes do not coincide, both the control pair and the target pair are discarded. That is, in the latter case, the protocol is restarted.

We denote the density matrix of the former control pair after this successful iteration as $\rho_{12}^{=}$ and its density matrix after an unsuccessful iteration as $\rho_{12}^{\neq}$. A successful iteration of the entanglement distillation protocol is visualized in Figure 3.6.

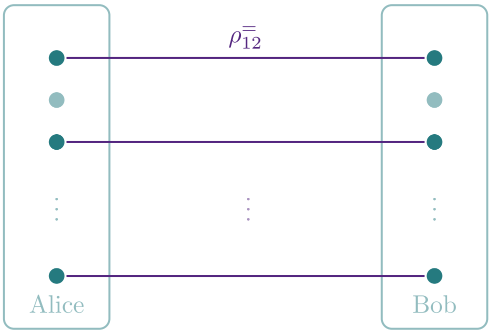


Figure 3.6: Schematic of the quantum systems of Alice and Bob after the termination of a successful round of the entanglement distillation protocol.

We will now examine in more detail how this protocol works. Assume that Alice and Bob start out with a tensor product $\rho_{12} \otimes \rho_{34}$ of two 2-qubit density matrices that are diagonal in the Bell basis. That is, we have

$$\begin{aligned} \rho_{ab} &= \alpha|\phi^+\rangle\langle\phi^+| + \beta|\phi^-\rangle\langle\phi^-| + \gamma|\psi^+\rangle\langle\psi^+| + \delta|\psi^-\rangle\langle\psi^-| && (3.14) \\ &= \frac{1}{2(\alpha+\beta+\gamma+\delta)} \begin{pmatrix} \alpha+\beta & 0 & 0 & \alpha-\beta \\ 0 & \gamma+\delta & \gamma-\delta & 0 \\ 0 & \gamma-\delta & \gamma+\delta & 0 \\ \alpha-\beta & 0 & 0 & \alpha+\beta \end{pmatrix}. && (3.15) \end{aligned}$$

This can be further simplified, since ρ_{ab} has unit trace in the Bell basis, *i.e.*, $\alpha + \beta + \gamma + \delta = 1$. Alice holds the qubits $a \in \{1, 3\}$, while Bob holds the qubits $b \in \{2, 4\}$.

First, Alice performs the single-qubit Clifford unitary $\sqrt{-i\sigma_1}$ on both of her qubits and Bob its inverse $\sqrt{i\sigma_1}$ on both of his qubits. We find

$$\begin{aligned} \tilde{\rho}_{ab} &:= \left(\sqrt{-i\sigma_1} \otimes \sqrt{i\sigma_1}\right) \rho_{ab} \left(\sqrt{-i\sigma_1} \otimes \sqrt{i\sigma_1}\right)^\dagger && (3.16) \\ &= \left(\sqrt{-i\sigma_1} \otimes \sqrt{i\sigma_1}\right) \rho_{ab} \left(\sqrt{i\sigma_1} \otimes \sqrt{-i\sigma_1}\right) && (3.17) \\ &= \frac{1}{2} \begin{pmatrix} \alpha+\delta & 0 & 0 & \alpha-\delta \\ 0 & \beta+\gamma & \gamma-\beta & 0 \\ 0 & \gamma-\beta & \beta+\gamma & 0 \\ \alpha-\delta & 0 & 0 & \alpha+\delta \end{pmatrix}, && (3.18) \end{aligned}$$

i.e., the effect of the local Clifford operations of Alice and Bob is that the coefficients β and δ are effectively exchanged.

In the next step, Alice and Bob perform the coordinated controlled-NOT gates on their qubits. The control qubit is 1 for Alice and 2 for Bob, while the target qubit is 3 for Alice and 4 for Bob. The 4-qubit density matrix after these controlled-NOT gates is given by

$$\rho_{1234}^{\mathrm{CNOT}} := \left(\underset{1\to 3}{\mathrm{CNOT}}\,\underset{2\to 4}{\mathrm{CNOT}}\right) \tilde{\rho}_{12} \otimes \tilde{\rho}_{34} \left(\underset{1\to 3}{\mathrm{CNOT}}\,\underset{2\to 4}{\mathrm{CNOT}}\right)^\dagger . \tag{3.19}$$

In the final step, the target qubits 3 and 4 of the state $\rho_{1234}^{\mathrm{CNOT}}$ are then measured in the computational basis, and the former control qubits 1 and 2 are retained if and only if the measurement outcomes coincide, *i.e.*, if both outcomes are 0 or if both outcomes are 1.

If both measurements do not return the same outcome, the quantum system of qubits 1 and 2 is represented by the post measurement density matrix

$$\rho_{12}^{\neq} = \begin{pmatrix} \frac{1}{4} & 0 & 0 & \frac{(\alpha-\delta)(\gamma-\beta)}{4(\alpha+\delta)(\beta+\gamma)} \\ 0 & \frac{1}{4} & \frac{(\alpha-\delta)(\gamma-\beta)}{4(\alpha+\delta)(\beta+\gamma)} & 0 \\ 0 & \frac{(\alpha-\delta)(\gamma-\beta)}{4(\alpha+\delta)(\beta+\gamma)} & \frac{1}{4} & 0 \\ \frac{(\alpha-\delta)(\gamma-\beta)}{4(\alpha+\delta)(\beta+\gamma)} & 0 & 0 & \frac{1}{4} \end{pmatrix}, \tag{3.20}$$

where we calculated the partial trace of the 16 × 16 post measurement density matrix with respect to the Hilbert space of qubit 3 and qubit 4.

The measurement outcomes do not coincide with a probability of $2(\alpha+\delta)(\beta+\gamma)$. In the Bell basis, $\rho_{12}^{\neq}$ can be expressed as

$$\begin{aligned}\rho_{12}^{\neq} =& \frac{\alpha\gamma+\beta\delta}{2(\alpha+\delta)(\beta+\gamma)}|\phi^+\rangle\langle\phi^+| \\ &+\frac{\alpha\beta+\gamma\delta}{2(\alpha+\delta)(\beta+\gamma)}|\phi^-\rangle\langle\phi^-| \\ &+\frac{\alpha\gamma+\beta\delta}{2(\alpha+\delta)(\beta+\gamma)}|\psi^+\rangle\langle\psi^+| \\ &+\frac{\alpha\beta+\gamma\delta}{2(\alpha+\delta)(\beta+\gamma)}|\psi^-\rangle\langle\psi^-|.\end{aligned}$$

If both measurements do return the same outcome, the quantum system of qubits 1 and 2 is represented by the post measurement density matrix

$$\rho_{12}^{=} = \frac{1}{2(\alpha_+^2+\beta_+^2)}\begin{pmatrix} \alpha_+^2 & 0 & 0 & \alpha_-^2 \\ 0 & \beta_+^2 & \beta_-^2 & 0 \\ 0 & \beta_-^2 & \beta_+^2 & 0 \\ \alpha_-^2 & 0 & 0 & \alpha_+^2 \end{pmatrix}, \tag{3.21}$$

The measurement outcomes coincide with a probability of $(\alpha+\delta)^2+(\beta+\gamma)^2$.

where $\alpha_\pm := \alpha \pm \delta$ and $\beta_\pm := \beta \pm \gamma$. In the Bell basis, this density matrix can be expressed as

$$\rho_{12}^{=} = \frac{\alpha^2+\delta^2}{(\alpha+\delta)^2+(\beta+\gamma)^2}|\phi^+\rangle\langle\phi^+| \tag{3.22}$$

$$+\frac{2\alpha\delta}{(\alpha+\delta)^2+(\beta+\gamma)^2}|\phi^-\rangle\langle\phi^-| \tag{3.23}$$

$$+\frac{\beta^2+\gamma^2}{(\alpha+\delta)^2+(\beta+\gamma)^2}|\psi^+\rangle\langle\psi^+| \tag{3.24}$$

$$+\frac{2\beta\gamma}{(\alpha+\delta)^2+(\beta+\gamma)^2}|\psi^-\rangle\langle\psi^-|. \tag{3.25}$$

The Bell state $|\phi^+\rangle\langle\phi^+|$ is a fixed point of the map f on $\mathbb{C}^4$ defined by

$$(\alpha,\beta,\gamma,\delta) \mapsto \left(\frac{\alpha^2+\delta^2}{\alpha_+^2+\beta_+^2}, \frac{2\alpha\delta}{\alpha_+^2+\beta_+^2}, \frac{\beta^2+\gamma^2}{\alpha_+^2+\beta_+^2}, \frac{2\beta\gamma}{\alpha_+^2+\beta_+^2}\right), \tag{3.26}$$

in the sense that $(1,0,0,0)$ is mapped to itself. For values of $\alpha > \frac{1}{2}$ the recursive successful protocol iterations converge to this fixed point.

Note that, technically, the map f is only well defined for those values of $\alpha,\beta,\gamma,\delta$ that yield valid density matrices in Equation 3.14 –in particular, $\alpha+\beta+\gamma+\delta = 1$. A second fixed point of the map is given by $(\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4})$.

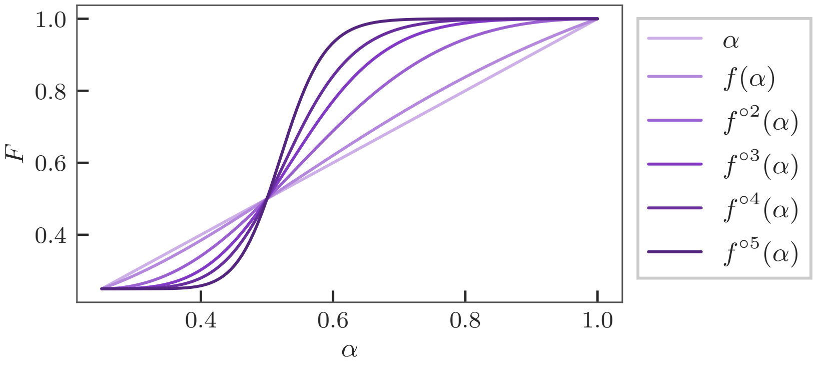


Figure 3.7: A visualization of the fact that the fixed point $(1,0,0,0)$ is a local attractor of the map f for values of $\alpha > \frac{1}{2}$. We consider the simple one dimensional case $\beta = \gamma = \delta = \frac{1-\alpha}{3}$ and write $f^{\circ n}(\alpha)$ as a shorthand for $f \circ \cdots \circ f(\alpha, \frac{1-\alpha}{3}, \frac{1-\alpha}{3}, \frac{1-\alpha}{3})$.

Such a minimum fidelity threshold –here α, which must be greater than one half– is required for all entanglement distillation schemes to work. For large distances between Alice and Bob, this minimum fidelity can no longer be guaranteed. This requires the combination of entanglement swapping and entanglement distillation, giving us the notion of quantum repeaters.

Repeater protocols

The combined action of repeated entanglement swapping and entanglement distillation is called a *quantum repeater*. Nested quantum repeater protocols allow for quantum communication protocols bridging larger distances than protocols without them.

"[T]he attenuation of light in standard fibres at the telecom wavelength of 1550 nm *is* 0.2 dB/km *(or* 0.16 dB/km *in newly developed ultralow loss fibres)."* —Diamanti et al. [Dia+16, p. 2]

Quantum repeaters are essential for real-world implementations of long distance quantum communication protocols, since in optical fibers, the probability of both photon loss and photon depolarization increases exponentially in the length of the fiber.

The standard remedy of classical communication –sending the same bit multiple times and performing a majority vote error correction– is not an option for quantum communication due to the no-cloning theorem [WZ82]. Luckily, quantum repeater schemes can overcome the exponential loss limitation in a different way. Their core idea is to merge a collection of noisy entangled states with interspersed entanglement purification steps, yielding a single long distance entangled state of sufficiently high fidelity.

Quantum repeaters where originally introduced by Briegel *et al.* in Reference [Bri+98] to overcome these fundamental limitations of direct quantum communication. Their possible implementations are discussed in the review [San+11]. The idea of Reference [Bri+98] is to combine entanglement distillation and entanglement swapping by dividing the desired communication distance between A and B into 2^n segments with connecting repeater stations $\{C_i\}_{i=1}^{2^n-1}$ in between.

First, entanglement sources share noisy Bell pairs between neighboring stations, *i.e.*, between $(A, C_1), (C_1, C_2), \dots, (C_{2^n-1}, B)$. During successive entanglement swapping steps, the distance of the entanglement doubles with each swapping step: The entanglement is first swapped from nearest neighbors to connect next nearest neighbors, then from next nearest neighbors to distance four neighbors and so on.

Before and after every entanglement swapping step the entanglement is purified with entanglement distillation. Overall, $n = \log 2^n$ entanglement swapping steps and $n + 1$ entanglement distillation steps yield a single long distance entangled state.

For a visualization of the quantum repeater protocol described above see Figures 3.8 to 3.13.

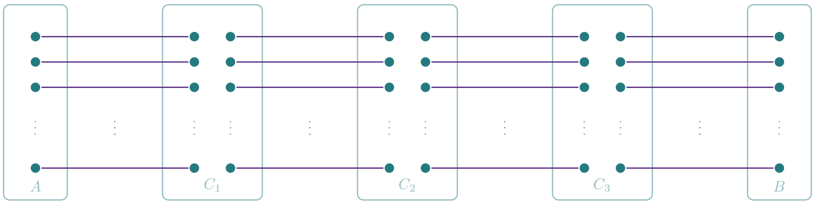


Figure 3.8: Schematic of the quantum systems of Alice, Bob and three quantum repeater stations C_1, C_2, C_3 at the beginning of a quantum repeater protocol.

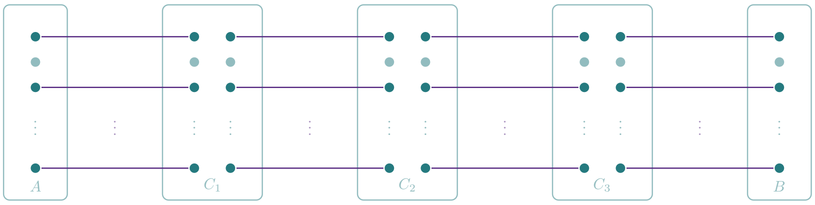


Figure 3.9: Alice, Bob and three quantum repeater stations C_1, C_2, C_3 after the first entanglement distillation step of a quantum repeater protocol.

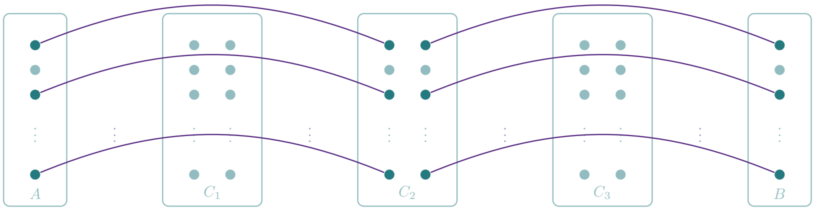


Figure 3.10: Alice, Bob and three quantum repeater stations C_1, C_2, C_3 after the first entanglement swapping step of a quantum repeater protocol.

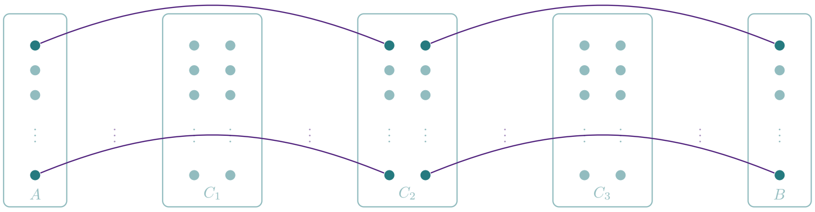


Figure 3.11: Alice, Bob and three quantum repeater stations C_1, C_2, C_3 after the second entanglement distillation step of a quantum repeater protocol.

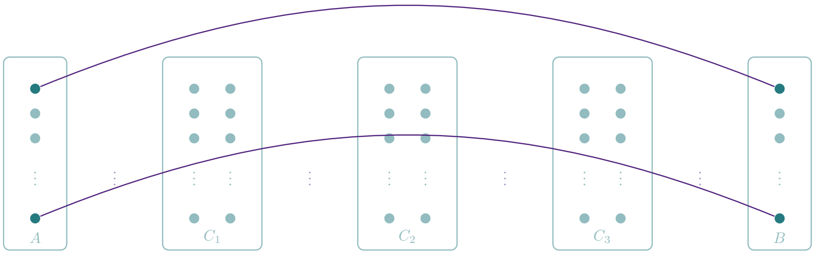


Figure 3.12: Alice, Bob and three quantum repeater stations C_1, C_2, C_3 after the last entanglement swapping step of a quantum repeater protocol.

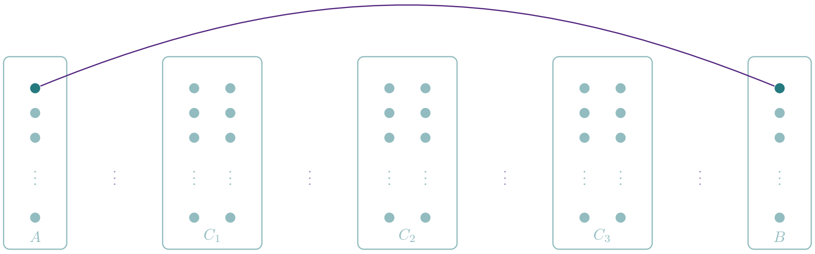


Figure 3.13: Alice, Bob and three quantum repeater stations C_1, C_2, C_3 after the last entanglement distillation step of a quantum repeater protocol.

3.3 Quantum key distribution

> *"Sixteen years' banking experience gives the compiler confidence to hope that this Code will be carefully examined by bankers, and that it will correct a positive evil, to wit, the relying upon hastily formed cryptographs, which continually repeat, and which are therefore dangerous, because, if an operator should decipher such a system, and send a message in such a cipher, great suspicion would arise against all parties having access to such cryptographs."*
>
> *—Miller [Mil82, p. 3]*

> *"[T]he key tape must be at least as long as the sum of all the message tapes used with it, as the messages will lose their secrecy to some extent if the key tape is used repeatedly. The use of a short repeating key may give sufficient secrecy for some uses however."*
>
> *—Vernam [Ver26, p. 114]*

Why quantum key distribution?

Currently used public-key encryption schemes such as RSA [RSA78] and Diffie-Hellman [DH76; Mer78] are not secure from an information-theoretic point of view. Their security relies on computational assumptions: They are only computationally secure, which means that one must solve a computationally hard problem to break them.

In the case of RSA, for example, the corresponding computational problem is to decompose large integers into their prime factors. Integer factorization is a problem in NP for which no classical polynomial-time algorithm is known. As the size of the integer n increases, the computational power required for factorization quickly exceeds even the capabilities of the world's most powerful classical computers. Therefore, to ensure the security of RSA, the size of the prime numbers used for encryption must be constantly increased to keep pace with technological progress.

This is true even without any technological breakthroughs in the field of quantum computing, where a polynomial-time algorithm for factoring integers has been known since the seminal work of Shor [Sho99]. An error-correcting quantum computer would make procedures such as RSA entirely insecure.

It is however not true that all encryption will be broken at some point, even with the help of a quantum computer. In fact, we know how to encrypt communication in a way that remains secure even if an adversary has all the quantum and/or classical computational capabilities imaginable. Such cryptographic schemes are called information-theoretically secure.

Information-theoretically secure encryption protocols require a cryptographic key, *i.e.*, a uniform random bit sequence known only to the communicating parties. Apart from the uniform randomness of the key, it is of utmost importance that the communicating parties keep the key secret at all times and do not reuse even part of it.

When the uniformly random key is at least the length of the communication that the parties wish to encrypt, it is called a *one-time pad* scheme [Ver26; Mil82; Bel11]. The one-time pad is used by modulo two adding the key bitwise to the plaintext message yielding a so-called ciphertext. This ciphertext is in turn sent to the intended recipients. Since the recipients are also in possession of the one-time pad, they can recover the original plaintext by adding it to the message a second time.

The procedure of bitwise adding an encryption key to the plaintext is often called *Vernam cipher*, since Gilbert S. Vernam patented the procedure in 1918 (patent number US001310719).However, Vernam was not its original inventor. Already 36 years earlier, in 1882, Frank Miller had created the same cipher and should be considered the original inventor of the one-time pad [Mil82; Bel11].

Any attacker who got hold of the encrypted text on its way to the intended recipients has no chance of decrypting the message that is better than a random guess. As long as the one-time pad is uniformly random and not available to the attacker, the attacker is out of luck because the ciphertext is completely uncorrelated with the plaintext due to the one-time pad. Without the key, the ciphertext cannot reveal any information about the plaintext.

With the information-theoretic security of the one-time pad in mind, the main challenge of encryption shifts to designing protocols that generate cryptographic keys that are uniformly random and inaccessible to attackers. While there are efforts in the field of classical cryptography, known as post-quantum cryptography, to address the vulnerabilities of classical encryption to adversaries with quantum computing power, quantum information theory also lends itself directly to solving these problems.

There are at least three features of quantum mechanics that seem to ideally fit this mold. First and foremost, the randomness of quantum states and their measurements. Second, the non-locality of entanglement, which allows spatially separated locations to be connected by sharing this randomness. And third, the no-cloning property, which prevents quantum states in unknown superpositions from being perfectly copied.

The third property is primarily important when an attacker tries to access the information encoded in a quantum state. In principle, every classical communication channel can be passively monitored –albeit with technical difficulties– without the legitimate communication parties knowing that there is an attack on their channel. In contrast, interaction with a quantum state disturbs it, resulting in detectable changes. The communicating parties can therefore be informed of an attack on their communication channel even before secret information has been exchanged.

Communication protocols between two parties that exploit these fundamental properties of quantum mechanics are called quantum key distribution (QKD) protocols. Prominent variants are the BB84 protocol [BB84b] and its entanglement-based variant, the E91 protocol [Eke91; Eke92]. Their security is based on physical laws and not just computationally hard problems.

The BB84 protocol

Distributed quantum states can be used not only for direct transmission of quantum information through quantum teleportation, but also for quantum cryptography. In quantum key distribution, the communication partners Alice and Bob attempt to generate a chain of random bits from qubits, which they in turn use to encrypt their classical communication.

The first quantum key distribution scheme was presented by Bennett and Brassard in 1984 and is thus aptly named the BB84 protocol [BB84b]. The protocol uses single qubits sent iteratively between the two parties wishing to create an encryption key, and is mathematically based on the work of Wiesner in Reference [Wie83], in which he proposed a method for creating a quantum currency that cannot be forged a year earlier.

The security of the protocol was not proven until a decade and a half later by Biham *et al.*, Lo and Chau and Mayers *et al.* [Bih+98; LC99; May01] and, in simplified form, by Shor and Preskill [SP00].

In the BB84 protocol, Alice sends a sequence of qubits to Bob one after the other. However, she does not send the qubits in arbitrary states, but in the eigenstates of either σ_1 or σ_3. Importantly, although the eigenstates of σ_1 and σ_3 form orthogonal bases, they are not orthogonal to each other. Rather, the bases overlap in a symmetric manner such that an eigenstate of one basis projects into one of the two base states of the other eigenbasis with 50 % probability. In the following, we will explain the successive steps that Alice and Bob take during the BB84 protocol.

In the first step, Alice uses a personal and trusted random number generator to generate two uniformly random bit strings of the same length n. One of these bit strings Alice uses to select either the σ_1 basis or the σ_3 basis. The second bit sequence then determines in which of the two possible basis states she prepares her qubits to send to Bob: If the first bit string determined the σ_1-basis, a zero in the second bit sequence causes her to prepare the next qubit in the $|+\rangle$ state, and a one in the second bit string causes her to prepare the next qubit in the $|-\rangle$ state. Similarly, if the first bit sequence determines the σ_3 basis, she will prepare the next qubit in the $|0\rangle$ or $|1\rangle$ state.

In the second step, Alice sends the qubits to Bob. She can either use the quantum teleportation protocol presented above or send flying qubits –*i.e.* photons– directly. In the latter case, the polarization of the photons can be used to encode the qubit. Vertical and horizontal polarization represent the $|1\rangle$ and $|0\rangle$ states, while the $45\,^\circ = \frac{\pi}{4}$ rotated basis of $|+\rangle$ and $|-\rangle$ is represented by the diagonal and antidiagonal polarization, respectively.

In the third step, Bob also chooses a uniformly random bit sequence of the same length n. Bob uses his random bits to determine whether to measure the qubits he receives from Alice in the σ_1 basis or in the σ_3 basis. Due to the nature of the two non-orthogonal bases, we observe the following. The result of the measurement will either be deterministic –if the basis chosen by Bob is identical to the one previously determined by Alice– or it will be uniformly random –if the basis chosen by Bob is not identical to the one previously determined by Alice. This ensures that if the bases of Alice and Bob match (and there is neither noise nor the undue influence of an evil eavesdropper), Bob's measurement result will be perfectly correlated with the random bit encoded by Alice. However, with mismatched bases, Bob receives no information about Alice's encoding. His measurement result is still uniformly random but not correlated with the random bit that Alice encoded.

In the final step, Alice and Bob reveal their measurement bases to each other, while the bit sequence encoded by Alice remains hidden. The cases

👤 's random bit	1	0	1	1	1	0	0	0
👤 's random basis	+	+	×	+	×	×	×	+
Polarization 👤 sends	↑	→	↖	↑	↖	↗	↗	→
🕵 's random basis	+	×	×	×	+	×	+	+
Polarization 🕵 measures	↑	↗ or ↖	↖	↗ or ↖	→ or ↑	↗	→ or ↑	→
Public discussion of basis	++	+×	××	+×	×+	××	×+	++
Shared secret 🔑	1	—	1	—	—	0	—	0

Table 3.1: Visualization of the steps of the BB84 protocol. The first two steps are highlighted in green, the third step in brown and the last step in violet.

where their measurement bases do not match are discarded by both of them. Due to the probabilistic nature of the process, they approximately keep a bit sequence of length $\frac{n}{2}$. That is, asymptotically half of Bob's uniformly random bit sequence of measurement results is identical to the half of the bit sequence that Alice encoded at the beginning of the protocol.

While this feat of quantum key distribution is impressive in itself, Alice and Bob can even check to see if an eavesdropper has been listening into their quantum communication. To do so, they only have to sacrifice a fraction of the shared bit sequence they have established.

In 1991, Artur K. Ekert introduced a variant of the BB84 protocol that is today referred to as the E91 protocol [Eke91]. Ekert extended Bennett and Brassard's idea by bringing entanglement into play, and proposed a different kind of quantum key distribution based on Bell's theorem [Bel64]. Notably, he showed that an extended version of Bell's theorem by Clauser, Horne, Shimony and Holt (CHSH) [Cla+69] has a practical cryptographic application, as it can test the security of quantum key distribution.

The generalized Bell inequality

In his 1964 work [Bel64] –today referred to as *Bell's theorem* or the famous *Bell inequality*– John S. Bell substantially sharpened the argument presented by Einstein, Podolsky and Rosen [EPR35b] with respect to a feature that makes quantum mechanics seem paradoxical from the standpoint of classical physics. The latter had come to the conclusion that the probabilistic theory of quantum mechanics should be supplemented by so-called *hidden variables*, whose specification would predetermine the otherwise random result of the measurements of the system.

By describing a physical system of two spatially separated parties with deterministic hidden variables, Bell derived an inequality that systems that can be described by such a hidden variable model must satisfy. The emergent paradox is that nature does in fact not obey Bell's inequality. Quantum mechanical systems allow us to violate Bell's inequality and quantum theory allows us to explain this violation, whereas a description using deterministic hidden variables cannot.

In fact, the derivation of Bell's inequality does not require a description in terms of hidden variables. Arthur Fine showed that Bell's inequality holds whenever there is a joint probability distribution for all observables in an experiment [Fin82]. Here we examine a generalized version of Bell's theorem by Clauser, Horne, Shimony and Holt (CHSH) [Cla+69].

For an experiment that allows a statistical description, we can define the Bell correlations as follows.

Definition 3.1 (Bell correlations) *With the probability* $\Pr\left(a, b \mid A_i, B_j\right)$ *for receiving measurement outcomes* $(a, b) \in \{+1, -1\}^2$ *using measurement devices* A_i *and* B_j*, we define the corresponding correlation coefficient as*

$$C\left(A_i, B_j\right) := \sum_{a,b} ab \Pr\left(a, b \mid A_i, B_j\right) \in [-1, 1]. \tag{3.27}$$

Four measurement devices $\{A_1, A_2, B_1, B_2\}$ *produce the Bell correlations as*

$$\beta := C\left(A_1, B_1\right) + C\left(A_1, B_2\right) + C\left(A_2, B_1\right) - C\left(A_2, B_2\right). \tag{3.28}$$

Since correlation coefficients lie in the interval between -1 and $+1$, the absolute value of β is bounded by 4 from above by construction. However, Bell's theorem gives a different bound. We express it in its CHSH form and use the equivalence between deterministic hidden variables models for an experiment and joint probability distributions for all observables of the experiment [Fin82].

Theorem 3.1 (Bell inequality [Bel64; Cla+69; Fin82]) *A joint probability distribution describes four observables* $\{A_1, A_2, B_1, B_2\}$ *if and only if*

$$-2 \leqslant \beta \leqslant 2. \tag{3.29}$$

Proof. Assuming that Alice has a joint measuring device A_1A_2 and Bob B_1B_2 we can consider P, *i.e.* the joint probability distribution

$$P\left(a_1, a_2, b_1, b_2\right) = \Pr\left(\left(a_1, a_2\right), \left(b_1, b_2\right) \mid A_1A_2, B_1B_2\right) \tag{3.30}$$

of the four variables a_1, a_2, b_1, b_2. Formally, the joint measuring devices for Alice and Bob mean that the observed probabilities

$$\Pr\left(a_i, b_i \mid A_i, B_i\right) \tag{3.31}$$

are found as the marginal statistics of the joint probability distribution P. That is, we have the four marginal relations

$$\sum_{a_1,b_1} P\left(a_1, a_2, b_1, b_2\right) = \Pr\left(a_2, b_2 \mid A_2, B_2\right) \tag{3.32}$$

$$\sum_{a_1,b_2} P\left(a_1, a_2, b_1, b_2\right) = \Pr\left(a_2, b_1 \mid A_2, B_1\right) \tag{3.33}$$

$$\sum_{a_2,b_1} P\left(a_1, a_2, b_1, b_2\right) = \Pr\left(a_1, b_2 \mid A_1, B_2\right) \tag{3.34}$$

$$\sum_{a_2,b_2} P\left(a_1, a_2, b_1, b_2\right) = \Pr\left(a_1, b_1 \mid A_1, B_1\right). \tag{3.35}$$

Using these marginal relations and the definition of the Bell correlations, we can write

$$
\begin{aligned}
\beta &:= C\left(A_1, B_1\right) + C\left(A_1, B_2\right) + C\left(A_2, B_1\right) - C\left(A_2, B_2\right) && (3.36)\\
&= \sum_{a,b} ab \Pr\left(a, b \mid A_1, B_1\right) + \sum_{a,b} ab \Pr\left(a, b \mid A_1, B_2\right) && (3.37)\\
&\quad + \sum_{a,b} ab \Pr\left(a, b \mid A_2, B_1\right) - \sum_{a,b} ab \Pr\left(a, b \mid A_2, B_2\right) && (3.38)\\
&= \sum_{a_1,b_1} a_1 b_1 \Pr\left(a_1, b_1 \mid A_1, B_1\right) + \sum_{a_1,b_2} a_1 b_2 \Pr\left(a_1, b_2 \mid A_1, B_2\right) && (3.39)\\
&\quad + \sum_{a_2,b_1} a_2 b_1 \Pr\left(a_2, b_1 \mid A_2, B_1\right) - \sum_{a_2,b_2} a_2 b_2 \Pr\left(a_2, b_2 \mid A_2, B_2\right) && (3.40)\\
&= \sum_{a_1,a_2,b_1,b_2} a_1 b_1\, P\left(a_1, a_2, b_1, b_2\right) && (3.41)\\
&\quad + \sum_{a_1,a_2,b_1,b_2} a_1 b_2\, P\left(a_1, a_2, b_1, b_2\right) && (3.42)\\
&\quad + \sum_{a_1,a_2,b_1,b_2} a_2 b_1\, P\left(a_1, a_2, b_1, b_2\right) && (3.43)\\
&\quad - \sum_{a_1,a_2,b_1,b_2} a_2 b_2\, P\left(a_1, a_2, b_1, b_2\right) && (3.44)\\
&= \sum_{a_1,a_2,b_1,b_2} \left[a_1 b_1 + a_1 b_2 + a_2 b_1 - a_2 b_2\right] P\left(a_1, a_2, b_1, b_2\right) && (3.45)\\
&= \sum_{a_1,a_2,b_1,b_2} \left[a_1(b_1 + b_2) + a_2(b_1 - b_2)\right] P\left(a_1, a_2, b_1, b_2\right) && (3.46)\\
&\leqslant \sum_{a_1,a_2,b_1,b_2} 2\, P\left(a_1, a_2, b_1, b_2\right) = 2. && (3.47)
\end{aligned}
$$

In the last step, we used that summing over all possible outcomes of the probability distribution $P\left(a_1, a_2, b_1, b_2\right)$ we obtain one. The inequality holds since for four variables satisfying $a_1, a_2, b_1, b_2 \in \{\pm 1\}$ we find that

$$a_1\left(b_1 + b_2\right) + a_2\left(b_1 - b_2\right) \leqslant 2. \tag{3.48}$$

The first term vanishes for $b_1 = -b_2$ and the second term for $b_1 = b_2$. As

$$a_1\left(b_1 + b_2\right) + a_2\left(b_1 - b_2\right) \geqslant -2 \tag{3.49}$$

we find $-2 \leqslant \beta \leqslant 2$ by the same argument.

Conversely, we can start from the assumption $|\beta| \leqslant 2$ and infer that the four observables $\{A_1, A_2, B_1, B_2\}$ are described by a joint probability distribution [Fin82]. This concludes the proof. □

Surprisingly, some quantum mechanical systems violate Bell's inequality. Experiments violating Theorem 3.1 thus show us that deterministic hidden variable models cannot describe real natural phenomena. Quantum theory on the other hand allows us to explain this violation. In the following we will see how.

Bell inequality violations

In this section, we show how two parties can violate Bell's inequality by the statistics of their measurements on an entangled quantum state. Bell's inequality has been experimentally violated in many different ways.

Already at the end of the last millennium, it was possible to violate Bell's inequality between photons separated by a distance greater than 10 km [Tit+98]. Since then, related experiments have shown violations between atomic and photon entanglement [Moe+04] and between spatially separated atoms [Mat+08]. Recently, even the last experimental loopholes were closed [Hen+15].

In the following, we will show how exactly Alice and Bob can violate Bell's inequality by collecting the statistics of quantum measurements on an maximally entangled two qubit quantum state.

Assume that Alice and Bob share multiple copies of the *singlet state*

$$|\psi^-\rangle := \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{3.50}$$

with Alice holding the fist and Bob the second qubit of each. We want to show that $|\psi^-\rangle$ is not only entangled but also allows for a violation of Bell's inequality (see Inequality 3.29 in Theorem 3.1).

Due to the fact that $|\psi^-\rangle$ is the only two qubit state that has zero total angular momentum it is regularly referred to as the *singlet state*. We can calculate the angular momentum of any two-qubit quantum state $|\psi\rangle$ with respect to the Pauli σ_i axis as $\langle\psi|L_i|\psi\rangle$, where

$$L_i := \frac{1}{2}(\sigma_i \otimes \mathbb{1}_2 + \mathbb{1}_2 \otimes \sigma_i)$$

is the corresponding angular momentum operator. While all Bell states have zero angular momentum with respect to one of the Pauli axes, the singlet state $|\psi^-\rangle$ is –up to a global phase– the only two-qubit state that has a total angular momentum of zero, *i.e.*, zero angular momentum with respect to all Pauli axes.

> **Theorem 3.2** (Bell inequality violation) *Copies of the singlet state $|\psi^-\rangle$ can be measured by Alice and Bob to generate Bell correlations with*
>
> $$\beta = 2\sqrt{2} \geqslant 2. \tag{3.51}$$

Proof. The singlet state fulfills the trace identity

$$\langle\psi^-|(A \otimes \mathbb{1}_2)|\psi^-\rangle = \frac{1}{2}\operatorname{Tr} A = \langle\psi^-|(\mathbb{1}_2 \otimes A)|\psi^-\rangle \tag{3.52}$$

for an arbitrary 2×2 matrix A. The identity will help us later to compute more complicated expectation values.

Alice and Bob each choose two three-dimensional unit vectors, which we denote as a_1, a_2 for Alice and b_1, b_2 for Bob. To maximally violate Bell's inequality, we will add some constraints on the unit vectors, but for now any unit vector is a valid choice.

Each of the unit vectors can be used to define a projection as follows. First, we denote by $v \in \{a_1, a_2, b_1, b_2\}$ any of the above unit vectors and by $\sigma := (\sigma_1, \sigma_2, \sigma_3)$ a second vector containing the Pauli matrices as entries. From their scalar product we obtain $\sigma \cdot v = \sum_{i=1}^{3} \sigma_i v_i$ and –using this scalar product– measurement projectors

$$P_\pm(v) := \frac{1}{2}(\mathbb{1}_2 \pm \sigma \cdot v). \tag{3.53}$$

We can now calculate the correlations between the measurement devices

$P_\pm(a_i)$ for Alice and $P_\pm(b_j)$ for Bob. Following Definition 3.1 we find

$$C\left(P_\pm(a_i), P_\pm(b_j)\right) := \sum_{a,b=\pm} ab \Pr\left(a, b \mid P_a(a_i), P_b(b_j)\right) \tag{3.54}$$

$$= \sum_{a,b=\pm} ab\langle\psi^-|P_a(a_i) \otimes P_b(b_j)|\psi^-\rangle \tag{3.55}$$

$$= + \langle\psi^-|P_+(a_i) \otimes P_+(b_j)|\psi^-\rangle - \langle\psi^-|P_+(a_i) \otimes P_-(b_j)|\psi^-\rangle \tag{3.56}$$

$$- \langle\psi^-|P_-(a_i) \otimes P_+(b_j)|\psi^-\rangle + \langle\psi^-|P_-(a_i) \otimes P_-(b_j)|\psi^-\rangle \tag{3.57}$$

$$= + \left(\frac{1}{4} - \frac{1}{4} - \frac{1}{4} + \frac{1}{4}\right) + (0 + 0 - 0 - 0 - 0 - 0 + 0 + 0) \tag{3.58}$$

$$+ \left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right) \langle\psi^-| \left(\sigma \cdot a_i\right) \otimes \left(\sigma \cdot b_j\right) |\psi^-\rangle \tag{3.59}$$

$$=\langle\psi^-| \left(\sigma \cdot a_i\right) \otimes \left(\sigma \cdot b_j\right) |\psi^-\rangle, \tag{3.60}$$

where for the fourth equality we used that $\mathrm{Tr}\left(\sigma \cdot a_i\right) = 0 = \mathrm{Tr}\left(\sigma \cdot b_j\right)$ since all $\{\sigma_i\}_{i=1}^3$ are traceless, that Equation 3.52 holds and that therefore

$$\langle\psi^-|P_a(a_i) \otimes P_b(b_j)|\psi^-\rangle = \frac{1}{4} + \frac{ab}{4}\langle\psi^-| \left(\sigma \cdot a_i\right) \otimes \left(\sigma \cdot b_j\right) |\psi^-\rangle. \tag{3.61}$$

Equation 3.60 can be simplified further by using that the singlet state has zero total angular momentum (see margin note). In particular, we have

$$\left(\sigma_i \otimes \mathbb{1}_2 + \mathbb{1}_2 \otimes \sigma_i\right) |\psi^-\rangle = 0 \tag{3.62}$$

and thus $\left(-\sigma_i \otimes \mathbb{1}_2\right) |\psi^-\rangle = \left(\mathbb{1}_2 \otimes \sigma_i\right) |\psi^-\rangle$. Since the latter holds for all Pauli matrices, we can write

$$\left(\left(-\sigma \cdot b_j\right) \otimes \mathbb{1}_2\right) |\psi^-\rangle = \left(\mathbb{1}_2 \otimes \left(\sigma \cdot b_j\right)\right) |\psi^-\rangle \tag{3.63}$$

and thus

$$\left(\sigma \cdot a_i\right) \otimes \left(\sigma \cdot b_j\right) |\psi^-\rangle = \left(\left(\sigma \cdot a_i\right) \otimes \mathbb{1}_2\right) \left(\mathbb{1}_2 \otimes \left(\sigma \cdot b_j\right)\right) |\psi^-\rangle \tag{3.64}$$

$$= \left(\left(\sigma \cdot a_i\right) \otimes \mathbb{1}_2\right) \left(\left(-\sigma \cdot b_j\right) \otimes \mathbb{1}_2\right) |\psi^-\rangle \tag{3.65}$$

$$= \left(\left(\sigma \cdot a_i\right) \left(-\sigma \cdot b_j\right) \otimes \mathbb{1}_2\right) |\psi^-\rangle, \tag{3.66}$$

where we used Equation 3.63 for the second equality. Simplifying Equation 3.60 with Equation 3.66 and, again, with Equation 3.52 we find

$$C\left(P_\pm(a_i), P_\pm(b_j)\right) = \langle\psi^-| \left(\sigma \cdot a_i\right) \otimes \left(\sigma \cdot b_j\right) |\psi^-\rangle \tag{3.67}$$

$$= \langle\psi^-| \left(\left(\sigma \cdot a_i\right) \left(-\sigma \cdot b_j\right) \otimes \mathbb{1}_2\right) |\psi^-\rangle \tag{3.68}$$

$$= \frac{1}{2} \mathrm{Tr}\left(\left(\sigma \cdot a_i\right) \left(-\sigma \cdot b_j\right)\right) \tag{3.69}$$

$$= -a_i \cdot b_j, \tag{3.70}$$

i.e., the correlations between the measurement devices $P_\pm(a_i)$ for Alice and $P_\pm(b_j)$ for Bob can simply be described by the negative scalar product of the corresponding unit vectors. The Bell correlations (see Definition 3.1) are then

$$\beta = -a_1 \cdot b_1 - a_1 \cdot b_2 - a_2 \cdot b_1 + a_2 \cdot b_2 \tag{3.71}$$

$$= -\left(a_1 + a_2\right) \cdot b_1 - \left(a_1 - a_2\right) \cdot b_2 \tag{3.72}$$

for arbitrary choices of three-dimensional unit vectors a_1, a_2 for Alice and b_1, b_2 for Bob.

If we additionally impose the constraint $a_1 \neq a_2$ and construct Bob's unit vectors as $b_1 = -\frac{1}{\sqrt{2}}(a_1 + a_2)$ and $b_2 = -\frac{1}{\sqrt{2}}(a_1 - a_2)$ we find that the correlations of our chosen measurements violate Bell's inequality as

$$\beta = \frac{1}{\sqrt{2}}(a_1 + a_2)^2 + \frac{1}{\sqrt{2}}(a_1 - a_2)^2 \tag{3.73}$$

$$= \frac{1}{\sqrt{2}}\left(a_1^2 + a_1 \cdot a_2 + a_2 \cdot a_1 + a_2^2 + a_1^2 - a_1 \cdot a_2 - a_2 \cdot a_1 + a_2^2\right) \tag{3.74}$$

$$= \frac{2(a_1^2 + a_2^2)}{\sqrt{2}} = (a_1^2 + a_2^2)\sqrt{2} = 2\sqrt{2} \geqslant 2. \tag{3.75}$$

This concludes the proof. □

Having introduced Bell's inequality and the possibility of its violation by quantum states, we can now turn to the entanglement-based variant of the BB84 protocol introduced by Artur K. Ekert in 1991 [Eke91].

The E91 protocol

In his protocol [Eke91], Ekert extended Bennett and Brassard's idea by bringing entanglement into play and proposed a different kind of quantum key distribution, based on Bell's theorem [Bel64]. In particular, he showed that the extended version of Bell's theorem of Clauser, Horne, Shimony and Holt (CHSH) [Cla+69] which we have discussed in the previous subsections has a practical cryptographic application, as it can test the security of the quantum key distribution.

The key quantum state for the implementation of the E91 protocol [Eke91; Eke92] is the singlet state, which we have already studied in the previous section (*cf.* Equation 3.50). Again, given multiple copies of $|\psi_-\rangle$, Alice has the first qubit and Bob the second qubit of all singlet states.

On their qubits, Alice and Bob now perform measurements of the type $P_\pm(v)$ given in Equation 3.53. Instead of the two unit vectors v chosen by each Alice and Bob to violate the Bell inequality, for the E91 protocol they each choose three unit vectors $\{a_i\}_{i=1}^3$ and $\{b_j\}_{j=1}^3$ with $a_i, b_j \in \mathbb{R}^3$.

However, for the protocol to work, it is not necessary to use all degrees of freedom. In fact, it is sufficient to choose vectors that lie in the same plane. In the following we will use the following vectors in the σ_1-σ_2 (or X-Y) plane as proposed by Ekert.

For $i, j \in \{1, 2, 3\}$ Alice and Bob choose the angles $\phi_1^a = 0, \phi_2^a = \frac{1}{4}\pi, \phi_3^a = \frac{1}{2}\pi$ and $\phi_1^b = \frac{1}{4}\pi, \phi_2^b = \frac{1}{2}\pi, \phi_3^b = \frac{3}{4}\pi$ respectively and define their measurement projectors as $\{P_\pm(a_i)\}_{i=1}^3$ and $\{P_\pm(b_j)\}_{j=1}^3$ with

$$a_i := (\cos\phi_i^a,\ \sin\phi_i^a,\ 0) \tag{3.76}$$

$$b_j := (\cos\phi_j^b,\ \sin\phi_j^b,\ 0). \tag{3.77}$$

For each of the qubits they hold, Alice and Bob randomly measure one of these three measurement settings. For each measurement setting they record the respective result (either + or −). The correlation between their measurements (*cf.* Equation 3.27 and Definition 3.1) is described by

$$C\left(P_\pm(a_i), P_\pm(b_j)\right) = -a_i \cdot b_j, \tag{3.78}$$

which we have already calculated in the previous section for the correlation coefficients when measuring in the direction of arbitrary vectors a_i and b_j (see Equation 3.70).

Since the scalar product of a vector with itself $v \cdot v$ is one, the measurement outcomes of Alice and Bob are exactly anti-correlated, *i.e.*,

$$C\left(P_\pm(a_i), P_\pm(b_j)\right) = -1 \tag{3.79}$$

if they happen to measure in the same orientation. With the angles chosen above for the Equations 3.76 and 3.77, this is the case when Bob measures along b_1 and Alice measures along a_2 or when Bob measures along b_2 and Alice measures along a_3.

However, if the orientation of their measurements is different, Alice and Bob can use the correlations of their measurement results to violate Bell's inequality, just as shown in the previous section. For example Bob's measurements along b_1 and b_3 and Alice's measurements along a_1 and a_3 can be combined to violate Bell's inequality since

$$\begin{aligned}
\beta :=& + C\left(P_\pm(a_3), P_\pm(b_1)\right) + C\left(P_\pm(a_3), P_\pm(b_3)\right) && (3.80)\\
&+ C\left(P_\pm(a_1), P_\pm(b_1)\right) - C\left(P_\pm(a_1), P_\pm(b_3)\right) && (3.81)\\
=& - a_3 \cdot b_1 - a_3 \cdot b_3 - a_1 \cdot b_1 + a_1 \cdot b_3 && (3.82)\\
=& - \cos\phi_a^3 \cos\phi_b^1 - \sin\phi_a^3 \sin\phi_b^1 && (3.83)\\
&- \cos\phi_a^3 \cos\phi_b^3 - \sin\phi_a^3 \sin\phi_b^3 && (3.84)\\
&- \cos\phi_a^1 \cos\phi_b^1 - \sin\phi_a^1 \sin\phi_b^1 && (3.85)\\
&+ \cos\phi_a^1 \cos\phi_b^3 + \sin\phi_a^1 \sin\phi_b^3 && (3.86)\\
=& - 2\sqrt{2} \leqslant -2, && (3.87)
\end{aligned}$$

Since the vectors b_1 and b_3 are orthogonal and can be obtained from a_1 and a_3 by rotating them about the angle $\frac{\pi}{4} = 45°$, the scalar products

$$\begin{aligned}
a_1 \cdot b_1 &= \cos\phi_a^1 \cos\phi_b^1 + \sin\phi_a^1 \sin\phi_b^1\\
a_1 \cdot b_3 &= \cos\phi_a^1 \cos\phi_b^3 + \sin\phi_a^1 \sin\phi_b^3\\
a_3 \cdot b_1 &= \cos\phi_a^3 \cos\phi_b^1 + \sin\phi_a^3 \sin\phi_b^1\\
a_3 \cdot b_3 &= \cos\phi_a^3 \cos\phi_b^3 + \sin\phi_a^3 \sin\phi_b^3
\end{aligned}$$

all have the same absolute value of

$$\cos\frac{\pi}{4} = \frac{1}{\sqrt{2}} = -\cos\frac{5\pi}{4}.$$

where compared to Equation 3.28 we have the measurement devices

$$\{A_1 := P_\pm(a_3), A_2 := P_\pm(a_1), B_1 := P_\pm(b_1), B_2 := P_\pm(b_3)\}. \tag{3.88}$$

The trick of the E91 protocol is to exploit this violation of Bell's inequality to check whether there are eavesdroppers who might manipulate the singlet states that Alice and Bob use. To this end, after their measurements, Alice and Bob publicly discuss in which orientation they measured which qubit.

If they have measured along different directions, they reveal not only their measurement basis but also their measurement results. As shown in Equation 3.87 above, the Bell correlations that can be calculated from these measurement statistics should violate Bell's inequality.

If they have measured along the same direction, they know that their measurement results are anti-correlated. In this case, they do not reveal their measurement results. Instead Bob mirrors his measurement result, *i.e.* he maps + ↦ − and vice versa, and both Alice and Bob translate + ↦ 0 and − ↦ 1. In this manner, they obtain a random bit sequence, which they use for one-time pad encryption.

QKD with quantum repeaters

We have now seen that quantum repeaters are essential for long-distance quantum communication: Only quantum repeaters enable the faithful distribution of entanglement to larger distances. This entanglement can then be used for teleportation or quantum key distribution.

For practical applications, it is important to understand the precise interplay between different experimental implementation platforms with their specific noise parameters and distance scaling. The distance scaling is important in the context of comparing communication in free-space with communication over optical fibers because photon losses in vacuum decrease only polynomially with distance, while losses in optical fibers are exponential.

Unfortunately, however, this precise interaction is difficult to study analytically. While simple repeater scenarios are well understood, there is a need to analyze more advanced strategies for realistic models with individual shortcomings in the system. This difficulty becomes particularly apparent when scenarios with several different components and with multiple communication links are examined.

