Sorbonne Université - EDITE de Paris

Laboratoire d'informatique de Sorbonne Université (LIP6) / Quantum Information

Multipartite communications over quantum networks

Par Clément Meignant

Thèse de Doctorat d'Informatique

Dirigée par Damian Markham et Frédéric Grosshans

Présentée et soutenue publiquement en Décembre 2021, devant un jury composé de :

- Dür