To address this problem, we used ReQuSim [Wal+22a], a simulation framework for quantum repeaters. ReQuSim can help experimentalist to identify limitations of their systems before they encounter them in their actual experiments –saving them time and resources.

For simulations of free-space communication using sattelites we refer the interested reader to Reference [Wal+22a]. For simulations of fiber-based repeaters with multiple links and entanglement purification we refer them to Reference [Wal+22b].

By investigating realistic parameter regimes for both free-space and fiber-optic communication with ReQuSim, we simulated real hardware components and compared different scenarios in terms of their achievable key rates. The detailed presentation of the results is beyond the scope of this thesis, since here we want to investigate the network aspect of quantum communication. In the following, we will therefore leave the bipartite setting and focus on more networked scenarios.

Beyond bipartite key distribution

The distribution of quantum keys is not limited to two parties. Beyond QKD, we can explore more general scenarios where multiple parties in a quantum network wish to create a shared secret key. As the name implies, these networks of quantum states can have more diverse connectivity than the linear connections for bipartite key distribution. To analyze these more complex networks, it is useful to consider their topologies in the language of graph theory: we need to identify network topologies as mathematical graphs.

Part II
Communication in Quantum Networks

Network topologies as graphs 4

We argue that so-called quantum graph states are a suitable mathematical representation to explore the possibilities of real world quantum networks. We justify this abstraction as follows.

It may be trivial to say this, but quantum networks are first and foremost networks. Generic networks are primarily characterized by their connectivity structure. It is this connectivity structure –the network's topology– that determines from the ground up what purposes the network can ultimately serve.

Network topology is already relevant for classical networks, but it is even more so for quantum ones: In classical networks, the topology is fully determined by the physical network infrastructure. In quantum networks, however, there are two topologies that must be considered separately:

One topology is again imposed by the physical network infrastructure over which the quantum entanglement can be distributed. The second topology is emergent from the first and describes the entanglement between the parties connected by the physical network.

At first glance, it appears that this second topology is identical to the first. At second glance, however, the second topology is not unique: Purely local operations at individual network nodes can redistribute –or route– entanglement to form new topologies that are different from the physical network infrastructure used for the initial entanglement distribution.

To analyze network topologies, it is useful to consider them abstractly in the language of graph theory. Mathematical graphs allow us to represent the entanglement topology between multiple quantum systems in an intuitive way. In this abstraction, the graph's vertices represent the spatially separated quantum systems and its edges represent the entanglement between them.

4.1 Graph states

Graph states play an essential role in both quantum computing and quantum communication. Graph states are multipartite entangled quantum states. As examples of stabilizer states, graph states can be easily implemented on quantum computers [Jon+22b; Bri+09] and are ubiquitous in the theory of quantum networks [EKB16a; EKB16b; Epp+17; HPE19; MMG19; Hah+22].

As their name suggests, graph states can be visually represented by graphs. The associated graph's vertices correspond to the qubits, while the edges correspond to controlled two-qubit operations for the experimental implementation of the graph state. In this language of graph theory, local Clifford operations acting on a graph state correspond to local

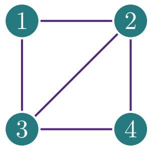


Figure 4.1: The simple graph $G = (V, E)$ with vertices $V = \{1, 2, 3, 4\}$ and edges $E = \{(1, 2), (1, 3), (2, 3), (2, 4), (3, 4)\}$.

complementations of the associated graph. This visual correspondence is essential for understanding the manipulation of entanglement in quantum networks.

History of graph states

Graph states have been studied independently as *graph codes* in quantum error correction by Schlingemann and Werner [SW01] and as a generalization of cluster states [BR01] by Raussendorf, Browne and Briegel [RBB03]. With respect to their entanglement, graph states were first systematically investigated and classified by Hein, Eisert and Briegel in Reference [HEB04]. For a thorough introduction we refer the reader to the review in Reference [Hei+06].

For the purpose of analyzing multipartite entanglement distributed in quantum networks we will look at graph states in the framework that their qubits are distributed between remote network parties which can only act through local (quantum) operations and classical communication. In present quantum communication theory research it is common to regard shared graph states in this framework as a resource for communicational tasks in networks whose connectivity pattern is captured by a suitable graph [Hah+22; HPE19; Pap+12a; UM22; DHW20c; DHW22].

In the following we will define graph states and describe them from different perspectives.

Mathematical description of graph states

Graph states can be looked at from different mathematical perspectives. The first perspective is one where we imagine an experimental procedure in which the entangling operations between the available qubits are following the connection patterns of simple graphs that lend them their name. An example of a simple graph is visualized in Figure 4.1.

Definition 4.1 (Graph, simple graph) *A graph $G = (V, E)$ consists of a finite set of vertices $V \subsetneq \mathbb{N}$ and of edges $E \subseteq V \times V$. Simple graphs neither contain edges connecting a vertex to itself nor multiple edges between the same vertices.*

The set of vertices sharing an edge with a vertex v in V is called its *neighborhood* and denoted as N_v.

For example N_1 in Figure 4.1 is $\{2, 3\}$.

Definition 4.2 (Neighborhood) *For a graph $G = (V, E)$ and a vertex $v \in V$, we define the neighborhood of v in G to be the subset*

$$N_v := \{w \in V \mid (v, w) \in E\} \subset V. \tag{4.1}$$

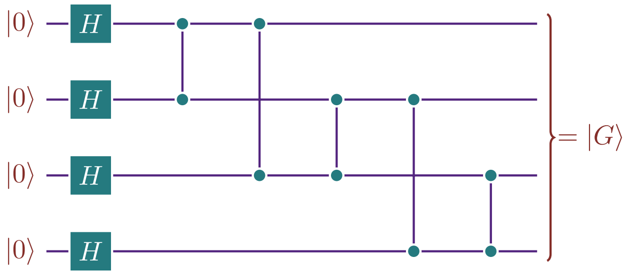


Figure 4.2: The graph state $|G\rangle$ of the graph G shown in Figure 4.1 can be prepared by the quantum circuit displayed.

The graph's *adjacency matrix* Γ_G is encoding the position of its edges.

Definition 4.3 (Adjacency matrix) *Given a graph $G = (V, E)$ with $n := |V|$ vertices, we can encode its neighborhood as an $(n \times n)$-matrix over $\mathbb{F}_2$ and denote it by*

$$(\Gamma_G)_{i,j} := \begin{cases} 1 & \text{if } (i,j) \in E \\ 0 & \text{if } (i,j) \notin E. \end{cases} \tag{4.2}$$

The adjacency matrix of the example graph in Figure 4.1 is given by

$$\Gamma_G = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Adjacency matrices are symmetric if the edges of the corresponding graph are undirected. Since the entanglement properties we want to describe are symmetric, we will only work with undirected graphs.

Given an arbitrary adjacency matrix of a simple graph, we can describe the imagined experimental procedure alluded to above. In this thought experiment, each vertex is associated with a qubit, while each edge is associated with an interaction: For every vertex in V, we initialize a qubit in the $|+\rangle = H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ state. From the initialized $|V| = \dim(\Gamma_G)$ qubits we obtain the graph state vector $|G\rangle$ by applying entangling conditional phase gates between those qubits that correspond to neighboring vertices in the graph G. This graph state $|G\rangle$ is a pure quantum state of $|V|$ qubits, *i.e.* $|G\rangle \in (\mathbb{C}^2)^{\otimes |V|}$. An example of a corresponding *quantum circuit* is shown in Figure 4.2.

A conditional phase gate or controlled-Z gate on two qubits acts as

$$CZ_{i,j}|i\,j\rangle = (-1)^{ij}|i\,j\rangle$$

and can be represented by the matrix

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

Definition 4.4 (Graph state) *A graph state vector $|G\rangle$ is defined by $|V|$ qubits in $|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$ entangled via CZ gates for each edge $(i,j) \in E$,*

$$|G\rangle := \prod_{(i,j)\in E} CZ_{i,j}|+\rangle^{\otimes |V|}. \tag{4.3}$$

From Equation 4.3 it is then straightforward to obtain the expression

$$|G\rangle = \frac{1}{\sqrt{2^{|V|}}} \sum_{b \in \{0,1\}^{\times |V|}} (-1)^{\frac{1}{2} b^T \Gamma_G b} |b\rangle \tag{4.4}$$

giving the expansion of any graph state vector in the computational basis. Here, we sum over all binary strings $(b_1, b_2, \dots, b_{|V|}) \in \{0,1\}^{\times |V|}$ of length $|V|$ and the product $b^T \Gamma_G b$ is describing the matrix multiplication of the adjacency matrix with a row vector b^T from the left and with a column vector b from the right. That is, in Equation 4.4, we get a relative phase of -1 in front of those vectors of the computational basis expansion that have $b_i = 1 = b_j$ if and only if $(i,j) \in E$. Consequently, every vector

The expansion of the graph state vector $|L_3\rangle$ corresponding to the linear graph L_3 in the computational basis is given by

$$|L_3\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle - |011\rangle$$
$$+|100\rangle + |101\rangle - |110\rangle + |111\rangle).$$

As the adjacency matrix of L_3 is given by

$$\Gamma_{L_3} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

the summation over the binary strings in Equation 4.4 yields a relative phase of -1 for the strings $(0,1,1)$ and $(1,1,0)$ as well as two phases of -1 canceling each other for the string $(1,1,1)$.

$|b_1 b_2 \dots b_{|V|}\rangle$ with an odd number of edges (i, j) such that $b_i = 1 = b_j$ has a relative phase of -1. All other vectors carry a relative phase of $+1$.

The computational basis expansion given by Equation 4.4 is a sum involving exponentially many terms in the number of graph state qubits. While for some structured subclasses of graph states –such as GHZ states– we can find basis expansions involving fewer terms by choosing different local bases for each qubit, these explicit basis expansions are often tedious or even impractical.

Fortunately, graph states can also be be described in the so-called stabilizer formalism introduced in Reference [Got97]. In this framework, $|G\rangle$ is described by a set of $|V|$ linear equations.

4.2 The stabilizer formalism

The underlying idea of the stabilizer formalism is that we can describe a large number of quantum states more efficiently by the operators that stabilize them than by explicitly writing out their state vectors [Got97; NC10]. An operator is said to stabilize a state vector if the state vector is an eigenvector of the operator with eigenvalue plus one.

In the stabilizer formalism we can regard graph states as examples of so-called stabilizer states. While not every stabilizer state is a graph state, every stabilizer state is equivalent to a graph state under local Clifford operations [Sch01; VDD04b].

Local Clifford operations were defined in Definition 2.26 in the introduction.

The Pauli group on n qubits $\mathcal{P}_n$ was defined in Definition 2.24 in the introduction.

Definition 4.5 (Stabilizer, stabilizer state) *Every Abelian subgroup $\mathcal{S}$ of the Pauli group $\mathcal{P}_n$ that does not contain $-\mathbb{1}_{2n}$ is called a stabilizer. If $|\mathcal{S}| = 2^n$, we can find a unique quantum state $|\psi\rangle$ on n qubits that is the joint plus one Eigenstate of all matrices S in $\mathcal{S}$, that is, $|\psi\rangle = S|\psi\rangle$ for all $S \in \mathcal{S}$. We can write the density matrix of this stabilizer state as*

$$|\psi\rangle\langle\psi| = \frac{1}{2^n} \sum_{S \in \mathcal{S}} S. \tag{4.5}$$

Since the number of elements in the stabilizer corresponding to a stabilizer state scales equally exponentially with the number of qubits as the number of terms in the expansion of the respective state vector in the computational basis, one could ask, what the advantage of of the description of graph states in the stabilizer formalism is to begin with.

The answer to this question is that nontrivial finite groups of size $|\mathcal{G}|$ can be completely described by a set of at most $\log_2(|\mathcal{G}|)$ generators. For stabilizer states this means that we can characterize the stabilizer $\mathcal{S}$ with $n = \log_2(2^n)$ generators denoted as $\{K_i\}_{i=1}^n$ and write

$$\mathcal{S} = \langle K_1, \dots, K_n \rangle \, . \tag{4.6}$$

It is easy to show by induction that that finite groups of size $|\mathcal{G}| > 1$ can be described by at most $\log_2(|\mathcal{G}|)$ generators [NC10].

Let K be any element in $\langle K_1, \dots, K_i\rangle$ and K_{i+1} not in $\langle K_1, \dots, K_i\rangle$. Then $K_{i+1}K$ is in $\langle K_1, \dots, K_i, K_{i+1}\rangle$ but not in $\langle K_1, \dots, K_i\rangle$, since that would imply $K_{i+1} = (K_{i+1}K)K^{-1} \in \langle K_1, \dots, K_i\rangle$ in contradiction to our assumption.

With the elements of the type $K_{i+1}K$, we explicitly constructed $|\langle K_1, \dots, K_i\rangle|$ elements that are in $\langle K_1, \dots, K_i, K_{i+1}\rangle$ but not in $\langle K_1, \dots, K_i\rangle$, that is,

$$|\langle K_1, \dots, K_i, K_{i+1}\rangle| \geq 2|\langle K_1, \dots, K_i\rangle|.$$

Starting from a nontrivial generator K_1, *i.e.* $|\langle K_1\rangle| \geq 2$, we can conclude by induction over i that $|\langle K_1, \dots, K_n\rangle| \geq 2^n$.

Since graph states are examples of stabilizer states, a graph state $|G\rangle$ on $n := |V|$ qubits is –up to a global phase– uniquely described by the set $\{K_v|G\rangle = |G\rangle\}_{v=1}^n$ of linear equations.

A set of generators for the stabilizer of a graph state is exceptionally easy to to obtain from the corresponding graph. For each vertex v in V, we define K_v to be the tensor product of σ_1 acting on the qubit corresponding to v, of σ_3 acting on the qubits corresponding to the neighborhood N_v and of $\mathbb{1}_2$ on all other qubits:

$$K_v := \sigma_1^v \otimes \sigma_3^{N_v} \otimes \mathbb{1}_2^{V\setminus(N_v\cup\{v\})}. \tag{4.7}$$

We can rewrite the sum of all 2^n elements of the stabilizer as a product involving just these n generators, *i.e.*, in analogy to Equation 4.5

$$|\psi\rangle\langle\psi| = \frac{1}{2^n}\prod_{v=1}^{n}\left(\mathbb{1}_{2^n} + K_v\right). \tag{4.8}$$

In the explicit calculation of the matrices described by $\{K_v\}_{v=1}^n$, it is important to calculate the tensor products in the same order for all vertices. The graph state corresponding to the graph depicted in Figure 4.1 is for example described by the generators

$$K_1 = +\sigma_1^1 \otimes \sigma_3^2 \otimes \sigma_3^3 \otimes \mathbb{1}_2^4 \tag{4.9}$$
$$K_2 = +\sigma_3^1 \otimes \sigma_1^2 \otimes \sigma_3^3 \otimes \sigma_3^4 \tag{4.10}$$
$$K_3 = +\sigma_3^1 \otimes \sigma_3^2 \otimes \sigma_1^3 \otimes \sigma_3^4 \tag{4.11}$$
$$K_4 = +\mathbb{1}_2^1 \otimes \sigma_3^2 \otimes \sigma_3^3 \otimes \sigma_1^4 \tag{4.12}$$

Since the matrices $\sigma_1, \sigma_2, \sigma_3$ can also be represented by the letters X, Y, Z, due to the position of their eigenvectors on the Bloch sphere (*cf.* Figure 2.1), we can use them for a more compact notation. For an even more compact notation, both the identity matrices and tensor products are often omitted from Equation 4.7. This compact representation of the same generators is shown in Figure 4.3 (with ± phases written in the first column).

So far we have not addressed the question of why we excluded $-\mathbb{1}$ from our definition of stabilizers (Definition 4.5). Non-trivial stabilizer states $|\psi\rangle \neq 0$ do not have $-\mathbb{1}$ as an element of their stabilizer, because $-|\psi\rangle = |\psi\rangle$ implies $|\psi\rangle = 0$. For the same reason, $i\mathbb{1}$ and $-i\mathbb{1}$ are not elements of a nontrivial stabilizer, since their square is equal to $-\mathbb{1}$.

Since neither $-\mathbb{1}$ nor $\pm i\mathbb{1}$ are elements of any stabilizer $\mathcal{S}$, we can also use Equation 2.11 to show that $S^2 = \mathbb{1}$ and therefore $S^\dagger = S$ for all $S \in \mathcal{S}$.

By a similar argument, we can conclude that all elements of a stabilizer commute with each other. Since tensor products of Pauli matrices either commute (see Equation 2.12) or anticommute (see Equation 2.13), this is also true for the elements of a stabilizer. However, the assumption that two elements S, T of a stabilizer anticommute implies that $-\mathbb{1}$ is also an element of the stabilizer, which leads to the same contradiction as in the previous paragraph: With $ST = -TS$ we can explicitly write

$$(-\mathbb{1})\,|\psi\rangle = -|\psi\rangle = -TS|\psi\rangle = ST|\psi\rangle = |\psi\rangle, \tag{4.13}$$

where we used that both ST and TS stabilize $|\psi\rangle$.

+	X	Z	Z	
+	Z	X	Z	Z
+	Z	Z	X	Z
+		Z	Z	X

Figure 4.3: The canonical generators $\{K_1, K_2, K_3, K_4\}$ of the graph state stabilizer corresponding to the simple graph $G = (V, E)$ with vertices $V = \{1, 2, 3, 4\}$ and edges $E = \{(1, 2), (1, 3), (2, 3), (2, 4), (3, 4)\}$ of Figure 4.1. The i-th row is representing K_i.

Measurements in the stabilizer formalism

Projective measurements of Pauli observables on stabilizer states can be easily described using the stabilizer formalism we introduced in the previous section [Got97; NC10]. For measurements of elements of the stabilizer, this is particularly straightforward.

Measuring a stabilizer element of a stabilizer state deterministically yields the outcome +1. The stabilizer state is left unchanged. It is invariant under the measurement of any of its stabilizer elements.

If we instead want to measure a Pauli observable that is not included in the stabilizer, the following theorem applies.

Theorem 4.1 (Stabilizer formalism measurements [Got97; NC10]) *When measuring a Pauli observable P on a stabilizer state with generators $\{K_1, K_2, K_3, \ldots, K_n\}$,[a] the stabilizer generators after the measurement are given by $\{\pm P, K_2, K_3, \ldots, K_n\}$ if the measurement result was ± 1.*

[a] W.l.o.g. there is only one generator K_1 of the stabilizer that P does not commute with.

We say that w.l.o.g. there is only one generator K_1 of the stabilizer that P does not commute with. This is justified by the observation, that the product of any two stabilizer elements S, T that anticommute with P, commutes with P itself, since

$$STP = S(-PT) = (-PS)(-T) = PST.$$

Therefore –if there is more than one generator that P does not commute with– any generator K_i of $\mathcal{S}$ that P does not commute with can be replaced by $K_1 K_i$ in the set of generators.

Proof. Since tensor products of Pauli matrices either commute (see Equation 2.12) or anticommute (see Equation 2.13), there are only two different cases to consider for the projective measurement of any Pauli observable P on a stabilizer state. To see this, we fix a generator of said stabilizer state. Then either P commutes with all generators or there is w.l.o.g. one generator of the stabilizer which P does not commute with.

In the former case, we again get a deterministic measurement outcome since in this case either P or $-P$ is an element of the stabilizer. This is evident by observing that for each stabilizer generator K of a stabilizer state $|\psi\rangle$ we find

$$P|\psi\rangle = PK|\psi\rangle = KP|\psi\rangle, \tag{4.14}$$

i.e., $P|\psi\rangle$ is an eigenvector of K. Since $K^2 = \mathbb{1}$, we can conclude $P|\psi\rangle = \pm|\psi\rangle$ which means that either P or $-P$ is an element of the stabilizer.

In the latter case, we denote the one stabilizer generator that P does not commute with as K_1. The probability of obtaining the measurement outcome ±1 is according to Definition 2.18 given by

$$\Pr(\pm) = \langle\psi|\frac{\mathbb{1} \pm P}{2}|\psi\rangle = \operatorname{Tr}\left(\frac{\mathbb{1} \pm P}{2}|\psi\rangle\langle\psi|\right), \tag{4.15}$$

and by this measurement the quantum system is projected into the state

$$|\psi_\pm\rangle := \frac{(\mathbb{1} \pm P)}{2\sqrt{\Pr(\pm)}}|\psi\rangle. \tag{4.16}$$

Using that $K_1|\psi\rangle = |\psi\rangle$ and that K_1 anticommutes with P, we can write

$$\operatorname{Tr}\left(\frac{\mathbb{1}+P}{2}|\psi\rangle\langle\psi|\right) = \operatorname{Tr}\left(\frac{\mathbb{1}+P}{2}K_1|\psi\rangle\langle\psi|\right) = \operatorname{Tr}\left(K_1\frac{\mathbb{1}-P}{2}|\psi\rangle\langle\psi|\right) \quad (4.17)$$

and with the cyclicity of the trace and the fact that $K_1 = K_1^\dagger$

$$\operatorname{Tr}\left(K_1\frac{\mathbb{1}-P}{2}|\psi\rangle\langle\psi|\right) = \operatorname{Tr}\left(\frac{\mathbb{1}-P}{2}|\psi\rangle\langle\psi|K_1\right) = \operatorname{Tr}\left(\frac{\mathbb{1}-P}{2}|\psi\rangle\langle\psi|\right) \quad (4.18)$$

we can conclude $\Pr(+) = \Pr(-)$ from Equations 4.17, 4.18 and 4.15. As no other measurement results are possible, it follows directly that $\Pr(+) = \frac{1}{2} = \Pr(-)$.

If we substitute this result into Equation 4.16, it follows for the state of the quantum system after the measurement

$$|\psi_\pm\rangle = \frac{\mathbb{1} \pm P}{\sqrt{2}}|\psi\rangle. \quad (4.19)$$

A simple, but lengthy computation (for details see Appendix 12.1) shows that the density matrix of this post measurement state is given by

$$|\psi_\pm\rangle\langle\psi_\pm| = \frac{1}{2^n}\left(\mathbb{1}_{2^n} \pm P\right)\prod_{v=2}^{n}\left(\mathbb{1}_{2^n} + K_v\right). \quad (4.20)$$

Comparing to Equation 4.8, we see that the stabilizer generators of $|\psi_\pm\rangle$ are given by $\{\pm P, K_2, K_3, \ldots, K_n\}$. □

Binary representation of stabilizers

We can express the stabilizer formalism in terms of linear algebra over the binary field $\mathbb{F}_2 := \{0, 1\}$ in a simple way. Each n-qubit stabilizer state can be written as an n-dimensional linear subspace of $\mathbb{F}_2^{2n}$. This is particularly useful since local Clifford operations can be represented as symplectic transformations of $\mathbb{F}_2^{2n}$. The subspaces corresponding to the stabilizer states are self-orthogonal with respect to a symplectic inner product [DD03; Got97; Cal+97].

The key insight to the binary representation of the stabilizer formalism is the construction of a group homomorphism between the Pauli group $\mathscr{P}_1$ (see Definition 2.24) with matrix multiplication modulo phases of $\{\pm 1, \pm i\}$ and two-dimensional vectors in $\mathbb{F}_2^2$ with standard addition modulo two inherited from $\mathbb{F}_2$. We can construct the group homomorphism as follows. The identity matrix σ_0 is mapped to the row vector with two zero entries, *i.e.*, $\sigma_{00} := \sigma_0 \mapsto (0\ 0)$. Similarly, $\sigma_{01} := \sigma_1 \mapsto (0\ 1)$, $\sigma_{10} := \sigma_3 \mapsto (1\ 0)$, and $\sigma_{11} := \sigma_2 \mapsto (1\ 1)$.

Note that in this convention the binary string ab, which can be read from the two-dimensional row vector $(a\ b)$, is not equal to the base two representation of the Pauli matrix index.

It is easy to see that the four row vectors form a group under modulo two addition. The map is a group homomorphism since the group structure is preserved under the map. For example, $\sigma_1\sigma_3 \propto \sigma_2 \propto \sigma_3\sigma_1$ is represented by $(0\ 1) + (1\ 0) = (1\ 1) = (1\ 0) + (0\ 1)$ as an equality in $\mathbb{F}_2^2$. The identity element σ_0 is mapped onto the identity element $(0\ 0)$ and in both groups all elements are self inverse with respect to the group operation.

The group homomorphism above can be extended by mapping the Pauli group of n qubits $\mathscr{P}_n$ (again modulo phases) to $2n$-dimensional vectors in $\mathbb{F}_2^{2n}$. The conventional extension maps tensor products of n Pauli matrices $\{\sigma_{a_i b_i}\}_{i=1}^n$ to $2n$ dimensional row vectors by sorting the n first index bits $\{a_i\}_{i=1}^n$ into the first half and the n second index bits $\{b_i\}_{i=1}^n$ into the second half of the row vector, *i.e.*,

$$\sigma_{a_1 b_1} \otimes \sigma_{a_2 b_2} \otimes \cdots \otimes \sigma_{a_n b_n} \mapsto (a_1\ a_2 \cdots a_n \mid b_1\ b_2 \cdots b_n)\,. \tag{4.21}$$

As an example, we consider the stabilizer generators of the graph state visualized in Figures 4.1 and 4.3. The tensor product $\sigma_1 \otimes \sigma_3 \otimes \sigma_3 \otimes \sigma_0$, *i.e.*, the first generator of the stabilizer is mapped to $(0\ 1\ 1\ 0 \mid 1\ 0\ 0\ 0)$ by the group homomorphism. Writing the n binary row vectors of the stabilizer generators $\{K_i\}_{i=1}^4$ as the rows of a $(n \times 2n)$-matrix, allows us to see the structure of the stabilizer generators in the $\mathbb{F}_2$ representation. This is especially true for graph states whose stabilizer generators have no Y-type support on any of their qubits. For our example, we find

$$\begin{pmatrix} K_1 \\ K_2 \\ K_3 \\ K_4 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{4.22}$$

for the group homomorphism acting on the entire set of stabilizer generators. The coloring allows for an easier comparison with the illustration in Figure 4.3.

4.3 Examples of graph states

The various interaction patterns of graph states according to their graphs gives rise to different subclasses of graph states. In the following we will introduce some of these relevant subclasses – the first of which is the class of GHZ states.

GHZ states

Greenberger-Horne-Zeilinger (GHZ) states were introduced in 1989 [GHZ89a] and first experimentally implemented ten years later with three spatially separated and polarization entangled photons [Bou+99]. Today it is feasible to control multiple degrees of freedom for each photon –*e.g.* their paths and orbital angular momentum in addition to their polarization– allowing for up to $3n$-partite GHZ states on n photonic qubits [Wan+18].

Similarly, after the first proof of principle experiments with three superconducting phase qubits [Nee+10] and four trapped ions [Sac+00] it is possible to generate GHZ states with twenty to thirty qubits in ion-trap [Pog+21] and superconducting quantum computers [Moo+21] today.

Thomas *et al.* succeeded in using controlled single-photon emissions interleaved with custom atomic qubit rotations to efficiently generate Greenberger-Horne-Zeilinger states of up to 14 photons and linear cluster states of up to 12 photons with a fidelity lower bounded by 76 % and 56 %, respectively [Tho+22].

GHZ states can be defined as follows.

Definition 4.6 (GHZ state) *A GHZ state on n qubits is defined as*

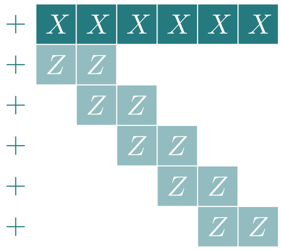
$$|\mathrm{GHZ_n}\rangle := \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}). \tag{4.23}$$

When measuring the qubits of a GHZ state in the computational basis, the measurement outcomes are perfectly correlated. Performing a projective measurement of one of the qubits will project the GHZ state into $|0\rangle^{\otimes n}$ or $|1\rangle^{\otimes n}$ with equal probability of $\frac{1}{2}$. A measurement of any of the other qubits, will subsequently yield the same outcome.

Both the graph states corresponding to the complete graph, as well as the star graphs are locally equivalent to the GHZ state. This becomes clear by showing that their stabilizers can be transformed into each other with only local Clifford operations which are applied to the individual qubits. Without loss of generality, we show the transformation for the 6-qubit case.

The complete graph can be obtained from the star graph by so-called *local complementation* with respect to the central node of the star graph and vice versa. We will investigate this further in Section 4.4.

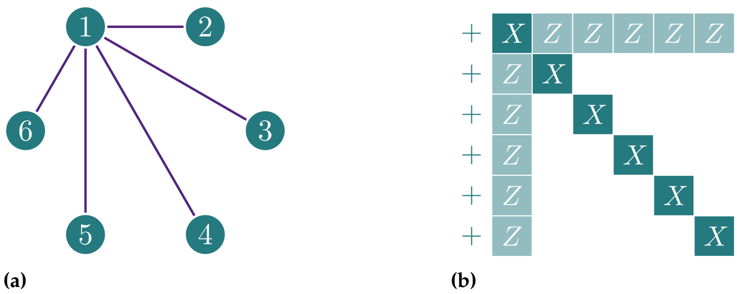
Since $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$ and the addition of kets is commutative, it follows that $|\mathrm{GHZ_n}\rangle$ is an eigenstate of $X^{\otimes n}$ with eigenvalue +1. With $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$ the same is true for any tensor product of an even number of Z operators, *e.g.* tensor products of the type $Z_i \otimes Z_{i+1}$. For example, we can write down a set of generators of the stabilizer of a 6-partite GHZ as presented in Figure 4.4.



+	X	X	X	X	X	X
+	Z	Z				
+		Z	Z			
+			Z	Z		
+				Z	Z	
+					Z	Z

Figure 4.4: The stabilizer of a $|\mathrm{GHZ}_6\rangle$ state as defined in Definition 4.6.

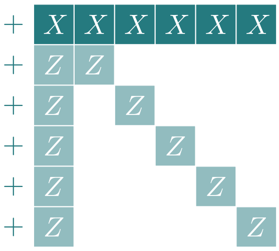
For the star graph centered on the first vertex **(a)**, we find the canonical stabilizer generators **(b)**.



+	X	Z	Z	Z	Z	Z
+	Z	X				
+	Z		X			
+	Z			X		
+	Z				X	
+	Z					X

Figure 4.5: The stabilizer **(b)** of the graph state corresponding to the star graph **(a)** with six vertices and edges $\{(1,2),(1,3),(1,4),(1,5),(1,6)\}$ that are centered on the first vertex.

Via Hadamard operations on all but the first qubit (see Equation 2.17) this is equivalent to the stabilizer in Figure 4.6.



+	X	X	X	X	X	X
+	Z	Z				
+	Z		Z			
+	Z			Z		
+	Z				Z	
+	Z					Z

Figure 4.6: The stabilizer of the star graph of Figure 4.5b with additional Hadamard operations on all but the first qubit.

This stabilizer is now representing the 6-qubit GHZ state again: Multiplying the second generator with the third, the third with the fourth and so on, the Z support is transferred from the first qubit to the second, from the first to the third, and so on, since the Pauli matrices are self-inverse (see Equation 2.11). This means that we again obtain the same generators as those presented for the GHZ state in Figure 4.4.

4.4 Local transformations of graph states

Local Clifford unitaries on graph states

The graph states introduced in the previous section (see Definition 4.4) can notably be transformed into other graph states without additional CZ-gates only by local Clifford operations [DD03; HEB04; VDD04b; VDD04a; VDD05c].

A particularly useful local Clifford unitary for graph states is denoted as U_a^τ. It acts nontrivially on the qubits of a graph state, that is, on qubit a and the set of its neighboring qubits N_a as

$$U_a^\tau := \exp\left(-i\frac{\pi}{4}X_a\right) \otimes \exp\left(i\frac{\pi}{4}Z_{N_a}\right) \otimes \mathbb{1}_2^{V\setminus(N_a\cup\{a\})} \tag{4.24}$$

$$\exp\left(-i\frac{\pi}{4}X\right) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$$

$$\exp\left(i\frac{\pi}{4}Z\right) = \begin{pmatrix} e^{\frac{i}{4}\pi} & 0 \\ 0 & e^{-\frac{i}{4}\pi} \end{pmatrix}$$

or equivalently as $U_a^\tau := (-iX_a)^{1/2} \otimes (iZ_{N_a})^{1/2} \otimes \mathbb{1}_2^{V\setminus(N_a\cup\{a\})}$.

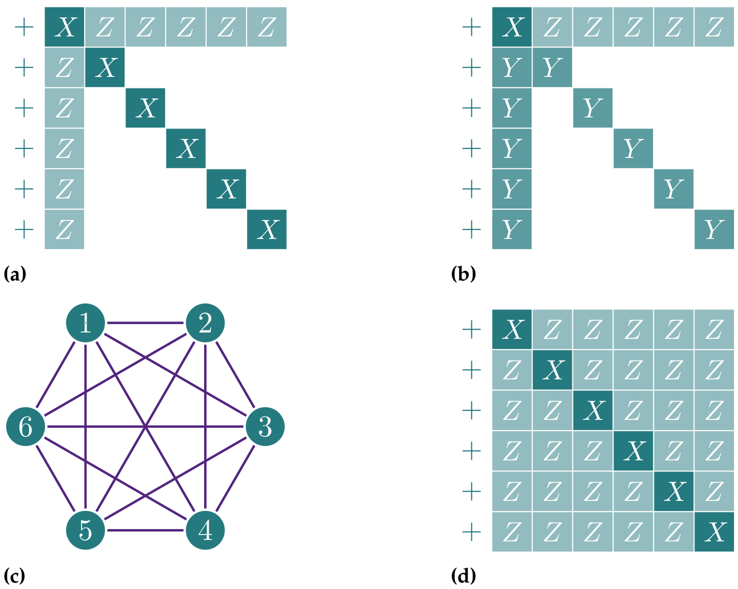
The action of any unitary U on a stabilizer state $|\psi\rangle$ corresponds to a conjugation of the stabilizer $\mathcal{S} = \langle K_1, \ldots, K_n\rangle$ with U. To be precise, under the action of U_a^τ the generators K_i transform as the conjugation

$$U_a^\tau K_i (U_a^\tau)^\dagger. \tag{4.25}$$

In particular, the $\exp\left(-i\frac{\pi}{4}X_a\right)$ part of U_a^τ maps σ_1 to σ_1, σ_2 to σ_3 and σ_3 to $-\sigma_2$ or, in short form, $(X, Y, Z) \mapsto (X, Z, -Y)$. Similarly, the $\exp\left(i\frac{\pi}{4}Z_{N_a}\right)$ part acts as $(X, Y, Z) \mapsto (-Y, X, Z)$.

For graph states this means that the X-type and Z-type support of their stabilizer generators is invariant under the action of the $\exp\left(-i\frac{\pi}{4}X\right)$ part and the $\exp\left(i\frac{\pi}{4}Z\right)$ part of U_a^τ respectively, but transformed into $-Y$-type support when $\exp\left(-i\frac{\pi}{4}X\right)$ acts on Z-type support and when $\exp\left(i\frac{\pi}{4}Z\right)$ acts on X-type support. Notably, the stabilizer generator $K_a := X_a \otimes Z_{N_a} \otimes \mathbb{1}_2^{V\setminus(N_a\cup\{a\})}$ is therefore invariant under conjugation with U_a^τ.

Conversely, the conjugation with U_a^τ transforms all other generators into having $-Y$-type support or $\mathbb{1}_2$-type support on the qubits corresponding to the graph vertices in $N_a \cup \{a\}$. More precisely, the X-type and Z-type



(a)

+	X	Z	Z	Z	Z	Z
+	Z	X				
+	Z		X			
+	Z			X		
+	Z				X	
+	Z					X

(b)

+	X	Z	Z	Z	Z	Z
+	Y	Y				
+	Y		Y			
+	Y			Y		
+	Y				Y	
+	Y					Y

(d)

+	X	Z	Z	Z	Z	Z
+	Z	X	Z	Z	Z	Z
+	Z	Z	X	Z	Z	Z
+	Z	Z	Z	X	Z	Z
+	Z	Z	Z	Z	X	Z
+	Z	Z	Z	Z	Z	X

Figure 4.7: The stabilizer generators **(a)** of the graph state corresponding to the star graph with six vertices and edges $\{(1,2),(1,3),(1,4),(1,5),(1,6)\}$ that are centered on the first vertex transform under the local Clifford unitary

$$U_1^\tau = e^{-i\frac{\pi}{4}X_1} \otimes e^{i\frac{\pi}{4}Z_2} \otimes \ldots \otimes e^{i\frac{\pi}{4}Z_6}$$

to new stabilizer generators **(b)**. Note that $(-Y) \otimes (-Y) = Y \otimes Y$.
By multiplying the first generator of **(b)** with each of the other generators, it is obvious, that **(d)** describes the same stabilizer state. The stabilizer generators of **(d)** are in turn the canonical stabilizer generators of the fully connected graph K_6 depicted in **(c)**.

support of a generator K_b is transformed into $-Y$-type support on the qubits corresponding to the graph vertices in $(N_a \cup \{a\}) \cup (N_b \cap \{b\})$.

As an example, the transformation of the stabilizer of the six node star graph that is centered on the first vertex (see Figure 4.5) under conjugation with U_1^τ is visualized in Figure 4.7.

Local complementation of graphs

The transformation of the star graph from Figure 4.5a to the complete graph from Figure 4.7c is a simple example of a more general pattern that is called *local complementation* in graph theory. Local complementation on a graph is exactly equivalent to applying local Clifford unitaries on the qubits of the respective graph state [VDD04b]. We denote the graph transformation corresponding to a local Clifford unitary of type U_a^τ by $G \mapsto \tau_a(G)$. In the following, we will examine these graph transformations in more detail.

First, note that applying the same unitary U_a^τ twice does not affect the underlying graph, *i.e.*, since

$$\exp\left(-i\frac{\pi}{4}X\right)^2 = -iX \tag{4.26}$$

$$\exp\left(i\frac{\pi}{4}Z\right)^2 = iZ \tag{4.27}$$

we know that $(U_a^\tau)^2 \propto K_a$. Obviously, K_a is but a stabilizer generator of the graph state. Thus, using the same unitary U_a^τ twice only leads to a global phase, which has no physical meaning and, in particular, does not change the entanglement properties of the graph state.

When we talk about graph states not in the stabilizer formalism but in the state vector picture, global phases also appear frequently. Indeed, both $U_a^\tau|G\rangle$ and $(U_a^\tau)^\dagger|G\rangle$ differ from $|\tau_a(G)\rangle$ by a global phase. However, since $|\psi\rangle = e^{i\alpha}|\phi\rangle$ implies

$$|\psi\rangle\langle\psi| = e^{i\alpha}e^{-i\alpha}|\phi\rangle\langle\phi| = |\phi\rangle\langle\phi|,$$

this is not physically relevant. An explicit example of this for graph states can be found in Appendix 11 in Section 11.1.

There is also nothing special about the role of the first vertex in the local Clifford transformation from the star graph to the complete graph. Just as τ_1 mapped the star graph from Figure 4.5a to the full complete from Figure 4.7c, all other star graphs can be reached with local Clifford operations. The full orbit under all possible local complementations

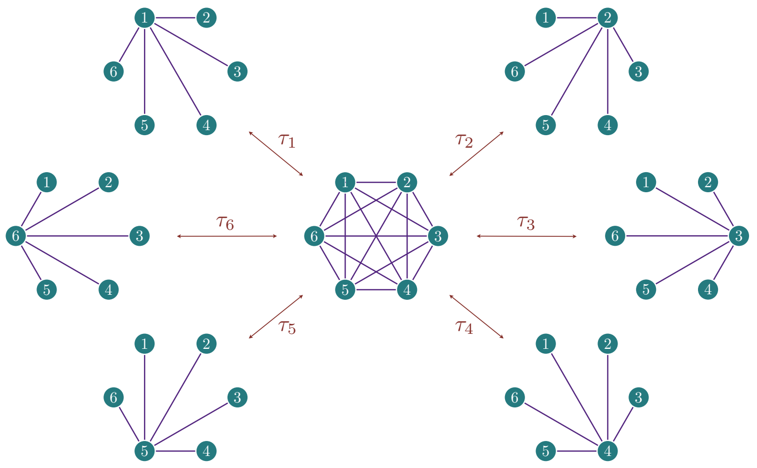


Figure 4.8: The complete graph K_6 is transformed with local complementations with respect to all its vertices. The full orbit under local complementation $[K_6]_{\mathrm{LC}}$ is represented as the star graphs remain invariant through all local complementations except those with respect to their central node. A GHZ state with n qubits is represented by an orbit of $n+1$ graphs: The complete graph and the n star graphs.

acting on graphs representing 6-qubit GHZ states is shown in Figure 4.8. Note that for a star graph centered on vertex a, all local complementations τ_b with $b \neq a$ leave the graph invariant.

Through this example of the complete and star graphs, it is easy to understand the more general pattern. The local complementation of a graph with respect to one of its vertices affects only the neighborhood of the vertex within the graph (*cf.* Definitions 4.2 and 4.3).

Definition 4.7 (Local complementation) *Every vertex $a \in V$ of a graph $G = (V, E)$ defines a graph $\tau_a(G)$ with adjacency matrix*

$$\Gamma_{\tau_a(G)} := \Gamma_G + \Gamma_{K_{N_a}} \mod 2, \tag{4.28}$$

where $K_{N_a} := (V, \{(i,j) \mid (i,j \in N_a) \wedge (i \neq j)\})$ is the complete graph on the neighborhood N_a and empty on all other vertices.

Although many problems in graph theory are computationally hard, it is surprisingly possible to verify whether two graph states can be transformed into each other via a sequence of local complementations in polynomial time [Bou91; VDD04a].

All graphs that can be reached from an initial graph only by local complementation form a set called the *local complementation orbit*.

Definition 4.8 (Local complementation orbit) *The set of graphs that are equivalent via local complementation to a starting graph G is called the local complementation orbit of G and denoted as $[G]_{LC}$.*

In mathematics, local complementation orbits were studied even before their importance for the theory of graph state entanglement was known. They were first introduced by Anton Kotzig in Reference [Kot68] and are therefore sometimes called *Kotzig-orbits*. In principle, there are two different ways to study local complementation orbits. We can either examine orbits arising from local complementation, in which isomorphic graphs are considered equal, or orbits in which isomorphic graphs are not considered equal.

In the context of quantum communication, the latter is the more common case: the usual framework is characterized by individual qubits

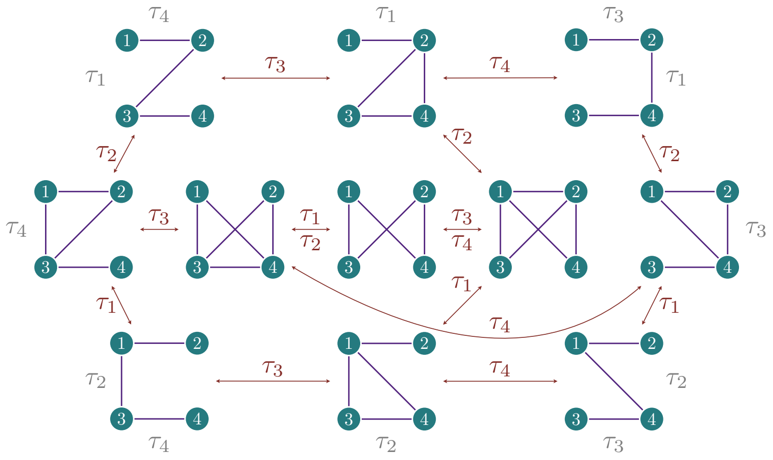


Figure 4.9: The line graph L_4 (top left) is transformed with local complementations with respect to all of its vertices. The local complementations with respect to the leaves of a graph leave this graph invariant and are simply written next it without an arrow. The full orbit $[L_4]_{\mathrm{LC}}$ consists of eleven graphs. Relabeling the central graph of the orbit yields the box-shaped graph (a cycle/ring graph of size four).

held by the respective parties of a network belonging to an entangled graph state shared via that network. Due to the local complementation transformations enabled by local Clifford operations, the connectivity pattern of the network may differ from the edges of the graph state shared over the very same network. This way of thinking enables the routing of quantum information in quantum networks through local operations [HPE19; DHW20b; DHW22] (see Section 5.1).

In Figure 4.8 we examine the local complementation orbit $[K_6]_{\mathrm{LC}}$ of the completely connected graph K_6 as a first simple example. However, most graphs have a much richer structure in their local complementation orbits. In Reference [Adc+20], Adcock *et al.* study the structure of local complementation orbits in detail for graphs with up to 9 vertices. As the number of nodes in the graphs increases, the structures become more complicated: Dahlberg *et al.* showed in Reference [DHW20a] that even counting the size of the local complementation orbit of a generic graph is a #P-complete problem.

Why is local complementation so fascinating?

The smallest nontrivial local complementation orbit is that of the line L_4 with four vertices. It is visualized in Figure 4.9. Note that swapping the positions of vertices 1 and 3 (or 2 and 4) yields the box-shaped graph –a cycle/ring graph of size four. Ring and line graphs are therefore closely related.

We denote line graphs on the vertex set $V_L := \{1, 2, \ldots, n\}$ as $L_n := (V_L, E_L)$ with edges $E_L := \{(1,2), (2,3), \ldots, (n-1, n)\}$. The corresponding graph states are referred to as *linear cluster states.*

The linear cluster state with four qubits also allows us to illustrate what makes local complementations so intriguing. Using local complementations, it is possible to project a subset of qubits of the linear cluster state, whose respective reduced density matrices are fully separable, into an entangled state by simply performing local Clifford operations accompanied by classical correction information.

We will start with the explicit extension of the graph state which corresponds to L_4. It is shown in the top left of Figure 4.9 and defined by the

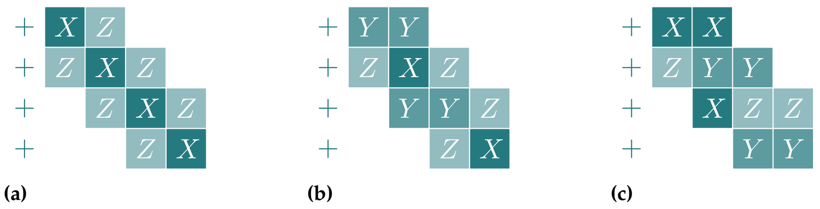


Figure 4.10: The stabilizer generators **(a)** of $|L_4\rangle$, **(b)** of $U_2^\tau|L_4\rangle$, **(c)** of $U_3^\tau U_2^\tau|L_4\rangle$.

adjacency matrix

$$\Gamma_{L_4} := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{4.29}$$

Up to a normalization factor of $\frac{1}{4}$ this amounts to the graph state

$$\begin{aligned} |L_4\rangle \propto\ & |0000\rangle + |0001\rangle + |0010\rangle - |0011\rangle & (4.30)\\ & +|0100\rangle + |0101\rangle - |0110\rangle + |0111\rangle & (4.31)\\ & +|1000\rangle + |1001\rangle + |1010\rangle - |1011\rangle & (4.32)\\ & -|1100\rangle - |1101\rangle + |1110\rangle - |1111\rangle. & (4.33) \end{aligned}$$

Note that the same is not true for tracing out the first (or the last) pair of quibts. In the latter case we obtain instead

$$\mathrm{Tr}_{34}\left(|L_4\rangle\langle L_4|\right) = \frac{1}{4}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}.$$

Calculating the partial trace (see Definition 2.21) with respect to the second and third qubit, we obtain the separable –even maximally mixed– state with the reduced density matrix

$$\rho_{14} = \mathrm{Tr}_{23}\left(|L_4\rangle\langle L_4|\right) = \frac{1}{4}\mathbb{1}_4 \tag{4.34}$$

for the first and fourth qubit of $|L_4\rangle$.

If we perform local complementations with respect to the second and third vertices, *i.e.*, the local Clifford unitaries

Note that U_2^τ is calculated with respect to the graph L_4, but U_3^τ is calculated with respect to the graph $\tau_2(L_4)$.

$$U_2^\tau = \exp\left(i\frac{\pi}{4}Z_1\right) \otimes \exp\left(-i\frac{\pi}{4}X_2\right) \otimes \exp\left(i\frac{\pi}{4}Z_3\right) \otimes \mathbb{1}_2 \tag{4.35}$$

$$U_3^\tau = \exp\left(i\frac{\pi}{4}Z_1\right) \otimes \exp\left(-i\frac{\pi}{4}X_2\right) \otimes \exp\left(i\frac{\pi}{4}Z_3\right) \otimes \exp\left(i\frac{\pi}{4}Z_4\right) \tag{4.36}$$

before taking the partial trace, we still get

$$\rho_{14} = \mathrm{Tr}_{23}\left(\left(U_3^\tau U_2^\tau\right)|L_4\rangle\langle L_4|\left(U_3^\tau U_2^\tau\right)^\dagger\right) = \frac{1}{4}\mathbb{1}_4. \tag{4.37}$$

However, when the same states are considered in the stabilizer formalism, a different picture emerges. The linear cluster state $|L_4\rangle$ is represented by the stabilizer generators shown in Figure 4.10a and those of $U_2^\tau|L_4\rangle$ and $U_3^\tau U_2^\tau|L_4\rangle$ in Figures 4.10b and 4.10c respectively.

From this we can see that measuring the second and third qubits of $|L_4\rangle$ and $U_3^\tau U_2^\tau|L_4\rangle$ in the computational basis gives remarkably different results. For the Z-measurement of the second and third qubits, we consider

$$P_2 := \mathbb{1}_2 \otimes \sigma_3 \otimes \mathbb{1}_2 \otimes \mathbb{1}_2 \tag{4.38}$$

$$P_3 := \mathbb{1}_2 \otimes \mathbb{1}_2 \otimes \sigma_3 \otimes \mathbb{1}_2 \tag{4.39}$$

in the sense of Theorem 4.1: When measuring our Pauli observables

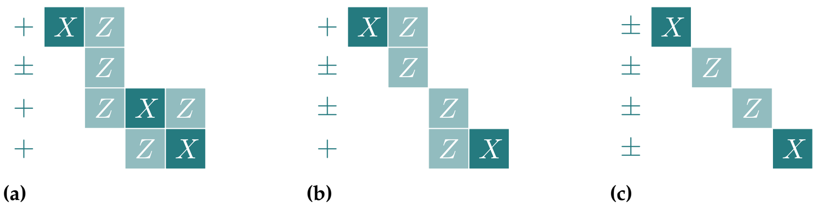


Figure 4.11: The stabilizer generators **(a)** of $|L_4\rangle$ after the Z-measurement of the second qubit and **(b)** after the Z-measurement of the third qubit. The latter is also more neatly represented **(c)** by multiplying the first generator by the second and the fourth by the third.

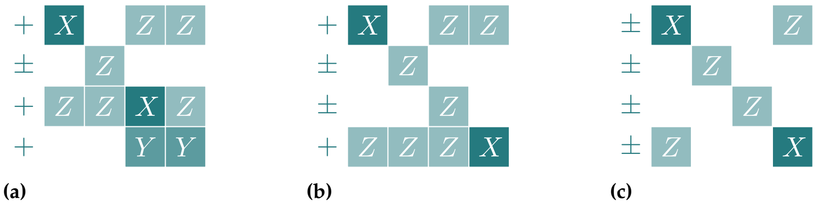


Figure 4.12: The stabilizer generators **(a)** of $U_3^\tau U_2^\tau|L_4\rangle$ after the Z-measurement of the second qubit and **(b)** after the Z-measurement of the third qubit. The latter is also more neatly represented **(c)** by multiplying the first generator by the third and the fourth by the second.

P_i with measurement outcome ±1 on the respective stabilizer states with generators $\{K_1, K_2, K_3, \ldots, K_n\}$, the stabilizer of each state after the measurement is given by $\{\pm P_i, K_2, K_3, \ldots, K_n\}$. We just need to transform the set of stabilizer generators so that there is only one stabilizer generator that does not commute with P_i.

For P_2, the only non-commuting stabilizer generator of $|L_4\rangle$ is K_2, whereas the first three stabilizer generators of $U_3^\tau U_2^\tau|L_4\rangle$ anticommute with P_2. The three anticommuting generators of the latter case can be reduced to just one anticommuting generator by multiplying K_3K_1 and K_2K_3. The stabilizer generators after the measurement of P_2 are shown in Figures 4.11a and 4.12a, respectively.

For P_3 we then find (as shown in Figure 4.11a) again only one non-commuting stabilizer generator –namely K_3. This results in the postmeasurement stabilizer generators in Figures 4.11b and 4.11c. For the two non-commuting stabilizer generators in Figure 4.12a –K_3 and K_4– their product

$$K_3K_4 = \sigma_3 \otimes \sigma_3 \otimes \sigma_3 \otimes \sigma_1 \tag{4.40}$$

does commute with P_3 and we obtain the postmeasurement stabilizer generator in Figures 4.12b and 4.12c.

The difference between the stabilizer generators in Figures 4.11c and 4.12c is striking: Whereas the first and fourth qubits of $|L_4\rangle$ are disentangled after the Z-measurements of qubit two and three, the same measurements on $U_3^\tau U_2^\tau|L_4\rangle$ lead to a maximally entangled state between the same qubits! Local Clifford operations (or local complementation of the graphs representing multipartite entanglement) can –together with the classical information about the measurement outcomes– redirect entanglement such that qubits that may never have physically interacted with each other end up in a maximally entangled state. This is why local complementation is so fascinating.

Quantum network routing and local complementation | 5

5.1 Entanglement routing with local complementation

The following sections closely follow the text of Reference [HPE19], which was written by both myself and my co-authors.

Our analysis in the previous section ended with the intriguing observation that the entanglement of multipartite graph states can be redistributed –or rerouted– by local Clifford unitaries and classical communication. As a multipartite generalization of entanglement swapping, we can use graph local complementation to redirect entanglement in a quantum network. This routing with local complementation was the key idea of the first publication as part of my dissertation research [HPE19].

As we have seen in the first examples of quantum communication protocols presented in this thesis –such as quantum teleportation via quantum repeaters (see Sections 3.1 and 3.2) or quantum key distribution and quantum conference key agreement (see Sections 3.3 and 9.1)– quantum communication between spatially separated parties relies on appropriate instances of shared entanglement.

Reducing the number of measurements

An abundant number of quantum communication protocols rely either on maximally entangled bipartite quantum states –the Bell pairs presented in Definition 2.12 Section 2.5– or on multipartite maximally entangled GHZ states -as presented in Definition 4.6 and Section 4.3. A simple goal of routing entanglement in a quantum network with a given topology is to generate such maximally entangled Bell or GHZ states among all users of the network that request their use. Depending on the given network topology, there may be different strategies that lead to success.

Given a shared graph state, it is not known what the optimal strategy for entanglement routing between nodes that are not connected by physical links is. In [HPE19] we have shown that a repeater method is not optimal in terms of the number of measurements to be made. A significantly reduced number of measurements is extremely useful in quantum networks, as it allows more entanglement to be extracted from the shared graph state.

For the first theorem of the paper, we compared a naive *repeater protocol* with a subtly different *X-protocol* that effectively uses local complementations along a path in the graph connecting potential users of a Bell pair. While this main routing goal of extracting a specific Bell pair is achieved by both protocols, the latter also allows to reduce the number of required measurements while preserving a larger amount of extractable entanglement for other users of the network. Formally, we defined the two protocols as follows.

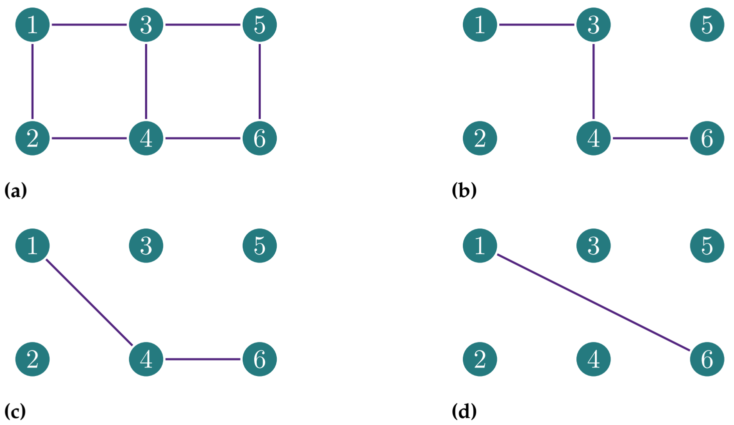


Figure 5.1: The repeater protocol of Definition 5.1 for the butterfly graph. From the graph state with butterfly network topology **(a)** a path connecting nodes 1 and 6 is isolated **(b)** by Z-measuring its neighborhood, *i.e.*, the qubits corresponding to nodes 2 and 5. The successive measurements along the path with respect to nodes 3 **(c)** and 4 **(d)** yield a Bell pair $(1, 6)$.

Definition 5.1 (Repeater protocol [HPE19]) *The repeater protocol entails first isolating a path between two nodes a and b and then connecting a to b by measuring the intermediate nodes of the path. This can be optimized by selecting the shortest path connecting a to b that has the minimum combined neighborhood. Every node that lies in the union of neighborhoods of this path but not on the path itself is then Z-measured. This isolates the path from the rest of the graph creating a repeater line. Finally, every intermediate vertex on the line is X-measured yielding the EPR pair between the two nodes.*

An example of the repeater protocol is shown in Figure 5.1 with $a = 1$ and $b = 6$. The X-protocol is following a slightly different approach.

Definition 5.2 (X-protocol [HPE19]) *First, the intermediate vertices along a shortest path between a and b as in Definition 5.1 are X-measured. Subsequently, the neighborhoods of the two nodes are Z-measured (except the nodes themselves), creating the desired EPR pair between a and b. The choice of the shortest path may vary depending on requests for the secondary use of the remaining graph entanglement.*

For example, in Figure 5.3, the primary goal would be to establish entanglement between qubits 1 and 9. After executing the X-protocol, several secondary uses of the graph state on qubits $3, 4, 7, 8$ are conceivable. Other shortest paths would result in other qubits being available for secondary use.

Both protocols can be used to generate maximally entangled Bell pairs between two qubits corresponding to nodes a and b of any connected graph state. In fact, the X-protocol never requires more measurements than the repeater protocol –regardless of the graph state and thus regardless of the network topology.

Theorem 5.1 (Creating Bell pairs [HPE19]) *We can create a Bell pair between two nodes a and b of an arbitrary graph state using the X-protocol with at most as many measurements as with the repeater protocol.*

While there are simple graph topologies such as cycles and lines where the number of measurements of both protocols match, there are impressive examples that show how much more powerful the X-protocol is for extracting useful entangled states from an arbitrary entangled graph state resource. Even if it is not obvious at first glance, the X-protocol is the strategy underlying the well-known quantum version of the so-called butterfly network [LOW10a; EKB16b].

The butterfly network as a graph state is shown in both Figure 5.1 (for the repeater protocol from Definition 5.1) and Figure 5.2 (for the X-protocol

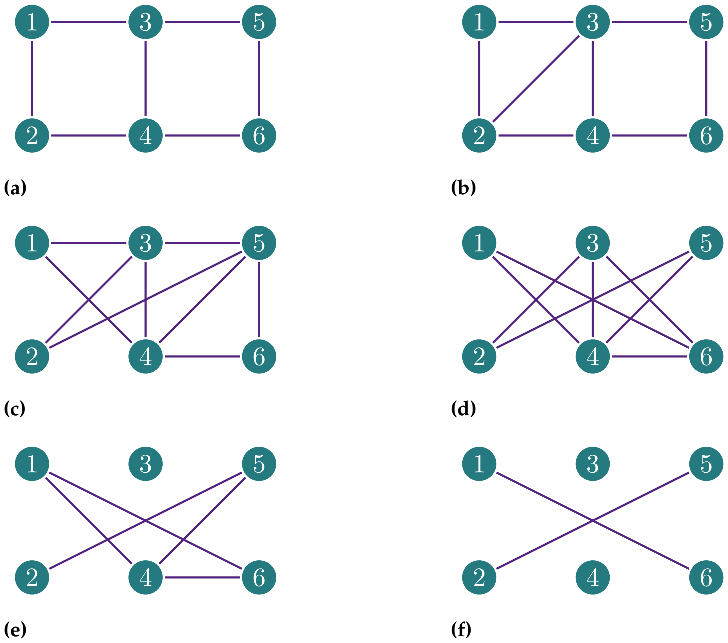


Figure 5.2: The X-protocol of Definition 5.2 for the butterfly graph. The graph state with butterfly network topology **(a)** is transformed by local complementations along the shortest path $1, 3, 4, 6$ connecting nodes 1 and 6. The successive local complementations with respect to nodes 1 **(b)**, 3 **(c)**, and finally 4 **(d)** result in a graph in which the edges $(1, 6)$ and $(2, 5)$ exist, whereas no edges exist between sets $\{1, 6\}$ and $\{2, 5\}$. The Z-measurement of the two qubits corresponding to nodes 3 **(e)** and 4 **(f)** yield two Bell pairs $(1, 6)$ and $(2, 5)$ despite a bottleneck in the network.

from Definition 5.2). The X-protocol is strikingly more effective than the repeater protocol. While the latter only creates the target Bell pair between qubits 1 and 6, the former generates Bell pairs between qubits $1, 6$ and qubits $2, 5$ simultaneously.

For the X-protocol, we start from the butterfly graph state Figure 5.2a, where to form Bell pairs between nodes $1, 6$ and $2, 5$ two X-measurements can be performed on the qubits corresponding to nodes 3 and 4 (*cf.* Figure 5.2f). Figure 5.2 shows the relationship between local complementations on the butterfly graph state and the X-protocol.

Such two X-measurements are effectively equivalent to finding a graph in the local complementation orbit of the butterfly graph in which edges $(1, 6)$ and $(2, 5)$ exist whereas no edges exist between the sets $\{1, 6\}$ and $\{2, 5\}$. This graph is found by successive local complementations with respect to vertices $1, 3$ and 4 (see Figures 5.2b, 5.2c and 5.2d). Two consecutive Z-measurements at vertices 3 and 4 then allow for the extraction of the two desired Bell pairs (Figures 5.2e and 5.2f).

Note that without the second request to connect nodes 2 and 5, a shortest path algorithm alone might have chosen a different path to perform the X-measurements.

Similar to the butterfly network, the sequence of graphs in Figure 5.3 shows the corresponding process for the two-dimensional nine-qubit cluster state. In this sense, local complementation allows the bypassing of bottlenecks. The difference to the repeater protocol is even more evident here than for the butterfly network (compare Figures 5.3 and 5.4). In particular, the X-protocol requires fewer measurements and retains more graph state entanglement for secondary use.

As a side note, we mention that our observations on the routing of entanglement in graph states can be generalized beyond the case of discrete variables to continuous variables.

In continuous variable quantum information, information in the state of a quantum system can be encoded using continuous variables, such as the position and momentum of a particle. For example, continuous variable graph states can be created with squeezed light.

We describe the mechanism for local complementation of continuous variable graph states in the Appendix 12.2. For comparison, we also show a continuous variable version of Figure 5.2 in Figure 12.3.

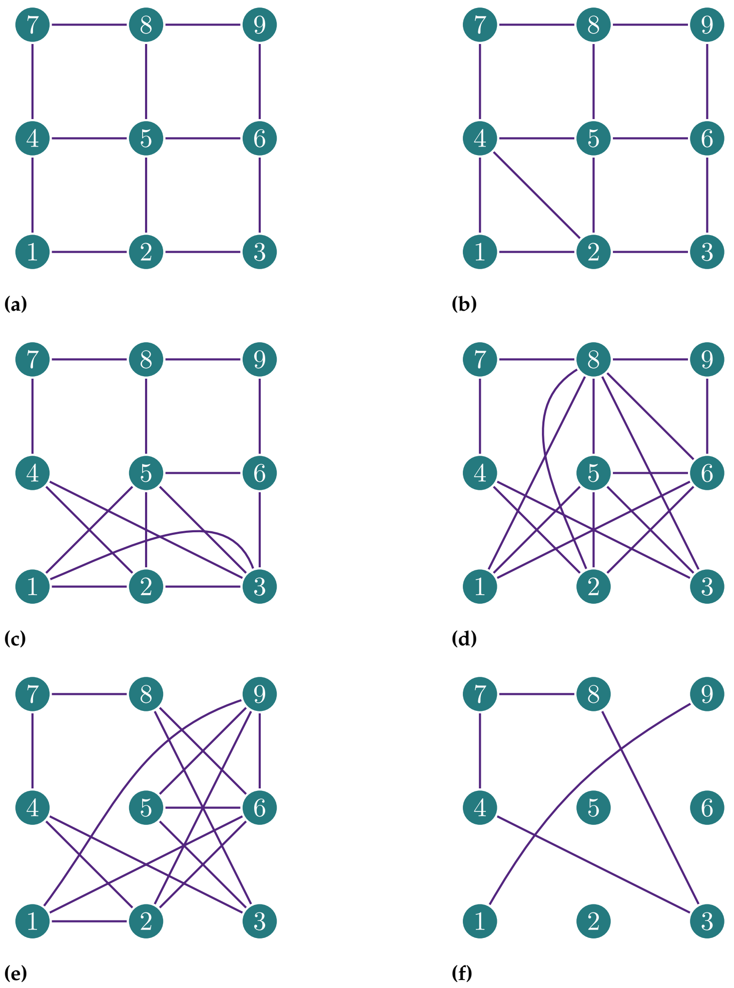


Figure 5.3: Example for the X-protocol of Definition 5.2. A two-dimensional nine-qubit cluster state **(a)** is transformed by local complementations along the shortest path $1, 2, 5, 6, 9$ connecting nodes 1 and 9. The successive local complementations with respect to nodes 1 **(b)**, 2 **(c)**, 5 **(d)**, and finally 6 **(e)** result in a graph in which the edge $(1, 9)$ exists and one of the three edges $(3, 4)$, $(3, 4)$, $(3, 7)$ or $(3, 8)$ could easily be created from the second connected component of the graph. The Z-measurement of the three qubits corresponding to nodes $2, 5$ and 6 **(f)** can therefore either yield two Bell pairs $(1, 9)$ and $(i, j) \in \{(3, 4), (3, 7), (3, 8)\}$ (measuring a total of five nodes) or the Bell pair $(1, 9)$ and any three-partite GHZ state with qubits in the set $\{3, 4, 7, 8\}$ (measuring a total of four nodes) –again despite a bottleneck in the network.

Bottlenecks in quantum networks

The butterfly network we introduced in Figures 5.1 and 5.2 is particularly interesting in the context of network bottlenecks. In terms of network efficiency, we say that a network has a bottleneck with respect to a given communication request if all possible routing solutions involve overlapping paths between at least two pairs of nodes. In quantum networks, a bottleneck is equivalent to requiring more than one Bell pair per physical link when trying to establish long-range quantum communication via teleportation (see Section 3.1).

The butterfly network is not only relevant for communication in quantum networks, but also in the context of quantum computing. In Reference [AM16], for example, it was shown that any two-qubit unitary operation can be deterministically implemented via such a butterfly scheme.

For example, we observe that one of the edges of the butterfly becomes a bottleneck when we try to build repeater lines (such as the ones in Figures 5.4a and 5.1a) to create entanglement between nodes $\{1, 6\}$ and $\{2, 5\}$ in Figure 5.2.

The X-protocol solves the above communication task bypassing the bottleneck in the network as we showed in the previous section. We can further show that the butterfly network is minimal in terms of the number of nodes. The following two theorems formalize this fact, and their proof is by exhaustive search of all possible graphs with the respective number of nodes.

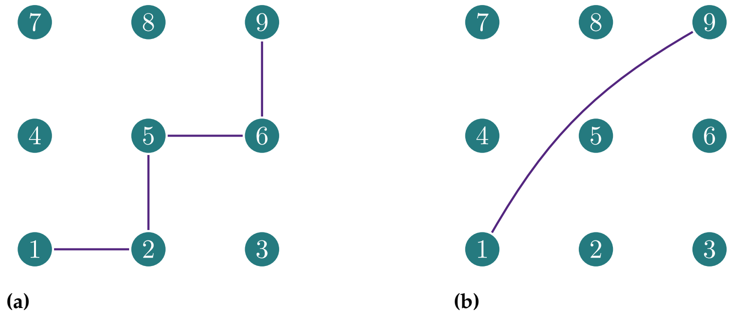


Figure 5.4: The repeater protocol of Definition 5.1 for the two-dimensional nine-qubit cluster state (see Figure 5.3a). A path connecting nodes 1 and 9 is isolated **(a)** by Z-measuring its neighborhood, *i.e.*, the qubits corresponding to nodes $3, 4$ and 8. The successive measurements along the path with respect to nodes $2, 5$ and 6 **(b)** yield a Bell pair $(1, 9)$.

Theorem 5.2 (No bottleneck [HPE19]) *There is no* 5*-node graph state that has a bottleneck for simultaneous communication between two pairs of nodes and that can be solved using local Clifford unitaries and a Pauli measurement of a single node.*

Theorem 5.3 (Bottleneck [HPE19]) *There are only four* 6*-node graph states that have a bottleneck for simultaneous communication between two pairs of nodes and that can be solved using local Clifford unitaries and Pauli measurements.*

The four 6-node graph states that have a bottleneck for simultaneous communication between two pairs of nodes, which can be solved using local Clifford unitaries and Pauli measurements, are obtained by relabeling the butterfly network (*cf.* Figures 5.2a or 5.1a). Thus, if we want to form Bell pairs between nodes $\{1, 6\}$ and $\{2, 5\}$, we obtain the four graphs by exchanging labels within the sets $\{3, 4\}$ and $\{1, 6\}$.

Note that by allowing arbitrary local Clifford unitaries and Pauli measurements, we have considered a broader class of possible algorithms than just the X-protocol introduced in Definition 5.2.

Obtaining GHZ states and other multipartite resources

In addition to studying bottlenecks for parallel bipartite quantum communication, we also investigated the key question of how to extract multipartite resource states such as GHZ states (see Section 4.3) from a given graph state.

The more general question of whether one can extract another graph state vector $|H\rangle$ from a given graph state vector $|G\rangle$ via a sequence of local Pauli measurements has recently been shown to be NP-complete [DHW22]. It is called the vertex minor problem and will be discussed in more detail in Section 5.3. Here we will highlight some cases for which algorithms with polynomial runtime exist.

A first relevant instance involves GHZ states [GHZ89b], which are common and essential resources for multipartite communication schemes in quantum networks beyond point-to-point architectures. For connected graph states, it is straightforward to prove the following lemma.

Lemma 5.4 (Extraction of GHZ3) *It is possible to extract a tripartite GHZ state between any vertices of a connected graph state in polynomial time.*

The reason for this is essentially that tripartite GHZ states are equivalent to tripartite linear cluster states by local complementation. Since any three qubits of a connected graph state lie along a path that can be extracted –following the idea behind the repeater protocol of the previous section (see Definition 5.1)– they can also be transformed into a linear cluster state of just these three qubits. This linear cluster state is then locally equivalent to a tripartite GHZ state, *i.e.* it can be transformed with the appropriate local unitaries.

In the following section we will show how to calculate these local unitaries. As a running example in the next section, we will further investigate the linear cluster state of five qubits and its relationship to the GHZ state of four qubits. Based on this relationship, we can give a sufficient criterion to extract four-qubit GHZ states from connected graphs, although extracting a complete graph with four nodes –which is a graph representing GHZ4 states (see Figure 4.8)– is considered to be hard in general [Dab+18].

↑ ↑ ↑
The preceding sections closely follow the text of Reference [HPE19], which was written by both myself and my co-authors.

Lemma 5.5 (Extraction of GHZ4) *It is possible to extract a quadripartite GHZ state from a graph state if the underlying graph has a linear cluster state vertex minor containing all four nodes of the final GHZ state and at least one additional node between the two outer pairs of nodes.*

5.2 Local Pauli measurements

Projective measurements of σ_1, σ_2, or σ_3 (see Definitions 2.18 and 2.19) on graph state qubits corresponding to nodes of a graph yield, up to local unitaries, new graph states on the remaining nodes that were not measured. In the following, we briefly summarize how such local Pauli measurements transform the graphs of graph states.

In Definition 2.19 we set $P_{j,\pm} := \frac{1}{2}\left(\mathbb{1}_2 \pm \sigma_j\right)$, or –expressed differently– $P_{1,\pm} = |\pm\rangle\langle\pm|$, $P_{2,\pm} = |\pm i\rangle\langle\pm i|$ and $P_{3,\pm} = |\frac{1\mp1}{2}\rangle\langle\frac{1\mp1}{2}|$. For local Pauli measurements on a graph state $G = (V, E)$, we extend this definition to

$$\left(P_{j,\pm}\right)_a := \frac{1}{2}\left(\mathbb{1}_2 \pm \sigma_j\right)_a \otimes (\mathbb{1}_2)_{V\setminus\{a\}}. \tag{5.1}$$

This allows us to describe the graph state transformation under local Pauli measurements in terms of local complementations of the corresponding graph. A measurement in the Z-basis essentially removes the measured vertex from the graph and thus removes the measured qubit from the graph state. A Y-measurement involves a local complementation before removal and an X-measurement involves a series of three local complementations in combination with removal.

Formally, we have the following theorem for the Pauli projections $\left(P_{j,\pm}\right)_a$ acting on an arbitrary graph state $|G\rangle$ as first described by [Sch04] and independently by by [HEB04]. Our presentation corresponds most closely to that in [Hei+06].

The proof of the following theorem is analogous to that in [Hei+06], but more extensive than it. We repeat it here primarily for clarity in the arguments that follow.

Theorem 5.6 (Local Pauli measurements [Hei+06]) *We can describe the effect of Pauli projections $\left(P_{j,\pm}\right)_a$ for any graph vertex $a \in V$ on a graph state $|G\rangle$ by local complementations τ_a and τ_b for $b \in N_a$ and by deleting the measured node from the graph $G = (V, E)$. The latter is denoted by $G - a := G[V \setminus \{a\}] = (V \setminus \{a\}, \{(v, w) \in E \mid v \neq a \neq w\})$ and we find* [a]

$$\frac{(P_{1,\pm})_a|G\rangle}{\sqrt{\Pr(\pm|X)}} \propto |\pm\rangle_a \otimes U_a^{1,\pm}|\tau_b\left(\tau_a \circ \tau_b(G) - a\right)\rangle_{V\setminus\{a\}}, \tag{5.2}$$

$$\frac{(P_{2,\pm})_a|G\rangle}{\sqrt{\Pr(\pm|Y)}} \propto |\pm i\rangle_a \otimes U_a^{2,\pm}|\tau_a(G) - a\rangle_{V\setminus\{a\}}, \tag{5.3}$$

$$\frac{(P_{3,\pm})_a|G\rangle}{\sqrt{\Pr(\pm|Z)}} = |\frac{1 \mp 1}{2}\rangle_a \otimes U_a^{3,\pm}|G - a\rangle_{V\setminus\{a\}}. \tag{5.4}$$

The local unitaries $U_a^{j,\pm}$ are defined as

$$U_a^{1,-} := \left(e^{-i\frac{\pi}{4}\sigma_2}\right)_b \otimes \left(e^{+i\frac{\pi}{4}\sigma_3}\right)_{N_a\setminus(N_b\cup\{b\})} \otimes (\mathbb{1}_2)_{V\setminus(\{a,b\}\cup(N_a\setminus N_b))} \tag{5.5}$$

$$U_a^{1,+} := \left(e^{+i\frac{\pi}{4}\sigma_2}\right)_b \otimes \left(e^{-i\frac{\pi}{4}\sigma_3}\right)_{N_a\setminus(N_b\cup\{b\})} \otimes (\mathbb{1}_2)_{V\setminus(\{a,b\}\cup(N_a\setminus N_b))} \tag{5.6}$$

$$U_a^{2,-} := \left(e^{+i\frac{\pi}{4}\sigma_3}\right)_{N_a} \otimes (\mathbb{1}_2)_{V\setminus(\{a\}\cup N_a)} \tag{5.7}$$

$$U_a^{2,+} := \left(e^{-i\frac{\pi}{4}\sigma_3}\right)_{N_a} \otimes (\mathbb{1}_2)_{V\setminus(\{a\}\cup N_a)} \tag{5.8}$$

$$U_a^{3,-} := (\sigma_3)_{N_a} \otimes (\mathbb{1}_2)_{V\setminus(\{a\}\cup N_a)} \tag{5.9}$$

$$U_a^{3,+} := (\mathbb{1}_2)_{V\setminus\{a\}}. \tag{5.10}$$

[a] For the σ_1 measurement, any neighbor $b \in N_a$ can be chosen. Whenever it is not made at an isolated vertex, Equation 5.2 holds. If instead a is an isolated vertex, then the measurement result is always +1 and the state remains unaltered.

$U_a^{1,\pm}$ depends on the choice of b. However, the resulting graph states for different decisions b_1, b_2 are equivalent via the local Clifford unitary (*cf.* Equation 4.24)

$$U_{b_1}^{\tau}\left(U_{b_2}^{\tau}\right)^{\dagger}.$$

Equations 5.2 and 5.3 are written with "∝" instead of "=" since the equality holds only up to a global phase (see Section 11.1 in the appendix).

Proof. The rule for the Z-measurement follows from the definition of graph states in terms of the CZ-gates along the graphs edges (*cf.* Equation 4.3), namely

$$|G\rangle := \prod_{(i,j)\in E} CZ_{i,j}|+\rangle^{\otimes|V|}. \tag{5.11}$$

We find that the graph state can be rewritten as

$$|G\rangle = \prod_{\substack{((i,j)\in E)\\ \wedge(a\in\{i,j\})}} CZ_{i,j}\left[\prod_{\substack{((i,j)\in E)\\ \wedge(a\notin\{i,j\})}} CZ_{i,j}|+\rangle^{\otimes|V|}\right] \tag{5.12}$$

$$= \prod_{\substack{((i,j)\in E)\\ \wedge(a\in\{i,j\})}} CZ_{i,j}\left[|+\rangle_a \otimes |G - a\rangle_{V\setminus\{a\}}\right] \tag{5.13}$$

$$= \left[\prod_{(a,b)\in E} CZ_{a,b}\right]|+\rangle_a \otimes |G - a\rangle_{V\setminus\{a\}} \tag{5.14}$$

$$= \left[(P_{3,+})_a \otimes (\mathbb{1}_2)_{N_a} + (P_{3,-})_a \otimes (\sigma_3)_{N_a}\right]|+\rangle_a \otimes |G - a\rangle_{V\setminus\{a\}}, \tag{5.15}$$

The conditional phase gate on two qubits can be represented by the matrix

$$CZ = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \mathbb{1}_2 + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \sigma_3,$$

which is equal to $P_{3,+} \otimes \mathbb{1}_2 + P_{3,-} \otimes \sigma_3$.

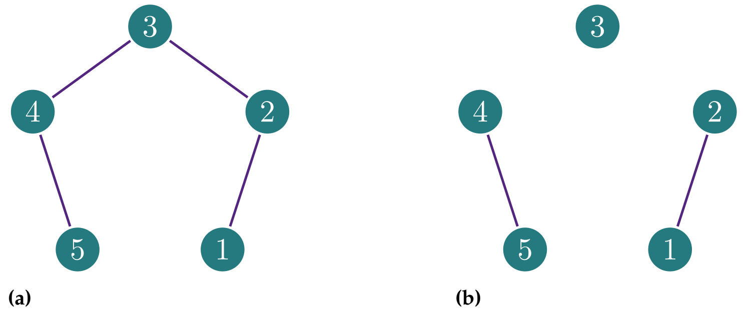


Figure 5.5: A local Pauli measurement on a linear cluster state $|L_5\rangle$ described by the line graph L_5 **(a)** on the vertex set $V_{L_5} := \{1, 2, 3, 4, 5\}$ with edges $E_{L_5} := \{(1, 2), (2, 3), (3, 4), (4, 5)\}$. According to Equation 5.4 a Z-measurement **(b)** on the qubit corresponding to node 3 projects said qubit into the state $|\frac{1\mp 1}{2}\rangle$ and the remainder of the graph state into $|L_5 - 3\rangle$ up to additional local unitary corrections described by Equations 5.9 and 5.10.

and thus for the Z-measurement outcome probabilities (*cf.* Equation 2.56)

$$\Pr(\pm|Z) = \langle G|(P_{3,\pm})_a|G\rangle \tag{5.16}$$
$$= \langle +|_a \otimes \langle G - a|_{V\setminus\{a\}} \left[(P_{3,\pm})_a \otimes (\mathbb{1}_2)_{V\setminus\{a\}}\right] |+\rangle_a \otimes |G - a\rangle_{V\setminus\{a\}} \tag{5.17}$$
$$= \langle +|(P_{3,\pm})|+\rangle_a \cdot \langle G - a|G - a\rangle_{V\setminus\{a\}} = \frac{1}{2} \tag{5.18}$$

since $(\sigma_3)^2_{N_a} = (\mathbb{1}_2)_{N_a}$, $(P_{3,+})_a(P_{3,-})_a = 0$ and $(P_{3,\pm})^2_a = (P_{3,\pm})_a$.

The graph state is then –depending on the outcome (*cf.* Equation 2.57)– projected (note that $\delta_{+,+} = 1 = \delta_{-,-}$ and $\delta_{+,-} = 0 = \delta_{-,+}$) into the state

$$\frac{(P_{3,\pm})_a|G\rangle}{\sqrt{\Pr(\pm|Z)}} \tag{5.19}$$
$$=\sqrt{2}\left[\delta_{\pm,+}(P_{3,+})_a \otimes \mathbb{1} + \delta_{\pm,-}(P_{3,-})_a \otimes (\sigma_3)_{N_a} \otimes \mathbb{1}\right]|+\rangle_a \otimes |G - a\rangle \tag{5.20}$$
$$=\frac{\sqrt{2}}{\sqrt{2}}\left[\delta_{\pm,+}|0\rangle_a \otimes \mathbb{1} + \delta_{\pm,-}|1\rangle_a \otimes (\sigma_3)_{N_a} \otimes \mathbb{1}\right]|G - a\rangle \tag{5.21}$$
$$= \left[\delta_{\pm,+}|0\rangle_a \otimes \mathbb{1} + \delta_{\pm,-}|1\rangle_a \otimes (\sigma_3)_{N_a} \otimes \mathbb{1}\right] |G - a\rangle \tag{5.22}$$
$$=|\frac{1 \mp 1}{2}\rangle_a \otimes U_a^{3,\pm}|G - a\rangle_{V\setminus\{a\}} \tag{5.23}$$

after measurement, where for simplicity the identity matrices $(\mathbb{1}_2)_{V\setminus\{a\}}$ and $(\mathbb{1}_2)_{V\setminus(\{a\}\cup N_a)}$ are written as $\mathbb{1}$ and $|G - a\rangle_{V\setminus\{a\}}$ is denoted as $|G - a\rangle$. The last equality (and hence Equation 5.4) follows with

$$U_a^{3,+} := (\mathbb{1}_2)_{V\setminus\{a\}} \tag{5.24}$$
$$U_a^{3,-} := (\sigma_3)_{N_a} \otimes (\mathbb{1}_2)_{V\setminus(\{a\}\cup N_a)}. \tag{5.25}$$

As an example, the Z-measurement of the central qubit in a linear cluster state with five qubits $|L_5\rangle$ is shown in Figure 5.5.

For the remaining claims, we analyze the conjugation of the measurement projectors with the local complementation unitaries (*cf.* Equation 4.24) and find

$$U_a^\tau := \left(e^{-i\frac{\pi}{4}\sigma_1}\right)_a \otimes \left(e^{i\frac{\pi}{4}\sigma_3}\right)_{N_a} \otimes (\mathbb{1}_2)_{V\setminus(\{a\}\cup N_a)} \tag{5.26}$$
$$(U_a^\tau)^\dagger = \left(e^{i\frac{\pi}{4}\sigma_1}\right)_a \otimes \left(e^{-i\frac{\pi}{4}\sigma_3}\right)_{N_a} \otimes (\mathbb{1}_2)_{V\setminus(\{a\}\cup N_a)}. \tag{5.27}$$

Thereby we can express $(P_{2,\pm})_a$ via conjugation with U_a^τ. Since further the identity $\left(e^{i\frac{\pi}{4}\sigma_3}\right)_{N_a}\left(e^{-i\frac{\pi}{4}\sigma_3}\right)_{N_a} = (\mathbb{1}_2)_{N_a}$ holds we obtain

$$U_a^\tau (P_{3,\pm})_a (U_a^\tau)^\dagger = \left(e^{-i\frac{\pi}{4}\sigma_1}\right)_a (P_{3,\pm})_a \left(e^{i\frac{\pi}{4}\sigma_1}\right)_a = (P_{2,\mp})_a. \tag{5.28}$$

With another local complementation with respect to a neighbor $b \in N_a$, we can further transform $(P_{2,\pm})_a$ to $(P_{1,\pm})_a$. Conjugation with the local complementation unitaries

$$U_b^\tau := \left(e^{-i\frac{\pi}{4}\sigma_1}\right)_b \otimes \left(e^{i\frac{\pi}{4}\sigma_3}\right)_{N_b} \otimes (\mathbb{1}_2)_{V\setminus(\{b\}\cup N_b)} \tag{5.29}$$

$$\left(U_b^\tau\right)^\dagger = \left(e^{i\frac{\pi}{4}\sigma_1}\right)_b \otimes \left(e^{-i\frac{\pi}{4}\sigma_3}\right)_{N_b} \otimes (\mathbb{1}_2)_{V\setminus(\{b\}\cup N_b)} \tag{5.30}$$

yields

$$U_b^\tau (P_{2,\pm})_a \left(U_b^\tau\right)^\dagger = \left(e^{i\frac{\pi}{4}\sigma_3}\right)_a (P_{2,\pm})_a \left(e^{-i\frac{\pi}{4}\sigma_3}\right)_a = (P_{1,\pm})_a \tag{5.31}$$

since $a \in N_b$ and $\left(e^{-i\frac{\pi}{4}\sigma_1}\right)_b\left(e^{i\frac{\pi}{4}\sigma_1}\right)_b = (\mathbb{1}_2)_b$. The Equations 5.28 and 5.31 together lead to

$$U_b^\tau U_a^\tau (P_{3,\pm})_a (U_a^\tau)^\dagger \left(U_b^\tau\right)^\dagger = U_b^\tau (P_{2,\mp})_a \left(U_b^\tau\right)^\dagger = (P_{1,\mp})_a. \tag{5.32}$$

The unitary conjugations transforming $(P_{1,\pm})_a$, $(P_{2,\pm})_a$, and $(P_{3,\pm})_a$ into each other reveal that not only the outcome probabilities of the Z-measurement (*cf.* Equation 5.16), but also those of the X- and Y- measurements are uniformly random.

Using our previous result for $\Pr(\pm|Z)$ from Equation 5.18 we find

$$\Pr(\pm|Y) = \langle G|(P_{2,\pm})_a|G\rangle = \langle \tau_a(G)|(P_{3,\mp})_a|\tau_a(G)\rangle = \frac{1}{2}, \tag{5.33}$$

where the second equality holds since (*cf.* Section 11.1 in the appendix)

$$\langle G|U_a^\tau (P_{3,\mp})_a (U_a^\tau)^\dagger{}_a|G\rangle = \langle \tau_a(G)|(P_{3,\mp})_a|\tau_a(G)\rangle \tag{5.34}$$

and the third follows from the fact that Equation 5.18 is independent of the graph G. In particular, this equality also holds for the graph $\tau_a(G)$ instead of G.

By the same argument, we have

$$\Pr(\pm|X) = \langle G|(P_{1,\pm})_a|G\rangle = \langle \tau_a \circ \tau_b(G)|(P_{3,\mp})_a|\tau_a \circ \tau_b(G)\rangle = \frac{1}{2} \tag{5.35}$$

since with Equation 5.32 we can rewrite $(P_{1,\pm})_a$ and obtain

$$\langle G|U_b^\tau (P_{2,\pm})_a \left(U_b^\tau\right)^\dagger|G\rangle = \langle \tau_a \circ \tau_b(G)|(P_{3,\mp})_a|\tau_a \circ \tau_b(G)\rangle. \tag{5.36}$$

After the measurement, the results for the state vectors are as follows.

The Y-measurement projects the graph state –again depending on the measurement outcome– into the postmeasurement state

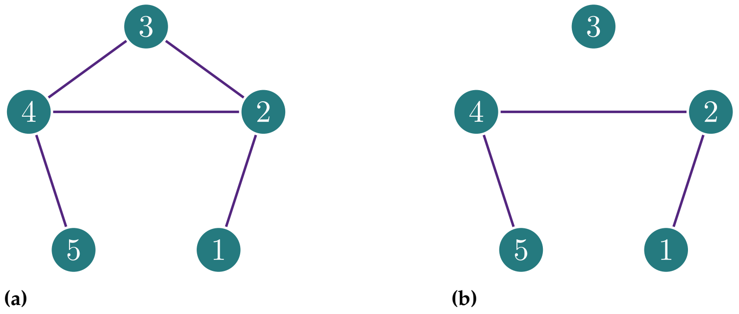


Figure 5.6: A local Pauli measurement on a linear cluster state $|L_5\rangle$ described by the line graph L_5 on the vertex set $V_{L_5} := \{1,2,3,4,5\}$ with edges $E_{L_5} := \{(1,2),(2,3),(3,4),(4,5)\}$. Subfigure **(a)** shows the locally complemented graph $\tau_3(L_5)$. According to Equation 5.3 a Y-measurement **(b)** on the qubit corresponding to node 3 projects said qubit into the state $|\pm i\rangle$ and the remainder of the graph state into $|\tau_3(L_5) - 3\rangle$ up to additional local unitary corrections described by Equations 5.7 and 5.8.

$$\frac{(P_{2,\pm})_a|G\rangle}{\sqrt{\Pr(\pm|Y)}} = \sqrt{2}\left[U_a^\tau (P_{3,\mp})_a (U_a^\tau)^\dagger\right]|G\rangle \tag{5.37}$$

$$\propto\sqrt{2}U_a^\tau (P_{3,\mp})_a|\tau_a(G)\rangle \tag{5.38}$$

$$=U_a^\tau\left[\delta_{\mp,+}|0\rangle_a \otimes \mathbb{1} + \delta_{\mp,-}|1\rangle_a \otimes (\sigma_3)_{N_a} \otimes \mathbb{1}\right]|\tau_a(G) - a\rangle \tag{5.39}$$

$$=\left[\delta_{\mp,+}|-i\rangle_a \otimes \left(e^{i\frac{\pi}{4}\sigma_3}\right)_{N_a} - \delta_{\mp,-} i|+i\rangle_a \otimes \left(e^{i\frac{\pi}{4}\sigma_3}\sigma_3\right)_{N_a}\right] \otimes \mathbb{1}|\cdots\rangle \tag{5.40}$$

$$=\left[\delta_{\mp,+}|-i\rangle_a \otimes \left(e^{i\frac{\pi}{4}\sigma_3}\right)_{N_a} + \delta_{\mp,-}|+i\rangle_a \otimes \left(-ie^{i\frac{\pi}{4}\sigma_3}\sigma_3\right)_{N_a}\right] \otimes \mathbb{1}|\cdots\rangle \tag{5.41}$$

$$=\left[\delta_{\mp,+}|-i\rangle_a \otimes \left(e^{+i\frac{\pi}{4}\sigma_3}\right)_{N_a} + \delta_{\mp,-}|+i\rangle_a \otimes \left(e^{-i\frac{\pi}{4}\sigma_3}\right)_{N_a}\right] \otimes \mathbb{1}|\cdots\rangle \tag{5.42}$$

$$=|\pm i\rangle_a \otimes U_a^{2,\pm}|\tau_a(G) - a\rangle_{V\setminus\{a\}}, \tag{5.43}$$

where we used Equation 5.28 to rewrite $(P_{2,\pm})_a$ and Equation 5.22 to rewrite $(P_{3,\mp})_a$, while the identity matrices $(\mathbb{1}_2)_{V\setminus\{a\}}$ and $(\mathbb{1}_2)_{V\setminus(\{a\}\cup N_a)}$ are written as $\mathbb{1}$ and $|\tau_a(G) - a\rangle_{V\setminus\{a\}}$ is shortened to $|\cdots\rangle$ for the sake of brevity. Together with the action of U_a^τ as described in Equation 5.26 we obtain the last equality (and hence Equation 5.3) with

$$U_a^{2,-} := \left(e^{+i\frac{\pi}{4}\sigma_3}\right)_{N_a} \otimes (\mathbb{1}_2)_{V\setminus(\{a\}\cup N_a)} \tag{5.44}$$

$$U_a^{2,+} := \left(e^{-i\frac{\pi}{4}\sigma_3}\right)_{N_a} \otimes (\mathbb{1}_2)_{V\setminus(\{a\}\cup N_a)}. \tag{5.45}$$

As an example, the Y-measurement of the central qubit in a linear cluster state with five qubits $|L_5\rangle$ is shown in Figure 5.6.

When considering the X-measurement, note that after the first local complementation with respect to the chosen neighbor b in N_a, a second local complementation with respect to a itself must be considered. This second local complementation must take into account the first one in the sense that it is not the neighborhoods in the graph G that are contemplated, but those in the graph $\tau_b(G)$. However, in both G and $\tau_b(G)$ we find a to be an element of N_b.

For the X-measurement, any neighbor $b \in N_a$ can be chosen –if there is a neighbor. If a is an isolated vertex, then the measurement result is always +1 and the state remains unaltered since then the graph state is $|G\rangle = |+\rangle \otimes |G'\rangle$ for a graph G' on the vertices $V \setminus \{a\}$. Otherwise, the X-measurement projects the graph state into the state

$$\frac{(P_{1,\pm})_a|G\rangle}{\sqrt{\Pr(\pm|X)}} = \sqrt{2}\left[U_b^\tau(P_{2,\pm})_a\left(U_b^\tau\right)^\dagger\right]|G\rangle \tag{5.46}$$

$$\propto\sqrt{2}U_b^\tau(P_{2,\pm})_a|\tau_b(G)\rangle \tag{5.47}$$

$$=U_b^\tau\,[\mp cf.\text{ Eq. }5.42]\otimes\mathbb{1}|\tau_a\circ\tau_b(G)-a\rangle \tag{5.48}$$

$$=U_b^\tau\,([\mp cf.\text{ Eq. }5.42]\otimes\mathbb{1})\left(U_b^\tau\right)^\dagger U_b^\tau|\tau_a\circ\tau_b(G)-a\rangle \tag{5.49}$$

$$\propto U_b^\tau\,([\mp cf.\text{ Eq. }5.42]\otimes\mathbb{1})\left(U_b^\tau\right)^\dagger|\tau_b(\tau_a\circ\tau_b(G)-a)\rangle \tag{5.50}$$

$$\propto|\pm\rangle_a\otimes U_a^{1,\pm}|\tau_b(\tau_a\circ\tau_b(G)-a)\rangle_{V\setminus\{a\}} \tag{5.51}$$

depending on the measurement outcome, where we used Equation 5.32 to rewrite $(P_{1,\pm})_a$, Equation 5.42 to rewrite $(P_{2,\mp})_a$,

$$\mp cf.\text{ Eq. }5.42 = \delta_{\mp,+}|-i\rangle_a\otimes\left(e^{+i\frac{\pi}{4}\sigma_3}\right)_{N_a} + \delta_{\mp,-}|+i\rangle_a\otimes\left(e^{-i\frac{\pi}{4}\sigma_3}\right)_{N_a} \tag{5.52}$$

and shortened the identity matrices $(\mathbb{1}_2)_{V\setminus\{a\}}$ and $(\mathbb{1}_2)_{V\setminus(\{a\}\cup N_a)}$ to $\mathbb{1}$.

Under the conjugation with

$$U_b^\tau := \left(e^{-i\frac{\pi}{4}\sigma_1}\right)_b\otimes\left(e^{i\frac{\pi}{4}\sigma_3}\right)_{N_b}\otimes(\mathbb{1}_2)_{V\setminus(\{b\}\cup N_b)} \tag{5.53}$$

$$\exp\left(-i\frac{\pi}{4}X\right) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$$

$$\exp\left(i\frac{\pi}{4}Z\right) = \begin{pmatrix} e^{\frac{i}{4}\pi} & 0 \\ 0 & e^{-\frac{i}{4}\pi} \end{pmatrix}$$

Equation 5.52 transforms into (note that $b \in N_a$ and $a \in N_b$)

$$\delta_{\mp,+}|-\rangle_a\otimes\left(e^{-i\frac{\pi}{4}\sigma_2}\right)_b\otimes\left(e^{+i\frac{\pi}{4}\sigma_3}\right)_{N_a\setminus(N_b\cup\{b\})} \tag{5.54}$$

$$+\delta_{\mp,-}|+\rangle_a\otimes\left(e^{+i\frac{\pi}{4}\sigma_2}\right)_b\otimes\left(e^{-i\frac{\pi}{4}\sigma_3}\right)_{N_a\setminus(N_b\cup\{b\})} \tag{5.55}$$

up to a global phase of $e^{i\frac{\pi}{4}}$. That is, we obtain the last equality of Equation 5.51 (and hence Equation 5.2) with the definition

$$U_a^{1,-} := \left(e^{-i\frac{\pi}{4}\sigma_2}\right)_b\otimes\left(e^{+i\frac{\pi}{4}\sigma_3}\right)_{N_a\setminus(N_b\cup\{b\})}\otimes(\mathbb{1}_2)_{V\setminus(\{a,b\}\cup(N_a\setminus N_b))} \tag{5.56}$$

$$U_a^{1,+} := \left(e^{+i\frac{\pi}{4}\sigma_2}\right)_b\otimes\left(e^{-i\frac{\pi}{4}\sigma_3}\right)_{N_a\setminus(N_b\cup\{b\})}\otimes(\mathbb{1}_2)_{V\setminus(\{a,b\}\cup(N_a\setminus N_b))} \tag{5.57}$$

and the combination of Equations 5.50, 5.52, 5.54, 5.55. This concludes the proof.

As an example, the X-measurement of the central qubit in a linear cluster state with five qubits $|L_5\rangle$ is shown in Figure 5.7. □

As we have seen, local Pauli measurements and local Clifford operations transform graph states by local complementations and vertex deletions. Naturally, the question arises as to which graph states can be obtained from other, larger graph states with sequences of local Pauli measurements and local Clifford operations. The problem of answering the question of whether a given graph state can be obtained from a second larger graph state is known as the vertex minor problem.

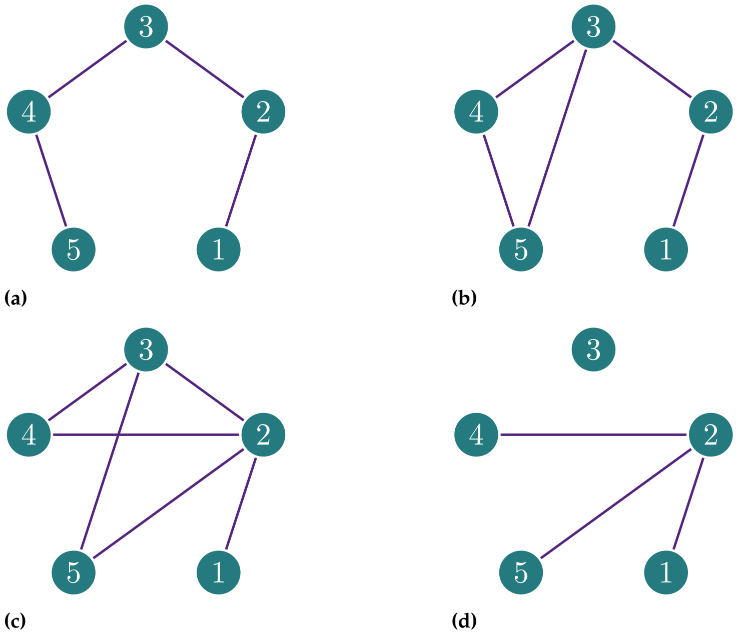


Figure 5.7: A local Pauli measurement on a linear cluster state $|L_5\rangle$ described by the line graph L_5 **(a)** on the vertex set $V_{L_5} := \{1,2,3,4,5\}$ with edges $E_{L_5} := \{(1,2),(2,3),(3,4),(4,5)\}$. Subfigure **(b)** shows the locally complemented graph $\tau_4(L_5)$ and Subfigure **(c)** the twofold locally complemented graph $\tau_3 \circ \tau_4(L_5)$. According to Equation 5.2 an X-measurement **(d)** on the qubit corresponding to node 3 projects said qubit into the state $|\pm\rangle$ and the remainder of the graph state into $|\tau_4(\tau_3 \circ \tau_4(L_5) - 3)\rangle$ up to additional local unitary corrections described by Equations 5.7 and 5.8. Note that the third local complementation with respect to the leaf 4, leaves the graph $\tau_3 \circ \tau_4(L_5) - 3$ invariant.

5.3 The vertex minor problem

We formally define *vertex minors* as follows.

Definition 5.3 (Vertex minor) *A graph $H = (V_H, E_H)$ corresponding to a graph state vector $|H\rangle$ is called a vertex minor of a larger graph $G = (V_G, E_G)$ if $|H\rangle$ can be obtained from $|G\rangle$ via a sequence of local Clifford operations and local Pauli measurements*[a]*. We denote vertex minor relations as $H < G$.*

[a] The measured qubits correspond to the vertices in the set $V_G \setminus V_H$.

The vertex-minor problem was recently proven to be NP-complete in Reference [DHW22]. Similarly, extracting a set of Bell pairs on a fixed set of vertices of general graphs is NP-complete [DHW20c].

Vertex-minor relations of graphs and their connections to the so-called rank-width is discussed in Reference [Oum05].

In Reference [DHW22], the authors even showed that the problem of deciding whether a given graph has a vertex minor that is isomorphic to a second graph remains NP-complete when the graphs are restricted to be circle graphs: Circle graphs are a narrower class of graphs that have a very natural relation to local complementations and therefore to the vertex minor problem. We will investigate this relation in Chapter 8.

While vertex-minor relations are hard in general, it is instructive to study graphs with constraints on their connectivity. For line and ring graphs that exhibit simple nearest-neighbor connectivity, we can in fact determine the limits of their use for quantum communication.

Limitations of nearest-neighbor quantum networks 6

As we discovered in Section 5.1, one of the main features of the multipartite entanglement in graph states is the promise of solving communication bottlenecks in quantum networks. Perhaps the best known and practically motivated example is the butterfly network, where two pairs of nodes intend to send quantum messages between them, bypassing the existing bottleneck in the network.

In particular, we have uncovered the underlying property that allows to bypass existing bottlenecks in the networks of the butterfly (*cf.* Figure 5.2) and similar types (*cf.* Figure 5.3). In the case of the butterfly graph state, simple X-measurements at the two central qubits lead to the formation of two crossing maximally entangled pairs, allowing further quantum communication by teleportation (see Section 3.1). This inspired the X-protocol 5.2 of Reference [HPE19].

However, we have also shown that this corresponds to a more broadly applicable technique that uses local complementation (see Definition 4.7) and, more specifically, explores local complementation orbits (see Definition 4.8), allowing us to optimize the available quantum resources. By allowing arbitrary local Clifford unitaries and Pauli measurements, local complementation orbits describe a larger class of possible algorithms than just the X-protocol introduced in Definition 5.2.

The following sections closely follow the text of Reference [Hah+22], which was written by both myself and my co-authors. ↓ ↓ ↓

When considering random network topologies, it is overall more likely that a bottleneck will occur in sparse networks where connectivity between different nodes is limited. Specific cases of sparse networks that are of great importance to quantum communication are nearest-neighbor architectures. Such networks allow quantum information to travel only over short distances and therefore aim to minimize noise and losses during transmission.

The butterfly network is one of the smallest examples of a grid network, while other common nearest-neighbor architectures are lines and rings. Since, apart from the case of the butterfly and related examples, not much was known about what is possible in this type of network architectures, we explored their capabilities in Reference [Hah+22].

In Reference [Hah+22] we investigate in detail whether it is possible to extend the butterfly network example to these nearest-neighbor type architectures. In particular, we ask whether simultaneous communication of two pairs of nodes in bottleneck scenarios is possible when the underlying architecture is a ring or a line.

We conclude that these nearest-neighbor networks are unsuitable for bypassing bottlenecks, and that therefore an additional long-distance communication link is required for line and ring network topologies. In the next sections we show why.

6.1 Local Pauli measurements in the graphical representation

As discussed in Section 5.2, we can describe graph state transformations under local Pauli measurements in terms of local complementations of the corresponding graph and additional local unitaries. If we consider only the general entanglement properties (rather than a specific communication protocol implementation where we are interested in the exact state), we can exclude the latter local unitaries from our consideration.

Local Pauli measurements on $|G\rangle$ result in a different graph state up to local unitary corrections (see Theorem 5.6).

We then can describe measurements in the Z-basis simply as the removal of the measured vertex from the graph (and thus the removal of the measured qubit from the graph state), Y-measurements with a local complementation before this removal, and X-measurements with a set of three local complementation in combination with the removal. Following Theorem 5.6, we therefore define local Pauli measurements P_v with respect to these graph actions, *i.e.*, $P_v \in \{X_v, Y_v, Z_v\}$ maps a graph with n vertices to one with $n-1$ by removing v.

Definition 6.1 (Pauli measurements) *The graph action of* Z_v *is* $Z_v(G) := (\tilde{V}, E \cap \tilde{V} \times \tilde{V})$ *with* $\tilde{V} := V \setminus \{v\}$*, that is, deleting the row and column of* v *from* Γ_G *gives* $\Gamma_{Z_v(G)}$*. With local complementations we further have* $Y_v(G) := Z_v \circ \tau_v(G)$ *and* $X_v(G) := Z_v \circ \tau_w \circ \tau_v \circ \tau_w(G)$*, where* $w \in N_v$*.*

As described in Section 5.3, a graph H that can be obtained from a graph G by a sequence of local complementations and vertex deletions is called a vertex minor of G. We refer to this as $H < G$ and call a graph v*-minor* of another graph if v is the single deleted vertex, *e.g.* $X_v(G)$, $Y_v(G)$ and $Z_v(G)$ are v-minors of G.

Since solving general problems in quantum network routing is provably hard, we focus on impossibility results for widely used network architectures: rings and lines. Because of their symmetry, we consider the former first.

6.2 Ring graphs

We first consider graph state vectors $|R_n\rangle$ corresponding to ring graphs, *i.e.* $R_n := (V_n, E_n)$ with $V_n := \{1, \ldots, n\}$ and $E_n := \{(1,2), (2,3), \ldots, (n-$

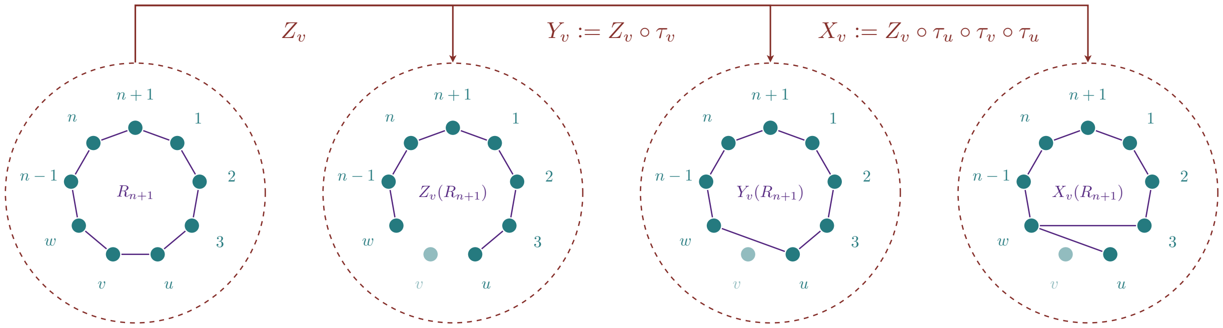
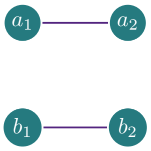


Figure 6.1: Measurements on a ring. From left to right: Ring R_{n+1} with $n+1$ vertices, node v is measured in the Z-, Y- and X-basis.

$1, n), (n, 1)\}$; see Figure 6.1. Our goal is to obtain two maximally entangled pairs between qubits $\{a_1, a_2\}$ and $\{b_1, b_2\}$ via local Clifford operations and Pauli measurements. That is, we want to determine if the most simple graph with two connected components

$$K_2 \cup K_2 := (\{a_1, a_2, b_1, b_2\}, \{(a_1, a_2), (b_1, b_2)\}) \qquad (6.1)$$



The simple graph $K_2 \cup K_2$.

is a vertex-minor of R_n. Without loss of generality we can restrict to $a_1 < a_2$, $b_1 < b_2$ and set $a_1 = 1$. In order to show that it is not possible to achieve our goal if $a_1 < b_1 < a_2 < b_2$, we will make use of the following lemmas.

Lemma 6.1 ([DHW20b]) *Let G and H be two graphs and $(v_1, v_2, \ldots, v_k)$ be an ordered tuple of vertices that contains each element of $V_G \setminus V_H$ exactly once. We define the corresponding set of possible Pauli operations as*

$$\mathcal{P}_{(v_1,v_2,\ldots,v_k)} := \{P_{v_k} \circ P_{v_{k-1}} \circ \cdots \circ P_{v_1} | P_v \in \{X_v, Y_v, Z_v\}\}. \qquad (6.2)$$

Then H is a vertex-minor of G if and only if there exists an operation $P \in \mathcal{P}_{(v_1,v_2,\ldots,v_k)}$ such that H can be obtained from $P(G)$ via a sequence of local complementations.

It will also be useful to single out two specific types of vertices, namely *leaves* and *axils*.

Definition 6.2 (Leaf and axil) *A leaf is a vertex with degree one. An axil is the unique neighbor of a leaf.*

For leaves and axils, we have the following lemma regarding the relevant vertex-minors.

Lemma 6.2 ([DW18]) *Let G and H be graphs and v be a vertex in V_G but not in V_H. Then it holds that:*

(a) If v is a leaf: $H < G \Leftrightarrow H < G \backslash v$.
(b) If v is an axil: $H < G \Leftrightarrow H < \tau_w \circ \tau_v(G) \backslash v$,

where w is the leaf associated with v.

Note that (b) follows from (a) as leaf and associated axil can be transformed into each other via local complementation. With Lemmas 6.1 and 6.2 we can prove our no-go results (Theorems 6.3 and 6.8). In combination with Theorem 6.7, we provide a tool that can find application to more general network architectures that are not limited to nearest-neighbor ones.

Theorem 6.3 (No crossing on a ring) *It is not possible to extract two maximally entangled pairs from $|R_n\rangle$ if $a_1 = 1 < b_1 < a_2 < b_2$ for any $n \in \mathbb{N}$ with local Clifford operations, local Pauli measurements and classical communication.*

Proof. The proof works by induction. The base case is trivial for $1 \leq n \leq 4$. For $n = 5$ and $n = 6$ it can be derived by Propositions 1 and 2 in Reference [HPE19], since ring graphs have a bottleneck with respect to communication requests of the type $a_1 < b_1 < a_2 < b_2$.

For the inductive step, we now assume that Theorem 6.3 holds up to a given n. We can then build an argument on three case distinctions to show the same follows for $n+1$. In order to see this, note that $K_2 \cup K_2$ is a vertex-minor of R_{n+1} if and only if it is a vertex-minor of at least one of $X(R_{n+1})$, $Y(R_{n+1})$ or $Z(R_{n+1})$; see Lemma 6.1. In the following we will show that it is not a vertex-minor of any of them.

More specifically, any v-minor H of R_{n+1} is, according to Lemma 6.1, equivalent to either $X_v(R_{n+1})$, $Y_v(R_{n+1})$ or $Z_v(R_{n+1})$ via a sequence of local complementations. As the vertex-minor relationship is inherited via local complementations, $K_2 \cup K_2$ can only be a vertex-minor of H if it is a vertex-minor of at least one of $X(R_{n+1})$, $Y(R_{n+1})$ or $Z(R_{n+1})$. It is therefore enough to show that $K_2 \cup K_2 \not< P_v(R_{n+1})$ for all $P_v \in \{X_v, Y_v, Z_v\}$, where we have $v \notin \{a_1, a_2, b_1, b_2\}$. We consider the three cases separately.

Lemma 6.4 $K_2 \cup K_2 \not< Z_v(R_{n+1})$.

$Z_v(R_{n+1})$ is the line graph L_n with n vertices as depicted in Figure 6.1. With Theorem 6.8 we find that maximally entangled pairs (a_1, a_2) and (b_1, b_2) can not be extracted from the corresponding graph state vector $|L_n\rangle$, *i.e.*, $K_2 \cup K_2 \not< Z_v(R_{n+1})$.

Lemma 6.5 $K_2 \cup K_2 \not< Y_v(R_{n+1})$.

Since $Y_v(R_{n+1}) = R_n$ (see also Figure 6.1), we can use our induction hypothesis to infer that $|Y_v(R_{n+1})\rangle$ does not allow for the extraction of maximally entangled pairs (a_1, a_2) and (b_1, b_2), that is, we have $K_2 \cup K_2 \not< Y_v(R_{n+1})$.

Lemma 6.6 $K_2 \cup K_2 \not< X_v(R_{n+1})$.

$X_v(R_{n+1})$ is the ring graph R_n with an additional leaf as depicted in Figure 6.1. The former neighbors of v within the graph R_{n+1} constitute leaf u and axil w –note that the roles of u, w are reversed if the other vertex is chosen as a special neighbor in the sense of Definition 6.1.

If both leaf and axil are part of the target graph and constitute one of the target Bell pairs, *i.e.*, $\{u, w\} \in \{\{a_1, a_2\}, \{b_1, b_2\}\}$, this contradicts the assumption $a_1 < b_1 < a_2 < b_2$, since there is no vertex between u and w.

Both leaf and axil can also not be part of the target graph while being in different Bell pairs: Leaf-axil pairs either remain such pairs under local complementations or turn into twins (*cf.* Theorem 6.7, Figure 6.2 and Definitions 6.3, 6.4). This is a contradiction to u and w being in different Bell pairs of the target graph, since measuring the neighborhood of axils or twins can never result in a graph with two connected components.

If just the axil w is part of the target graph, Lemma 6.2 (a) with $v = u$ reduces the problem to R_n and we can use our induction hypothesis.

If just the leaf u is part of the target graph, we can use Lemma 6.2 (b) with $v = w$. □

6.3 The foliage of graph states is LC-invariant

In addition to the two types of vertices we singled out in Definition 6.2, a third type becomes relevant with respect to the transformation of axils and leaves under local complementation. This third type regards vertices that have the same neighborhood with respect to a given graph; thus, we call them twins.

Definition 6.3 (Twin) *A twin is a vertex v that has the same neighborhood as a second vertex $w \neq v$ in the sense that*

$$N_v \setminus \{w\} = N_w \setminus \{v\}. \tag{6.3}$$

The foliage is the set that contains all three types of vertices combined.

Definition 6.4 (Foliage) *The set containing all the leaves, axils and twins of a graph is called the foliage of that graph.*

Theorem 6.7 (Foliage is LC-invariant) *The foliage of a graph G is invariant under local complementation.*

Proof. For $G = K_2 = \tau_v(K_2)$ the statement is trivial as both vertices are leaves, axils, and twins at the same time. For all other graphs note that a twin can be transformed into a leaf (or an axil) via local complementations:

If twins v and w are neighbors, τ_w disconnects v from all its other neighbors, that is, in $\tau_w(G)$ the vertex v is a leaf and w its axil.

If twins v and w are not neighbors, note that a twin pair always has a common neighbor u (unless $G = K_2$). In the graph $\tau_u(G)$, the two vertices are then neighboring twins. With the above argument we know that in $\tau_w \circ \tau_u(G)$ vertex v is a leaf and w the corresponding axil. Conversely, given a pair of leaf v and axil w, the local complementation τ_w connects v to every vertex in N_w, *i.e.*, a twin pair is created. Again, choosing a common neighbor u allows us to go to the graph $\tau_u \circ \tau_v(G)$ in which w is a leaf and v its axil.

In fact, Figure 6.2 shows that all LCs on u, v, w with $u \in N_v$ and/or $u \in N_w$ leave the foliage invariant. Since LCs can only transform the neighborhood, we thus have shown that leaves, axils and twins can *only* be transformed into each other with local complementations.

As LCs are self-inverse this concludes the proof: Assume that a node in the foliage can be created via LCs out of a node that is not in the foliage. Then the reverse sequence of LCs would transform a node in the foliage to one that is not –contradicting the last sentence of the previous paragraph. □

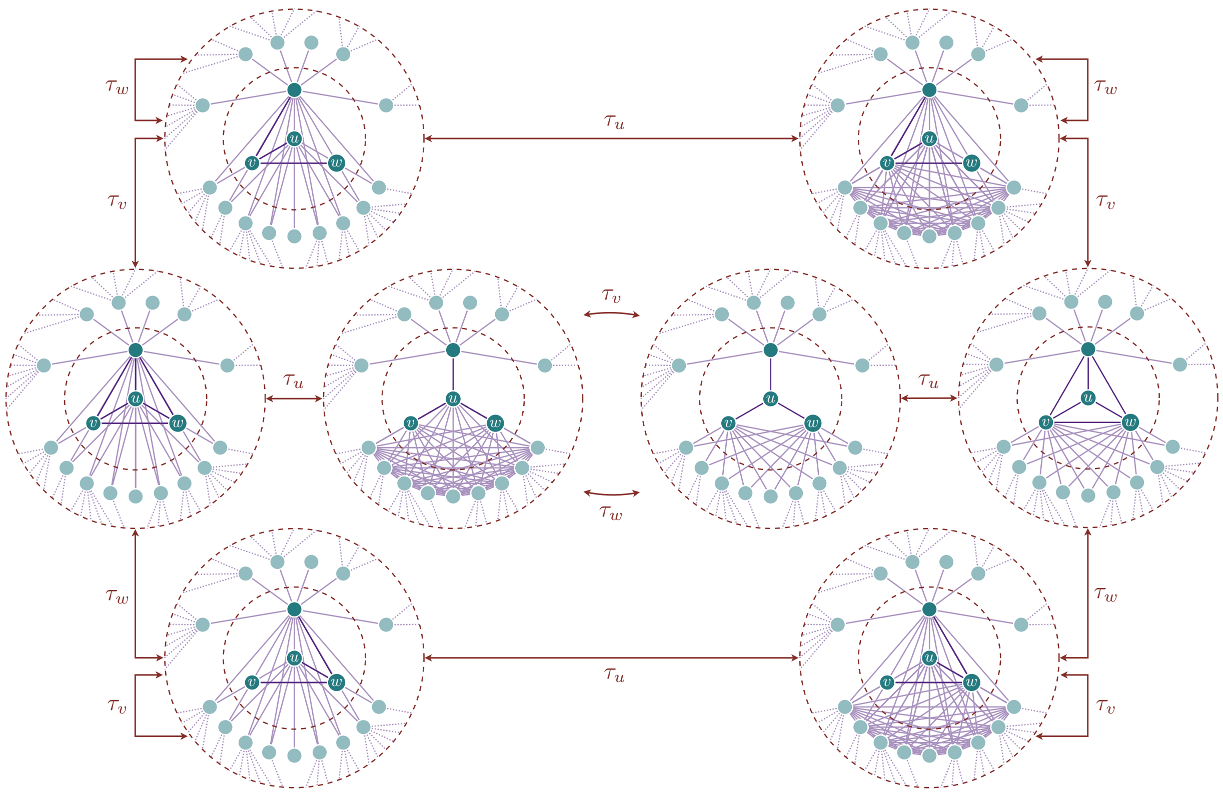


Figure 6.2: The foliage is LC-invariant. The arrows indicate how foliage nodes u, w transform under LCs. The central four graphs show twins v, w that can be (dis-) connected via a LC with respect to one of their neighbors u. The LCs τ_v and τ_w transform the outer graphs with the connected twins into graphs where either v (upper row) or w (lower row) is an axil and their former twin partner a leaf.

6.4 Line graphs

In analogy to Theorem 6.3, we can prove a no-go theorem for line graphs, *i.e.*, $L_n := (V_n, E_n)$ with vertices $V_n := \{1, \ldots, n\}$ and edges $E_n := \{(1,2), (2,3), \ldots, (n-1, n)\}$.

Theorem 6.8 (No crossing on a line) *It is not possible to extract two maximally entangled pairs from $|L_n\rangle$ if $a_1 < b_1 < a_2 < b_2$ for any $n \in \mathbb{N}$ with local Clifford operations, local Pauli measurements and classical communication.*

Proof. Again, the base case for $1 \leq n \leq 4$ is trivial and for $n = 5$ and $n = 6$ given by [HPE19]. For the inductive step, we assume that Theorem 6.8 holds up to a given n. By the same argument as above, $K_2 \cup K_2$ is a vertex-minor of L_{n+1} if and only if it is a vertex-minor of at least one of $X(L_{n+1})$, $Y(L_{n+1})$ or $Z(L_{n+1})$. We will now show that $K_2 \cup K_2 \nless P_v(L_{n+1})$ for all $P_v \in \{X_v, Y_v, Z_v\}$, where we have $v \notin \{a_1, a_2, b_1, b_2\}$. Again, we consider three cases.

Lemma 6.9 $K_2 \cup K_2 \nless Z_v(L_{n+1})$.

If $v = 1$ or $v = n + 1$, we find $Z_v(L_{n+1}) = L_n$ and can use our induction hypothesis. Otherwise, the Z_v-measurement splits the line into two line segments L_i and L_j with $i + j = n$. This implies $i, j \in \{1, 2, \ldots, n-1\}$

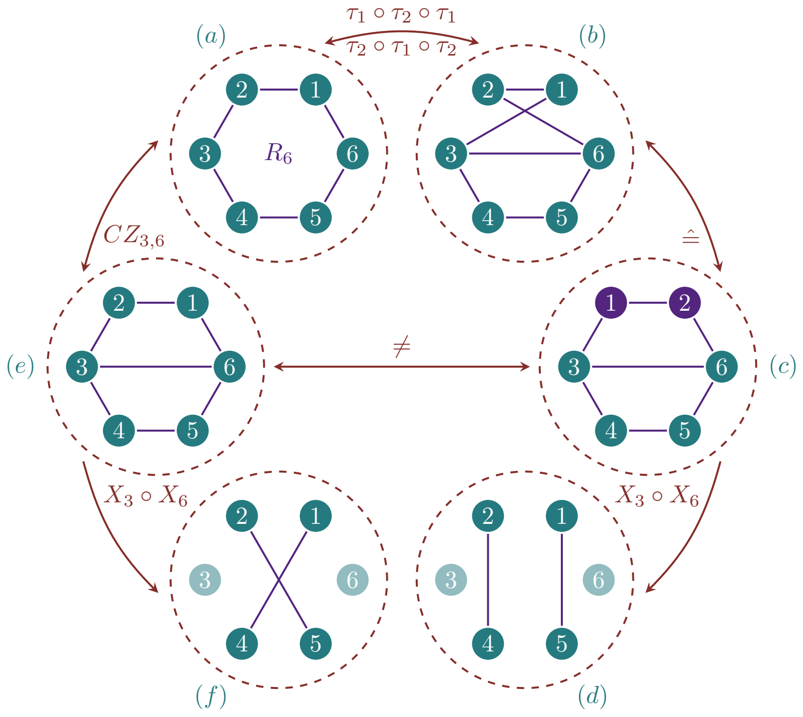


Figure 6.3: Ring (a) and butterfly (e) network. While ring and butterfly networks are not LC-equivalent, a ring graph (a) can be transformed via LCs into a butterfly-like graph (c), where two nodes, here 1 and 2, are swapped ($\hat{=}$). The ring R_6 is transformed via a local complementation sequence (a), $(b)\hat{=}(c)$. From the resulting graph (c), one can obtain maximally entangled pairs (d) between nodes $(2, 4)$ and $(1, 5)$ by measuring 3 and 6. When allowing for 2-local operations (specifically CZ-gates) between nodes 3 and 6 (e) one can obtain crossing Bell pairs $(1, 4)$ and $(2, 5)$ (f).

and we can again use the induction hypothesis.

Lemma 6.10 $K_2 \cup K_2 \not< Y_v(L_{n+1})$.

We have $Y_v(L_{n+1}) = L_n$, a graph on the n vertices $\{1, 2, \dots, v-1, v+1, \dots, n+1\}$, since local complementation with respect to v connects $v-1$ to $v+1$ but leaves the remaining graph unchanged. Again, $K_2 \cup K_2$ cannot be a vertex-minor of $Y_v(L_{n+1})$ by our induction hypothesis.

Lemma 6.11 $K_2 \cup K_2 \not< X_v(L_{n+1})$.

If $v = 1$ or $v = n+1$, we find $X_v(L_{n+1}) = L_{n-1}$ and can use our induction hypothesis. Similarly, in the cases $v = 2$ and $v = n$ we get $X_v(L_{n+1}) = L_n$. In all other cases, we have $X_v(L_{n+1})$ equal to L_{n-1} with an additional leaf, where the leaf-axil pair is made up by the set $\{v-1, v+1\}$. Using the same argument as in the proof of Lemma 6.6 –involving Theorem 6.7 and Lemma 6.2– we can conclude our proof.

□

6.5 Beyond nearest-neighbor networks

In Reference [Hah+22], we build upon quantum network routing research to examine whether commonly used nearest-neighbor architectures can aid with bypassing bottlenecks. We established two no-go results for ring and line topologies with Theorems 6.3 and 6.8. We showed that, unlike the grid, whose smallest instance is the butterfly network (*cf.* Figure 5.2), these two architectures are not suitable for bypassing bottlenecks without additional longer communication links.

However, it should be noted that ring and line architectures would be suitable if we allowed 2-local operations over longer distances; as shown in Figure 6.3 with such longer distance operations that entangle two non-nearest-neighbors we can indeed transform a ring graph state to a butterfly graph state and thereby enable the generation of crossing maximally entangled pairs.

The preceding sections closely follow the text of Reference [Hah+22], which was written by both myself and my co-authors.

The techniques from Reference [Hah+22] presented in the preceding sections are not limited to the particular scenarios of ring and line networks. In principle, they are applicable to all specifiable graph topologies: The invariance of the foliage under local complementation (*i.e.* Theorem 6.7) is not limited to graphs with ring or line topology. Importantly, this notion of the foliage of a graph can even be refined, as we will explore in the following section.

Foliage and foliage partition 7

7.1 LC-invariant construction

In this chapter, we present an easy-to-compute LC-invariant for graph states.

While other, known invariants completely characterize the LC-equivalence class of any graph state, these invariants are computationally inefficient. Their computation requires knowledge of the given state's full stabilizer set, which is exponential in the number of its qubits [VDD05b; VDD05a]. This inefficiency makes the known invariants impractical.

To mitigate this inefficiency, we introduce the *foliage partition*: An easy-to-compute LC-invariant of computational complexity $\mathcal{O}(n^3)$ in the number of qubits n, which eliminates this need to compute the exponential stabilizer set.

I would like to thank Adam Burchardt for the entertaining discussions at the quantum information conference in Seefeld and for the countless videoconferences afterwards in which we got to the heart of this idea. We are currently preparing a manuscript for the publication of our results. Part of it are the results presented in this chapter. *(During the review period of this thesis, this chapter was extended to the preprint [BH23].)*

Closely related to the foliage of a graph, which we introduced in the previous chapter, the foliage partition also has a simple graphical representation in terms of leaves, axils, and twins.

We define a graph's foliage partition by partitioning the corresponding vertex set with a simple equivalence relation.

We show that foliage partitions are invariant under local complementations of their graph –yielding a LC-invariant for graph states.

Surprisingly, the foliage partition invariance also holds for the generalization from qubits to *qudits*: we prove the invariance under the generalized qudit local complementation operations for *weighted graphs*. Hence, the foliage partition of any (weighted) graph constitutes an easy-to-compute LC-invariant of the corresponding (qudit) graph state.

7.2 The foliage partition

In this section, we will first develop some intuition for the foliage partition before defining it more abstractly a second time in the next section.

The foliage that we introduced in Definition 6.4 and that proved to be a helpful tool due to its invariance under local complementation does exhibit a rich substructure that we can investigate further. With the help of set partitions we formalize this structure that the foliage of a graph induces on its vertex set.

Definition 7.1 (Partition) *A partition of a set V is a collection of its subsets $V_i \subseteq V$, such that they are pairwise disjoint, that is, $V_i \bigcap V_j = \emptyset$ for $i \neq j$, and such that they sum up to the whole set as $\bigcup_{i=1}^{k} V_j = V$. We denote a partition as $V_1, \dots, V_k \vdash V$.*

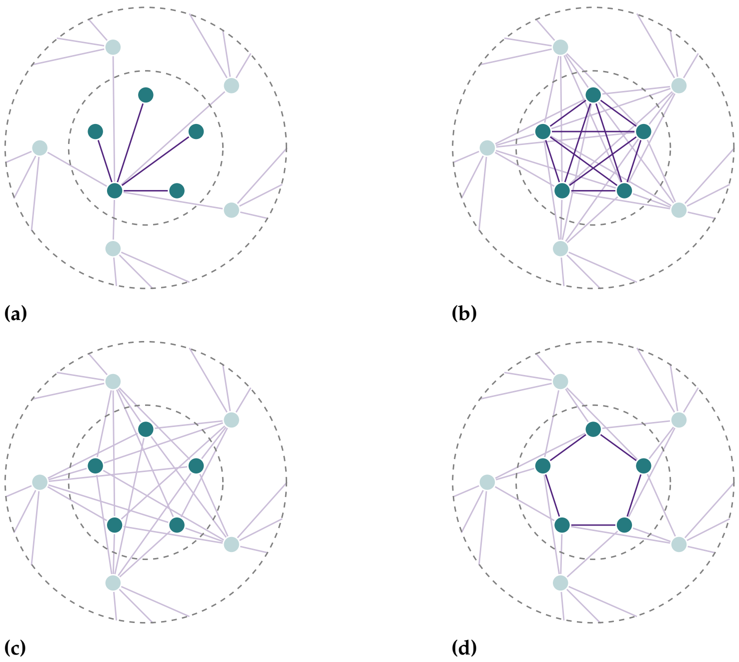


Figure 7.1: Possible structures for subsets V_i in foliage partitions. While the three graphs **(a)**, **(b)** and **(c)** highlight one partition of each type V_i (*cf.* Definition 6.4) in the inner circle, the graph **(d)** shows five partition sets $V_i, V_{i+1}, V_{i+2}, V_{i+3}$, and V_{i+4}, each containing only a single vertex.

Definition 7.2 (Foliage partition) *The foliage partition of a graph $G = (V, E)$ is the unique partition of its vertices $V_1, \dots, V_k \vdash V$ such that for each $i \in \{1, \dots, k\}$ the corresponding subset V_i of size $m := |V_i|$ is of one of the following three types:*

- ✶ *$V_i = \{a, l_1, l_2, \dots, l_{m-1}\}$ consists of an axil a and all adjacent leaves $\{l_k\}_{j=1}^{m-1}$;*
- ⛤ *$V_i = \{t_1, t_2, \dots, t_m\}$ is a set of all connected twins. i.e. $G[V_i]$ is the complete graph K_m, with pairwise the same neighborhood;*
- ⁙ *$V_i = \{t_1, t_2, \dots, t_m\}$ is a set of all disconnected twins, i.e. $G[V_i]$ is the empty graph $(V_i, \emptyset)$, with pairwise the same neighborhood;*

For $m = 1$, all three types coincide and we have $V_i = \{z_i\}$, that is, a set containing a vertex that is not in the foliage of G. If a subset V_i contains only one element, i.e. $m = 1$, it is of all three types at the same time, and we use • to denote the set. For $G = K_2$, ✶ and ⛤ coincide. The union $\cup_{i:|V_i|\geq 2} V_i$ is the foliage of G.

Examples of the types ✶, ⛤, ⁙ and are visualized in Figure 7.1. Local complementation can transform the types ✶, ⛤ and ⁙ into each other, as shown in Figure 7.2:

A local complementation τ_a with respect to the axil a of ✶ transforms the type ✶ into the type ⛤. Conversely, any vertex t of ⛤ can be transformed with τ_t into the axil of ✶.

Likewise, a local complementation τ_b with respect to a neighbor b of a set of disconnected twins ⁙ transforms the type ⁙ into the type ⛤. Conversely, any vertex t of ⛤ can be transformed with τ_t into a disconnected twin in ⁙.

A local complementation with respect to a leaf in type ✶ or a disconnected twin in type ⁙ leaves the sets invariant. Indeed, we observe that the foliage partition is invariant under local complementation.

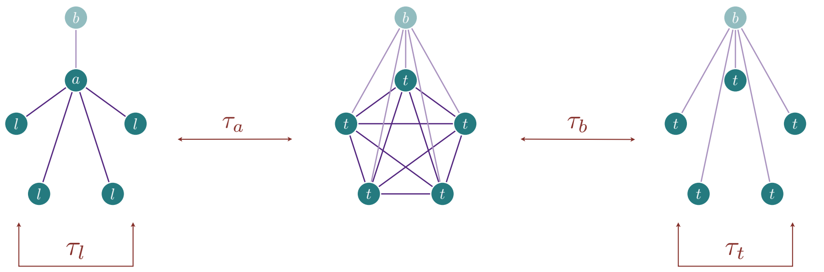


Figure 7.2: Transformation of foliage partition types into each other. Note that for simplicity only one neighbor b is shown.

Lemma 7.1 (Foliage is a partition) *The foliage partition of any graph G is indeed a partition of the set of vertices V.*

Proof. For the trivial case $G = K_2$, the foliage partition is simply $\{1, 2\} \vdash V$ and the definitions for ✳ and ⛤ coincide. For all other graphs, the four types of sets the are distinct:

Let $V_1, \ldots, V_k \vdash V$ be a foliage partition of $G \neq K_2$. Since each vertex $v \in V$ is either part of the graph's foliage or not, we know that $v \in V_i$ for some $i \in \{1, \ldots, k\}$. This implies that $\bigcup_{i=1}^{k} V_j = V$.

The subsets are also pairwise disjoint: The sets of type $V_i = \{z_i\}$ lie outside of the foliage and and therefore cannot overlap with the sets of type ✳, ⛤, ⁙. Likewise, a set of disconnected twins ⁙ cannot overlap with a set of connected twins ⛤ since this would violate Equation 6.3. Neither can a set of twins of either kind overlap with a set of an axil and its leaves ✳ since $G \neq K_2$. Any overlap would imply that a leaf has more than one neighbor. □

Theorem 7.2 (Foliage partition is LC-invariant) *Foliage partitions are LC-invariant.*

For every local complementation orbit of graph states with up to 8 qubits, we visualize the corresponding foliage partition in Appendix 11.2.

Proof. In Section 6.3 we showed that the foliage of any graph G is invariant under local complementation by illustrating that leaves, twins, and axils can be transformed only into each other via local complementation. In particular, any set of disconnected twins ⁙ can be transformed into a set of connected twins ⛤ and any one of the twins can be transformed into an axil with the remaining twins transformed into its leaves ✳.

But the argument applies separately to any set of twins or axils & leaves in the foliage. It is therefore not possible to move a twin, leaf, or axil from one subset of the foliage partition to another, *i.e.* the argument from Reference [Hah+22] presented in Section 6.3 shows that not only the entire foliage of a graph, but also the individual subsets forming a foliage partition are invariant under local complementation. □

Corollary 7.3 immediately follows: We can use the foliage partition as a simple necessary condition to find out whether two graphs can be LC-equivalent.

Corollary 7.3 *Consider two graphs G_1 and G_2 on the same set of vertices V. Having the same foliage partition is a necessary condition for graphs G_1 and G_2 to be LC-equivalent.*

7.3 The foliage relation

In this section, we will use the intuition that we built above for the foliage partition to find a more abstract definition for the same object. For now we will omit the proofs for brevity, but we will include them in the section on the more general results for qudits. Equivalently to Definition 7.2 we can define the foliage partition by a remarkably simple relation.

Definition 7.3 (Foliage relation $\sim$) *Let $G = (V, E)$ be a graph and its adjacency matrix be $\Gamma_G = (a_{ij})_{i,j \in V}$. We define a binary relation on V. Two vertices are related $v \sim w$ if and only if they are in the same connected component and for any other pair of vertices u_1, u_2 it holds that*

$$a_{v,u_1} \cdot a_{w,u_2} = a_{v,u_2} \cdot a_{w,u_1}. \tag{7.1}$$

The relation presented in Definition 7.3 is an equivalence relation and therefore induces a partition on the set of vertices.

Lemma 7.4 *The relation presented in Definition 7.3 is an equivalence relation.*

The partition induced by the foliage relation $\sim$ is exactly the foliage partition defined in Definition 7.2.

7.4 The foliage representation

The foliage partition allows us to establish a further useful representation of the corresponding graph.

We group all vertices in the same set V_i together and take this set as a vertex of a new graph, which we call the *foliage graph*. In order for the representation to be reversible, we assign to each set V_i (new vertex) its type (one of three types listed in Definition 7.2) and if the subset was of type ⁂, we further indicate the axil.

The foliage graph together with an aforementioned *type function* and an *axil set* form the *foliage representation* of a graph. Formally, we define the following.

Definition 7.4 (Type function, axil set) *Consider the foliage partition $V_1, \ldots, V_k \vdash V$ of a graph $G = (V, E)$. Each subset V_i is of exactly one of the following types* ⁂, ⛤, ⁙, • *, which uniquely define the type function $T : \{V_1, \ldots, V_k\} \to \{$*⁂, ⛤, ⁙, •*$\}$. We further denote by $A \subset V$ the axil set of G, i.e. the set containing all axils of G.*

Note that A contains exactly one element from each V_i with $T(V_i) =$ ⁂, and no elements from other subsets.

Definition 7.5 (Foliage graph) *To a given graph $G = (V, E)$, with a foliage partition $V_1, \ldots, V_k \vdash V$, we associate a graph $\widetilde{G} = (\widetilde{V}, \widetilde{E})$ on vertices $\widetilde{V} = \{V_1, \ldots, V_k\}$. Two vertices V_i, V_j are connected in $\widetilde{G}$ if and only if subsets V_i, V_j were connected in the initial graph G. In other words*

$\{V_i, V_j\} \in \widetilde{E}$ if and only if there are $v_i \in V_i, v_j \in V_j$ such that $\{v_i, v_j\} \in E$.

Together we obtain the foliage representation.

Definition 7.6 (Foliage representation) *With any given graph G we associate a tuple $\hat{G} = (\widetilde{G}, T, A)$, where $\widetilde{G}$ is a foliage graph, and T is a type function, and A is an axil set. We call $\hat{G}$ the foliage representation of G.*

Lemma 7.5 *Foliage representations of graphs allow to recover the initial graphs.*

Proof. Let $\hat{G} = (\widetilde{G}, T, A)$ be a tuple, where $\widetilde{V}$ is a partition of a set V, $\widetilde{G} = (\widetilde{V}, \widetilde{E})$ is a graph, $T : \widetilde{V} \longrightarrow \{$✳, ✪, ⁙, •$\}$ is an arbitrary type function, and $A \subset V$ is a subset containing exactly one element from each V_i such that $T(V_i) =$ ✳, and no elements from other subsets.

We define graph G on the set of V vertices by defining the set of its edges $E \subset V \times V$. Consider any two vertices $v, w \in V$. If both vertices v, w belong to the same subset V_i in the $\widetilde{V}$ partition, we connect them by an edge if and only if either $T(V_i) =$ ✪, or $T(V_i) =$ ✳ and $v \in A$ or $w \in A$. Suppose that vertices v, w belong to different parts of the $\widetilde{V}$ partition, *i.e.* $v \in V_i, w \in V_j$, $i \neq j$. We connect v and w by an edge if and only if the following three conditions are simultaneously satisfied: $\{V_i, V_j\} \in \widetilde{E}$, and $T(V_i) =$ ✳ $\Rightarrow v \in A$, and $T(V_j) =$ ✳ $\Rightarrow w \in A$. □

Local complementation operations can change the foliage representation of a graph. As we will see, local complementation operations $\tau_a(\cdot)$ on a graph can be lifted onto lifted local complementation operations $\hat{\tau}_a(\cdot)$ on the graph's foliage representation.

Definition 7.7 (Lifted local complementation) *Let $G = (V, E)$ be a graph with foliage graph $\widetilde{G} = (\widetilde{V}, \widetilde{E})$. and foliage representation $\hat{G} = (\widetilde{G}, T, A)$.*

For any vertex $a \in V$, we define a lifted local complementation $\hat{\tau}_a(\hat{G}) := (\tau_{V_i}(\widetilde{G}), T', A')$, where $V_i \in \widetilde{V}$ such that $a \in V_i$, $\tau_{V_i}(\widetilde{G})$ is a local complementation of the foliage graph $\widetilde{G}$ with respect to its vertex $V_i \in \widetilde{V}$, and

$$T'(V_j) = \begin{cases} \text{✳} & \text{if } j = i \text{ and } T(V_i) = \text{✪}, \\ \text{✪} & \text{if } j = i \text{ and } T(V_i) = \text{✳}, \\ \text{⁙} & \text{if } \{V_i, V_j\} \in \widetilde{E} \text{ and } T(V_j) = \text{✪}, \\ \text{✪} & \text{if } \{V_i, V_j\} \in \widetilde{E} \text{ and } T(V_j) = \text{⁙}, \\ T(V_j) & \text{otherwise}, \end{cases} \tag{7.2}$$

where in the first case a is the axil and

$$A' = \begin{cases} A \cup \{a\} & \text{if } T(V_i) = \text{✪}, \\ A \setminus \{a\} & \text{if } T(V_i) = \text{✳}, \\ A & \text{otherwise}. \end{cases} \tag{7.3}$$

The foliage representation of a locally complemented graph is the same as its lifted locally complemented foliage representation. In other words

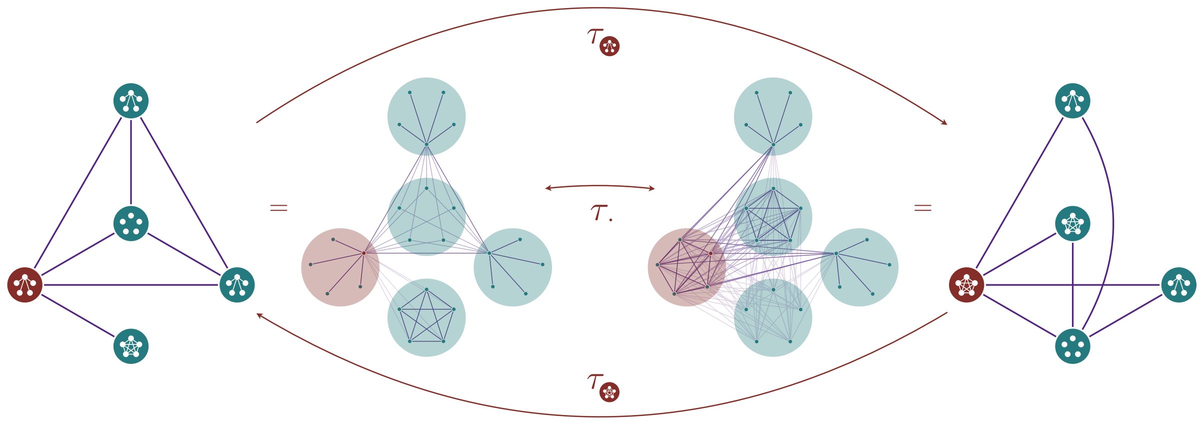


Figure 7.3: Lifted local complementation operations on the foliage representation a graph. The two middle graphs are related via local complementation with respect to the node highlighted in dark brown, while the two outer graphs are the foliage representations of the two inner ones and are related via lifted local complementation with respect to the node (set) highlighted in light brown.

when given a graph G and its foliage representation $\hat{G}$, we know that $\widehat{\tau_a(G)} = \hat{\tau}_a(\hat{G})$. Figure 7.3 shows a corresponding example.

Together with Corollary 7.3, we obtain the necessary and sufficient condition for LC-equivalence in terms of the foliage representation.

Corollary 7.6 *Consider two graphs G_1 and G_2 on the same sets of vertices V with the same foliage partition. The graphs G_1 and G_2 are LC-equivalent if and only if the corresponding foliage representations $\hat{G}_1$ and $\hat{G}_2$ are lifted LC-equivalent.*

7.5 An algorithm to find the foliage partition

Here, we give an algorithm to find the foliage partition of a given graph that runs in $\mathcal{O}(n^3)$ in the number of graph vertices n.

Theorem 7.7 (An algorithm to find foliage partition) *There is an algorithm to find a foliage partition of a given graph that runs in $\mathcal{O}(n^3)$ time in the number of vertices n in the graph.*

Proof. We start by considering a graph $G = (V, E)$ represented by its adjacency matrix $\Gamma_G := (a_{vw})_{v,w \in V}$ and denote by Γ_v the v-row of the Γ_G matrix. In each step, the algorithm returns a subset V_i of a foliage partition which contains a chosen vertex $v \in V$ of the graph, *i.e.* $v \in V_i$. We store this information and delete subset V_i from the graph. We continue this procedure for a graph with deleted subset V_i unless the graph is empty.

Choose a vertex $v \in V$. Firstly, check if is a leaf. Note that v is a leaf if and only if Γ_v contains only one non-zero element. If such a unique non-zero element is in position w, then w is the corresponding axil. Then Γ_w contains the information of all other leaves connected to w. The set of those leaves together with w constitutes a subset V_i in the foliage partition. The complexity cost is $\mathcal{O}(n^2)$, since for each of the neighbors of w we need to check if they are leafs.

Secondly, if v is not a leaf, check if it is an axil. This can be done by choosing any neighbor of v and checking if it is a leaf. If this is the case, v together with all its neighbors (read Γ_v) constitutes a subset V_i in the foliage partition. The complexity cost is $\mathcal{O}(n^2)$ again.

Finally, if v is neither a leaf nor an axil, we will determine all twins sharing the same neighborhood with v. Choose any other vertex $w \in V$ and decide if v and w share the same neighborhood. For instance, compare Γ_v against Γ_w, both agree on all positions except v and w if and only if they share the same neighborhood. Repeat this for every vertex $w \in V$ in the graph and store all vertices sharing the same neighbors as v. Those vertices together with v constitute a subset V_i in the foliage partition. The complexity cost is $\mathcal{O}(n^2)$.

As the computational complexity in each step is at most $\mathcal{O}(n^2)$, and we will repeat this procedure at most n times, the combined computational complexity is $\mathcal{O}(n^3)$. □

7.6 Qudit foliage partitions

Before we are able to define foliage partitions for qudit graph states, we must first define weighted graphs.

Qudit graph states

Weighted graphs are a natural generalization of graphs, where edges are equipped with additional weights, here taken from a finite group $\mathbb{Z}_d$.

Definition 7.8 (d-weighted graph) *A d-weighted graph (G, ω) is a graph $G = (V, E)$ with weights $\omega_{vw} \in \mathbb{Z}_d$ on its edges $vw \in E$. By convention, $vw \notin E$ if and only if the corresponding weight vanishes $\omega_{vw} = 0$. (G, ω) is fully characterized by its adjacency matrix $\Gamma_G := (\omega_{vw})_{v,w \in V}$.*

Definition 7.9 (Qudit graph state) *For any d-weighted graph (G, ω) we can then associate a qudit graph state*

$$|\psi_G\rangle := \prod_{(v,w)\in E} \left(\boldsymbol{CZ}_{\{vw\}}\right)^{\omega_{vw}} |+\rangle^{\otimes V} \in \mathbb{C}_d^{\otimes|V|}, \tag{7.4}$$

where $\boldsymbol{CZ}^{\{vw\}} := \omega_d^{ij} |ij\rangle_{vw}\langle ij|$ is a controlled-Z operator acting on qubits v, w, $|+\rangle := \frac{1}{\sqrt{d}}(|0\rangle + \cdots + |d-1\rangle)$, and ω_d is a root of unity of order d.

The weighted graphs corresponding to qudit graph states can be locally complemented too.

Qudit local complementation

Our generalization of local complementation for d-weighted graphs is taken from Reference [BB07]. Contrary to the qubit case, we have two distinct operations $\circ_b v$ and $*_a w$ acting on the adjacent edges and of the

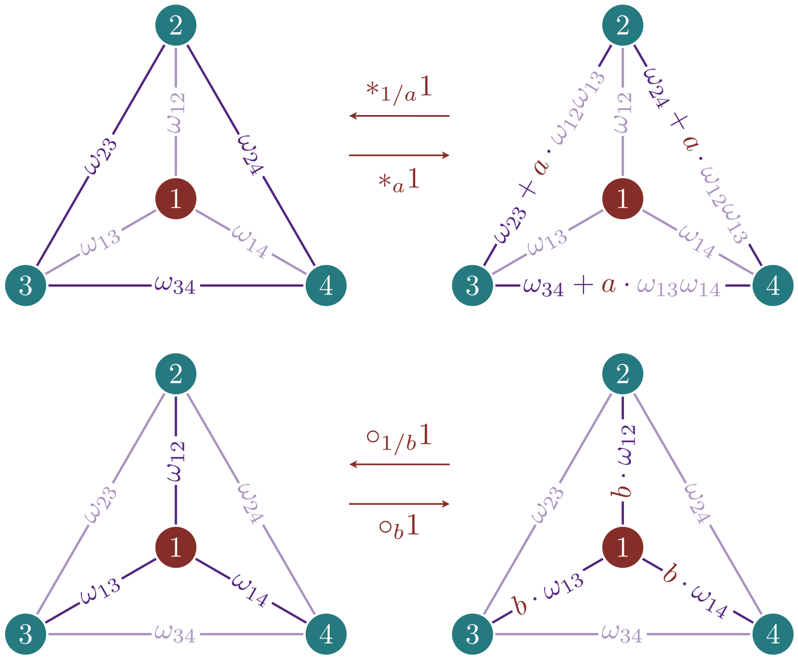


Figure 7.4: The two local complementation operations $*_a w$ and $\circ_b v$ for d-weighted graphs.

complete graph of the neighborhood, respectively. The operations $*_a w$ and $\circ_b v$ are visualized in Figure 7.4.

Definition 7.10 ($*_a w$, $\circ_b v$) *For d-weighted graphs (G, ω) on a vertex set V, we define their adjacency matrices Γ_G as the zero diagonal, symmetric matrices over $\mathbb{Z}_d$ with elements $(\Gamma_G)_{ij} := \omega_{ij}$. For every vertex w, and $a \in \mathbb{Z}_d$ define the operator $*_a w$ on the graph as follows; $G *_a w$ is the graph on V, with adjacency matrix Γ'_G, where*

$$(\Gamma_G)'_{jk} = (\Gamma_G)_{jk} + a(\Gamma_G)_{vj}(\Gamma_G)_{vk} \tag{7.5}$$

for $j \neq k$, and $(\Gamma_G)'_{jj} = 0$ for all j. Further, for every vertex v, and $0 \neq b \in \mathbb{Z}_d$, we define the operator $\circ_b v$ on the graph as follows; $G \circ_b v$ is the graph with adjacency matrix $I(v,b)\Gamma_G I(b,a)$, where $I(v,b) =$ diag$(1,\dots,1,b,1,\dots,1)$, b being on the v-th entry.

For d-weighted graphs we can again define a foliage partition.

Qudit foliage relation

Definition 7.11 (Weighted foliage relation) *Let (G, ω) be a d-weighted graph and its adjacency matrix be $\Gamma_G = (\omega_{vw})_{v,w \in V}$, $\omega_{vw} \in \mathbb{Z}_d$. We define a binary relation on relation $\sim$ on the set of vertices V. Two vertices v, w are related $v \sim w$ if and only if they are in the same connected component and for any other pair of vertices $u_1, u_2 \neq v, w$ it holds that*

$$\omega_{v,u_1} \cdot \omega_{w,u_2} = \omega_{v,u_2} \cdot \omega_{w,u_1}. \tag{7.6}$$

Note that Lemma 7.4 is the special case $d = 2$ of Lemma 7.8. Hence it is enough to prove the latter one.

Lemma 7.8 (Qudit foliage partition) *The relation defined in Definition 7.11 is an equivalence relation and therefore provides a set partition $V_1, \ldots, V_k \vdash V$. We call it the foliage partition of the d-weighted graph (G, ω).*

Denote by $\Gamma_G = (\omega_{vw})_{v,w \in V}$, $\omega_{vw} \in \mathbb{Z}_d$ an adjacency matrix of a d-weighted graph (G, ω), with G being a simple graph $G = (V, E)$.

Proof. Without loss of generality, we can assume that the graph G is connected. Indeed, for disconnected graphs, vertices from different connected component are never related, hence the relation splits into relations on the separate connected components.

It is straightforward to see that the relation $\sim$ is reflexive and symmetric. We will see that it is also transitive, *i.e.*, $v \sim w,\ w \sim z \Rightarrow v \sim z$. Suppose that the following conditions holds

$$\forall_{x,y \neq v,w} \quad \omega_{vx} \cdot \omega_{wy} = \omega_{vy} \cdot \omega_{wx}, \tag{7.7}$$

$$\forall_{x,y \neq w,z} \quad \omega_{wx} \cdot \omega_{zy} = \omega_{wy} \cdot \omega_{zx}; \tag{7.8}$$

we will show that

$$\forall_{u_1,u_2 \neq v,z} \quad \omega_{vu_1} \cdot \omega_{zu_2} = \omega_{vu_2} \cdot \omega_{zu_1}. \tag{7.9}$$

Choose any $u_1, u_2 \neq v, z$. We will consider two cases, either $u_1, u_2 \neq w$ or $u_1 = w$ (or by similarity $u_2 = w$).

Case 1 ($u_1, u_2 \neq w$). We will show that Equation 7.9 holds. Consider two possibilities, either both sides of this equation vanish and it is trivially satisfied, or one of the sides is non-vanishing. Without loss of generality, suppose $\omega_{vu_1} \cdot \omega_{zu_2} \neq 0$. Therefore $\omega_{vu_1} \neq 0 \wedge \omega_{zu_2} \neq 0$.

We will see, that $\omega_{wu_1} \neq 0 \wedge \omega_{wu_2} \neq 0$. Indeed, suppose on the contrary that $\omega_{wu_1} = 0$. By Equation 7.7 with $x = u_1, y = u_2$, we have $\omega_{wu_2} = 0$ since $\omega_{vu_1} \neq 0$. Further, taking Equation 7.7 with $x = u_1, y = z$, we have $\omega_{wz} = 0$ also since $\omega_{vu_1} \neq 0$. Finally, by Equation 7.8 with $x = v, y = u_2$, we have $\omega_{wv} = 0$ since $\omega_{zu_2} \neq 0$. Therefore vertex w is not connected to any of v, z, u_1, u_2. However, since the graph is connected, there exists another vertex u_3, such that $\omega_{wu_3} \neq 0$. Observe that this contradicts Equation 7.8 with $x = u_2, y = u_3$, since $\omega_{wu_3} \neq 0$ and $\omega_{zu_2} \neq 0$ on the right hand side, whereas $\omega_{wu_2} = 0$ on the left hand side. An analogous argument applies when assuming $\omega_{wu_2} = 0$ instead of $\omega_{wu_1} = 0$.

As we have shown, if $\omega_{vu_1} \cdot \omega_{zu_2} \neq 0$, then $\omega_{wu_1} \neq 0$ and $\omega_{wu_2} \neq 0$. Taking Equation 7.7 and Equation 7.8 with $x = u_1, y = u_2$, we have $\omega_{vu_1} \cdot \omega_{wu_2} = \omega_{vu_2} \cdot \omega_{wu_1}$ and $\omega_{wu_1} \cdot \omega_{zu_2} = \omega_{wu_2} \cdot \omega_{zu_1}$, after multiplying by sides, we get

$$\omega_{vu_1} \cdot \omega_{wu_2} \cdot \omega_{wu_1} \cdot \omega_{zu_2} = \omega_{vu_2} \cdot \omega_{wu_1} \cdot \omega_{wu_2} \cdot \omega_{zu_1}.$$

Note that ω_{wu_1} and ω_{wu_2} appear on both sides of the equation above, and as we have shown both are non-zero. Therefore, we conclude that $\omega_{vu_1} \cdot \omega_{zu_2} = \omega_{vu_2} \cdot \omega_{zu_1}$, which concludes the proof in Case 1.

(Case 2, $u_1 = w$). We will show that Equation 7.9 holds, that is, $\omega_{vw} \cdot \omega_{zu_2} = \omega_{vu_2} \cdot \omega_{zw}$.

By substituting $x = z$, $y = u_2$ in Equation 7.7 and $x = v$, $y = u_2$ in Equation 7.8, we have $\omega_{vz} \cdot \omega_{wu_2} = \omega_{vu_2} \cdot \omega_{wz}$, and $\omega_{wv} \cdot \omega_{zu_2} = \omega_{wu_2} \cdot \omega_{zv}$ and thus $\omega_{wv} \cdot \omega_{zu_2} = \omega_{vu_2} \cdot \omega_{wz}$, which completes the proof of Case 2 since the weights $\omega_{ab} = \omega_{ba}$ are symmetric.

The equivalence classes with respect to the equivalence relation imply a partition for any d-weighted graph (G, ω). □

Surprisingly, the qudit foliage partition is invariant under both local complementation operations $*_a w$ and $\circ_b v$ for d-weighted graphs.

Theorem 7.9 *The foliage partition of a d-weighted graph (G, ω) remains invariant under any local complementation operations $*_a w$ and $\circ_b v$.*

Proof. Without loss of generality, we can assume that all graphs are connected. Note that property of being a connected graph is invariant under LC-transformations. Indeed, suppose that the graph has two connected components C_1 and C_2. Applying any LC-transformation on C_1 component (C_2 equivalently) does not create any connection between C_1 and C_2. Therefore LC-transformations cannot decrease the number of connected components. Since they are invertible, they cannot increase this number either.

Suppose that two vertices v, w belong to the same subset in a foliage partition. It means that for any other pair of vertices $u_1, u_2 \neq v, w$ the following holds $\omega_{vu_1} \cdot \omega_{wu_2} = \omega_{vu_2} \cdot \omega_{wu_1}$. We will see that this is preserved under any LC transformation. We consider two types of operations: $\circ_a$ and $*_a$ acting on all possible vertices (see Definition 7.10). Without loss of generality, we can consider operations acting on v, u_1 and any other vertex $z \neq v, w, u_1, u_2$.

For clarity of presentation, we denote by $\omega_{x,y}$ the weights of an initial graph, and by $\omega'_{x,y}$ the weights of the transformed graph. We will show

$$\omega'_{vu_1} \cdot \omega'_{wu_2} = \omega'_{vu_2} \cdot \omega'_{wu_1} \tag{7.10}$$

assuming

$$\omega_{vx} \cdot \omega_{wy} = \omega_{vy} \cdot \omega_{wx} \tag{7.11}$$

for all of the following $x, y \neq v, w$ six distinct cases.

Case 1 ($\circ_a v$). Note that in this case $\omega'_{vu_1} = a\omega_{vu_1}$, $\omega'_{wu_2} = \omega_{wu_2}$, $\omega'_{vu_2} = a\omega_{vu_2}$, and $\omega'_{wu_1} = \omega_{wu_1}$. Hence Equation 7.10 is trivially satisfied by Equation 7.11 with $x = u_1$ and $y = u_2$ for any $a \neq 0$.

Case 2 ($\circ_a u_1$) and Case 3 ($\circ_a z$), are analogous to Case 1.

Case 4 ($*_a v$). Note that in this case the following weights remain unchanged: $\omega'_{vu_1} = \omega_{vu_1}$, and $\omega'_{vu_2} = \omega_{vu_2}$, while two other weights changed in the following way: $\omega'_{wu_2} = \omega_{wu_2} + a\omega_{vu_2}\omega_{wv}$, and $\omega'_{wu_1} = \omega_{wu_1} + a\omega_{vu_1}\omega_{wv}$. Hence the left-hand side of Equation 7.10 equals $\omega_{vu_1}\omega_{wu_2} + a\omega_{vu_2}\omega_{wv}\omega_{vu_1}$, while the right-hand side equals $\omega_{vu_2}\omega_{wu_1} + a\omega_{vu_1}\omega_{wv}\omega_{vu_2}$. Note that in both expressions there is the same term $a\omega_{vu_2}\omega_{wv}\omega_{vu_1}$, furthermore $\omega_{vu_1}\omega_{wu_2} = \omega_{vu_2}\omega_{wu_1}$ by Equation 7.11 with $x = u_1, y = u_2$. This concludes the proof in this case.

Case 5 ($*_a u_1$) is analogous to the previously considered Case 4.

Case 6 ($*_a z$). In this case weights change in the following way: $\omega'_{vu_1} = \omega_{vu_1} + a\omega_{vz}\omega_{zu_1}$, $\omega'_{vu_2} = \omega_{vu_2} + a\omega_{vz}\omega_{zu_2}$, $\omega'_{wu_2} = \omega_{wu_2} + a\omega_{wz}\omega_{zu_2}$, and $\omega'_{wu_1} = \omega_{wu_1} + a\omega_{wz}\omega_{zu_1}$. Therefore the left-hand side and the right-hand side of Equation 7.10 are of the following form

$$\begin{aligned} L &= \omega_{vu_1}\omega_{wu_2} + a\Big(\omega_{vz}\omega_{zu_1}\omega_{wu_2} + \omega_{wz}\omega_{zu_2}\omega_{vu_1}\Big) \\ &\quad + a^2\omega_{vz}\omega_{zu_1}\omega_{wz}\omega_{zu_2} \\ R &= \omega_{vu_2}\omega_{wu_1} + a\Big(\omega_{vz}\omega_{zu_2}\omega_{wu_1} + \omega_{wz}\omega_{zu_1}\omega_{vu_2}\Big) \\ &\quad + a^2\omega_{vz}\omega_{zu_2}\omega_{wz}\omega_{zu_1}, \end{aligned}$$

respectively. Note that $\omega_{vu_1}\omega_{wu_2} = \omega_{vu_2}\omega_{wu_1}$, hence the first terms in both expressions are equal. Furthermore terms with the a^2 prefactors are trivially equal. Finally, applying Equation 7.11 with $x = z$, $y = u_2$ in the first term, and with $x = z$, $y = u_1$ in the second term, we have $\omega_{vz}\omega_{zu_1}\omega_{wu_2} + \omega_{wz}\omega_{zu_2}\omega_{vu_1} = \omega_{vu_2}\omega_{zu_1}\omega_{wz} + \omega_{wu_1}\omega_{zu_2}\omega_{vz}$, which shows that $L = R$ and concludes the proof. □

Since the $d = 2$ special case of Theorem 7.9 is exactly Theorem 7.2, the above proof is at the same time an alternative proof of Theorem 7.2.

After this excursion to qudit graph states, we now return back to simple qubit graph states. We will restrict ourselves even further by studying the interesting subclass of circle graph states.

Circle graph formalism 8

8.1 Circle graph states

Some graphs have a so-called *circle graph* structure that makes the description of the corresponding graph states (see Definition 4.4) and their local complementation orbits (see Definition 4.8) remarkably elegant.

Two examples of this class are line graphs describing linear cluster states –of which we already encountered the four-qubit example in Figure 4.9– and complete graphs describing GHZ states (see Definition 4.6). In the following paragraphs, we denote line graphs on the vertex set $V_L := \{1, 2, \ldots, n\}$ as $L_n := (V_L, E_L)$ with edges $E_L := \{(1, 2), (2, 3), \ldots, (n - 1, n)\}$ and complete graphs as $K_n := (V_K := V_L, E_K)$ with edges $E_K := \{(v, w) \mid (v, w \in V_K) \wedge (v \neq w)\}$.

In fact, the butterfly network (*cf.* Figures 5.2a or 5.1a) is also a circle graph, while the two-dimensional nine-qubit cluster state (*cf.* Figure 5.3a) is not.

Before formally defining circle graphs, we introduce the notion of a *double-occurrence word*. Double-occurrence words facilitate our description of the transformation of circle graphs under local complementation by equivalence classes of such words.

Definition 8.1 (Double-occurrence word) *A double-occurrence word $\mathcal{W}$ is a sequence of labels from a set W in which every label appears twice.*[a] *For a subset of labels $V \subset W$, we define $\mathcal{W}[V]$ to be the shorter double-occurrence word obtained by removing the labels in $W \setminus V$ from $\mathcal{W}$ while preserving the order of labels.*[b]

[a] The sets of (mirrored) cyclic permutations of double-occurrence words form equivalence classes.

[b] Examples can be found in the caption of Figure 8.5.

Equivalence classes of double-occurrence words describe circle graphs via intersection graphs of finite numbers of chords inscribed in a circle. Both line graphs and complete graphs can be described as double-occurrence words and are therefore circle graphs as shown in Figure 8.1.

Definition 8.2 (Circle graph) *A graph G is a circle graph if it is isomorphic to the intersection graph of a finite number of chords of a circle. Naming the cords and labeling both endpoints of the cords accordingly, every circle graph is described by a double-occurrence word $\mathcal{W}(G)$ and its (mirrored) cyclic permutations.*

We can describe local complementations (see Definition 4.7) with respect to vertices of circle graphs by the following simple transformations of the corresponding double-occurrence words.

For a circle graph G induced by a given double-occurrence word $AvBvC$ with subwords $A := a_1a_2 \ldots a_{|A|}$, $B := b_1b_2 \ldots b_{|B|}$ and $C := c_1c_2 \ldots c_{|C|}$, the locally complemented graph $\tau_v(G)$ is exactly the graph induced by $Av\bar{B}vC$, where $\bar{B}$ is the reversed subword $\bar{B} := b_{|B|}b_{|B|-1} \ldots b_1$.

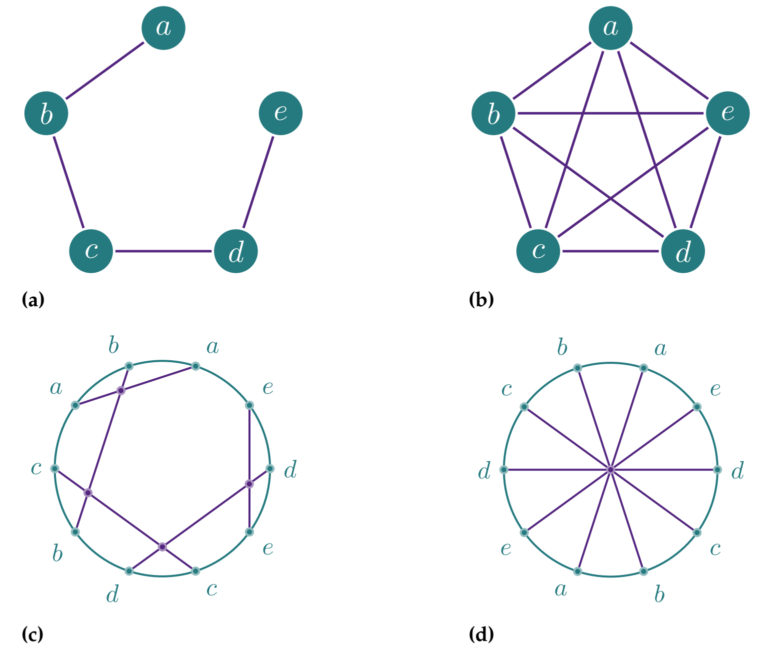


Figure 8.1: Line graphs and complete graphs are circle graphs. The line graph L_5 **(a)** can be described by the double-occurrence word $\mathcal{W}(L_5) = abacbdcede$ and the complete graph K_5 **(b)** by $\mathcal{W}(K_5) = abcdeabcde$ or by their (mirrored) cyclic permutations. A chord diagram of $\mathcal{W}(L_5)$ is shown in **(c)** and one of $\mathcal{W}(K_5)$ is shown in **(d)**. Double-occurrence words W describing circle graphs with n nodes have a length of $|W| = 2n$ and can be read of (anti-) clockwise from their chord diagram.

Examples of local complementations with respect to vertices of the graphs from Figure 8.1 are shown in Figure 8.2.

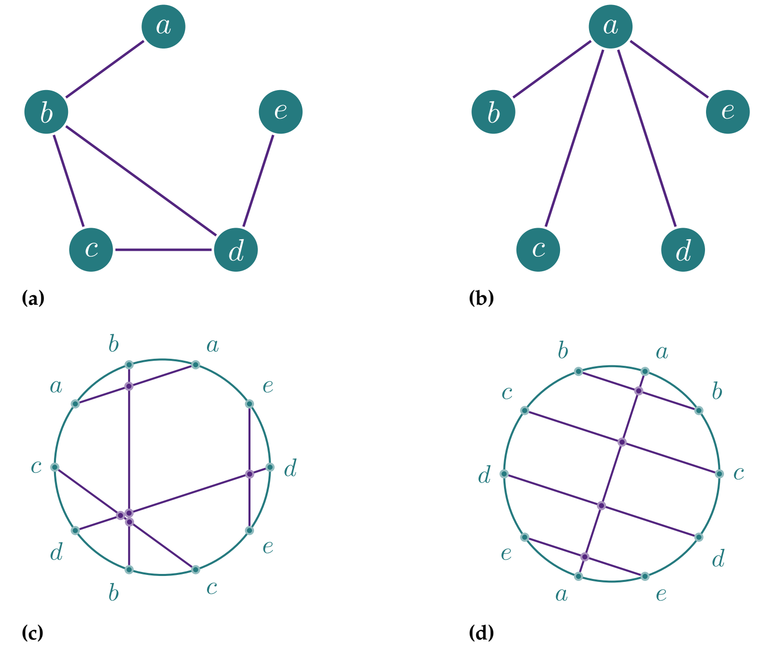


Figure 8.2: Line graphs and complete graphs remain circle graphs after local complementations. A local complementation with respect to the central vertex c of the line graph L_5 yields the graph $\tau_c(L_5)$ shown in **(a)**. The corresponding double-occurrence word $\mathcal{W}(L_5) = abacbdcede$ is simply transformed by reversing the subword bd between the two occurrences of c, so that $\mathcal{W}(\tau_c(L_5)) = abacdbcede$. A chord diagram of $\tau_c(L_5)$ is shown in **(c)**. Note that the chords b and d did not intersect before the local complementation, but only after. A local complementation with respect to an arbitrary vertex a of the complete graph K_5 yields the graph $\tau_a(K_5)$ shown in **(b)**. The corresponding double-occurrence word $\mathcal{W}(K_5) = abcdeabcde$ is again transformed by reversing the subword $bcde$ between the two occurrences of a, so that $\mathcal{W}(\tau_a(K_5)) = abcdeaedcb$. A chord diagram of $\tau_a(K_5)$ is shown in **(d)**. Note that the chords b, c, d and e did intersect before the local complementation, but not after.

Notably, this implies that the local complementation orbits (see Definition 4.8) of circle graphs can be represented as so-called *4-regular multigraphs* in a canonical way. For this canonical construction, we introduce the notion of an *Eulerian tour* on a multigraph.

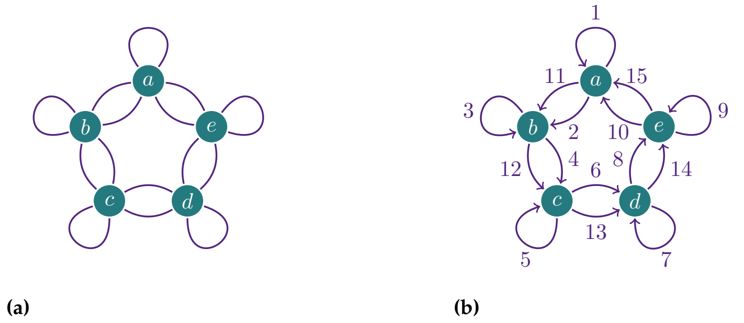


Figure 8.3: Example of a multigraph **(a)** and of an Eulerian tour **(b)** on it. This multigraph is 6-regular since each vertex has degree six. The vertex set of the multigraph is given by $\{a, b, c, d, e\}$, while its edge multiset is defined as

$$\{(a, a), (b, b), (c, c), (d, d), (e, e), \\ (a, b), (a, b), (b, c), (b, c), (c, d), \\ (c, d), (d, e), (d, e), (e, a), (e, a)\}.$$

In **(b)**, a possible Eulerian tour on the multigraph $\mathscr{E} = a(a, b)b(b, b)b \dots (e, a)a$ is visualized as $a(a, b)b = a \longrightarrow b$.

8.2 Eulerian tours

Eulerian tours take their name from the famous Swiss mathematician Leonhard Euler. Originally, the problem of the "Seven Bridges of Königsberg" was solved by him in 1736 [Eul36] (article in Latin). The problem is considered the founding problem of graph theory. In the city of Königsberg (now Kaliningrad) at that time, seven bridges crossed the Pregel River dividing the city. The bridges allowed people to reach two large islands, to cross between the islands, and to cross to the other side of the city via the islands.

The question, which Euler answered in the negative, was whether it was possible to take a walk and cross each of the seven bridges exactly once. Euler's solution was easily generalizable: each piece of land can be considered as a node of a graph, while the bridges can be considered its edges. An Eulerian tour on such a graph would mean walking along the edges and vertices, crossing each edge exactly once.

Since traversing a vertex by entering via one edge and exiting through another requires that the traversed vertex be connected to two other vertices, an Eulerian tour starting and ending at the same vertex is only possible on graphs with even degree for every vertex. Note that if the tour is allowed to start and end at different vertices, these two vertices can be of odd degree.

Definition 8.3 (Multigraph) *A multigraph $F = (V_F, E_F)$ is a graph that allows for multiple edges between the same pair of vertices and for loops –i.e. for edges between a vertex and itself. The set of edges E_F is a multiset.*

An example of a multigraph is shown in Figure 8.3a and an Eulerian tour on it is shown in Figure 8.3b.

Definition 8.4 (Eulerian tour) *An Eulerian tour on a multigraph $F = (V_F, E_F)$ is an alternating sequence $\mathscr{E} := v_1 e_1 v_2 e_2 \dots e_i v_{i+1}$ of vertices $v_k \in V_F$ and edges $e_k = (v_k, v_{k+1}) \in E_F$ such that all edges appear exactly once and the tour ends where it started, i.e. $v_1 = v_{i+1}$.*[a]

[a] The sets of reversed and/or cyclicy permutated Eulerian tours are equivalence classes.

The equivalence classes of Eulerian tours on 4-regular multigraphs – multigraphs where every vertex has degree four– have a simple one to one correspondence to those of double-occurrence words. Every

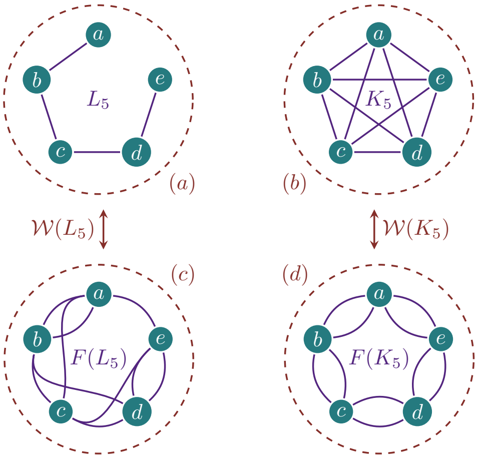


Figure 8.4: Local complementation orbits as 4-regular multigraphs. The double-occurrence word of the line graph $\mathscr{W}(L_5) = abacbdcede$ and that of the complete graph $\mathscr{W}(K_5) = abcdeabcde$ give rise to 4-regular multigraph representations of the local complementation orbits of the linear cluster and GHZ state with five quits.

double-occurrence word $\mathscr{W}(G)$ can be seen as an Eulerian tour $\mathscr{E}(G)$ on a connected 4-regular multigraph.

Such a 4-regular multigraph can be constructed from a double-occurrence word by taking its letters as the vertex set and drawing an edge between adjacent letters in the double occurrence word as well as between the first and the last letter; Figure 8.4 visualizes this for L_5 and K_5. The double-occurrence word is in turn representing an Eulerian tour on this graph, since it is describing a tour along the graph's edges such that every edge is visited exactly once.

As local complementations on a circle graph simply reverse the order of subwords in the underlying double-occurrence word, reversals of the corresponding subtours will give new Eulerian tours on the same multigraph: It is indeed true that circle graphs are local complementation equivalent if and only if they can be seen as Eulerian tours on the same 4-regular multigraph [Bou88].

8.3 Vertex minors of circle graphs

Vertex minor relations (see Definition 5.3) for circle graphs can also be described in this framework. Lemma 8.1 uses the above representation of local complementation orbits as 4-regular multigraphs: Every circle graph G defines a 4-regular multigraph F induced by the double-occurrence word $\mathscr{W}(G)$ that describes an Eulerian tour $\mathscr{E}(G)$ on F.

Lemma 8.1 ([DHW20b]) *Let F be the 4-regular multigraph defined by a circle graph G. A circle graph H is a vertex minor of G if and only if there exists an Eulerian tour $\mathscr{E}'(G)$ on F such that H is given by deleting the vertices $V_G \setminus V_H$ from the corresponding double-occurrence word $\mathscr{W}'(G)$, i.e. $\mathscr{W}(H) = \mathscr{W}'(G)[V_H]$.*

For a proof of the lemma, we refer the reader to Reference [DHW20b].

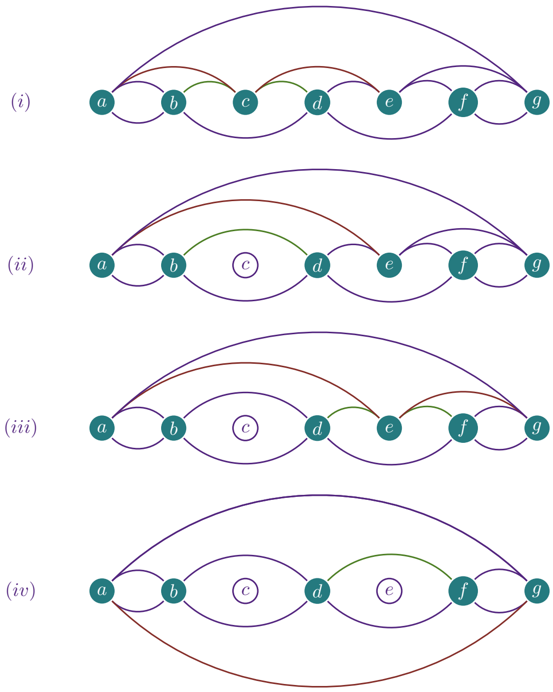


Figure 8.5: The 4-regular multigraph corresponding to the seven vertex line graph (i) has an Eulearian tour given by the double-occurrence word

$$a\,b\,d\,f\,g\,a\,b\,c\,d\,e\,f\,g\,e\,c.$$

Deleting the letters c and e in the steps $(i) \rightarrow (ii)$ and $(iii) \rightarrow (iv)$ yields the double-occurrence words

$$a\,b\,d\,f\,g\,a\,b\,\cancel{c}\,d\,e\,f\,g\,e\,\cancel{c}$$

$$a\,b\,d\,f\,g\,a\,b\,\cancel{c}\,d\,e\,f\,g\,e\,\cancel{c}$$

and

$$a\,b\,d\,f\,g\,a\,b\,\cancel{c}\,d\,\cancel{e}\,f\,g\,\cancel{e}\,\cancel{c}$$

respectively. As the latter is also describing an Eulerian tour on the 4-regular multigraph corresponding to the complete graph on five vertices, $H = K_5$ is a vertex minor of $G = L_7$ according to Lemma 8.1 with $V_G \setminus V_H = \{c, e\}$.

8.4 Transforming linear cluster to GHZ states

With Lemma 8.1, it is easy to see that a linear cluster state of size $2k+1$ can be transformed into a GHZ state of size $k+2$ by local Clifford operations, local Pauli measurements and classical communication. The case $k = 3$ is visualized in Figure 8.5.

The transformation shown in Figure 8.5 explains which GHZ extraction patterns are allowed when aiming to transform a linear cluster state into a GHZ state. The special structure of the 4-regular multigraph at the ending vertices of the linear cluster state allows for two vertices to be part of the final GHZ state, whereas for the interior nodes only every second can be part of the final GHZ state.

A similar figure as Figure 8.5 for linear cluster states of size $2k$ would show that they can be transformed into GHZ states of size $k+1$. Both results taken together imply that a linear cluster state on n qubits can be transformed into a GHZ state of size $\lfloor (n+3)/2 \rfloor$.

We can even show that $\lfloor (n+3)/2 \rfloor$ is the size of the largest possible GHZ state that $|L_n\rangle$ can be transformed into. To prove this by contradiction using the notion of the *Pauli persistency* of graph states.

Definition 8.5 (Pauli persistency [BR01]) *The minimal number of local Pauli measurements to disentangle a graph state its Pauli persistency.*

Definition 8.6 (Vertex cover) *A vertex cover of a graph $G = (V, E)$ is a subset of vertices $V_{cover} \subset V$ such that every edge $(v, w) \in E$ has at least one endpoint in V_{cover}. That is $(v, w) \in E \Leftrightarrow v \in V_{cover} \vee w \in V_{cover}$.*

In Reference [HEB04] it is shown that any vertex cover of a graph gives an upper bound $|V_{\text{cover}}|$ to the Pauli persistency of the corresponding graph state. This allows us to calculate the Pauli persistency for both linear cluster and GHZ states.

Lemma 8.2 (Pauli persistency of GHZ states) *The Pauli persistency of GHZ states of arbitrary size is* 1.

Lemma 8.3 (Pauli persistency of linear states) *The Pauli persistency of linear cluster states states with n qubits is* $\lfloor n/2 \rfloor$.

Proof. While finding a minimal vertex cover is known to be NP-hard, it is straightforward for K_n and L_n.

For star graphs and complete graphs K_n representing GHZ states, a minimal vertex cover is obviously given by the central vertex of the star or any vertex of the complete graph.

For linear graphs L_n, a minimal vertex cover is given by $V_{\text{cover}} = \{2, 4, \dots, n\}$ for even n and by $V_{\text{cover}} = \{2, 4, \dots, n-1\}$ for odd n. In the first case we have $|V_{\text{cover}}| = n/2 = \lfloor n/2 \rfloor$ and in the second case $V_{\text{cover}} = \lfloor n/2 \rfloor$. □

We can now use the above lemmas to prove the upper bound on the size of the GHZ states into which linear cluster states can be transformed.

A slightly lower value for the upper bound of was mentioned without proof in Reference [BR01]. The authors claimed that one can extract GHZ states of size $n/2$ –which is true but not optimal.

Theorem 8.4 (Transforming $|L\rangle$ into $|K\rangle$) *The size of a GHZ state that a linear cluster state on n qubits can be transformed into with local Clifford operations, local Pauli measurements and classical communication is upper bounded by* $\lfloor (n+3)/2 \rfloor$.

Proof. Assume that it would be possible to transform $|L_n\rangle$ into a GHZ state of size larger than $\lfloor (n+3)/2 \rfloor$, *i.e.* that it is possible to transform it into an $(\lfloor (n+3)/2 \rfloor + 1)$-partite GHZ state. Then, since the two equalities

$$\lfloor (n+3)/2 \rfloor + 1 = \lfloor (n+1)/2 \rfloor + 2 \tag{8.1}$$

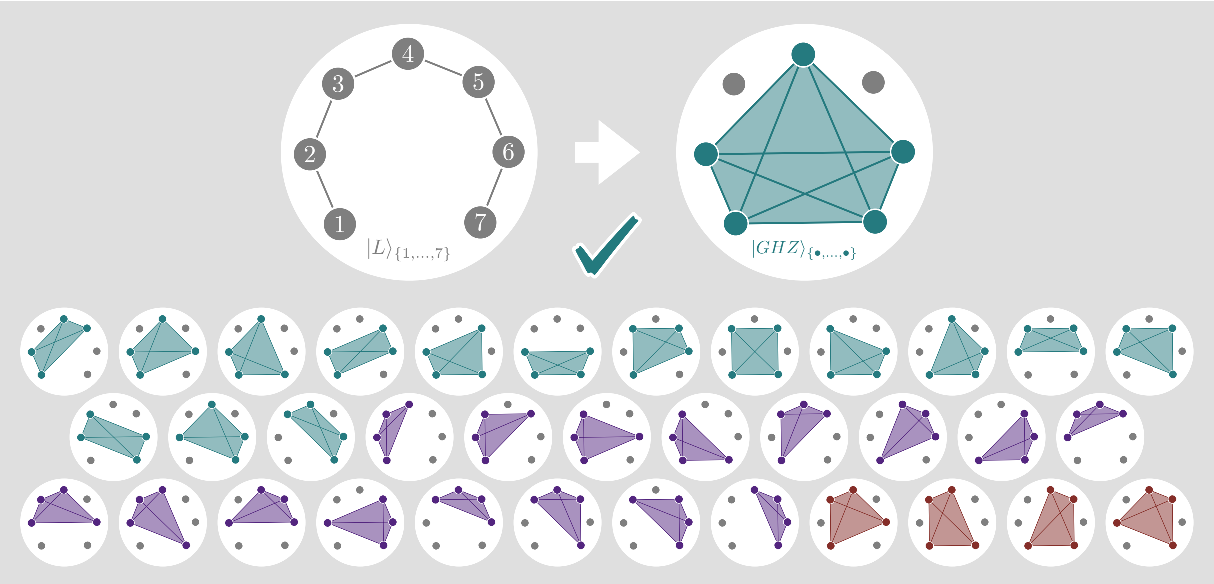
$$n = (\lfloor (n+1)/2 \rfloor + 2) + (\lceil (n+1)/2 \rceil - 2) - 1 \tag{8.2}$$

hold, we know that at least $\lceil (n+1)/2 \rceil - 3$ qubits of the linear cluster state $|L_n\rangle$ were Pauli measured.

Since GHZ states have Pauli persistency 1, just one additional Pauli measurement can disentangle the $(\lfloor (n+3)/2 \rfloor + 1)$-partite GHZ state. But that means that

$$\lceil (n+1)/2 \rceil - 3 + 1 = \lceil (n+1)/2 \rceil - 2$$

Pauli measurements disentangled a linear cluster state of size n. This is a contradiction to linear cluster states having Pauli persistency $\lfloor n/2 \rfloor$ since $\lceil (n+1)/2 \rceil - 2 < \lfloor n/2 \rfloor$. □



4
3
5
2
6
1
7
$|L\rangle_{\{1,\ldots,7\}}$
$|GHZ\rangle_{\{\bullet,\ldots,\bullet\}}$

Figure 8.6: Example of extracting GHZ states from a linear cluster state with seven qubits: The only 5-partite GHZ state that this resource can be transformed into is on the qubits corresponding to $1, 2, 4, 6, 7$ and is highlighted in green. For 4-partite GHZ states, we also highlight all 15 possible extraction patterns in green, while the patterns in brown are impossible due to Lemma 8.5 and the patterns shown in violet are impossible due to both Corollary 8.6 and Lemma 8.5. Note that due to Theorem 8.4 it is impossible to extract GHZ states with six or more qubits from this resource –it is however trivially possible to extract all combinations of three-partite GHZ states.

8.5 An alternative proof

We provide an alternative proof of the upper bound of Theorem 8.4 in [Jon+22b]. This alternative proof can be succinctly formulated in the stabilizer formalism. Since its formulation offers some additional insight into which transformations are impossible, we will mention the proven statements here for completeness.

To formulate the impossibility results, we introduce some notation: As we have already seen the resource n-partite linear cluster state $|\mathrm{L}\rangle_{V_L}$ corresponds to a line graph on the vertices $V_L := \{1, 2, \ldots, n\}$. This ordered set structure allows us to use the terms *left* and *right* neighbors of i to indicate any vertices h, j with $h < i$.

The following sections closely follow the text of Reference [Jon+22b], which was written by both myself and my co-authors.

Let further $V_K \subset V_L$ be a set of vertices for which we can extract a GHZ state from the linear cluster resource state. Performing Pauli measurements on the qubits corresponding to $V_M := V_L \setminus V_K$, we obtain a postmeasurement state which is local Clifford equivalent to the $|V_K|$-partite GHZ state. By performing local operations based on the measurement outcomes, the state can then be locally transformed into this GHZ state.

This ordered set construction allows for V_K to inherit the neighbor structure from the linear network V_L. The set V_K has boundaries in the order induced by V_L. We refer to sequential neighbors in V_K as *islands*.

Definition 8.7 (Boundaries, k-island) *We refer to the smallest and largest element of V_K as the boundaries of the GHZ state. A k-island is any selection of consecutive vertices $i, i+1, \ldots, i+k \in V_K$.*

Now Lemma 8.5 is an impossibility result for 2-islands. The implications of Lemma 8.5 for the special case $n = 7$ are shown in Figure 8.6.

> **Lemma 8.5** (Constraints on 2-islands) *No 2-island can have both a left and a right neighbor in V_K. If two vertices $i, i+1$ are in V_K, then there is either no vertex to the left of i or no vertex to the right of $i+1$.*

Lemma 8.5 implies that all vertices i in the extracted GHZ state have to be isolated in the linear cluster state: With the exception of the boundaries, $i \in V_K$ implies that $i-1$ and $i+1$ cannot be in V_K.

A corollary for 3-islands follows directly by choosing two sequential nodes from the 3-island and using Lemma 8.5.

> **Corollary 8.6** *If V_K contains a 3-island, then $|V_K| = 3$.*

The alternative proof of Theorem 8.4, *i.e.* the upper bound $|V_K| \leqslant \lfloor (n+3)/2 \rfloor$, then follows directly.

Proof. As there are at most two 2-islands, for every other i in V_K both neighbors $i \pm 1$ are measured. Thus, to maximize $|V_K|$, we may have $1, 2, n-1, n$ in V_K, and V_M containing every other vertex in between: For n odd, $V_M = \{3, 5, \ldots, n-2\}$; for n even $V_M = \{3, 5, \ldots, n-5, n-3, n-2\}$.

In the even case, $n-2$ must be measured due to Corollary 8.6. In both cases $|V_K| = n - |V_M|$ is upper bounded by $\lfloor (n+3)/2 \rfloor$. □

Note that if n is even, there is more than one such pattern. While we have chosen here to measure the two consecutive vertices, $n-3$ and $n-2$, other possibilities would have been to measure consecutive vertices further to the left and measure only the even vertices to the right. Another possibility would have been to measure not two consecutive vertices, but a qubit of one of the 2-islands, *i.e.* either of 1,2,$n-1$ or n. It is important to note that here all the resulting sets V_M have the same size.

↑ ↑ ↑

The preceding sections closely follow the text of Reference [Jon+22b], which was written by both myself and my co-authors.

8.6 Why GHZ states?

Having thoroughly analyzed how to convert linear cluster states into GHZ states, we should naturally ask ourselves why we would want to obtain GHZ states in the first place.

The answer is simple. We can use GHZ states in a number of quantum communication protocols such as quantum secret sharing [HBB99; WE21], quantum Byzantine agreement [FGM01] and quantum conference key agreement [Mur+20].

Although all of these GHZ-protocols are interesting in their own right, we will here focus only on the latter: quantum conference key agreement. GHZ states not only allow us to generate secret conference encryption keys, but they even allow us to generate these keys anonymously.

Part III
Anonymity in Quantum Communication

Anonymous Quantum Conference Key Agreement 9

9.1 Quantum conference key agreement

As we explored in the previous chapters, an important application of quantum information processing is to provide additional security for communication.

Most commonly, two parties, Alice and Bob, are assumed to want to establish a shared secret key to encrypt their further communication (*cf.* Section 3.3). Since their introduction [BB84a], quantum key distribution (QKD) protocols have been proposed and implemented in a standard fashion, although there are still some practical challenges to be overcome [Dia+16].

Quantum conference key agreement (CKA) explores a more general scenario where multiple parties wish to establish a shared secret key. For a concise review, we refer the interested reader to Reference [Mur+20].

In a generic quantum conference key agreement protocol some number n of *users* or *participants* sharing entangled quantum resources aim to establish a secure conference key by public communication and local operations on their part of the entangled resources. While CKA could be achieved by establishing $n(n-1)$ bipartite QKD keys between n users and distributing a shared key securely encrypted by the bipartite keys, we will here only concern ourselves with protocols utilizing multipartite entanglement to generate the secure secret key directly.

Commonly, one of the participants –referred to as *Alice*– has a distinguished role in the CKA protocol. All other participants that do not occupy the special role of Alice are referred to as *Bobs*. Similar to the steps of the BB84 protocol presented in Figure 3.1 such key generation protocols typically include three steps: The (i) *distribution* of the entangled resource state to the users, some –often randomly chosen– (ii) *measurements* of this resource by the users over multiple rounds, followed by classical (iii) *postprocessing* of the generated measurement outcome data.

The measurement rounds are typically divided further into *key generation* rounds and *verification* rounds. While the former are the ones that are eventually used to obtain the conference key, the latter are just as important for the information theoretic security of the key. The verification rounds allow the participants to detect eavesdropping or any tampering with the entanglement source.

The measurement outcome data postprocessing typically involves three further steps.

First, the so-called *parameter estimation* serves both to detect malicious tempering and to estimate the correlations between the participants. In order to achieve this, they broadcast the outcomes of their verification rounds as well as the outcomes of some randomly selected key generation rounds. While parameter estimation reduces the size of the raw key generated in the key generation rounds, it is vital for both the correctness and the security of the key.

In a second step, an *error correction* or *information reconciliation* protocol is required for the participants to ensure that their raw keys match. The key that Alice generated is defined to be the correct raw key and the error correction protocol ensures that the Bobs modify their keys to match that of Alice. These protocols require the exchange of classical information for coordination.

Finally, *privacy amplification* is the process of turning the partly secure raw keys of all participants into a secure key shared by all participants. For this, Alice randomly chooses a hash function from a two-universal family of hash functions and sends her choice to the Bobs. All participants apply the hash function to the raw key to obtain the final secure conference key.

9.2 Anonymous Conference Key Agreement

In the multi-party setting of quantum conference key agreement, we introduced a new notion of anonymity, where we required that the identities of the parties sharing the secret key are all protected [HJP20].

The following sections closely follow the text of Reference [HJP20], which was written by both myself and my co-authors. ↓ ↓ ↓

Such scenarios are highly relevant for several reasons. One example is the case of whistleblowing; an individual might want to disseminate an encrypted message such that certain parties can decrypt it, while the identities of all parties involved remain secret. For such anonymous whistleblowing, the underlying protocol must involve non-participating parties, so that an authority managing the network cannot find out who is participating in the secret communication.

In Reference [HJP20], we introduced the first multipartite protocol that provides anonymity for both a sender and multiple receivers alike. To achieve this goal, we had to address two different elements: Anonymity and multiparty key generation. By combining both elements, we proposed an anonymous conference key agreement protocol that allows a sender to deliver a private message to specific recipients of her choice, while keeping her identity secret from external parties and even from each other. The protocol is visualized in Figure 9.1.

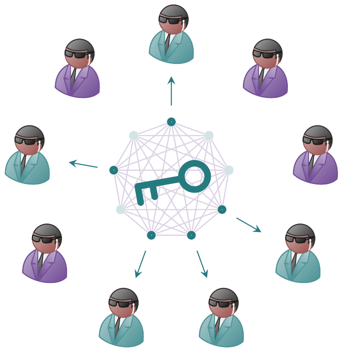


Figure 9.1: Reference [HJP20] introduced the first multipartite protocol that provides anonymity for both a sender and multiple receivers alike, while keeping the sender's identity secret from external parties and even from each other.

Previous work on anonymity

Previous work [CW05] had shown how to achieve anonymous transmission of classical bits using the natural correlations of the GHZ state [GHZ89b] and how to anonymously generate bipartite entanglement from a larger GHZ state. In Reference [Unn+19], the latter was further developed by adding a scheme for anonymously notifying the receiver and verifying the anonymous entanglement generation [Pap+12b; McC+16].

However, since it is impossible to extract multiple bipartite Bell states from a single GHZ state, we needed an alternative approach that allowed us to perform anonymous conference key agreement between a subset of parties in a given network. One approach could have been to use other multipartite entangled quantum states [LOW10b; HPE19; Goy+15] to generate bipartite entanglement between the sender and all receivers separately (see Chapter 5). However, this would have increased the consumption of quantum resources.

In Reference [HJP20], we showed that it is indeed possible to anonymously create the necessary entanglement between sender and receiver simultaneously by using a single GHZ state shared by a source over the network.

Protocol overview

Our anonymous conference key agreement protocol aims to establish a secret key between the sender, whom we call *Alice*, and m receiving parties of her choice. We use both *Bob* and *receiver* to refer to each of these receiving parties, and *participants* to refer to Alice and all Bobs.

The $m + 1 \leqslant n$ participants are part of a larger network of n parties. The m Bobs are notified anonymously by Alice via a notification protocol (*cf.* Section 9.2). A large GHZ state (see Section 4.3 and Figure 9.2) is then shared between all n parties, which can be done either centrally or using a given network infrastructure via quantum repeaters or quantum network coding [Epp+17]. From this n-partite GHZ state, we then show how to anonymously extract an $(m + 1)$-partite GHZ state that is shared only between the participants. The resulting state can then either be verified or used to perform a conference key agreement protocol.

Both the identities of the participants and their shared key are hidden from an attacker *Eve* in our protocols. We assume that Eve either follows the protocol and controls a single node in the network or deviates from the protocol and controls multiple non-participating nodes.

Preliminaries

We denote by $\mathbf{N}$ the set of all $n := |\mathbf{N}|$ parties in the network and by $\mathbf{P} := \{A, B_1, \ldots, B_m\}$ the set of protocol participants, where A refers to Alice and $\{B_i\}_{i=1}^{m}$ refers to the m Bobs she selects.

Let Eve be an attacker whose goal is to learn $\mathbf{P}$. When Eve corrupts some parties, she trivially learns their role in the protocol, *i.e.*, whether they belong to **P** or not. By $\mathcal{I}_{\text{Eve}}$ we denote this information as well as any prior information about $\{\Pr(\mathbf{G} = \mathbf{P})\}_{\mathbf{G}\subset\mathbf{N}}$, *i.e.*, the probability distribution that a subset **G** of the parties is equal to **P**. Denoting by $\mathcal{I}^{+}_{\text{Eve}}$ the additional information available to Eve during the protocol, one can define anonymity by requiring that the execution of the protocol increases Eve's knowledge only in a trivial way.

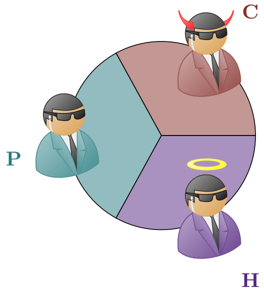
Definition 9.1 (Anonymity) *A protocol is anonymous from the perspective of Eve if for all subsets* $\mathbf{G} \subset \mathbf{N}$

$$\Pr\left(\mathbf{G} = \mathbf{P} \mid \mathcal{I}^{+}_{Eve}, \mathcal{I}_{Eve}\right) = \Pr\left(\mathbf{G} = \mathbf{P} \mid \mathcal{I}_{Eve}\right), \tag{9.1}$$

where $\mathcal{I}^{+}_{Eve}$ *is the information that becomes available to Eve during the protocol and* $\mathcal{I}_{Eve}$ *is both the information that Eve has beforehand and trivial information that she obtains about the parties that she corrupts.*

Here, by trivial information we mean the information available to each party regarding their role in the protocol, *i.e.*, whether they belong to **P** or not.

In the context of the key agreement, we can assume that the participants are not corrupted by a malicious Eve, as this would compromise the entire key. We therefore assume that the participants are honest but curious, *i.e.*, that they follow the protocol to establish a key, but may otherwise be interested in learning the identity of the other participants. For the non-participating parties, we consider the same honest-but-curious model as well as a completely dishonest model.



The set **N** of all parties in the network is partitioned into three disjoint sets such that $\mathbf{N} = \mathbf{P} \cup \mathbf{H} \cup \mathbf{C}$.

Accordingly, **N** can be partitioned into the following three disjoint sets:

P: honest-but-curious participating parties;
H: honest-but-curious non-participating parties;
C: dishonest and colluding non-participating parties.

We assume that Eve either follows the protocol and controls a single party in **P** or **H**, or that she deviates from the protocol and controls **C**. Note, however, that our definition of anonymity (Definition 9.1) is also applicable to other corruption models and therefore applies more generally to any cryptographic protocol.

As mentioned above, our CKA protocol exploits the correlations of a shared GHZ state to generate the conference key. Since the parties in **C** could apply an arbitrary quantum map to their system, this would result in a state ϵ close to $\rho_{\mathbf{N}} := |\mathbf{N}\rangle\langle\mathbf{N}|$, with

$$|\mathbf{N}\rangle = \frac{1}{\sqrt{2}}\left(|0\cdots0\rangle_{\mathbf{P}\cup\mathbf{H}} \otimes |\Psi\rangle_{\mathbf{C}} + |1\cdots1\rangle_{\mathbf{P}\cup\mathbf{H}} \otimes |\Phi\rangle_{\mathbf{C}}\right) \tag{9.2}$$

Here, the two states on **C** need not be orthogonal. Nor do they have to be pure, but since mixed states offer no advantage to Eve, we can assume that they are. For a discussion of untrusted or faulty sources see Section 9.

With the above definitions, we are now ready to present the subprotocols of the anonymous conference key agreement protocol. All the protocols we propose are anonymous according to Definition 9.1. Detailed proofs can be found in Appendix 12.3.

Generating anonymous multiparty entanglement

We begin by introducing two sub-protocols, *Notification* (Protocol 1) and *Anonymous Multiparty Entanglement* (*AME*, Protocol 2). Our version of *Notification* is based on Reference [BT07] and is a classical protocol used by Alice to notify the m receiving agents, while preserving anonymity for all parties involved. The protocol requires pairwise private classical communication –which can be established using a key generation protocol with a Bell pair as shown in Section 3.3– and access to private sources of randomness. An illustration of Protocol 1 can be found in Figure 9.2.

Protocol 1 is visualized in Figure 9.2, Protocol 2 in Figure 9.3, Protocol 3 in Figure 9.4 and Protocol 4 in Figure 9.5.

Protocol 1: Notification

```
Input  : Alice's choice of $m$ receivers.
Output : The $m$ receivers get notified.
forall agents $i$ in $\{1,\dots,n\}$ do
    forall agents $j$ in $\{1,\dots,n\}$ do
        if $j = j_a$ corresponds to Alice and $i$ is not a receiver then
            Alice chooses $n$ random bits $\left\{r^i_{j,k}\right\}_{k=1}^n$ such that
            $\bigoplus_{k=1}^n r^i_{j,k} = 0$. She sends bit $r^i_{j,k}$ to agent $k$.
        else if $j = j_a$ corresponds to Alice and $i$ is a receiver then
            Alice chooses $n$ random bits $\left\{r^i_{j,k}\right\}_{k=1}^n$ such that
            $\bigoplus_{k=1}^n r^i_{j,k} = 1$. She sends bit $r^i_{j,k}$ to agent $k$.
        else
            When $j \neq j_a$, the agent chooses $n$ random bits $\left\{r^i_{j,k}\right\}_{k=1}^n$
             such that $\bigoplus_{k=1}^n r^i_{j,k} = 0$ and sends bit $r^i_{j,k}$ to agent $k$.
    forall agents $k$ in $\{1,\dots,n\}$ do
        Agent $k$ receives $\left\{r^i_{j,k}\right\}_{j=1}^n$, computes $z^i_k = \bigoplus_{j=1}^n r^i_{j,k}$ and
         sends it to agent $i$.
    Agent $i$ takes the received $\{z^i_k\}_{k=1}^n$ to compute $z^i = \bigoplus_{k=1}^n z^i_k$; if
     $z^i = 1$ they are thereby notified to be a designated receiver.
```

In Protocol 1 anonymity is preserved following Reference [BT07]. Remember that due to the nature of our goal, the identities of the Bobs are available to Alice since she selected them. The *Notification* protocol requires $\mathcal{O}\left(n^3\right)$ communication channel uses between pairs of parties.

Note that the *Notification* protocol would allow Alice to anonymously transmit the same bit to all receivers to establish a common key. However, such a process would be extremely inefficient; if one Bell pair is required for each private classical communication round, then $\mathcal{O}\left(n^3\right)$ Bell pairs would be consumed for each bit of the generated key.

If instead we use *Notification* only once to notify the receivers, we can exploit the properties of the shared multipartite entanglement to establish a common key more efficiently while maintaining the anonymity that Protocol 1 provides.

Protocol 2 is visualized in Figure 9.3.

After the *Notification* protocol, we now introduce the second sub-protocol *Anonymous Multiparty Entanglement (AME)*, shown in Figure 9.3. As a generalization of the anonymous Bell state distribution protocol first proposed in Reference [CW05], it is a protocol for anonymously establishing GHZ states.

Here, n parties are sharing an n-partite GHZ state, and $m+1$ of them (Alice and the m receivers) want to anonymously end up with a smaller, $(m+1)$-partite GHZ state. To achieve this, all parties need access to a broadcast channel –a necessary requirement to achieve any kind of anonymity for participants in a communication setting [Fit+02].

Protocol 2: Anonymous Multiparty Entanglement (AME)

```
Input  : A shared GHZ$_n$ state;
         Alice knowing the identities of the non-participants $\overline{\mathbf{P}}$.
Output : A GHZ$_{m+1}$ state shared between $\mathbf{P}$.
1 forall agents $i$ in $\{1, \dots, n\}$ do
2     if $i \in \mathbf{P}$ then
3         When $i \in \mathbf{P}$, agent $i$ measures in the $X$-basis and stores the
          measurement outcome as $x_i$.
4     else
5         When $i \in \overline{\mathbf{P}}$, i.e. agent $i$ is Alice or one of the Bobs, agent $i$
          draws a uniformly random bit $x_i$.
6     Agent $i$ broadcasts $x_i$. These broadcasts are in a random order
      or, if possible, simultaneously.
7 Alice applies a $Z$ gate if $\sum_{i \in \overline{\mathbf{P}}} x_i = 1 \pmod{2}$, i.e. if the parity of the
  non-participating parties' bits is odd.
```

The correctness of the *Anonymous Multiparty Entanglement (AME)* protocol follows from the proof in Reference [CW05]. With the Hadamard matrix H we can rewrite the GHZ$_n$ state as proportional to

$$\sum_{x \in \{0,1\}^{|\overline{\mathbf{P}}|}} \left[|0 \cdots 0\rangle_{\mathbf{P}} + (-1)^{\Delta(x)} |1 \cdots 1\rangle_{\mathbf{P}} \right] \otimes H_{\overline{\mathbf{P}}} |x\rangle_{\overline{\mathbf{P}}}, \tag{9.3}$$

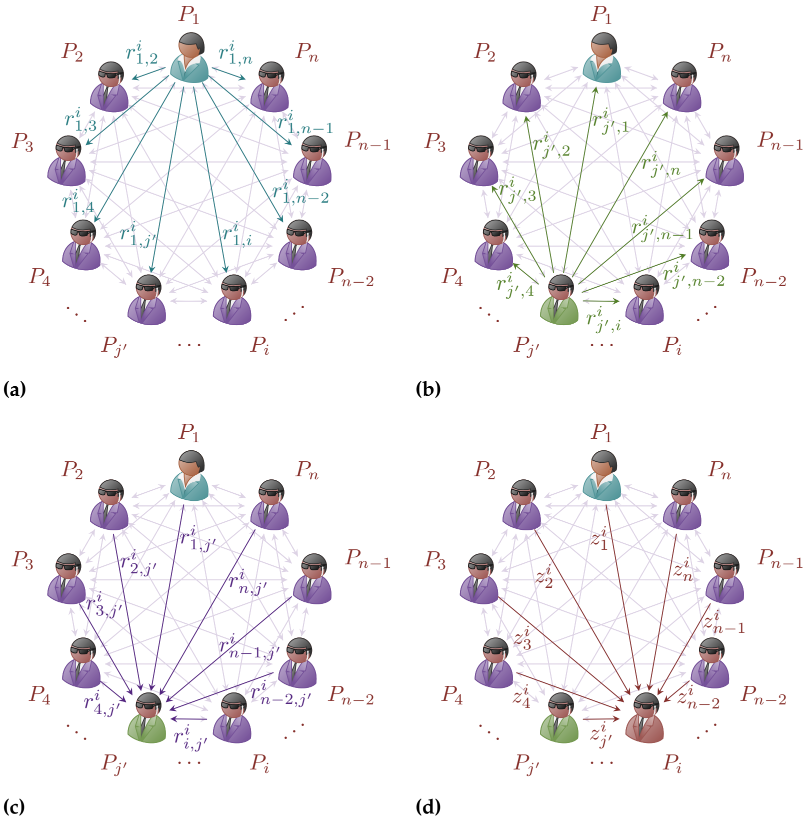
where $\Delta(x)$ is the Hamming weight of x and the indices $\mathbf{P}$ and $\overline{\mathbf{P}}$ indicate the participating and non-participating parties, respectively.

Since H transforms the X and Z bases into each other (see Definition 2.4), the state shared between Alice and the Bobs after the X-measurements in line 2 and 3 of Protocol 2 is

$$\frac{1}{\sqrt{2}} \left[|0 \cdots 0\rangle_{\mathbf{P}} + (-1)^{\Delta(x)} |1 \cdots 1\rangle_{\mathbf{P}} \right], \tag{9.4}$$

where x contains all measurement outcomes announced in line 6. Finally, calculating $\Delta(x)$, Alice locally corrects the state to obtain the desired GHZ$_{m+1}$ state.

In terms of anonymity, the key elements are the intrinsic correlations of GHZ states. As observed in Reference [CW05], any rotation around the z-axis (*cf.* Figure 2.1) applied to any qubit of a GHZ state has the same effect on the global state independent of the chosen qubit.



j \ k	1	2	3	···	j'	···	i	···	n
1	$r^i_{1,1}$	$r^i_{1,2}$	$r^i_{1,3}$	···	$r^i_{1,j'}$	···	$r^i_{1,i}$	···	$r^i_{1,n}$
2	$r^i_{2,1}$	$r^i_{2,2}$	$r^i_{2,3}$	···	$r^i_{2,j'}$	···	$r^i_{2,i}$	···	$r^i_{2,n}$
3	$r^i_{3,1}$	$r^i_{3,2}$	$r^i_{3,3}$	···	$r^i_{3,j'}$	···	$r^i_{3,i}$	···	$r^i_{3,n}$
···	···	···	···	···	···	···	···	···	···
j'	$r^i_{j',1}$	$r^i_{j',2}$	$r^i_{j',3}$	···	$r^i_{j',j'}$	···	$r^i_{j',i}$	···	$r^i_{j',n}$
···	···	···	···	···	···	···	···	···	···
i	$r^i_{i,1}$	$r^i_{i,2}$	$r^i_{i,3}$	···	$r^i_{i,j'}$	···	$r^i_{i,i}$	···	$r^i_{i,n}$
···	···	···	···	···	···	···	···	···	···
n	$r^i_{n,1}$	$r^i_{n,2}$	$r^i_{n,3}$	···	$r^i_{n,j'}$	···	$r^i_{n,i}$	···	$r^i_{n,n}$
$\bigoplus_j r^i_{j,k}$	z^i_1	z^i_2	z^i_3	···	$z^i_{j'}$	···	z^i_i	···	z^i_n

(e)

Figure 9.2: Visualization of Protocol 1. The table (**e**) contains all $r^i_{j,k}$ for a fixed agent $P_i \in \mathbf{N}$ in the *Notification* protocol. Here, we identify Alice with P_1. She chooses $\left\{r^i_{1,k}\right\}_{k=1}^{n}$ and (**a**) sends them to P_k in line 3 to 6 of Protocol 1. Note that only if P_i is a receiver, the green row adds up to 1 (mod 2); otherwise to 0 (mod2). Analogously, the second green highlighting shows line 7 and 8 of Protocol 1 from the perspective of $P_{j'}$ (**b**). This and all other rows add up to 0 (mod2). The $\left\{r^i_{j,j'}\right\}_{j=1}^{n}$ that $P_{j'}$ receives (**c**) in lines 9 and 10 are highlighted in violet. The last row, highlighted in brown, shows (**d**) the $\{z^i_k\}_{k=1}^{n}$ received by P_i in line 11. By construction, only if P_i is a receiver, it adds up to 1(mod2).

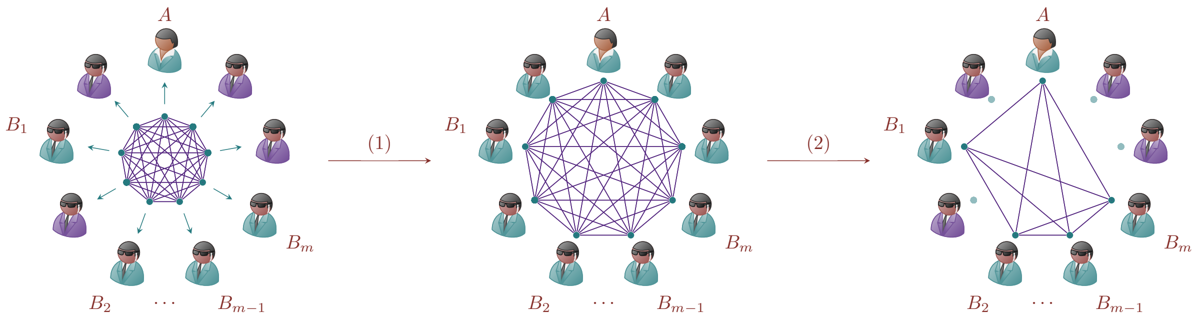


Figure 9.3: Visualization of Protocol 2. A GHZ$_n$ state is shared with all agents left of arrow (1). Here, the participants are highlighted in green and the non-participants in violet. Since the shared GHZ$_n$ state is agnostic of the receivers' identities and all agents are entangled right of arrow (1), they are all highlighted in green. Right of arrow (2), all non-participating parties are disentangled and therefore not highlighted anymore. The m Bobs and Alice now share a GHZ$_{m+1}$ state after completing the steps of *AME*.

To correct the state, Alice only needs the parity of the measurement outcomes of the non-participating parties, yet, masking their identity, each Bob announces a random bit too. No information about the operations performed by the different parties can be inferred, since all announced bits are provably uniformly random and a Z gate does not reveal the position of the qubit it was applied to either. Only Alice knows the identities of the Bobs, so only she is able to discern the measurement outcomes from the random bits. See Appendix 12.3 for a detailed discussion on why the protocol does not reveal information about the identity of either Alice or the Bobs in untrusted settings.

A combination of the above two protocols allows for an anonymous distribution of a GHZ$_{m+1}$ state, which in turn can be measured in the Z basis by all participants to generate a shared secret key. However, to be secure against dishonest or eavesdropping parties, the state must be verified.

Anonymous verification of entanglement

In the case of an untrusted source, any verification could be performed immediately after the state is distributed. However, one party in $\overline{\mathbf{P}}$ might not measure in Protocol 2 and thereby be part of the extracted, then ($> m+1$)-partite, GHZ state. This security risk was independently noticed in Reference [Yan+20] for the case of two-party communication.

To detect both a faulty source and dishonest parties, the verification of the state has to be postponed until after Protocol 2. Note that in this setting, only the communication of authorized parties is considered by Alice.

Protocol 3 is visualized in Figure 9.4.

Protocol 3 verifies that the state on $\mathbf{P}$ is close to the GHZ$_{m+1}$ state, and therefore also disentangled from all other parties, including the dishonest and colluding ones in $\mathbf{C}$. Protocol 3 is similar to Reference [Pap+12a] and inspired by the studies of Reference [BBT03], but adjusted here to protect the identities of the participants and to always set the verifier to be Alice. It requires private sources of randomness and a classical broadcasting channel. It is visualized in Figure 9.4.

```
Protocol 3: Verification
  Input  : A shared state between $|\mathbf{P}| = m + 1$ parties.
  Output : Verification or rejection of the shared state as a GHZ$_{m+1}$
           state by Alice.
  forall agents $j$ in $\{1, \ldots, n\}$ do
      if $j$ corresponds to Bob $B_i$ then
          $B_i$ draws a random bit $b_i$ and measures in the $X$- or the
            $Y$-basis if it equals 0 or 1, respectively. They store the
            measurement outcome $o_i$ and basis bit as $(b_i, o_i) = (b, o)$.
      else
          Agent $j$ is Alice or $j \in \overline{\mathbf{P}}$. They draw two uniformly random
            bits $(b, o)$. Alice's bits are $(b_0, o_0) = (b, o)$.
      Agent $j$ broadcasts both bits $(b, o)$.
  Alice resets her bit such that $\sum_{i=0}^{m} b_i = 0 \pmod 2$. She measures in
    the $X$- or $Y$-basis if her bit equals 0 or 1 –thereby also resetting $o_0$.
  If and only if $\frac{1}{2}\sum_i b_i + \sum_{i=0}^{m} o_i = 0 \pmod 2$, Alice accepts the state.
```

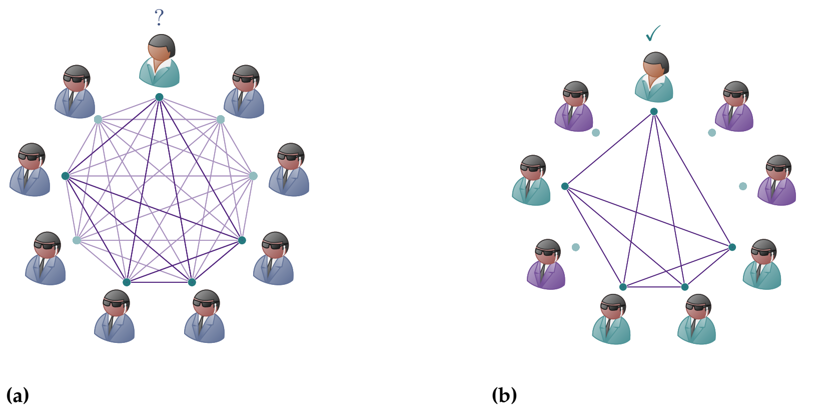


Figure 9.4: Visualization of Protocol 3 for the anonymous verification of entanglement. Although Alice should be entangled only with the Bobs she notified, she (**a**) does not know whether this is the case for certain. By running the verification protocol (**b**), Alice can statistically determine whether she is.

From Reference [Pap+12a], we know that the state is verified to be increasingly close to the GHZ state with the number of passed verification rounds. To conceal their identities, the parties in **P** need both **H** and **C** to announce random bits as well. This renders all public communication uniformly random. Since the relevant quantum correlations are only accessible to Alice, all parties are indistinguishable from Eve's point of view.

Anonymous conference key agreement

We are now ready to define Protocol 4 for anonymously generating a secret key between the participants **P**, where we introduce the parameters L as the number of shared GHZ states and D as a parameter both determining the level of security and the length of the generated shared key. Protocol 4 is visualized in Figure 9.5.

Protocol 4 is visualized in Figure 9.5.

The main difference between the proposed protocol and the one in Reference [Unn+19] is that the nonparticipating parties are asked to announce random values to mask the identities of the authorized parties and that the protocol aborts if the values are not announced in time. Protocol 4 combines all previous protocols and additionally requires a public source of randomness.

Protocol 4: Anonymous conference key agreement

```
Input  : Alice as initiator; parameters $L \in \mathbb{N}$ and $D > 0$.
Output : Anonymous secret key between P.
Alice notifies the $m$ Bobs with Protocol 1.
forall of the $L$ GHZ states generated by the source do
    The parties run Protocol 2 on the GHZ state. A public source of
      randomness broadcasts a bit $b$ such that $\Pr[b = 1] = \frac{1}{D}$.
    if $b = 0$ then
        Verification round: If $b = 0$, Alice runs Protocol 3 on the
          $(m + 1)$-partite state. The remaining parties announce
          random values.
    else
        Keygen round: If $b = 1$, Alice and the Bobs $Z$-measure to
          obtain a shared secret bit.
if Alice accepts all verification rounds then
    Alice anonymously validates the protocol.
```

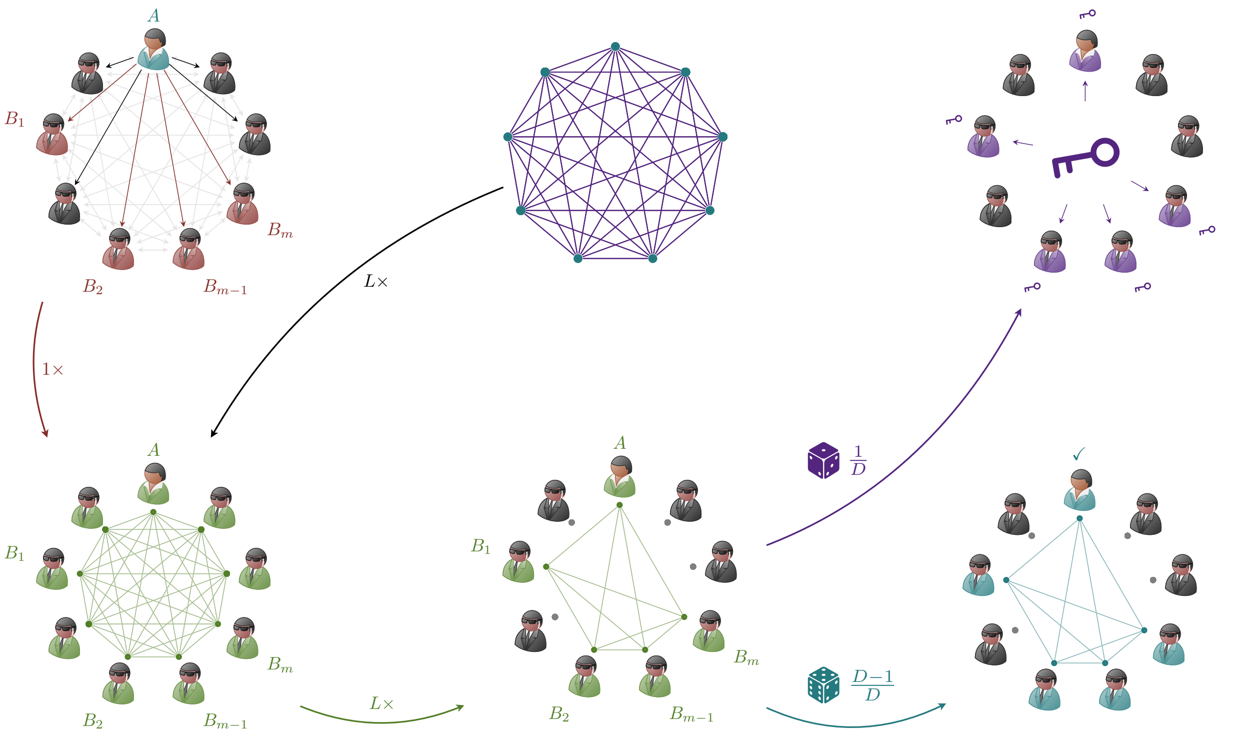


Figure 9.5: Visualization of Protocol 4. Alice notifies the m Bobs with Protocol 1. During all L rounds of Protocol 4 the parties run Protocol 2 on the GHZ state that is provided by the source. A public source of randomness broadcasts a bit b such that $\Pr[b = 1] = \frac{1}{D}$. If $b = 0$, Protocol 3 is run to verify the $(m+1)$-partite state. If $b = 1$, Alice and the Bobs Z-measure to generate a shared secret bit.

Protocol 4 establishes a secret key between the participants while keeping their identities secret from outsiders as well as from each other.

The verification rounds ensure that the state on **P** is on average ϵ close to the GHZ$_{m+1}$ state, where ϵ decreases monotonically with the number of verification rounds; the state thus contains correlations only observable by Alice. Likewise, neither the public communication nor the remainder of the state are correlated with the identities.

On average $L[1 - (1/D)]$ states are used to verify the state. Therefore the key rate of Protocol 4 approaches L/D in the asymptotic limit. See Appendix 12.3 for a detailed proof of anonymity.

Note that within our combined Protocol 4, the verification implicitly verifies the notification, as the bits that Alice considers would otherwise not exhibit the correct correlations.

All protocols are self-contained in the way we presented them. However, when combined, one could reduce both the communication overhead and the number of applied quantum operations.

Specifically, instead of issuing random values, the participants could simply announce the outputs of the verification process during the next round. In the same sense, Alice does not need to perform the Z-correction at the end of Protocol 2, since she can choose a complementary set of stabilizer measurements during the verification protocol.

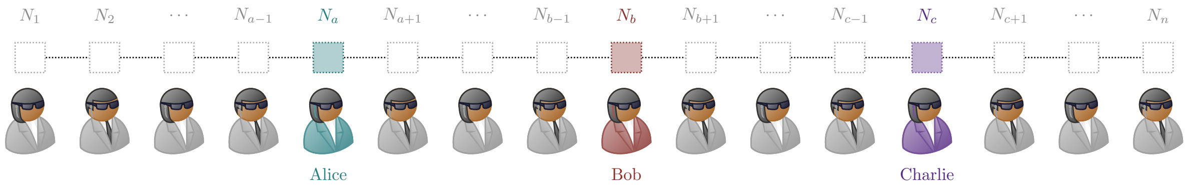


Figure 9.6: Alice, Bob and Charlie connected with non-participants in linear network. Their positions are unknown to the non-participants.

Related work

In Reference [HJP20] we introduced the above protocols to achieve anonymity for conference key agreement by using multipartite quantum states. Starting from a large GHZ state shared between n parties, Protocol 4 enables a sender to anonymously notify a set of receivers and establish a secret key that can be used to encrypt a message. This encrypted message can then be anonymously broadcast by the sender, using either a classical [BT07] or a quantum protocol [CW05]. While in Reference [HJP20] we focused on GHZ states, other types of quantum states have also been used for creating anonymous entanglement, as well as for conference key agreement [LMW18; GKB19]; it is however unknown whether they can be combined to achieve the same task as presented here.

We assumed that the source is not actively malicious. The protocol might still abort—either due to a noisy state or due to malicious participants—but anonymity is preserved. If the source is actively malicious, a privacy leak during a Protocol 2 round can never be caught in time, since it is run before each Verification round, that is before Protocol 3. This could be fixed by additionally verifying the n-partite GHZ after its initial sharing.

Finally, practical sources and channels can be faulty and hence the need for anonymous error correction and privacy amplification arises [Epp+17; Pro+21]. Likewise, a measure of anonymity should be introduced and is expected to be upper bounded by an appropriate validation via some closeness measure. While Definition 9.1 aims to capture composability, further study in appropriate security frameworks is required. We started to address these issues in follow-up work [Gra+22; Jon+22a], by adjusting the validation process for noisy states and taking into account the finite-key effects of real-world implementations.

↑ ↑ ↑
The preceding sections closely follow the text of Reference [HJP20]*, which was written by both myself and my co-authors.*

9.3 Anonymous conference key agreement with linear cluster states

In further follow-up work [Jon+22a], we bring together the extraction of GHZ states from linear cluster states with anonymous conference key agreement. The corresponding linear quantum network is visualized in Figure 9.6.

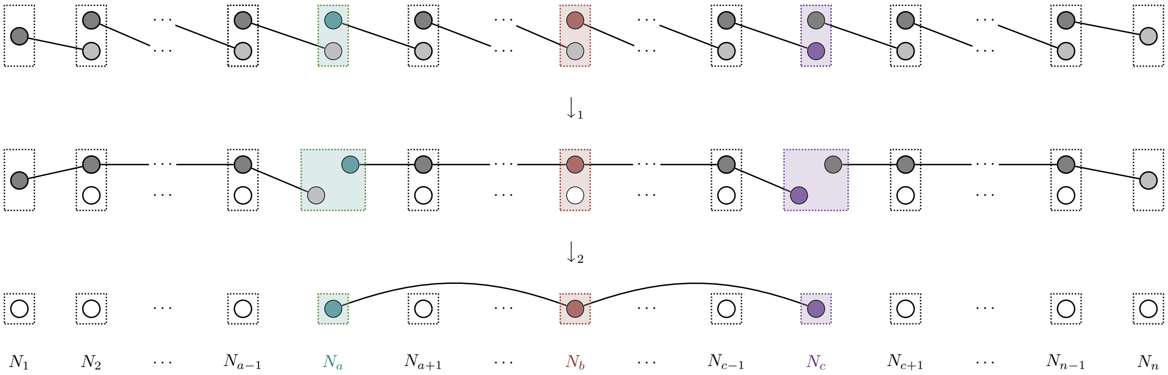


Figure 9.7: Top: In a first step, Bell pairs are shared between the neighboring nodes N_i and N_{i+1} of a linear network. The three qubits designated to be part of the GHZ state are colored green, brown and violet. **Middle:** In a second step, the Bell resources are used to create three linear cluster states via Bell state projection. Alice and Charlie do not perform the projection. **Bottom:** In a third step the central linear cluster states are transformed into tripartite GHZ states between Alice, Bob and Charlie.

ACKA with linear cluster states takes advantage of the fact that –for three qubits– cluster states are locally equivalent to GHZ states. For a detailed analysis of the relationship, we refer to Section 4.3 and Appendix 11.1.

The following sections closely follow the text of Reference [Jon+22a], which was written by both myself and my co-authors.

↓ ↓ ↓

Our anonymous conference key agreement protocol for linear quantum networks is divided into three parts: the preparation of the required multipartite states from the Bell pairs, the anonymous extraction a tripartite GHZ state from the multipartite states, and the subsequent key generation with post-processing. Figure 9.7 shows the first two of these steps.

In Reference [Jon+22a], we only prove that an anonymous quantum conference key agreement is possible for three parties in a linear network. Since extraction of larger GHZ states from linear cluster states is possible [Jon+22b], generalization of the protocol to more than three participants may be possible too. At the time of writing, however, this is still an open question.

↑ ↑ ↑

The preceding sections closely follow the text of Reference [Jon+22a], which was written by both myself and my co-authors.

9.4 Experimental implementations

We implemented both the first anonymous conference key agreement protocol and the one in linear networks experimentally in collaboration with the Barz Group at the university of Stuttgart. In the proof-of-principle demonstrations, the protocols were run for up to three participants in a network with four entangled parties.

The implementation of the former [HJP20] can be found in Reference [Tha+21], while the implementation of the latter [Jon+22a] can be found in Reference [Rüc+22].

In both proof-of-principle demonstrations, pairs of polarization-entangled photons were generated via so-called *type-II spontaneous parametric down-conversion*. For this purpose Barium borate was pumped with a pulsed (140 fs) Titanium-Sapphire laser, whose wavelength was upconverted from 780 nm to 390 nm, *i.e.*, from infrared light with a photon energy 1.59 eV to violet light with a photon energy 3.18 eV.

With polarization-dependent beam splitters, half wave plates and quarter wave plates the required multipartite entangled states were then generated upon postselection. The measurements of the qubits encoded in the polarization of the photons required further polarizing beam splitters, half and quarter wave plates for the necessary basis changes –followed by an avalanche photo diode detector for each party in the network.

Although with current technology the generation of multipartite entanglement is still rather noisy, the resulting asymptotic key rate was already positive in our experiments. Within realistic parameter regimes, we can hope to see positive finite key rates [Jon+22a; GKB18] for anonymous conference key agreement experiments in the near future.

Conclusion 10

Advances in quantum information theory combined with the rising demand for data security in networked communication, have made quantum networks a thriving area of study in recent years. Fundamental to this research is the manipulation of multipartite entanglement and its routing through the network, ultimately enabling quantum cryptography, and thereby information-theoretically secure communication between network users. This thesis highlights contributions to both fundamental research on multipartite entanglement and to the ongoing development of concrete communication protocols and cryptographic solutions.

We have explored the potential for the implementation of quantum networks for practical applications through the study of quantum graph states. We saw how these graph states, as instances of multipartite entangled states of quantum particles, can be manipulated by local operations on individual qubits to control the distribution of entanglement.

We showed how multipartite entangled resources can be transformed both into different multipartite entanglement [Jon+22b] and into bipartite entanglement between subsets of selected nodes [HPE19]. In this regime of local operations on single qubits we also showed no-go results for these transformations in nearest-neighbor network topologies [Hah+22].

To address the underlying graph-theoretic challenges, we explored the properties of graph states through the lens of graph invariants. Against the background of the computational inefficiency of known graph state invariants under local complementation, we derived a new and easy to compute invariant by overcoming the need to compute the full set of stabilizers, which grows exponentially with the number of qubits [BH23].

In the final part of the thesis, we then constructed a new quantum cryptography protocol in the multipartite setting. Using the complex correlation patterns of graph state entanglement, we proposed the first protocol for anonymous key agreement in quantum conferences [HJP20]. In a proof-of-principle experiment, our protocol was implemented with up to four participants [Tha+21]. An improved and noise robust version of our protocol has been published in [Gra+22] and a variant for linear network topologies in [Jon+22a] and experimentally implemented in [Rüc+22].

It is our hope that this work together with future explorations will contribute significantly to the realization of the dream of a quantum internet. Our anonymous communication protocols demonstrate the advantage of multipartite entanglement over bipartite entanglement for a concrete cryptographic task in quantum networks. While large-scale implementation of our protocols remain beyond current experimental capabilities, there is ample reason for optimism. Thus far, technical progress has enabled a steady improvement in the performance of experimentally realized physical qubits.

Appendix

Detailed examples 11

11.1 Global phases in the state vector picture

In this section, we study in detail how a linear cluster state of three qubits $|L_3\rangle$ is transformed by local complementation into the graph state represented by a triangle $|K_3\rangle$.

Their adjacency matrices are

$$\Gamma_{L_3} := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

and

$$\Gamma_{K_3} := \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

While it is clear from their graph representations that K_3 can be obtained from L_3 (and vice versa) via the local complementation τ_2, *i.e.*,

$$\tau_2(L_3) = K_3, \quad \tau_2(K_3) = L_3, \tag{11.1}$$

it is not true that the state vectors $U_2^\tau|L_3\rangle$, $(U_2^\tau)^\dagger|L_3\rangle$ and $|K_3\rangle$ are the same. They differ by global phases.

With Definition 4.4 we find that

$$|L_3\rangle = \frac{1}{2\sqrt{2}}[|000\rangle + |001\rangle + |010\rangle - |011\rangle \tag{11.2}$$

$$+|100\rangle + |101\rangle - |110\rangle + |111\rangle], \tag{11.3}$$

$$|K_3\rangle = \frac{1}{2\sqrt{2}}[|000\rangle + |001\rangle + |010\rangle - |011\rangle \tag{11.4}$$

$$+|100\rangle - |101\rangle - |110\rangle - |111\rangle]. \tag{11.5}$$

For the local complementation unitary, we can use Equation 4.24 to explicitly calculate that

$$U_2^\tau = \frac{1}{\sqrt{2}}\begin{pmatrix} i & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -i & 0 & 0 & 0 & 0 \\ 1 & 0 & i & 0 & 0 & 0 & 0 & 0 \\ 0 & -i & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & -i & 0 \\ 0 & 0 & 0 & 0 & 0 & -i & 0 & -1 \\ 0 & 0 & 0 & 0 & -i & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & -i \end{pmatrix}. \tag{11.6}$$

Thus, we can calculate the action of the local complementation unitary on the graph state vector $|L_3\rangle$ as

$$U_2^\tau|L_3\rangle = \left(\frac{1}{4} + \frac{i}{4}\right)[|000\rangle + |001\rangle + |010\rangle - |011\rangle \tag{11.7}$$

$$+|100\rangle - |101\rangle - |110\rangle - |111\rangle], \tag{11.8}$$

$$(U_2^\tau)^\dagger|L_3\rangle = \left(\frac{1}{4} - \frac{i}{4}\right)[|000\rangle + |001\rangle + |010\rangle - |011\rangle \tag{11.9}$$

$$+|100\rangle - |101\rangle - |110\rangle - |111\rangle]. \tag{11.10}$$

In comparison we can see that $U_2^\tau|L_3\rangle$, $(U_2^\tau)^\dagger|L_3\rangle$ and $|\tau_2(L_3)\rangle = |K_3\rangle$ differ by the global phases

$$\frac{1}{2\sqrt{2}\left(\frac{1}{4}+\frac{i}{4}\right)} = e^{-\frac{\pi}{4}i}, \quad \frac{1}{2\sqrt{2}\left(\frac{1}{4}-\frac{i}{4}\right)} = e^{\frac{\pi}{4}i}, \tag{11.11}$$

i.e., we have

$$|\tau_2(L_3)\rangle = e^{-\frac{\pi}{4}i}U_2^\tau|L_3\rangle, \quad |\tau_2(L_3)\rangle = e^{\frac{\pi}{4}i}(U_2^\tau)^\dagger|L_3\rangle. \tag{11.12}$$

However, since $|\psi\rangle = e^{i\alpha}|\phi\rangle$ implies

$$|\psi\rangle\langle\psi| = e^{i\alpha}e^{-i\alpha}|\phi\rangle\langle\phi| = |\phi\rangle\langle\phi|, \tag{11.13}$$

this global phase is not physically relevant. We can identify both $U_2^\tau|L_3\rangle$ and $(U_2^\tau)^\dagger|L_3\rangle$ with $|\tau_2(L_3)\rangle$, since both describe the same density matrix, that is, the same quantum state. In our case we have explicitly

$$|\tau_2(L_3)\rangle\langle\tau_2(L_3)| = U_2^\tau|L_3\rangle\langle L_3|(U_2^\tau)^\dagger = (U_2^\tau)^\dagger|L_3\rangle\langle L_3|U_2^\tau \tag{11.14}$$

and

$$|\tau_2(L_3)\rangle\langle\tau_2(L_3)| = \frac{1}{8}\begin{pmatrix} 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\ -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\ -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \end{pmatrix}. \tag{11.15}$$

Conversely, $U_2^\tau|K_3\rangle$, $(U_2^\tau)^\dagger|K_3\rangle$ and $|L_3\rangle$ differ by a global phase even though $\tau_2(K_3) = L_3$. However, we still find

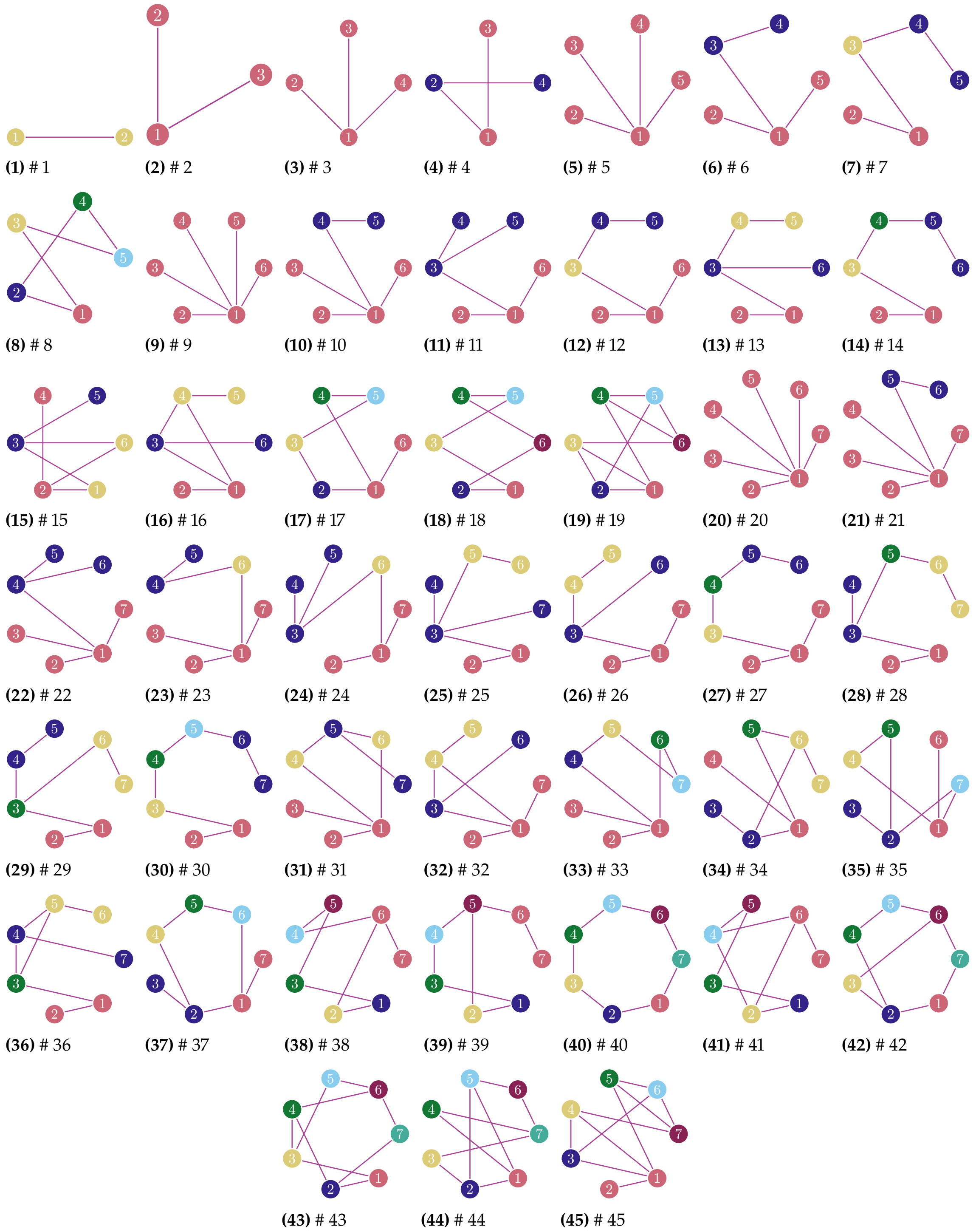
$$|\tau_2(K_3)\rangle\langle\tau_2(K_3)| = U_2^\tau|K_3\rangle\langle K_3|(U_2^\tau)^\dagger = (U_2^\tau)^\dagger|K_3\rangle\langle K_3|U_2^\tau \tag{11.16}$$

which equals

$$\frac{1}{8}\begin{pmatrix} 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \end{pmatrix}. \tag{11.17}$$

11.2 Foliage partitions for LC orbits

Here we show the foliage partitions for all local complementation orbits of all graph states up to 8 qubits. Each graph depicted is a representative of their LC orbit. As we have shown that the foliage partition of graphs are invariant under local Clifford operations, the foliage partition is exactly the same for each graph in the represented orbit.



(1) # 1 **(2)** # 2 **(3)** # 3 **(4)** # 4 **(5)** # 5 **(6)** # 6 **(7)** # 7

(8) # 8 **(9)** # 9 **(10)** # 10 **(11)** # 11 **(12)** # 12 **(13)** # 13 **(14)** # 14

(15) # 15 **(16)** # 16 **(17)** # 17 **(18)** # 18 **(19)** # 19 **(20)** # 20 **(21)** # 21

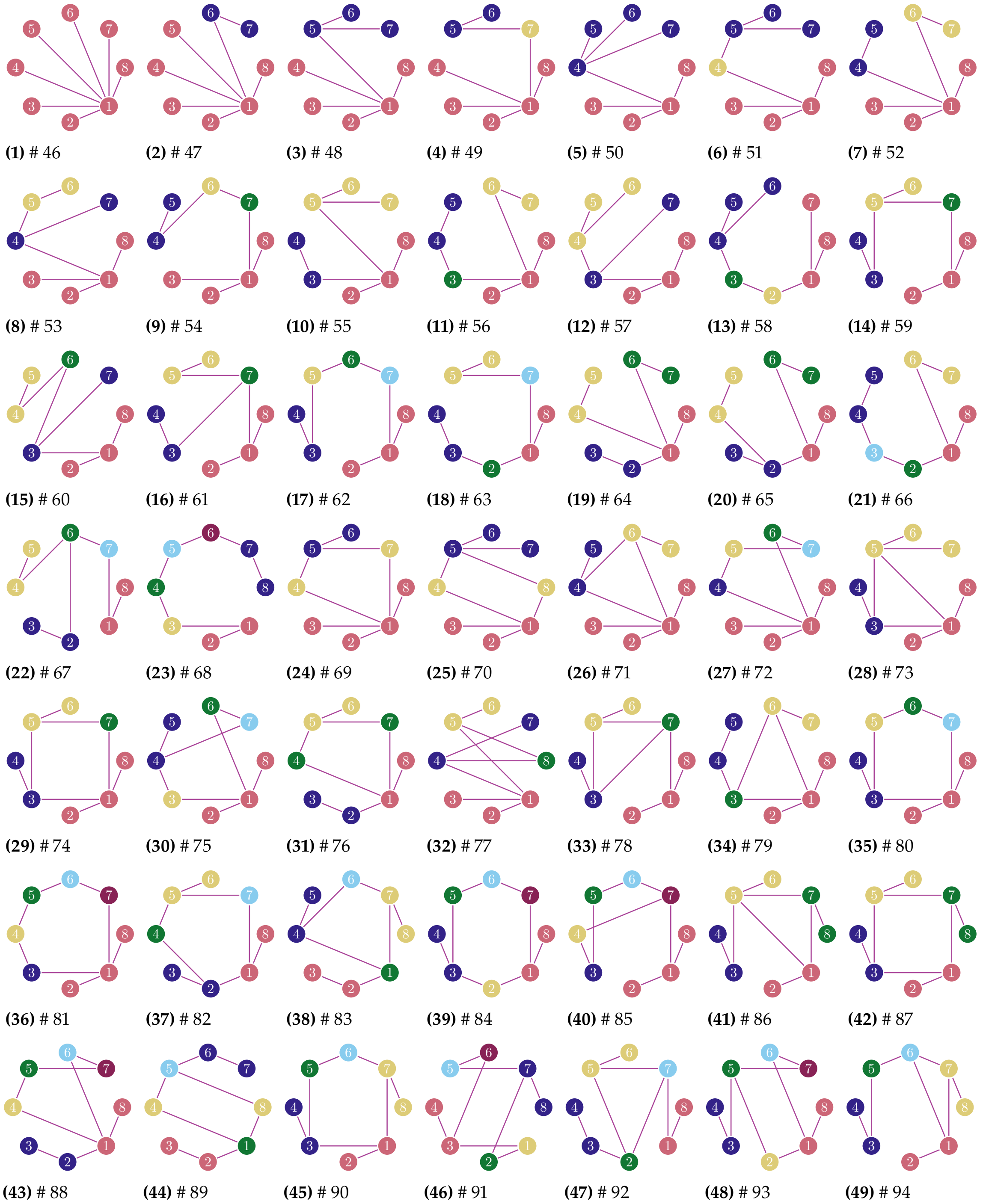
(22) # 22 **(23)** # 23 **(24)** # 24 **(25)** # 25 **(26)** # 26 **(27)** # 27 **(28)** # 28

(29) # 29 **(30)** # 30 **(31)** # 31 **(32)** # 32 **(33)** # 33 **(34)** # 34 **(35)** # 35

(36) # 36 **(37)** # 37 **(38)** # 38 **(39)** # 39 **(40)** # 40 **(41)** # 41 **(42)** # 42

(43) # 43 **(44)** # 44 **(45)** # 45

Figure 11.1: Representatives for each local complementation orbit up to 7 qubits with highlighted foliage partition.



(1) # 46 **(2)** # 47 **(3)** # 48 **(4)** # 49 **(5)** # 50 **(6)** # 51 **(7)** # 52

(8) # 53 **(9)** # 54 **(10)** # 55 **(11)** # 56 **(12)** # 57 **(13)** # 58 **(14)** # 59

(15) # 60 **(16)** # 61 **(17)** # 62 **(18)** # 63 **(19)** # 64 **(20)** # 65 **(21)** # 66

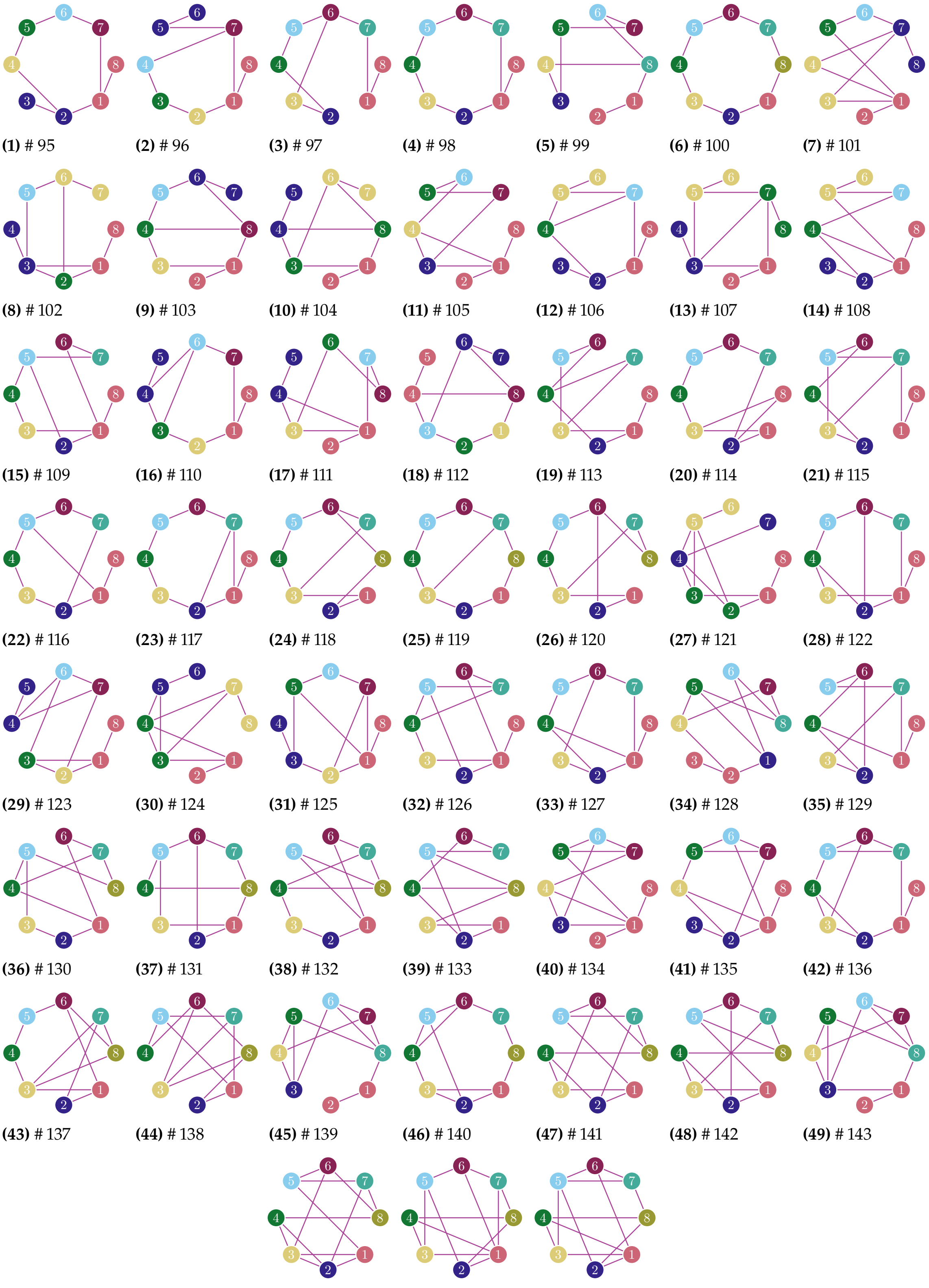
(22) # 67 **(23)** # 68 **(24)** # 69 **(25)** # 70 **(26)** # 71 **(27)** # 72 **(28)** # 73

(29) # 74 **(30)** # 75 **(31)** # 76 **(32)** # 77 **(33)** # 78 **(34)** # 79 **(35)** # 80

(36) # 81 **(37)** # 82 **(38)** # 83 **(39)** # 84 **(40)** # 85 **(41)** # 86 **(42)** # 87

(43) # 88 **(44)** # 89 **(45)** # 90 **(46)** # 91 **(47)** # 92 **(48)** # 93 **(49)** # 94

Figure 11.2: First part of representatives for each local complementation orbit for 8 qubits with highlighted foliage partition.



(1) # 95 **(2)** # 96 **(3)** # 97 **(4)** # 98 **(5)** # 99 **(6)** # 100 **(7)** # 101

(8) # 102 **(9)** # 103 **(10)** # 104 **(11)** # 105 **(12)** # 106 **(13)** # 107 **(14)** # 108

(15) # 109 **(16)** # 110 **(17)** # 111 **(18)** # 112 **(19)** # 113 **(20)** # 114 **(21)** # 115

(22) # 116 **(23)** # 117 **(24)** # 118 **(25)** # 119 **(26)** # 120 **(27)** # 121 **(28)** # 122

(29) # 123 **(30)** # 124 **(31)** # 125 **(32)** # 126 **(33)** # 127 **(34)** # 128 **(35)** # 129

(36) # 130 **(37)** # 131 **(38)** # 132 **(39)** # 133 **(40)** # 134 **(41)** # 135 **(42)** # 136

(43) # 137 **(44)** # 138 **(45)** # 139 **(46)** # 140 **(47)** # 141 **(48)** # 142 **(49)** # 143

(50) # 144 **(51)** # 145 **(52)** # 146

Figure 11.3: Second part of representatives for each local complementation orbit for 8 qubits with highlighted foliage partition.

Proofs 12

12.1 Measurements in the stabilizer formalism

The density matrix of a stabilizer state $|\psi\rangle$ can be expressed as

$$|\psi\rangle\langle\psi| = \frac{1}{2^n}\prod_{v=1}^{n}\left(\mathbb{1}_{2^n} + K_v\right) \tag{12.1}$$

in terms of the generators $\{K_v\}_{v=1}^n$ of its stabilizer.

In Subsection 4.2 on measurements in the stabilizer formalism we showed (*cf.* Equation 4.19) that the quantum state after the projective measurement of a Pauli observable that does not commute with one of the stabilizer generators K_1 of the stabilizer state measured, is described by

$$|\psi_\pm\rangle = \frac{\mathbb{1}_{2^n} \pm P}{\sqrt{2}}|\psi\rangle. \tag{12.2}$$

In order to highlight that this post measurement state is again a stabilizer state, we then stated in Equation 4.20 that its density matrix is given by

$$|\psi_\pm\rangle\langle\psi_\pm| = \frac{1}{2^n}\left(\mathbb{1}_{2^n} \pm P\right)\prod_{v=2}^{n}\left(\mathbb{1}_{2^n} + K_v\right). \tag{12.3}$$

and that therefore –comparing to Equation 12.1– its stabilizer generators are given by $\{\pm P, K_2, K_3, \dots, K_n\}$. In this appendix, we will show why this is the case.

With Equations 12.1 and 12.2, we can start our calculation by writing

$$\begin{aligned}
|\psi_\pm\rangle\langle\psi_\pm| &= \frac{\mathbb{1}_{2^n} \pm P}{\sqrt{2}}|\psi\rangle\langle\psi|\frac{\mathbb{1}_{2^n} \pm P^\dagger}{\sqrt{2}} && (12.4)\\
&= \frac{\mathbb{1}_{2^n} \pm P}{\sqrt{2}}\frac{1}{2^n}\prod_{v=1}^{n}\left(\mathbb{1}_{2^n} + K_v\right)\frac{\mathbb{1}_{2^n} \pm P^\dagger}{\sqrt{2}} && (12.5)\\
&= \frac{1}{2^{n+1}}\left[\left(\mathbb{1}_{2^n} \pm P\right)\prod_{v=1}^{n}\left(\mathbb{1}_{2^n} + K_v\right)\left(\mathbb{1}_{2^n} \pm P\right)\right], && (12.6)
\end{aligned}$$

where for the last equality we used that tensor products of Pauli matrices are Hermitian, *i.e.*, $P^\dagger = P$.

Since $\pm P$ commutes with all generators of $|\psi\rangle$ but K_1 and anticommutes with K_1, we can use the distributive law multiple times to obtain

$$|\psi_\pm\rangle\langle\psi_\pm| = \frac{1}{2^{n+1}}\left[(\mathbb{1}_{2^n} \pm P)\prod_{v=1}^{n}(\mathbb{1}_{2^n} + K_v)(\mathbb{1}_{2^n} \pm P)\right] \tag{12.7}$$

$$= \frac{1}{2^{n+1}}\left[(\mathbb{1}_{2^n} \pm P)(\mathbb{1}_{2^n} + K_1)\prod_{v=2}^{n}(\mathbb{1}_{2^n} + K_v)(\mathbb{1}_{2^n} \pm P)\right] \tag{12.8}$$

$$= \frac{\mathbb{1}_{2^n} \pm P}{2^{n+1}}\left[\prod_{v=1}^{n}(\mathbb{1}_{2^n} + K_v) + (\mathbb{1}_{2^n} + K_1)\prod_{v=2}^{n}(\mathbb{1}_{2^n} + K_v)(\pm P)\right] \tag{12.9}$$

$$= \frac{\mathbb{1}_{2^n} \pm P}{2^{n+1}}\left[\prod_{v=1}^{n}(\mathbb{1}_{2^n} + K_v) + (\pm P)(\mathbb{1}_{2^n} - K_1)\prod_{v=2}^{n}(\mathbb{1}_{2^n} + K_v)\right] \tag{12.10}$$

$$= \frac{\mathbb{1}_{2^n} \pm P}{2^{n+1}}\left[(\mathbb{1}_{2^n} + K_1) + (\pm P)(\mathbb{1}_{2^n} - K_1)\right]\prod_{v=2}^{n}(\mathbb{1}_{2^n} + K_v) \tag{12.11}$$

$$= \frac{\mathbb{1}_{2^n} \pm P}{2^{n+1}}\left[\mathbb{1}_{2^n} + K_1 \pm P \mp PK_1\right]\prod_{v=2}^{n}(\mathbb{1}_{2^n} + K_v) \tag{12.12}$$

$$= \frac{\left[\mathbb{1}_{2^n} + K_1 \pm P \mp PK_1 \pm P \pm PK_1 + \mathbb{1}_{2^n} - K_1\right]}{2^{n+1}}\prod_{v=2}^{n}(\mathbb{1}_{2^n} + K_v) \tag{12.13}$$

$$= \frac{\left[2\mathbb{1}_{2^n} \pm 2P\right]}{2^{n+1}}\prod_{v=2}^{n}(\mathbb{1}_{2^n} + K_v) \tag{12.14}$$

$$= \frac{1}{2^{n}}(\mathbb{1}_{2^n} \pm P)\prod_{v=2}^{n}(\mathbb{1}_{2^n} + K_v), \tag{12.15}$$

where we used $P^2 = \mathbb{1}_{2^n}$ in the third to last equality. This is the same statement as in Equations 4.20 and 12.3 and thus proves our claim.

12.2 Local complementation update rules for continuous variable graph states

In this section we prove local complementation update rules for the adjacency matrix weights of continuous variable graph states.

Continuous variable (CV) graph states are associated with weighted graphs. These weighted graphs $G = (V, E, W)$ consist of a finite set of vertices $V \subsetneq \mathbb{N}$, a set $E \subseteq V \times V$ of edges and a set of weights $W := \{w_e \in \mathbb{R}\}_{e \in E}$. The set of all vertices that have a shared edge with a given vertex a is called the neighborhood of a and denoted by N_a. Weighted graphs have a real-valued and symmetric adjacency matrix with entries

$$A_{i,j} := \begin{cases} w_{(i,j)} & \text{if } (i,j) \in E \\ 0 & \text{if } (i,j) \notin E \end{cases} \tag{12.16}$$

associated with them.

CV graph states can be thought of from this perspective of adjacency matrices and also in the covariance matrix formalism.

A CV graph state of n modes can be prepared from n modes of squeezed light with appropriate entangling controlled-Z operations. In the covariance matrix formalism the symplectic transformation corresponding to such a CV graph state is then defined by single-mode squeezing of strength r and subsequent entangling by controlled-Z operations for each edge of the graph where the strength of the interaction is detemined by the weight of the edge. Taking all modes to be momentum squeezed by r, *i.e.* their variance reduced by a factor of e^{-2r}, and using controlled-Z gates according to the graph's adjacency matrix A this defines the symplectic transformation (*cf.* Equation (2.28) in Reference [MFL11]) given by the $(2n \times 2n)$-matrix

$$\begin{pmatrix} \mathbb{1} & 0 \\ A & \mathbb{1} \end{pmatrix} \begin{pmatrix} e^{r}\mathbb{1} & 0 \\ 0 & e^{-r}\mathbb{1} \end{pmatrix} = \begin{pmatrix} e^{r}\mathbb{1} & 0 \\ e^{r}A & e^{-r}\mathbb{1} \end{pmatrix}. \tag{12.17}$$

Note that all symplectic transformations can be written as

$$S := \begin{pmatrix} U^{-\frac{1}{2}} & 0 \\ VU^{-\frac{1}{2}} & U^{\frac{1}{2}} \end{pmatrix} \tag{12.18}$$

and the corresponding covariance matrix obtained as

$$SS^{T} = \begin{pmatrix} U^{-1} & U^{-1}V \\ VU^{-1} & U + VU^{-1}V \end{pmatrix}. \tag{12.19}$$

With $U = e^{-2r}\mathbb{1}$ and $V = A$ our graph state is therefore described by the covariance matrix

$$\gamma = \begin{pmatrix} e^{2r}\mathbb{1} & e^{2r}A \\ e^{2r}A & e^{-2r}\mathbb{1} + e^{2r}A^{2} \end{pmatrix}, \tag{12.20}$$

where quadratures of the n modes are ordered as

$$x_1, x_2, \ldots, x_n, p_1, p_2, \ldots, p_n. \tag{12.21}$$

Along with the above covariance matrix formalism we use complex-weighted adjacency matrices $Z = V + iU$ to uniquely (up to a phase; *cf.* Appendix A in Reference [MFL11]) describe Gaussian pure states.

Both U and V are real and symmetric, U is positive definite.

A CV graph state as described above is then represented by

$$Z = A + ie^{-2r}\mathbb{1}. \tag{12.22}$$

Note that this new adjacency matrix Z now contains complex-weighted loops, *i.e.*, edges connecting a vertex to itself. We denote the elements of Z as $\Omega_{i,j} := Z_{i,j} = Z_{j,i}$.

The corresponding quantum state $|\psi_Z\rangle$ is defined via nullifier equations

$$(\vec{p} - Z\vec{q})\,|\psi_Z\rangle = 0. \tag{12.23}$$

With the phase gate $P_i(\lambda) = e^{i\frac{\lambda}{2}q_i^2}$ and the Fourier transformed $P_{X_i}(\lambda) = F\,P_i(\lambda)\,F^{-1} = e^{i\frac{\lambda}{2}p_i^2}$, local complementation with respect to vertex $a \in V$ and parameter $\delta \in \mathbb{R}$ is described by the unitary operation (*cf.* Equation (3) in Reference [Zha08])

$$U_a^{\tau}(\delta) = P_{X_a}(-\delta) \prod_{b \in N_a} P_b(\Omega_{a,b}^{2}\delta). \tag{12.24}$$

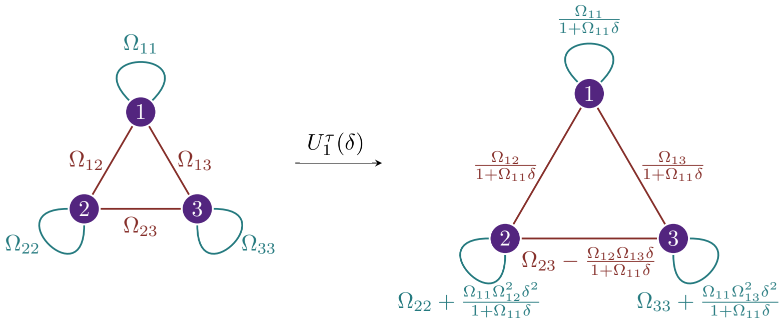

Ω_{11}
1
Ω_{12}
Ω_{13}
2
3
Ω_{23}
Ω_{22}
Ω_{33}
$U_1^\tau(\delta)$
$\frac{\Omega_{11}}{1+\Omega_{11}\delta}$
$\frac{\Omega_{12}}{1+\Omega_{11}\delta}$
$\frac{\Omega_{13}}{1+\Omega_{11}\delta}$
$\Omega_{23} - \frac{\Omega_{12}\Omega_{13}\delta}{1+\Omega_{11}\delta}$
$\Omega_{22} + \frac{\Omega_{11}\Omega_{12}^2\delta^2}{1+\Omega_{11}\delta}$
$\Omega_{33} + \frac{\Omega_{11}\Omega_{13}^2\delta^2}{1+\Omega_{11}\delta}$

Figure 12.1: Local complementation update rules at the example of the three mode GHZ state.

Now, the locally complemented CV graph state $|\psi_{Z'}\rangle := U_a^\tau(\delta)|\psi_Z\rangle$ is again a CV graph state described and by an updated adjacency matrix Z'. We find

$$Z'_{a,a} = \frac{\Omega_{a,a}}{1+\Omega_{a,a}\delta}, \tag{12.25}$$

$$Z'_{a,b} = Z'_{b,a} = \frac{\Omega_{ab}}{1+\Omega_{a,a}\delta}, \tag{12.26}$$

$$Z'_{b,b} = \Omega_{b,b} + \frac{\Omega_{a,a}\Omega_{ab}^2\delta^2}{1+\Omega_{a,a}\delta} \text{ and} \tag{12.27}$$

$$Z'_{b_1,b_2} = Z'_{b_2,b_1} = \Omega_{b_1,b_2} - \frac{\Omega_{a,b_1}\Omega_{a,b_2}\delta}{1+\Omega_{a,a}\delta}, \tag{12.28}$$

where $b_1, b_2(\neq b_1), b \in N_a$ are neighbors of a. For $c_1, c_2 \notin \{a\} \cup N_a$, the edge weights do not change, *i.e.*, $Z'_{c_1c_2} = Z_{c_1c_2}$.

We will now give a detailed derivation of the local complementation update rules for the complex adjacency matrix Z using the example of the three mode GHZ state $|\psi_Z\rangle$.

The resulting rules are visualized in Figure 12.1. Since the corresponding graph is fully connected, we have the matrix representation

$$Z = \begin{pmatrix} \Omega_{1,1} & \Omega_{1,2} & \Omega_{1,3} \\ \Omega_{1,2} & \Omega_{2,2} & \Omega_{2,3} \\ \Omega_{1,3} & \Omega_{2,3} & \Omega_{3,3} \end{pmatrix} \tag{12.29}$$

This adjacency matrix defines the nullifier equations (*cf.* Eq. 12.23) of $|\psi_Z\rangle$ as $\left(\vec{p} - Z\vec{q}\right)|\psi_Z\rangle = 0$, *i.e.*,

$$\textcircled{1}\,|\psi_Z\rangle := (p_1 - \Omega_{1,1}q_1 - \Omega_{1,2}q_2 - \Omega_{1,3}q_3)\,|\psi_Z\rangle = 0 \tag{12.30}$$

$$\textcircled{2}\,|\psi_Z\rangle := (p_2 - \Omega_{1,2}q_1 - \Omega_{2,2}q_2 - \Omega_{2,3}q_3)\,|\psi_Z\rangle = 0 \tag{12.31}$$

$$\textcircled{3}\,|\psi_Z\rangle := (p_3 - \Omega_{1,3}q_1 - \Omega_{2,3}q_2 - \Omega_{3,3}q_3)\,|\psi_Z\rangle = 0, \tag{12.32}$$

where we introduced $\textcircled{i} := p_i - \sum_j Z_{i,j}q_j$ as a shorthand notation for the expressions in parentheses.

As stated in Equation 12.24, local complementation with respect to vertex a and parameter δ is described by the unitary operation (*cf.* also

Equation (3) in Reference [Zha08])

$$U_a^{\tau}(\delta) = P_{X_a}(-\delta) \prod_{b\in N_a} P_b(\Omega^2_{ab}\delta), \tag{12.33}$$

where $P_i(\lambda) = e^{i\frac{\lambda}{2}q_i^2}$ is the phase gate and $P_{X_i}(\lambda) = F\,P_i(\lambda)\,F^{-1} = e^{i\frac{\lambda}{2}p_i^2}$ its Fourier transform.

Without loss of generality we choose $a = 1$ and thus have $N_1 = \{2, 3\}$, that is, we apply the unitary

$$U_1^{\tau}(\delta) = P_{X_1}(-\delta)\,P_2(\Omega^2_{1,2}\delta)\,P_3(\Omega^2_{1,3}\delta). \tag{12.34}$$

The commutation relation $[q_k, p_l] = i\delta_{k,l}$ (we choose $\hbar = 1$ and $\delta_{k,l}$ is the Kronecker-delta) directly implies

$$[q_k, p_l^n] = inp_l^{n-1}\delta_{kl} \tag{12.35}$$

$$[p_k, q_l^n] = -inq_l^{n-1}\delta_{kl} \tag{12.36}$$

for $n \in \{0, 1, 2, \dots\}$ and thus

$$[P_{X_k}(\lambda), q_l] = \lambda p_l\,P_{X_k}(\lambda)\delta_{kl} \tag{12.37}$$

$$[P_{X_k}(\lambda), p_l] = 0 \tag{12.38}$$

$$[P_k(\lambda), p_l] = -\lambda q_l\,P_k(\lambda)\delta_{kl} \tag{12.39}$$

$$[P_k(\lambda), q_l] = 0. \tag{12.40}$$

These relations allow us to determine the matrix elements of the adjacency matrix Z' of $|\psi_{Z'}\rangle := U_1^{\tau}(\delta)|\psi_Z\rangle$. With $\left(\vec{p} - Z\vec{q}\right)|\psi_Z\rangle = 0$ and $U := U_1^{\tau}(\delta)$ unitary, we find transformed nullifier equations

$$U\left(\vec{p} - Z\vec{q}\right)U^{\dagger}U|\psi_Z\rangle = 0. \tag{12.41}$$

Our shorthand $\textcircled{i} := p_i - \sum_j Z_{i,j}q_j$ allows us to write

$$U\,\textcircled{i}\,U^{\dagger} = \textcircled{i} + [U, \textcircled{i}]U^{\dagger} \tag{12.42}$$

and we can express the above nullifier equations as

$$\left(\textcircled{i} + [U, \textcircled{i}]U^{\dagger}\right)|\psi_{Z'}\rangle = 0. \tag{12.43}$$

Further, Equations 12.34 and 12.37 allow us to calculate

$$[U, \textcircled{1}]U^{\dagger} = \Omega_{1,1}\delta p_1, \tag{12.44}$$

$$[U, \textcircled{2}]U^{\dagger} = -\Omega^2_{1,2}\delta q_2 + \Omega_{1,2}\delta p_1, \tag{12.45}$$

$$[U, \textcircled{3}]U^{\dagger} = -\Omega^2_{1,3}\delta q_3 + \Omega_{13}\delta p_1. \tag{12.46}$$

With this we can determine the elements of the adjacency matrix Z' corresponding to $|\psi_{Z'}\rangle := U_1^{\tau}(\delta)|\psi_Z\rangle$ by comparing coefficients to the three equations $\left(p_i - \sum_j Z'_{i,j}q_j\right)|\psi_{Z'}\rangle = 0$.

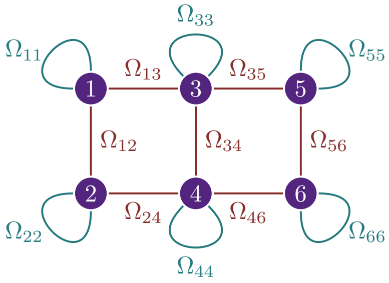


Figure 12.2: The CV butterfly network.

For $i = 1$, Equation 12.43 is

$$\left(p_1 - \underbrace{\frac{\Omega_{1,1}}{1+\Omega_{1,1}\delta}}_{=Z'_{1,1}} q_1 - \underbrace{\frac{\Omega_{1,2}}{1+\Omega_{1,1}\delta}}_{=Z'_{1,2}} q_2 - \underbrace{\frac{\Omega_{1,3}}{1+\Omega_{1,1}\delta}}_{=Z'_{1,3}} q_3 \right) |\psi_{Z'}\rangle = 0, \quad (12.47)$$

For $i = 2$ we find

$$\left(\Omega_{1,2}\delta p_1 + p_2 - \Omega_{1,2} q_1 - (\Omega_{2,2} + \Omega_{1,2}^2 \delta) q_2 - \Omega_{2,3} q_3 \right) |\psi_{Z'}\rangle = 0, \quad (12.48)$$

which together with Equation 12.47 implies that

$$p_2 - \underbrace{\frac{\Omega_{1,2}}{1+\Omega_{11}\delta}}_{=Z'_{2,1}} q_1 - \underbrace{\left(\Omega_{2,2} + \frac{\Omega_{1,1}\Omega_{1,2}^2\delta^2}{1+\Omega_{1,1}\delta} \right)}_{=Z'_{2,2}} q_2 - \underbrace{\left(\Omega_{2,3} - \frac{\Omega_{1,2}\Omega_{1,3}\delta}{1+\Omega_{1,1}\delta} \right)}_{=Z'_{2,3}} q_3$$

nullifies $|\psi_{Z'}\rangle$.

Finally, for $i = 3$ we have that

$$p_3 - \underbrace{\frac{\Omega_{1,3}}{1+\Omega_{1,1}\delta}}_{=Z'_{3,1}} q_1 - \underbrace{\left(\Omega_{23} - \frac{\Omega_{1,2}\Omega_{13}\delta}{1+\Omega_{11}\delta} \right)}_{=Z'_{32}} q_2 - \underbrace{\left(\Omega_{33} + \frac{\Omega_{11}\Omega_{13}^2\delta^2}{1+\Omega_{11}\delta} \right)}_{=Z'_{33}} q_3$$

nullifies $|\psi_{Z'}\rangle$.

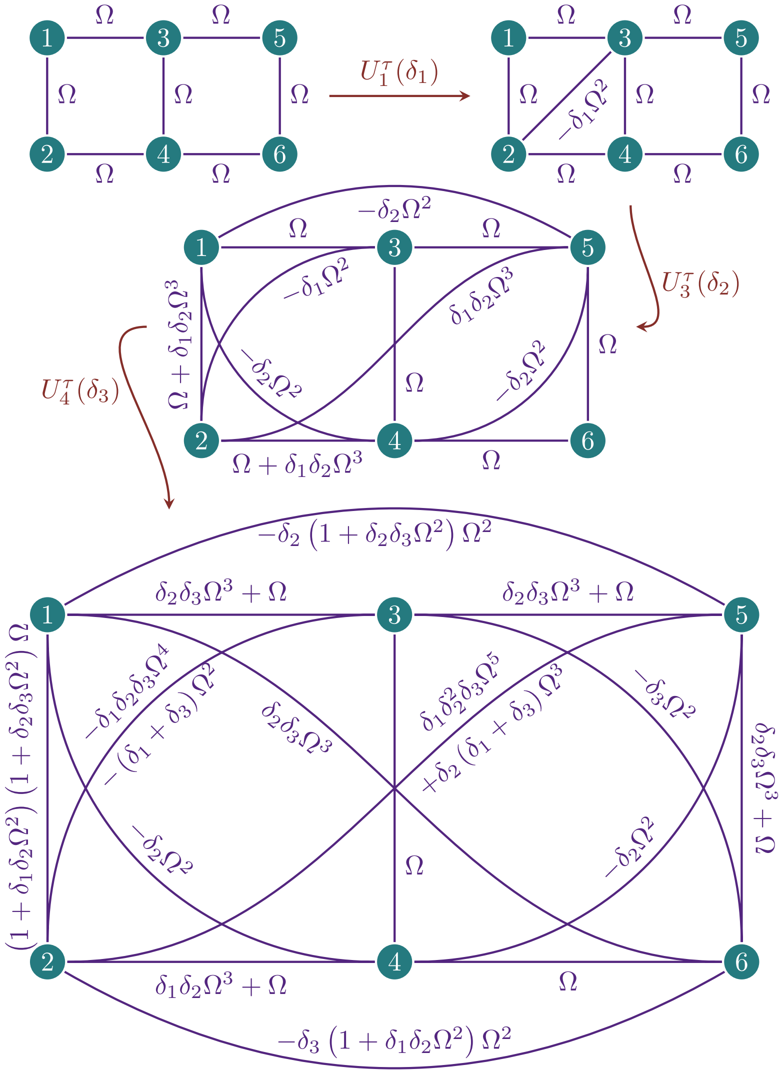
To sum up, we have found

$$Z' = \begin{pmatrix} \frac{\Omega_{1,1}}{1+\Omega_{1,1}\delta} & \frac{\Omega_{1,2}}{1+\Omega_{1,1}\delta} & \frac{\Omega_{1,3}}{1+\Omega_{1,1}\delta} \\ \frac{\Omega_{1,2}}{1+\Omega_{1,1}\delta} & \Omega_{2,2} + \frac{\Omega_{1,1}\Omega_{1,2}^2\delta^2}{1+\Omega_{1,1}\delta} & \Omega_{2,3} - \frac{\Omega_{1,2}\Omega_{1,3}\delta}{1+\Omega_{1,1}\delta} \\ \frac{\Omega_{1,3}}{1+\Omega_{1,1}\delta} & \Omega_{2,3} - \frac{\Omega_{1,2}\Omega_{1,3}\delta}{1+\Omega_{1,1}\delta} & \Omega_{3,3} + \frac{\Omega_{1,1}\Omega_{1,3}^2\delta^2}{1+\Omega_{1,1}\delta} \end{pmatrix}. \quad (12.49)$$

Note that Z' is again a symmetric matrix.

The (in)finitely squeezed butterfly network

Figure 12.2 shows the most general version of CV graph state from finitely squeezed resources, where the underlying graph is the so-called butterfly network.



Ω
$U_1^{\tau}(\delta_1)$
$-\delta_1\Omega^2$
$-\delta_2\Omega^2$
$U_3^{\tau}(\delta_2)$
$\delta_1\delta_2\Omega^3$
$\Omega+\delta_1\delta_2\Omega^3$
$U_4^{\tau}(\delta_3)$
$-\delta_2\left(1+\delta_2\delta_3\Omega^2\right)\Omega^2$
$\delta_2\delta_3\Omega^3+\Omega$
$\left(1+\delta_1\delta_2\Omega^2\right)\left(1+\delta_2\delta_3\Omega^2\right)\Omega$
$-\delta_1\delta_2\delta_3\Omega^4$
$-\left(\delta_1+\delta_3\right)\Omega^2$
$\delta_2\delta_3\Omega^3$
$\delta_1\delta_2^2\delta_3\Omega^5$
$+\delta_2\left(\delta_1+\delta_3\right)\Omega^3$
$-\delta_3\Omega^2$
$\delta_1\delta_2\Omega^3+\Omega$
$-\delta_3\left(1+\delta_1\delta_2\Omega^2\right)\Omega^2$
1
2
3
4
5
6

Figure 12.3: Transformation of the perfect –that is to say infinitely squeezed– butterfly network via local complementation on modes 1, 3 and 4 with parameters $\delta_1, \delta_2, \delta_3$. This is the continuous variable version of Figure 5.2 from the main text. The δ parameters can be chosen to set the weights of the undesired edges (*e.g.* $(1,2)$ and $(5,6)$) in the final graph to zero.

The corresponding matrix representation is given by

$$Z_{\mathrm{B}} := \begin{pmatrix} \Omega_{1,1} & \Omega_{1,2} & \Omega_{1,3} & 0 & 0 & 0 \\ \Omega_{1,2} & \Omega_{2,2} & 0 & \Omega_{2,4} & 0 & 0 \\ \Omega_{1,3} & 0 & \Omega_{3,3} & \Omega_{3,4} & \Omega_{3,5} & 0 \\ 0 & \Omega_{24} & \Omega_{3,4} & \Omega_{4,4} & 0 & \Omega_{4,6} \\ 0 & 0 & \Omega_{3,5} & 0 & \Omega_{5,5} & \Omega_{5,6} \\ 0 & 0 & 0 & \Omega_{4,5} & \Omega_{5,6} & \Omega_{6,6} \end{pmatrix}, \tag{12.50}$$

where the diagonal becomes zero in the limit of infinitely squeezed resources.

While such ideal (or *perfect*) CV graph states are not experimentally realizable as they would require an infinite amount of energy, they are instructive to discover strategies how to locally transform finitely squeezed ones.

12.3 Proofs Anonymous Quantum Conference Key Agreement

Below we present all proofs for the ACKA protocol, which we have removed from the presentation in the main text for clarity.

12.4 ACKA proof structure

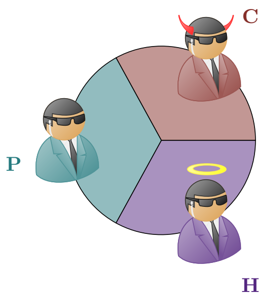
The following sections closely follow the text of Reference [HJP20], which was written by both myself and my co-authors. ⇣ ⇣ ⇣

Here we prove the anonymity of our protocol. We first repeat the definition of anonymity from Chapter 9.

Definition 12.1 (Anonymity) *A protocol is anonymous from the perspective of Eve if for all subsets* $\mathbf{G} \subset \mathbf{N}$

$$\Pr\left(\mathbf{G} = \mathbf{P} \mid \mathcal{I}^{+}_{\text{Eve}}, \mathcal{I}_{\text{Eve}}\right) = \Pr(\mathbf{G} = \mathbf{P} \mid \mathcal{I}_{\text{Eve}}), \qquad (12.51)$$

where $\mathcal{I}^{+}_{\text{Eve}}$ *is the information that becomes available to Eve during the protocol and* $\mathcal{I}_{\text{Eve}}$ *is both the information that Eve has beforehand and trivial information that she obtains about the parties that she corrupts.*



The set $\mathbf{N}$ of all parties in the network is partitioned into three disjoint sets such that $\mathbf{N} = \mathbf{P} \cup \mathbf{H} \cup \mathbf{C}$.

In order to satisfy Equation 12.51, $\mathcal{I}^{+}_{\text{Eve}}$ should not change Eve's probability distribution of uncovering the partitioning of $\mathbf{N}$ into its constituents; it does not reveal anything about $\mathbf{P}$, $\mathbf{H}$ or –implicitly– about $\mathbf{C}$. Apart from the trivial attacker A we consider three different types of Eve, namely any party in $\mathbf{P} \setminus A$ or $\mathbf{H}$ or all parties in $\mathbf{C}$.

We prove anonymity for all involved subprotocols separately; as a shorthand to refer to them, we introduce the symbols ★ (`AME`), ✓ (`Verification`) and 🔑 (`KeyGen`).

For each of the subprotocols, we give arguments to prove anonymity for all possible roles within the protocol that Eve may try to uncover –with respect to all types of Eve. Each argument is applicable to multiple Eve/role-combinations and is sequentially labelled by indexing the symbol for easy reference. Table 12.1 shows the structure of our proof summarizing all arguments for each Eve/role-combination.

Table 12.1: The rows are labeled by the types of Eve and the columns by the roles that Eve may try to uncover. The first row is mostly trivial, since the protocol is designed such that A chooses the partitioning $\mathbf{N} = \mathbf{P} \cup \mathbf{P}$ herself and it is irrelevant that she is unaware of who in $\mathbf{P}$ is colluding. The arguments corresponding to the symbols are given in Sections 12.5, 12.6 and 12.7. As an example, the first proof of the `AME` protocol is referred to as $\bigstar_1$ and applies to the case where the roles of the non-participants in $\mathbf{H}$ are protected from either any $B_i \in \mathbf{P} \setminus A$ as Eve or the parties in $\mathbf{C}$ as Eve.

Eve role	A	$B_i \in \mathbf{P} \setminus A$	$P_j \in \mathbf{H}$	$P_k \in \mathbf{C}$
A	trivial	trivial	irrelevant	irrelevant
$B_i \in \mathbf{P} \setminus A$	$\bigstar_3$ $\checkmark_2$ 🔑$_3$	$\bigstar_3$ $\checkmark_2$ 🔑$_3$	$\bigstar_1$ $\checkmark_2$ 🔑$_1$	$\bigstar_3$ $\checkmark_2$ 🔑$_1$
$P_j \in \mathbf{H}$	$\bigstar_2$ $\checkmark_1$ 🔑$_1$	$\bigstar_2$ $\checkmark_1$ 🔑$_1$	$\bigstar_2$ $\checkmark_1$ 🔑$_2$	$\bigstar_2$ $\checkmark_1$ 🔑$_1$
$P_k \in \mathbf{C}$	$\bigstar_3$ $\checkmark_3$ 🔑$_1$	$\bigstar_3$ $\checkmark_3$ 🔑$_1$	$\bigstar_1$ $\checkmark_3$ 🔑$_1$	trivial

For the `Notification` protocol we refer to the original paper by Broadbent and Tapp. The `AME` protocol and the `Verification` protocol will be examined in Section 12.5 and 12.6. The `KeyGen` subprotocol does not involve any public communication and will be examined in Section 12.7.

To prove our claim we consider the following two aspects:

The *public communication* (*cf.* Table 12.2) throughout the protocol does not help Eve to reveal the roles of the participating parties. We prove this by showing that all public communication is indistinguishable from Eve's point of view. As A announces only uniformly random and uncorrelated bits, we will show the same for the parties in $\mathbf{P} \setminus A$, $\mathbf{H}$ and $\mathbf{C}$ from Eve's perspective.

Likewise, the *quantum states* accessible to Eve do not help her to reveal the roles of the participating parties, even given access to the public communication. This means that the post-measurement states of Eve can neither be correlated with the measurement outcomes of other parties, nor with any direct information regarding their roles. Note that the global quantum state may encode such information regarding the roles as long as it is not accessible to anyone but Alice.

	AME	Verification
A	random bit r_0	random bits (b_0, o_0)
$B_i \in \mathbf{P} \setminus A$	random bit r_i	random bit b_i, outcome bit o_i
$P_j \in \mathbf{H}$	outcome bit x_j	random bits (b_j, o_j)
$P_k \in \mathbf{C}$	arbitrary bit $\tilde{x}_k$	arbitrary bits $(\tilde{b}_k, \tilde{o}_k)$

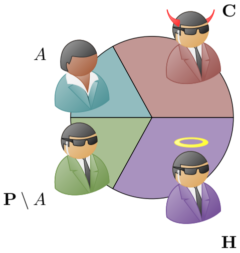


Table 12.2: Overview of all public communication for any party in $\mathbf{N} := \mathbf{P} \cup \mathbf{H} \cup \mathbf{C}$ when running the AME and Verification protocols. The communication summarized in the two columns needs to be indistinguishable from the perspective of any Eve. Since A only announces uniformly random and uncorrelated bits, all other communication must follow the same probability distribution. Only the communication from $\mathbf{C}$ can in principle diverge –should they choose not to hide their identities.

12.5 Anonymity during the AME protocol

At the start of the AME protocol, the shared quantum state is given by

$$|\mathbf{N}\rangle \approx_\epsilon \frac{1}{\sqrt{2}} \left(|0 \cdots 0\rangle_{\mathbf{P} \cup \mathbf{H}} \otimes |\Psi\rangle_{\mathbf{C}} + |1 \cdots 1\rangle_{\mathbf{P} \cup \mathbf{H}} \otimes |\Phi\rangle_{\mathbf{C}} \right). \tag{12.52}$$

While the AME protocol requires both $\mathbf{H}$ and $\mathbf{C}$ to measure, the parties in $\mathbf{C}$ might not measure and announce something unrelated to their arbitrary actions on the quantum state –therefore we now only calculate the probability of the measurement outcomes $\mu_{\mathbf{H}}^{\alpha} = \{\mu_j \mid j \in \mathbf{H}\}$ of $\mathbf{H}$ taking values $x_{\mathbf{H}}^{\alpha} = \{x_i^{\alpha}\} \in \{0,1\}^{|\mathbf{H}|}$.

We want to show that they are uniformly random and that there are no correlations between the outcomes and any Eve that she might exploit, where Eve could be anyone in the network but Alice. That is, we want to show that

$$\Pr\left(\mu_{\mathbf{H}}^{\alpha} = x_{\mathbf{H}}^{\alpha} \mid \mathcal{I}_{\text{Eve}}^{+}, \mathcal{J}_{\text{Eve}}\right) = \Pr\left(\mu_{\mathbf{H}}^{\alpha} = x_{\mathbf{H}}^{\alpha}\right) = \frac{1}{2^{|\mathbf{H}|}}, \tag{12.53}$$

where the second equality asserts that the probability distribution of the measurement outcomes is uniform, and the first equality implies that there are no correlations between the information accessible to Eve –including her quantum state– and the measurement outcomes.

Moreover, we want to show that the post-measurement state has no further correlations regarding the roles of the parties that are accessible or exploitable by Eve.

The projective measurements (*cf.* Definition 2.18) on **H** in the `AME` protocol have outcomes $\{x^\alpha_{\mathbf{H}}\}$ and associated projectors

$$X^\alpha_{\mathbf{H}} := H_{\mathbf{H}}|x^\alpha_{\mathbf{H}}\rangle\langle x^\alpha_{\mathbf{H}}|_{\mathbf{H}}H_{\mathbf{H}} = \bigotimes_{j\in\mathbf{H}} H_j|x^\alpha_j\rangle\langle x^\alpha_j|_j H_j, \tag{12.54}$$

which results in the probability $\Pr(\mu^\alpha_{\mathbf{H}} = x^\alpha_{\mathbf{H}})$ of the measurement outcome $\mu^\alpha_{\mathbf{H}}$ taking the value $x^\alpha_{\mathbf{H}}$ being determined by

$$\begin{align}
2\Pr(\mu^\alpha_{\mathbf{H}} = x^\alpha_{\mathbf{H}}) = 2\operatorname{Tr}\left[X^\alpha_{\mathbf{H}}|\mathbf{N}\rangle\langle\mathbf{N}|\right] \tag{12.55}\\
= \operatorname{Tr}\left[\,(|0\cdots0\rangle\langle0\cdots0|_{\mathbf{P}})\,\right]\operatorname{Tr}\left[X^\alpha_{\mathbf{H}}|0\cdots0\rangle\langle0\cdots0|_{\mathbf{H}}\right]\operatorname{Tr}\left[|\Psi\rangle\langle\Psi|_{\mathbf{C}}\right] \tag{12.56}\\
+\operatorname{Tr}\left[\,(|0\cdots0\rangle\langle1\cdots1|_{\mathbf{P}})\,\right]\operatorname{Tr}\left[X^\alpha_{\mathbf{H}}|0\cdots0\rangle\langle1\cdots1|_{\mathbf{H}}\right]\operatorname{Tr}\left[|\Psi\rangle\langle\Phi|_{\mathbf{C}}\right] \tag{12.57}\\
+\operatorname{Tr}\left[\,(|1\cdots1\rangle\langle0\cdots0|_{\mathbf{P}})\,\right]\operatorname{Tr}\left[X^\alpha_{\mathbf{H}}|1\cdots1\rangle\langle0\cdots0|_{\mathbf{H}}\right]\operatorname{Tr}\left[|\Phi\rangle\langle\Psi|_{\mathbf{C}}\right] \tag{12.58}\\
+\operatorname{Tr}\left[\,(|1\cdots1\rangle\langle1\cdots1|_{\mathbf{P}})\,\right]\operatorname{Tr}\left[X^\alpha_{\mathbf{H}}|1\cdots1\rangle\langle1\cdots1|_{\mathbf{H}}\right]\operatorname{Tr}\left[|\Phi\rangle\langle\Phi|_{\mathbf{C}}\right] \tag{12.59}
\end{align}$$

and thus as

$$\begin{align}
\Pr(\mu^\alpha_{\mathbf{H}} = x^\alpha_{\mathbf{H}}) =& \frac{1}{2}\operatorname{Tr}\Big[\left(\bigotimes_{j\in\mathbf{H}} H_j|x^\alpha_j\rangle\langle x^\alpha_j|_j H_j\right)|0\cdots0\rangle\langle0\cdots0|_{\mathbf{H}}\Big] \tag{12.60}\\
&+\frac{1}{2}\operatorname{Tr}\Big[\left(\bigotimes_{j\in\mathbf{H}} H_j|x^\alpha_j\rangle\langle x^\alpha_j|_j H_j\right)|1\cdots1\rangle\langle1\cdots1|_{\mathbf{H}}\Big] \tag{12.61}\\
=& \frac{1}{2}\left(\prod_{i\in\mathbf{H}}|\langle x^\alpha_i||+\rangle|^2 + \prod_{i\in\mathbf{H}}|\langle x^\alpha_i||-\rangle|^2\right) \tag{12.62}\\
=& \frac{1}{2}\left(\frac{1}{2^{|\mathbf{H}|}} + \frac{1}{2^{|\mathbf{H}|}}\right) = \frac{1}{2^{|\mathbf{H}|}}. \tag{12.63}
\end{align}$$

This satisfies the second equality in Equation 12.53, showing that the measurement outcomes are uniformly random, thereby ensuring that all the communication of the `AME` column of Table 12.2 is indistinguishable –excluding the trivial case where the dishonest and colluding non-participants in **C** reveal themselves.

The global post-measurement state $\rho_{\texttt{postAME}}$ is then

$$\begin{align}
\rho_{\texttt{postAME}} = X^\alpha_{\mathbf{H}}|\mathbf{N}\rangle\langle\mathbf{N}|X^\alpha_{\mathbf{H}} \tag{12.64}\\
=\frac{1}{2}\,(|0\cdots0\rangle\langle0\cdots0|_{\mathbf{P}})\otimes X^\alpha_{\mathbf{H}}|0\cdots0\rangle\langle0\cdots0|_{\mathbf{H}}X^\alpha_{\mathbf{H}}\otimes|\Psi\rangle\langle\Psi|_{\mathbf{C}} \tag{12.65}\\
+\frac{1}{2}\,(|0\cdots0\rangle\langle1\cdots1|_{\mathbf{P}})\otimes X^\alpha_{\mathbf{H}}|0\cdots0\rangle\langle1\cdots1|_{\mathbf{H}}X^\alpha_{\mathbf{H}}\otimes|\Psi\rangle\langle\Phi|_{\mathbf{C}} \tag{12.66}\\
+\frac{1}{2}\,(|1\cdots1\rangle\langle0\cdots0|_{\mathbf{P}})\otimes X^\alpha_{\mathbf{H}}|1\cdots1\rangle\langle0\cdots0|_{\mathbf{H}}X^\alpha_{\mathbf{H}}\otimes|\Phi\rangle\langle\Psi|_{\mathbf{C}} \tag{12.67}\\
+\frac{1}{2}\,(|1\cdots1\rangle\langle1\cdots1|_{\mathbf{P}})\otimes X^\alpha_{\mathbf{H}}|1\cdots1\rangle\langle1\cdots1|_{\mathbf{H}}X^\alpha_{\mathbf{H}}\otimes|\Phi\rangle\langle\Phi|_{\mathbf{C}}, \tag{12.68}
\end{align}$$

which can be rewritten as

$$\begin{aligned}
\rho_{\texttt{postAME}} =& \frac{1}{2}\left(|0\cdots0\rangle\langle0\cdots0|_{\mathbf{P}}\right)\otimes|\mathbf{H}\rangle\langle\mathbf{H}|\otimes|\Psi\rangle\langle\Psi|_{\mathbf{C}} && (12.69)\\
+&\frac{1}{2}\left(|0\cdots0\rangle\langle1\cdots1|_{\mathbf{P}}\right)\otimes(-1)^{\Delta(x^{\alpha}_{\mathbf{H}})}|\mathbf{H}\rangle\langle\mathbf{H}|\otimes|\Psi\rangle\langle\Phi|_{\mathbf{C}} && (12.70)\\
+&\frac{1}{2}\left(|1\cdots1\rangle\langle0\cdots0|_{\mathbf{P}}\right)\otimes(-1)^{\Delta(x^{\alpha}_{\mathbf{H}})}|\mathbf{H}\rangle\langle\mathbf{H}|\otimes|\Phi\rangle\langle\Psi|_{\mathbf{C}} && (12.71)\\
+&\frac{1}{2}\left(|1\cdots1\rangle\langle1\cdots1|_{\mathbf{P}}\right)\otimes|\mathbf{H}\rangle\langle\mathbf{H}|\otimes|\Phi\rangle\langle\Phi|_{\mathbf{C}} && (12.72)\\
=&|\mathbf{N}_{\texttt{postAME}}\rangle\langle\mathbf{N}_{\texttt{postAME}}|, && (12.73)
\end{aligned}$$

where $|\mathbf{H}\rangle := \bigotimes_{i\in\mathbf{H}} H_i|x^{\alpha}_{i}\rangle_i$ is the post-measurement state associated with measurement outcome $x^{\alpha}_{\mathbf{H}}$ and $|\mathbf{N}_{\texttt{postAME}}\rangle$ is the pure state vector

$$\frac{1}{\sqrt{2}}\left(|0\cdots0\rangle_{\mathbf{P}}\otimes|\Psi\rangle_{\mathbf{C}}+(-1)^{\Delta(x^{\alpha}_{\mathbf{H}})}|1\cdots1\rangle_{\mathbf{P}}\otimes|\Phi\rangle_{\mathbf{C}}\right)\otimes|\mathbf{H}\rangle, \qquad (12.74)$$

showing that the only correlation between the measurement outcome and the state on $\mathbf{P}\cup\mathbf{C}$ is in the phase, where one could in principle learn the parity of the measurement outcome $x^{\alpha}_{\mathbf{H}}$.

However, any such phase estimation is impossible if one does not have access to the complete state (*i.e.* tracing out $\mathbf{P}$ that does not collude with Eve results in a state on $\mathbf{C}$ that is uncorrelated with the measurement outcome $x^{\alpha}_{\mathbf{H}}$). This means that the post-measurement state of any attacker in $\mathbf{P}\setminus A$ or $\mathbf{C}$ is uncorrelated from the measurement outcome $x^{\alpha}_{\mathbf{H}}$ and the roles of $\mathbf{H}$. Therefore, for either of these types of Eve everyone in $\mathbf{H}$ remains anonymous (*cf.* ★$_1$ in Table 12.1).

Furthermore, $\mathbf{H}$ is disentangled from the rest of the network and $|\mathbf{H}\rangle$ itself is separable over the constituents of $\mathbf{H}$. Therefore, nobody in $\mathbf{H}$ can learn anything about the roles of any other party in the network. We can conclude that for Eve in $\mathbf{H}$, Definition 9.1 holds for any of the subsets of $\mathbf{N}$ (*cf.* ★$_2$ in Table 12.1).

When Eve is a party in $\mathbf{P}\setminus A$, the roles of the parties in either $\mathbf{P}$ or $\mathbf{C}$ are hidden because the relevant correlations of the state are unchanged by running the `AME` protocol –they essentially share a GHZ state, possibly including some additional phase, and therefore there are no revealing correlations available to anyone but Alice, meaning that here Definition 9.1 also holds. The exact same argument holds for Eve in $\mathbf{C}$ with respect to the anonymity of $\mathbf{P}$ (*cf.* ★$_3$ in Table 12.1).

12.6 Anonymity during the `Verification` rounds

At the start of the `Verification` round, the state is the post-measurement state from Equation 12.74, up to the correction by A. We allow for a faulty correction and therefore keep the phase arbitrary in the following analysis, denoting the phase as $(-1)^{\Delta}=\pm1$.

We again calculate the probability that, based on some basis choice $\{b_i\}$ and given the AME measurement outcome $x^\alpha_{\mathbf{H}}$, the measurement outcome $\mu^\alpha = \{\mu_j \mid j \in \mathbf{P} \setminus A\}$ takes some particular value $o^\alpha = \{o^\alpha_i\} \in \{0,1\}^{|\mathbf{P}\setminus A|}$, show that the outcome is uniformly random and that there are no correlations between the outcome and the quantum states of all possible Eves. That is, we want to show that

$$\Pr\left(\mu^\alpha = o^\alpha \mid \mathcal{I}^+_{\mathrm{Eve}}, \mathcal{I}_{\mathrm{Eve}}\right) = \Pr\left(\mu^\alpha = o^\alpha\right) = \frac{1}{2^{|\mathbf{P}\setminus A|}}, \tag{12.75}$$

where Eve may be anyone in $\mathbf{P} \setminus A$, $\mathbf{H}$ or $\mathbf{C}$. Again, we show that the post-measurement states do not have correlations regarding the roles of the parties which are exploitable by anyone in $\mathbf{P} \setminus A$, $\mathbf{H}$ or $\mathbf{C}$.

Each measurement outcome is associated with a corresponding measurement projector $O^\alpha_{\mathbf{P}\setminus A}$, which depends on the basis choice $\{b_i\}$. Explicitly, we define

$$O^\alpha_{\mathbf{P}\setminus A}(\{b_i\}) := \left[\bigotimes_{\{i\in\mathbf{P}\setminus A \mid b_i=0\}} H_i |o^\alpha_i\rangle\langle o^\alpha_i| H_i\right] \tag{12.76}$$

$$\otimes \left[\bigotimes_{\{i\in\mathbf{P}\setminus A \mid b_i=1\}} \sqrt{Z_i} H_i |o^\alpha_i\rangle\langle o^\alpha_i| H_i \sqrt{Z_i}^\dagger\right]. \tag{12.77}$$

Hence, for any outcome $x^\alpha_{\mathbf{H}}$ during the AME protocol, the probability of the measurement outcome μ^α being equal to o^α can be calculated with $\mathrm{Tr}\left[|0\rangle\langle 0|_A\right] = 1$, $\mathrm{Tr}\left[|0\rangle\langle 1|_A\right] = 0$, $\mathrm{Tr}\left[|1\rangle\langle 0|_A\right] = 0$ and $\mathrm{Tr}\left[|1\rangle\langle 1|_A\right] = 1$ (note that Δ may depend on $x^\alpha_{\mathbf{H}}$). We find

$$\Pr\left(\mu^\alpha = m^\alpha\right) = \mathrm{Tr}\left[O^\alpha |\mathbf{N}_{\texttt{postAME}}\rangle\langle \mathbf{N}_{\texttt{postAME}}|\right] \tag{12.78}$$

$$= \frac{1}{2}\, \mathrm{Tr}\left[O^\alpha |0\cdots 0\rangle\langle 0\cdots 0|_{\mathbf{P}\setminus A}\right] \mathrm{Tr}\left[|\mathbf{H}\rangle\langle \mathbf{H}|\right] \mathrm{Tr}\left[|\Psi\rangle\langle \Psi|_{\mathbf{C}}\right] \tag{12.79}$$

$$+ (-1)^\Delta \frac{0}{2}\, \mathrm{Tr}\left[O^\alpha |0\cdots 0\rangle\langle 1\cdots 1|_{\mathbf{P}\setminus A}\right] \mathrm{Tr}\left[|\mathbf{H}\rangle\langle \mathbf{H}|\right] \mathrm{Tr}\left[|\Psi\rangle\langle \Phi|_{\mathbf{C}}\right] \tag{12.80}$$

$$+ (-1)^\Delta \frac{0}{2}\, \mathrm{Tr}\left[O^\alpha |1\cdots 1\rangle\langle 0\cdots 0|_{\mathbf{P}\setminus A}\right] \mathrm{Tr}\left[|\mathbf{H}\rangle\langle \mathbf{H}|\right] \mathrm{Tr}\left[|\Phi\rangle\langle \Psi|_{\mathbf{C}}\right] \tag{12.81}$$

$$+ \frac{1}{2}\, \mathrm{Tr}\left[O^\alpha |1\cdots 1\rangle\langle 1\cdots 1|_{\mathbf{P}\setminus A}\right] \mathrm{Tr}\left[|\mathbf{H}\rangle\langle \mathbf{H}|\right] \mathrm{Tr}\left[|\Phi\rangle\langle \Phi|_{\mathbf{C}}\right] \tag{12.82}$$

and therefore

$$\Pr\left(\mu^\alpha = m^\alpha\right) \tag{12.83}$$

$$= \frac{1}{2}\left(\mathrm{Tr}\left[O^\alpha |0\cdots 0\rangle\langle 0\cdots 0|_{\mathbf{P}\setminus A}\right] + \mathrm{Tr}\left[O^\alpha |1\cdots 1\rangle\langle 1\cdots 1|_{\mathbf{P}\setminus A}\right]\right). \tag{12.84}$$

Substituting O^α we obtain

$$\Pr\left(\mu^{\alpha} = m^{\alpha}\right) \tag{12.85}$$

$$= \frac{1}{2} \prod_{\{i \in \mathbf{P} \setminus A | b_i = 0\}} \langle o_i^{\alpha} | H_i | 0 \rangle \langle 0 | H_i | o_i^{\alpha} \rangle \tag{12.86}$$

$$\times \prod_{\{i \in \mathbf{P} \setminus A | b_i = 1\}} \langle o_i^{\alpha} | H_i \sqrt{Z_i}^{\dagger} | 0 \rangle \langle 0 | \sqrt{Z_i} H_i | o_i^{\alpha} \rangle \tag{12.87}$$

$$+ \frac{1}{2} \prod_{\{i \in \mathbf{P} \setminus A | b_i = 0\}} \langle o_i^{\alpha} | H_i | 1 \rangle \langle 1 | H_i | o_i^{\alpha} \rangle \tag{12.88}$$

$$\times \prod_{\{i \in \mathbf{P} \setminus A | b_i = 1\}} \langle o_i^{\alpha} | H_i \sqrt{Z_i}^{\dagger} | 1 \rangle \langle 1 | \sqrt{Z_i} H_i | o_i^{\alpha} \rangle, \tag{12.89}$$

$$= \frac{1}{2} \prod_{\{i \in \mathbf{P} \setminus A | b_i = 0\}} | \langle o_i^{\alpha} | | + \rangle |^2 \prod_{\{i \in \mathbf{P} \setminus A | b_i = 1\}} | \langle o_i^{\alpha} | | + \rangle |^2 \tag{12.90}$$

$$+ \frac{1}{2} \prod_{\{i \in \mathbf{P} \setminus A | b_i = 0\}} | \langle o_i^{\alpha} | | - \rangle |^2 \prod_{\{i \in \mathbf{P} \setminus A | b_i = 1\}} | \langle o_i^{\alpha} | | - \rangle |^2 \tag{12.91}$$

and therefore

$$\Pr\left(\mu^{\alpha} = m^{\alpha}\right) = \frac{1}{2^{|\mathbf{P} \setminus A|}}, \tag{12.92}$$

which satisfies the second equation in Equation 12.75. The global post-measurement state ρ_{postVER} can be calculated to be

$$\rho_{\mathsf{postVER}} = O^{\alpha} | \mathbf{N}_{\mathrm{postAME}} \rangle \langle \mathbf{N}_{\mathrm{postAME}} | O^{\alpha} \tag{12.93}$$

$$= \frac{1}{2} |0\rangle\langle 0|_A \otimes \left(O^{\alpha} |0 \cdots 0\rangle\langle 0 \cdots 0|_{\mathbf{P} \setminus A} O^{\alpha} \right) \otimes |\Psi\rangle\langle\Psi|_{\mathbf{C}} \tag{12.94}$$

$$+ \frac{(-1)^{\Delta}}{2} |0\rangle\langle 1|_A \otimes \left(O^{\alpha} |0 \cdots 0\rangle\langle 1 \cdots 1|_{\mathbf{P} \setminus A} O^{\alpha} \right) \otimes |\Psi\rangle\langle\Phi|_{\mathbf{C}} \tag{12.95}$$

$$+ \frac{(-1)^{\Delta}}{2} |1\rangle\langle 0|_A \otimes \left(O^{\alpha} |1 \cdots 1\rangle\langle 0 \cdots 0|_{\mathbf{P} \setminus A} O^{\alpha} \right) \otimes |\Phi\rangle\langle\Psi|_{\mathbf{C}} \tag{12.96}$$

$$+ \frac{1}{2} |1\rangle\langle 1|_A \otimes \left(O^{\alpha} |1 \cdots 1\rangle\langle 1 \cdots 1|_{\mathbf{P} \setminus A} O^{\alpha} \right) \otimes |\Phi\rangle\langle\Phi|_{\mathbf{C}} \tag{12.97}$$

$$= \frac{1}{2} |0\rangle\langle 0|_A \otimes |\mathbf{P} \setminus A\rangle\langle \mathbf{P} \setminus A| \otimes |\Psi\rangle\langle\Psi|_{\mathbf{C}} \tag{12.98}$$

$$+ \gamma^{\dagger} \frac{1}{2} |0\rangle\langle 1|_A \otimes |\mathbf{P} \setminus A\rangle\langle \mathbf{P} \setminus A| \otimes |\Psi\rangle\langle\Phi|_{\mathbf{C}} \tag{12.99}$$

$$+ \gamma \frac{1}{2} |1\rangle\langle 0|_A \otimes |\mathbf{P} \setminus A\rangle\langle \mathbf{P} \setminus A| \otimes |\Phi\rangle\langle\Psi|_{\mathbf{C}} \tag{12.100}$$

$$+ \frac{1}{2} |1\rangle\langle 1|_A \otimes |\mathbf{P} \setminus A\rangle\langle \mathbf{P} \setminus A| \otimes |\Phi\rangle\langle\Phi|_{\mathbf{C}} \tag{12.101}$$

$$= | \mathbf{N}_{\mathsf{postVER}} \rangle \langle \mathbf{N}_{\mathsf{postVER}} |, \tag{12.102}$$

where we omitted the $|\mathbf{H}\rangle\langle\mathbf{H}|$-type tensor factors, $\gamma := (-1)^{\Delta} \times (-i)^{|\{b_i\}|}$ and $|\mathbf{N}_{\mathsf{postVER}}\rangle$ is the pure state

$$|\mathbf{N}_{\mathsf{postVER}}\rangle := \left(|0\rangle_A \otimes |\Psi\rangle_{\mathbf{C}} + \gamma |1\rangle_A \otimes |\Phi\rangle_{\mathbf{C}} \right) \otimes |\mathbf{P} \setminus A\rangle \otimes |\mathbf{H}\rangle \tag{12.103}$$

and $|\mathbf{P} \setminus A\rangle$ is the state associated with the measurement outcome o^{α}

$$|\mathbf{P} \setminus A\rangle := \left(\bigotimes_{i \in \{\mathbf{P}\setminus A | b_i = 0\}} H_i |o_i^\alpha\rangle_i \right) \otimes \left(\bigotimes_{i \in \{\mathbf{P}\setminus A | b_i = 1\}} \sqrt{Z_i} H_i |o_i^\alpha\rangle_i \right). \tag{12.104}$$

From the perspective of **H**, all communication is indistinguishable (*cf.* the `Verification` column in Table 12.2); **H** is dis-entangled from everyone else and the state on **H** is itself separable. We can conclude that –for anyone in **H** as Eve– the anonymity of everyone in the network is preserved (*cf.* $\checkmark_1$ in Table 12.1).

Further, $\mathbf{P} \setminus A$ is dis-entangled from all other parties in the network and their post-measurement state is separable as well. Again, all communication from their perspective is uniformly random (*cf.* the `Verification` column in Table 12.2), so we can conclude that –for anyone in $\mathbf{P} \setminus A$ as Eve– the anonymity of everyone in the network is maintained (*cf.* $\checkmark_2$ in Table 12.1).

The only relevant information is $|\{b_i\}|$, which is encoded into the phase of the state on $A \cup \mathbf{C}$; any phase estimation algorithm to retrieve this information would require access to the entire state, including the state of A, which is inaccessible to **C**. Again, from the perspective of **C** all communication is indistinguishable (*cf.* the `Verification` column in Table 12.2) and we can conclude that –with **C** as Eve– here too the anonymity of all parties in the network is preserved (*cf.* $\checkmark_3$ in Table 12.1).

Note that the `Verification` round can only pass if $|\Psi\rangle_{\mathbf{C}} = |\Phi\rangle_{\mathbf{C}}$, that is when **C** is not entangled to A and $\mathbf{P} \setminus A$. However, this is not a necessary condition for anonymity, since the identity of Alice is preserved even if the `Verification` round fails. There is no information encoded into the state regarding the distribution of **P** and **H**, nor into the measurement outcome o^α. The only valuable information in the state is the parity of the number of Y-measurements, encoded in the phase of the qubit of A, which is dis-entangled from all other parties and therefore only accessible to A.

12.7 Anonymity during the `KeyGen` rounds

As the `Verification` rounds ensure that the GHZ_{m+1} state on **P** is dis-entangled from the non-participating parties in **P** and after running the `AME` protocol no party in **H** is entangled to any other party, all subsets listed in Table 12.1 are dis-entangled from each other. Hence, we can write the full-network state at the start of the `KeyGen` round as

$$|\mathbf{N}_{\mathsf{KeyGen}}\rangle = |\mathrm{GHZ}\rangle_{\mathbf{P}} \otimes |\mathbf{H}\rangle \otimes |\Psi\rangle_{\mathbf{C}}. \tag{12.105}$$

Since there is no communication during the `KeyGen` rounds, there is no leakage from $\mathbf{P}, \mathbf{H}, \mathbf{C}$ outside the subset itself (*cf.* 🔑$_1$ in Table 12.1). As $|\mathbf{H}\rangle$ is a separable state, the case **H** is trivial (*cf.* 🔑$_2$ in Table 12.1). Finally, due to its symmetries, the GHZ_{m+1} state cannot reveal who the parties sharing the state are. This ensures that there is no privacy leakage for **P** either (*cf.* 🔑$_3$ in Table 12.1).

↑ ↑ ↑
The preceding sections closely follow the text of Reference [HJP20], which was written by both myself and my co-authors.

References

[Ací+07] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. 'Device-Independent Security of Quantum Cryptography against Collective Attacks'. en. *Physical Review Letters* 98.23 (2007), p. 230501. DOI: 10.1103/PhysRevLett.98.230501.

[Adc+20] J. C. Adcock, S. Morley-Short, A. Dahlberg, and J. W. Silverstone. 'Mapping graph state orbits under local complementation'. en. *Quantum* 4 (2020), p. 305. DOI: 10.22331/q-2020-08-07-305.

[AM16] S. Akibue and M. Murao. 'Network coding for distributed quantum computation over cluster and butterfly networks'. *IEEE Transactions on Information Theory* 62.11 (2016), pp. 6620–6637.

[ARV19] R. Arnon-Friedman, R. Renner, and T. Vidick. 'Simple and Tight Device-Independent Security Proofs'. en. *SIAM Journal on Computing* 48.1 (2019), pp. 181–225. DOI: 10.1137/18M1174726.

[BB07] M. Bahramgiri and S. Beigi. *Graph States Under the Action of Local Clifford Group in Non-Binary Case*. Tech. rep. arXiv:quant-ph/0610267. arXiv:quant-ph/0610267 type: article. arXiv, 2007.

[Bak05] H. F. Baker. 'Alternants and Continuous Groups'. en. *Proceedings of the London Mathematical Society* s2-3.1 (1905), pp. 24–47. DOI: 10.1112/plms/s2-3.1.24.

[Bel64] J. S. Bell. 'On the Einstein Podolsky Rosen paradox'. *Physics Physique Fizika* 1.3 (1964), p. 195.

[Bel11] S. M. Bellovin. 'Frank Miller: Inventor of the One-Time Pad'. en. *Cryptologia* 35.3 (2011), pp. 203–222. DOI: 10.1080/01611194.2011.583711.

[BB84a] C. H. Bennett and G. Brassard. *Proceedings of the ieee international conference on computers, systems and signal processing*. 1984.

[Ben+96a] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher. 'Concentrating partial entanglement by local operations'. en. *Physical Review A* 53.4 (1996), pp. 2046–2052. DOI: 10.1103/PhysRevA.53.2046.

[BB84b] C. H. Bennett and G. Brassard. 'Quantum cryptography: Public key distribution and coin tossing'. *IEEE New York, Proceedings of the IEEE international conference on computers, systems and signal processing, Bangalore, India* 560 (1984), pp. 7–11. DOI: 10.1016/j.tcs.2014.05.025.

[Ben+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. 'Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels'. en. *Physical Review Letters* 70.13 (1993), pp. 1895–1899. DOI: 10.1103/PhysRevLett.70.1895.

[Ben+96b] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. 'Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels'. en. *Physical Review Letters* 76.5 (1996), pp. 722–725. DOI: 10.1103/PhysRevLett.76.722.

[Ben+97] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. 'Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels[Phys. Rev. Lett. 76, 722 (1996)]'. en. *Physical Review Letters* 78.10 (1997), pp. 2031–2031. DOI: 10.1103/PhysRevLett.78.2031.

[Bih+98] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor. *Security of Quantum Key Distribution Against All Collective Attacks*. arXiv:quant-ph/9801022. 1998. URL: http://arxiv.org/abs/quant-ph/9801022.

[Boh51] D. Bohm. *Quantum theory*. Prentice-Hall Physics Series. 1951.

[Bou88] A. Bouchet. 'Graphic presentations of isotropic systems'. en. *Journal of Combinatorial Theory, Series B* 45.1 (1988), pp. 58–76. DOI: 10.1016/0095-8956(88)90055-X.

[Bou91] A. Bouchet. 'An efficient algorithm to recognize locally equivalent graphs'. en. *Combinatorica* 11.4 (1991), pp. 315–329. DOI: 10.1007/BF01275668.

[Bou+99] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger. 'Observation of Three-Photon Greenberger-Horne-Zeilinger Entanglement'. en. *Physical Review Letters* 82.7 (1999), pp. 1345–1349. DOI: 10.1103/PhysRevLett.82.1345.

[Bou+97] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. 'Experimental quantum teleportation'. en. *Nature* 390.6660 (1997), pp. 575–579. DOI: 10.1038/37539.

[BBT03] G. Brassard, A. Broadbent, and A. Tapp. 'Multi-Party Pseudo-Telepathy'. In: vol. 2748. arXiv:quant-ph/0306042. 2003, pp. 1–11. DOI: 10.1007/978-3-540-45078-8_1.

[Bri+09] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest. 'Measurement-based quantum computation'. en. *Nature Physics* 5.1 (2009), pp. 19–26. DOI: 10.1038/nphys1157.

[Bri+98] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. 'Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication'. en. *Physical Review Letters* 81.26 (1998), pp. 5932–5935. DOI: 10.1103/PhysRevLett.81.5932.

[BR01] H. J. Briegel and R. Raussendorf. 'Persistent Entanglement in Arrays of Interacting Particles'. en. *Physical Review Letters* 86.5 (2001), pp. 910–913. DOI: 10.1103/PhysRevLett.86.910.

[BT07] A. Broadbent and A. Tapp. 'Information-Theoretic Security Without an Honest Majority'. en. In: *Advances in Cryptology – ASIACRYPT 2007.* Ed. by K. Kurosawa. Vol. 4833. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 410–426. ISBN: 978-3-540-76899-9. DOI: 10.1007/978-3-540-76900-2_25.

[BH23] A. Burchardt and F. Hahn. 'The Foliage Partition: An Easy-to-Compute LC-Invariant for Graph States' (2023). DOI: 10.48550/ARXIV.2305.07645.

[Cal+97] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. 'Quantum Error Correction and Orthogonal Geometry'. en. *Physical Review Letters* 78.3 (1997), pp. 405–408. DOI: 10.1103/PhysRevLett.78.405.

[Cam96] J. E. Campbell. 'On a Law of Combination of Operators bearing on the Theory of Continuous Transformation Groups'. en. *Proceedings of the London Mathematical Society* s1-28.1 (1896), pp. 381–390. DOI: 10.1112/plms/s1-28.1.381.

[CW05] M. Christandl and S. Wehner. 'Quantum Anonymous Transmissions'. en. In: *Advances in Cryptology - ASIACRYPT 2005.* Ed. by D. Hutchison et al. Vol. 3788. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 217–235. ISBN: 978-3-540-30684-9 978-3-540-32267-2. DOI: 10.1007/11593447_12.

[CZ95] J. I. Cirac and P. Zoller. 'Quantum Computations with Cold Trapped Ions'. en. *Physical Review Letters* 74.20 (1995), pp. 4091–4094. DOI: 10.1103/PhysRevLett.74.4091.

[CW08] J. Clarke and F. K. Wilhelm. 'Superconducting quantum bits'. en. *Nature* 453.7198 (2008), pp. 1031–1042. DOI: 10.1038/nature07128.

[Cla+69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. 'Proposed Experiment to Test Local Hidden-Variable Theories'. en. *Physical Review Letters* 23.15 (1969), pp. 880–884. DOI: 10.1103/PhysRevLett.23.880.

[Dab+18] K. K. Dabrowski, J. Jeong, M. Kanté, O.-j. Kwon, S.-i. Oum, and D. Paulusma. 'Computing Small Pivot-Minors'. en (2018), p. 14.

[DHW20a] A. Dahlberg, J. Helsen, and S. Wehner. 'Counting single-qubit Clifford equivalent graph states is #P-Complete'. *Journal of Mathematical Physics* 61.2 (2020), p. 022202. DOI: 10.1063/1.5120591.

[DHW20b] A. Dahlberg, J. Helsen, and S. Wehner. 'How to transform graph states using single-qubit operations: computational complexity and algorithms'. *Quantum Science and Technology* 5.4 (2020), p. 045016. DOI: 10.1088/2058-9565/aba763.

[DHW20c] A. Dahlberg, J. Helsen, and S. Wehner. 'Transforming graph states to Bell-pairs is NP-Complete'. en. *Quantum* 4 (2020), p. 348. DOI: 10.22331/q-2020-10-22-348.

[DHW22] A. Dahlberg, J. Helsen, and S. Wehner. 'The complexity of the vertex-minor problem'. en. *Information Processing Letters* 175 (2022), p. 106222. DOI: 10.1016/j.ipl.2021.106222.

[DW18] A. Dahlberg and S. Wehner. 'Transforming graph states using single-qubit operations'. en. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376.2123 (2018), p. 20170325. DOI: 10.1098/rsta.2017.0325.

[DD03] J. Dehaene and B. De Moor. 'Clifford group, stabilizer states, and linear and quadratic operations over GF(2)'. en. *Physical Review A* 68.4 (2003), p. 042318. DOI: 10.1103/PhysRevA.68.042318.

[Deu+96] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera. 'Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels'. en. *Physical Review Letters* 77.13 (1996), pp. 2818–2821. DOI: 10.1103/PhysRevLett.77.2818.

[Dia+16] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan. 'Practical challenges in quantum key distribution'. en. *npj Quantum Information* 2.1 (2016), p. 16025. DOI: 10.1038/npjqi.2016.25.

[DH76] W. Diffie and M. Hellman. 'New directions in cryptography'. en. *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638.

[Doh+13] M. W. Doherty, N. B. Manson, P. Delaney, F. Jelezko, J. Wrachtrup, and L. C. Hollenberg. 'The nitrogen-vacancy colour centre in diamond'. en. *Physics Reports* 528.1 (2013), pp. 1–45. DOI: 10.1016/j.physrep.2013.02.001.

[EPR35a] A. Einstein, B. Podolsky, and N. Rosen. 'Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?' en. *Physical Review* 47.10 (1935), pp. 777–780. DOI: 10.1103/PhysRev.47.777.

[EPR35b] A. Einstein, B. Podolsky, and N. Rosen. 'Can quantum-mechanical description of physical reality be considered complete?' *Physical review* 47.10 (1935), p. 777.

[Eke91] A. K. Ekert. 'Quantum cryptography based on Bell's theorem'. en. *Physical Review Letters* 67.6 (1991), pp. 661–663. DOI: 10.1103/PhysRevLett.67.661.

[Eke92] A. K. Ekert. 'Quantum cryptography and bell's theorem'. In: *Quantum measurements in optics*. Springer, 1992, pp. 413–418.

[EKB16a] M. Epping, H. Kampermann, and D. Bruß. 'Large-scale quantum networks based on graphs'. en. *New Journal of Physics* 18.5 (2016), p. 053036. DOI: 10.1088/1367-2630/18/5/053036.

[EKB16b] M. Epping, H. Kampermann, and D. Bruß. 'Robust entanglement distribution via quantum network coding'. en. *New Journal of Physics* 18.10 (2016), p. 103052. DOI: 10.1088/1367-2630/18/10/103052.

[Epp+17] M. Epping, H. Kampermann, C. macchiavello, and D. Bruß. 'Multi-partite entanglement can speed up quantum key distribution in networks'. en. *New Journal of Physics* 19.9 (2017), p. 093012. DOI: 10.1088/1367-2630/aa8487.

[Eul36] L. Euler. *Mechanica sive motus scientia analytice exposita: Instar supplementi ad commentar. Acad. Scient. Imper*. Vol. 2. Ex typographia academiae scientiarum, 1736.

[Fin82] A. Fine. 'Hidden Variables, Joint Probability, and the Bell Inequalities'. en. *Physical Review Letters* 48.5 (1982), pp. 291–295. DOI: 10.1103/PhysRevLett.48.291.

[FGM01] M. Fitzi, N. Gisin, and U. Maurer. 'Quantum Solution to the Byzantine Agreement Problem'. en. *Physical Review Letters* 87.21 (2001), p. 217901. DOI: 10.1103/PhysRevLett.87.217901.

[Fit+02] M. Fitzi, N. Gisin, U. Maurer, and O. von Rotz. 'Unconditional Byzantine Agreement and Multi-party Computation Secure against Dishonest Minorities from Scratch'. en. In: *Advances in Cryptology — EUROCRYPT 2002*. Ed. by G. Goos, J. Hartmanis, J. van Leeuwen, and L. R. Knudsen. Vol. 2332. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 482–501. ISBN: 978-3-540-43553-2 978-3-540-46035-0. DOI: 10.1007/3-540-46035-7_32.

[Gal23] G. Galilei. *Il saggiatore*. 1623.

[Geo20] I. Georgescu. 'Trapped ion quantum computing turns 25'. en. *Nature Reviews Physics* 2.6 (2020), pp. 278–278. DOI: 10.1038/s42254-020-0189-1.

[GT07] N. Gisin and R. Thew. ‘Quantum communication’. en. *Nature Photonics* 1.3 (2007), pp. 165–171. DOI: 10.1038/nphoton.2007.22.

[Goe+08] A. M. Goebel, C. Wagenknecht, Q. Zhang, Y.-A. Chen, K. Chen, J. Schmiedmayer, and J.-W. Pan. ‘Multistage Entanglement Swapping’. en. *Physical Review Letters* 101.8 (2008), p. 080403. DOI: 10.1103/PhysRevLett.101.080403.

[Got97] D. Gottesman. *Stabilizer Codes and Quantum Error Correction*. Tech. rep. arXiv:quant-ph/9705052. arXiv:quant-ph/9705052 type: article. arXiv, 1997.

[Goy+15] D. Goyeneche, D. Alsina, J. I. Latorre, A. Riera, and K. Życzkowski. ‘Absolutely maximally entangled states, combinatorial designs, and multiunitary matrices’. en. *Physical Review A* 92.3 (2015), p. 032316. DOI: 10.1103/PhysRevA.92.032316.

[GKB18] F. Grasselli, H. Kampermann, and D. Bruß. ‘Finite-key effects in multipartite quantum key distribution protocols’. *New Journal of Physics* 20.11 (2018), p. 113014. DOI: 10.1088/1367-2630/aaec34.

[GKB19] F. Grasselli, H. Kampermann, and D. Bruß. ‘Conference key agreement with single-photon interference’. en. *New Journal of Physics* 21.12 (2019), p. 123002. DOI: 10.1088/1367-2630/ab573e.

[Gra+22] F. Grasselli, G. Murta, J. de Jong, F. Hahn, D. Bruß, H. Kampermann, and A. Pappa. ‘Secure Anonymous Conferencing in Quantum Networks’. en. *PRX Quantum* 3.4 (2022), p. 040306. DOI: 10.1103/PRXQuantum.3.040306.

[GHZ89a] D. M. Greenberger, M. A. Horne, and A. Zeilinger. *Bell's theorem, quantum theory, and conceptions of the universe*. 1989.

[GHZ89b] D. M. Greenberger, M. A. Horne, and A. Zeilinger. ‘Going Beyond Bell's Theorem’. en. In: *Bell's Theorem, Quantum Theory and Conceptions of the Universe*. Ed. by M. Kafatos. Dordrecht: Springer Netherlands, 1989, pp. 69–72. ISBN: 978-90-481-4058-9 978-94-017-0849-4. DOI: 10.1007/978-94-017-0849-4_10.

[Gru+97] A. Gruber, A. Dräbenstedt, C. Tietz, L. Fleury, J. Wrachtrup, and C. v. Borczyskowski. ‘Scanning Confocal Optical Microscopy and Magnetic Resonance on Single Defect Centers’. en. *Science* 276.5321 (1997), pp. 2012–2014. DOI: 10.1126/science.276.5321.2012.

[Hah+22] F. Hahn, A. Dahlberg, J. Eisert, and A. Pappa. ‘Limitations of nearest-neighbor quantum networks’. *Physical Review A: Atomic, Molecular, and Optical Physics* 106.1 (2022), p. L010401. DOI: 10.1103/PhysRevA.106.L010401.

[HPE19] F. Hahn, A. Pappa, and J. Eisert. ‘Quantum network routing and local complementation’. en. *npj Quantum Information* 5.1 (2019), p. 76. DOI: 10.1038/s41534-019-0191-6.

[HJP20] F. Hahn, J. de Jong, and A. Pappa. ‘Anonymous Quantum Conference Key Agreement’. en. *PRX Quantum* 1.2 (2020), p. 020325. DOI: 10.1103/PRXQuantum.1.020325.

[Hau06] F. Hausdorff. ‘Die symbolische Exponentialformel in der Gruppentheorie’. *Ber. Verh. Kgl. Sächs. Ges. Wiss. Leipzig., Math.-phys. Kl.* 58 (1906), pp. 19–48.

[Hei+06] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. V. d. Nest, and H.-J. Briegel. *Entanglement in Graph States and its Applications*. Tech. rep. arXiv:quant-ph/0602096 type: article. arXiv, 2006. DOI: 10.48550/arXiv.quant-ph/0602096.

[HEB04] M. Hein, J. Eisert, and H. J. Briegel. ‘Multiparty entanglement in graph states’. en. *Physical Review A* 69.6 (2004), p. 062311. DOI: 10.1103/PhysRevA.69.062311.

[Hen+20] L. Henriet, L. Beguin, A. Signoles, T. Lahaye, A. Browaeys, G.-O. Reymond, and C. Jurczak. ‘Quantum computing with neutral atoms’. en. *Quantum* 4 (2020), p. 327. DOI: 10.22331/q-2020-09-21-327.

[Hen+15] B. Hensen et al. ‘Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres’. en. *Nature* 526.7575 (2015), pp. 682–686. DOI: 10.1038/nature15759.

[Her+22a] S. L. N. Hermans, M. Pompili, H. K. C. Beukers, S. Baier, J. Borregaard, and R. Hanson. ‘Qubit teleportation between non-neighbouring nodes in a quantum network’. en. *Nature* 605.7911 (2022), pp. 663–668. DOI: 10.1038/s41586-022-04697-y.

[Her+22b] S. L. N. Hermans, M. Pompili, H. K. C. Beukers, S. Baier, J. Borregaard, and R. Hanson. 'Qubit teleportation between non-neighbouring nodes in a quantum network'. en. *Nature* 605.7911 (2022), pp. 663–668. DOI: 10.1038/s41586-022-04697-y.

[HBB99] M. Hillery, V. Bužek, and A. Berthiaume. 'Quantum secret sharing'. en. *Physical Review A* 59.3 (1999), pp. 1829–1834. DOI: 10.1103/PhysRevA.59.1829.

[Jon+22a] J. de Jong, F. Hahn, J. Eisert, N. Walk, and A. Pappa. 'Anonymous conference key agreement in linear quantum networks' (2022). DOI: 10.48550/ARXIV.2205.09169.

[Jon+22b] J. de Jong, F. Hahn, N. Tcholtchev, M. Hauswirth, and A. Pappa. 'Extracting maximal entanglement from linear cluster states' (2022). DOI: 10.48550/ARXIV.2211.16758.

[KL13] C. Kloeffel and D. Loss. 'Prospects for Spin-Based Quantum Computing in Quantum Dots'. en. *Annual Review of Condensed Matter Physics* 4.1 (2013), pp. 51–81. DOI: 10.1146/annurev-conmatphys-030212-184248.

[Kok+07] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn. 'Linear optical quantum computing with photonic qubits'. en. *Reviews of Modern Physics* 79.1 (2007), pp. 135–174. DOI: 10.1103/RevModPhys.79.135.

[Kot68] A. Kotzig. 'Eulerian lines in finite 4-valent graphs and their transformations'. *Theory of Graphs (Tihany, 1966)*. Proc. Colloqium on Graph Theory Tihany 1966 (1968), pp. 219–230.

[Kru+23] V. Krutyanskiy, M. Canteri, M. Meraner, J. Bate, V. Krcmarsky, J. Schupp, N. Sangouard, and B. P. Lanyon. 'Telecom-Wavelength Quantum Repeater Node Based on a Trapped-Ion Processor'. en. *Physical Review Letters* 130.21 (2023), p. 213601. DOI: 10.1103/PhysRevLett.130.213601.

[Lad+10] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien. 'Quantum computers'. en. *Nature* 464.7285 (2010), pp. 45–53. DOI: 10.1038/nature08812.

[LOW10a] D. Leung, J. Oppenheim, and A. Winter. 'Quantum Network Communication—The Butterfly and Beyond'. en. *IEEE Transactions on Information Theory* 56.7 (2010), pp. 3478–3490. DOI: 10.1109/TIT.2010.2048442.

[LOW10b] D. Leung, J. Oppenheim, and A. Winter. 'Quantum Network Communication—The Butterfly and Beyond'. en. *IEEE Transactions on Information Theory* 56.7 (2010), pp. 3478–3490. DOI: 10.1109/TIT.2010.2048442.

[Li+22] B. Li et al. 'Quantum State Transfer over 1200 km Assisted by Prior Distributed Entanglement'. en. *Physical Review Letters* 128.17 (2022), p. 170501. DOI: 10.1103/PhysRevLett.128.170501.

[LMW18] V. Lipinska, G. Murta, and S. Wehner. 'Anonymous transmission in a noisy quantum network using the W state'. en. *Physical Review A* 98.5 (2018), p. 052320. DOI: 10.1103/PhysRevA.98.052320.

[LC99] H.-K. Lo and H. F. Chau. 'Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances'. en. *Science* 283.5410 (1999), pp. 2050–2056. DOI: 10.1126/science.283.5410.2050.

[LD98] D. Loss and D. P. DiVincenzo. 'Quantum computation with quantum dots'. en. *Physical Review A* 57.1 (1998), pp. 120–126. DOI: 10.1103/PhysRevA.57.120.

[Mat+08] D. N. Matsukevich, P. Maunz, D. L. Moehring, S. Olmschenk, and C. Monroe. 'Bell Inequality Violation with Two Remote Atomic Qubits'. en. *Physical Review Letters* 100.15 (2008), p. 150404. DOI: 10.1103/PhysRevLett.100.150404.

[May01] D. Mayers. 'Unconditional security in quantum cryptography'. en. *Journal of the ACM* 48.3 (2001), pp. 351–406. DOI: 10.1145/382780.382781.

[McC+16] W. McCutcheon, A. Pappa, B. A. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis, J. G. Rarity, and M. S. Tame. 'Experimental verification of multipartite entanglement in quantum networks'. en. *Nature Communications* 7.1 (2016), p. 13251. DOI: 10.1038/ncomms13251.

[MMG19] C. Meignant, D. Markham, and F. Grosshans. 'Distributing graph states over arbitrary quantum networks'. en. *Physical Review A* 100.5 (2019), p. 052333. DOI: 10.1103/PhysRevA.100.052333.

[MFL11] N. C. Menicucci, S. T. Flammia, and P. van Loock. 'Graphical calculus for Gaussian pure states'. en. *Physical Review A* 83.4 (2011), p. 042335. DOI: 10.1103/PhysRevA.83.042335.

[Mer78] R. C. Merkle. 'Secure communications over insecure channels'. en. *Communications of the ACM* 21.4 (1978), pp. 294–299. DOI: 10.1145/359460.359473.

[Mil82] F. Miller. *Telegraphic code to insure privacy and secrecy in the transmission of telegrams*. CM Cornwell, 1882.

[Moe+04] D. L. Moehring, M. J. Madsen, B. B. Blinov, and C. Monroe. 'Experimental Bell Inequality Violation with an Atom and a Photon'. en. *Physical Review Letters* 93.9 (2004), p. 090410. DOI: 10.1103/PhysRevLett.93.090410.

[Moo+21] G. J. Mooney, G. A. L. White, C. D. Hill, and L. C. L. Hollenberg. 'Generation and verification of 27-qubit Greenberger-Horne-Zeilinger states in a superconducting quantum computer'. en. *Journal of Physics Communications* 5.9 (2021), p. 095004. DOI: 10.1088/2399-6528/ac1df7.

[Mur+20] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß. 'Quantum Conference Key Agreement: A Review'. en. *Advanced Quantum Technologies* 3.11 (2020), p. 2000025. DOI: 10.1002/qute.202000025.

[NCT97] Y. Nakamura, C. D. Chen, and J. S. Tsai. 'Spectroscopy of Energy-Level Splitting between Two Macroscopic Quantum States of Charge Coherently Superposed by Josephson Coupling'. en. *Physical Review Letters* 79.12 (1997), pp. 2328–2331. DOI: 10.1103/PhysRevLett.79.2328.

[Nee+10] M. Neeley, R. C. Bialczak, M. Lenander, E. Lucero, M. Mariantoni, A. D. O'Connell, D. Sank, H. Wang, M. Weides, J. Wenner, Y. Yin, T. Yamamoto, A. N. Cleland, and J. M. Martinis. 'Generation of three-qubit entangled states using superconducting phase qubits'. en. *Nature* 467.7315 (2010), pp. 570–573. DOI: 10.1038/nature09418.

[Neu27] J. v. Neumann. 'Wahrscheinlichkeitstheoretischer aufbau der quantenmechanik'. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse* 1927 (1927), pp. 245–272.

[NC10] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. 10th anniversary ed. Cambridge ; New York: Cambridge University Press, 2010. ISBN: 978-1-107-00217-3.

[Oum05] S.-i. Oum. 'Rank-width and vertex-minors'. en. *Journal of Combinatorial Theory* (2005), p. 22.

[Pan+98] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger. 'Experimental Entanglement Swapping: Entangling Photons That Never Interacted'. en. *Physical Review Letters* 80.18 (1998), pp. 3891–3894. DOI: 10.1103/PhysRevLett.80.3891.

[Pap+12a] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis. 'Multipartite Entanglement Verification Resistant against Dishonest Parties'. en. *Physical Review Letters* 108.26 (2012), p. 260502. DOI: 10.1103/PhysRevLett.108.260502.

[Pap+12b] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis. 'Multipartite Entanglement Verification Resistant against Dishonest Parties'. en. *Physical Review Letters* 108.26 (2012), p. 260502. DOI: 10.1103/PhysRevLett.108.260502.

[Pir+15] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein. 'Advances in quantum teleportation'. en. *Nature Photonics* 9.10 (2015), pp. 641–652. DOI: 10.1038/nphoton.2015.154.

[Pog+21] I. Pogorelov et al. 'Compact Ion-Trap Quantum Computing Demonstrator'. en. *PRX Quantum* 2.2 (2021), p. 020343. DOI: 10.1103/PRXQuantum.2.020343.

[PR22] C. Portmann and R. Renner. 'Security in quantum cryptography'. en. *Reviews of Modern Physics* 94.2 (2022), p. 025008. DOI: 10.1103/RevModPhys.94.025008.

[Pro+21] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and Alessandro Fedrizzi. 'Experimental quantum conference key agreement'. *Science Advances* 7.23 (2021), eabe0395. DOI: 10.1126/sciadv.abe0395.

[RBB03] R. Raussendorf, D. E. Browne, and H. J. Briegel. 'Measurement-based quantum computation on cluster states'. en. *Physical Review A* 68.2 (2003), p. 022312. DOI: 10.1103/PhysRevA.68.022312.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. 'A method for obtaining digital signatures and public-key cryptosystems'. en. *Communications of the ACM* 21.2 (1978), pp. 120–126. DOI: 10.1145/359340.359342.

[Rüc+22] L. Rückle, J. Budde, J. de Jong, F. Hahn, A. Pappa, and S. Barz. 'Experimental anonymous conference key agreement using linear cluster states' (2022). DOI: 10.48550/ARXIV.2207.09487.

[Sac+00] C. A. Sackett, D. Kielpinski, B. E. King, C. Langer, V. Meyer, C. J. Myatt, M. Rowe, Q. A. Turchette, W. M. Itano, D. J. Wineland, and C. Monroe. 'Experimental entanglement of four particles'. en. *Nature* 404.6775 (2000), pp. 256–259. DOI: 10.1038/35005011.

[SWM10] M. Saffman, T. G. Walker, and K. Mølmer. 'Quantum information with Rydberg atoms'. en. *Reviews of Modern Physics* 82.3 (2010), pp. 2313–2363. DOI: 10.1103/RevModPhys.82.2313.

[San+11] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin. 'Quantum repeaters based on atomic ensembles and linear optics'. en. *Reviews of Modern Physics* 83.1 (2011), pp. 33–80. DOI: 10.1103/RevModPhys.83.33.

[Sch01] D. Schlingemann. *Stabilizer codes can be realized as graph codes*. en. arXiv:quant-ph/0111080. 2001. URL: http://arxiv.org/abs/quant-ph/0111080.

[SW01] D. Schlingemann and R. F. Werner. 'Quantum error-correcting codes associated with graphs'. en. *Physical Review A* 65.1 (2001), p. 012308. DOI: 10.1103/PhysRevA.65.012308.

[Sch04] D.-M. Schlingemann. 'Error syndrome calculation for graph codes on a one-way quantum computer: Towards a quantum memory'. en. *Journal of Mathematical Physics* 45.11 (2004), pp. 4322–4333. DOI: 10.1063/1.1797533.

[Sch07] E. Schmidt. 'Zur Theorie der linearen und nichtlinearen Integralgleichungen'. *Math. Ann* 63 (1907), pp. 161–174.

[Sho99] P. W. Shor. 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer'. en (1999), p. 30.

[SP00] P. W. Shor and J. Preskill. 'Simple Proof of Security of the BB84 Quantum Key Distribution Protocol'. en. *Physical Review Letters* 85.2 (2000), pp. 441–444. DOI: 10.1103/PhysRevLett.85.441.

[Tha+21] C. Thalacker, F. Hahn, J. de Jong, A. Pappa, and S. Barz. 'Anonymous and secret communication in quantum networks'. *New Journal of Physics* 23.8 (2021), p. 083026. DOI: 10.1088/1367-2630/ac1808.

[Tho+22] P. Thomas, L. Ruscio, O. Morin, and G. Rempe. 'Efficient generation of entangled multiphoton graph states from a single atom'. en. *Nature* 608.7924 (2022), pp. 677–681. DOI: 10.1038/s41586-022-04987-5.

[Tit+98] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. 'Violation of Bell Inequalities by Photons More Than 10 km Apart'. en. *Physical Review Letters* 81.17 (1998), pp. 3563–3566. DOI: 10.1103/PhysRevLett.81.3563.

[Unn+19] A. Unnikrishnan, I. J. MacFarlane, R. Yi, E. Diamanti, D. Markham, and I. Kerenidis. 'Anonymity for Practical Quantum Networks'. en. *Physical Review Letters* 122.24 (2019), p. 240501. DOI: 10.1103/PhysRevLett.122.240501.

[UM22] A. Unnikrishnan and D. Markham. 'Verification of graph states in an untrusted network'. en. *Physical Review A* 105.5 (2022), p. 052420. DOI: 10.1103/PhysRevA.105.052420.

[Urs+04] R. Ursin, T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther, and A. Zeilinger. 'Quantum teleportation across the Danube'. en. *Nature* 430.7002 (2004), pp. 849–849. DOI: 10.1038/430849a.

[VDD04a] M. Van den Nest, J. Dehaene, and B. De Moor. 'Efficient algorithm to recognize the local Clifford equivalence of graph states'. en. *Physical Review A* 70.3 (2004), p. 034302. DOI: 10.1103/PhysRevA.70.034302.

[VDD04b] M. Van den Nest, J. Dehaene, and B. De Moor. ‘Graphical description of the action of local Clifford transformations on graph states’. en. *Physical Review A* 69.2 (2004), p. 022316. DOI: 10.1103/PhysRevA.69.022316.

[VDD05a] M. Van den Nest, J. Dehaene, and B. De Moor. ‘Finite set of invariants to characterize local Clifford equivalence of stabilizer states’. en. *Physical Review A* 72.1 (2005), p. 014307. DOI: 10.1103/PhysRevA.72.014307.

[VDD05b] M. Van den Nest, J. Dehaene, and B. De Moor. ‘Invariants of the local Clifford group’. en. *Physical Review A* 71.2 (2005), p. 022310. DOI: 10.1103/PhysRevA.71.022310.

[VDD05c] M. Van den Nest, J. Dehaene, and B. De Moor. ‘Local unitary versus local Clifford equivalence of stabilizer states’. en. *Physical Review A* 71.6 (2005), p. 062323. DOI: 10.1103/PhysRevA.71.062323.

[Van+22] T. Van Leent, M. Bock, F. Fertig, R. Garthoff, S. Eppelt, Y. Zhou, P. Malik, M. Seubert, T. Bauer, W. Rosenfeld, W. Zhang, C. Becher, and H. Weinfurter. ‘Entangling single atoms over 33 km telecom fibre’. en. *Nature* 607.7917 (2022), pp. 69–73. DOI: 10.1038/s41586-022-04764-4.

[Ver26] G. S. Vernam. ‘Cipher printing telegraph systems: For secret wire and radio telegraphic communications’. *Journal of the A.I.E.E.* 45.2 (1926), pp. 109–115. DOI: 10.1109/JAIEE.1926.6534724.

[WE21] N. Walk and J. Eisert. ‘Sharing Classical Secrets with Continuous-Variable Entanglement: Composable Security and Network Coding Advantage’. en. *PRX Quantum* 2.4 (2021), p. 040339. DOI: 10.1103/PRXQuantum.2.040339.

[Wal+22a] J. Wallnöfer, F. Hahn, M. Gündoğan, J. S. Sidhu, F. Wiesner, N. Walk, J. Eisert, and J. Wolters. ‘Simulating quantum repeater strategies for multiple satellites’. en. *Communications Physics* 5.1 (2022), p. 169. DOI: 10.1038/s42005-022-00945-9.

[Wal+22b] J. Wallnöfer, F. Hahn, F. Wiesner, N. Walk, and J. Eisert. ‘ReQuSim: Faithfully simulating near-term quantum repeaters’ (2022). DOI: 10.48550/ARXIV.2212.03896.

[Wan+20] J. Wang, F. Sciarrino, A. Laing, and M. G. Thompson. ‘Integrated photonic quantum technologies’. en. *Nature Photonics* 14.5 (2020), pp. 273–284. DOI: 10.1038/s41566-019-0532-1.

[Wan+18] X.-L. Wang, Y.-H. Luo, H.-L. Huang, M.-C. Chen, Z.-E. Su, C. Liu, C. Chen, W. Li, Y.-Q. Fang, X. Jiang, J. Zhang, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan. ‘18-Qubit Entanglement with Six Photons’ Three Degrees of Freedom’. en. *Physical Review Letters* 120.26 (2018), p. 260502. DOI: 10.1103/PhysRevLett.120.260502.

[Wie83] S. Wiesner. ‘Conjugate coding’. en. *ACM SIGACT News* 15.1 (1983), pp. 78–88. DOI: 10.1145/1008908.1008920.

[WZ82] W. K. Wootters and W. H. Zurek. ‘A single quantum cannot be cloned’. en. *Nature* 299.5886 (1982), pp. 802–803. DOI: 10.1038/299802a0.

[Yan+20] Y.-G. Yang, Y.-L. Yang, X.-L. Lv, Y.-H. Zhou, and W.-M. Shi. ‘Examining the correctness of anonymity for practical quantum networks’. en. *Physical Review A* 101.6 (2020), p. 062311. DOI: 10.1103/PhysRevA.101.062311.

[YS92] B. Yurke and D. Stoler. ‘Einstein-Podolsky-Rosen effects from independent particle sources’. en. *Physical Review Letters* 68.9 (1992), pp. 1251–1254. DOI: 10.1103/PhysRevLett.68.1251.

[Zha08] J. Zhang. ‘Graphical description of local Gaussian operations for continuous-variable weighted graph states’. en. *Physical Review A* 78.5 (2008), p. 052307. DOI: 10.1103/PhysRevA.78.052307.

[Żuk+93] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. ‘“Event-ready-detectors” Bell experiment via entanglement swapping’. en. *Physical Review Letters* 71.26 (1993), pp. 4287–4290. DOI: 10.1103/PhysRevLett.71.4287.

Selbstständigkeitserklärung S

> *"Wer ich bin und was ich kann, ist nicht abhängig von diesem Titel. Was mich als Mensch ausmacht, liegt nicht in diesem akademischen Grad begründet."*
>
> *—Franziska Giffey (Reg. Bürgermeistin von Berlin)*

Ich erkläre gegenüber der Freien Universität Berlin, dass ich die vorliegende Dissertation selbstständig und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel angefertigt habe. Die vorliegende Arbeit ist frei von Plagiaten. Alle Ausführungen, die wörtlich oder inhaltlich aus anderen Schriften entnommen sind, habe ich als solche kenntlich gemacht. Diese Dissertation wurde in gleicher oder ähnlicher Form noch in keinem früheren Promotionsverfahren eingereicht.

Mit einer Prüfung meiner Arbeit durch ein Plagiatsprüfungsprogramm erkläre ich mich einverstanden.

Frederik Hahn *Berlin, Dezember 2022*

Acknowledgements A

Fortunately, no one has to do research alone anymore. I have had the pleasure of collaborating, discussing and spending time with colleagues who have become friends. They are the ones who made the time of my PhD studies an enjoyable and enriching experience that I would not want to miss.

I am grateful to my PhD supervisor Jens Eisert for allowing me to work in his research group in which I could develop as a scientist. It was in large part his optimism and enthusiasm that first sparked my interest in the topics of this thesis. Thank you, Jens, for pushing me when I needed it and for still giving me the space to develop into an independent researcher.

Of all the postdocs I met and worked with during my academic life, Anna Pappa stands out in particular. Thank you, Anna, for not only providing me with some important insights that guided me during the first transitional phase of my PhD studies, but also for always being available and eventually allowing me to work in your research group at TU Berlin after my PhD fellowship ended.

I want to especially thank Jarn. Thank you for working so closely with me ever since you joined as Anna's first PhD student. Thanks for teaching me to become a better programmer, and for teaching me the joy of self-hosting. Also thank you to Julius for programming with me and introducing me to the secrets of the Curta cluster.

While writing this thesis, I was afraid to show it to anyone for a long time. Many thanks to Fabian, Julius and Ziad who insisted on and took the time for proofreading parts of this work. Thank you Elies for checking the Spanish summary and helping me to find the correct technical terms.

Thank you to Dominik for founding the star office with me. You made coming into the office one of the best parts of every day. I am almost certain that our office decoration will spark joy for generations of PhDs to come. Marios, Elies and Marcel –take good care of it!

Thank you as well to all of our other friends of the family at the ObstBlock for supervising my PhD with a plethora of stellar and fruitful discussions. You made the group meetings enjoyable even long after leaving the group. Thank you Andi, Papalex and Markus from the Obst Office for unimpressive sailing and impressive biking.

Thank you to Marek and Alex J for many a nice evening in the Luise Dahlem and discussions about science and beyond. Thank you to Ingo for sharing your ingenious business ideas with me and for your support of my political endeavors. Speaking of politics: Thank you to all of my friends and foes in local politics who were a welcome distraction to thinking. A special thank you goes to Alexandra and Anna, without whom I would have left this circus a long time ago. The foes shall remain unnamed –may they one day find themselves.

Thank you to everyone at the Studienstiftung (German Academic Scholarship Foundation). I am grateful that I was allowed to pursue my political interests as intensely as I did, grateful for the funding of most of my research and grateful for the financing of my Spanish classes.

Thank you fellow fans of the museum. In particular to Marcel, Jonas, Nick, Nathan, Jörg, Laura and Daniel. Thank you also to the few people that actually seem to like the "mainsa" more than the veggie No1: Alex J, Ingo, Carlos, Christian, Paul and Johannes.

A special thanks to Annette, Marianne, Christiane and Claudia for enduring the organizational chaos of this group.

Thank you to all my coauthors and collaborators; to Anna, Jens, Jarn, Axel, Christopher, Stefanie, Julius, Mustafa, Jasminder, Fabian, Nathan, Janik, Bülent, Lukas, Jakob, Federico, Gláucia, Dagmar, Hermann, Hendrik, Fulvio, Caterina, Adam.

Thank you to all of my colleagues at the Quantum Communication and Cryptography research group at the TU Berlin. To Jarn, Ziad and Lorenzo for enjoyable lunch breaks and to Fenja, Fabian and Niklas for their visits at the office. Many thanks also to Claudia, who keeps a cool head with all our administrative requests and always reminds us to respect file names.

I am also grateful for the translation website DeepL and for the LaTeX and Tikz stackexchange communities for answering all those questions that I was too lazy to look up in the respective documentations.

And finally, and most importantly, I want to thank my family. Thank you to my parents Renate and Jürgen, to my sister Mareike and her husband Malte, and to my partner María and her family in Chile. To my godmothers Sigrid and Ulrike with their husbands Martin and Torsten and their families. To my late grandparents Erika, Ilse and Hans-Joachim. You were and are always there for me and I am eternally thankful for that.

Y por último, y lo más importante, quiero dar las gracias a mi familia. Gracias a mis padres Renate y Jürgen, a mi hermana Mareike y su marido Malte, y a mi polola María y su familia en Chile. A mis madrinas Sigrid y Ulrike con sus maridos Martin y Torsten y sus familias. A mis difuntos abuelos Erika, Ilse y Hans-Joachim. Siempre estuvisteis y estáis ahí para mí, y por ello estoy eternamente agradecido.

Und schließlich, und das ist mir das Wichtigste, möchte ich meiner Familie danken. Danke an meine Eltern Renate und Jürgen, an meine Schwester Mareike und ihren Mann Malte und an meine Partnerin María und ihre Familie in Chile. Meinen Patentanten Sigrid und Ulrike mit ihren Ehemännern Martin und Torsten und ihren Familien. Meinen verstorbenen Großeltern Erika, Ilse und Hans-Joachim. Ihr wart und seid immer für mich da, und dafür bin ich euch unendlich dankbar.

Frederik Hahn
Berlin, 2022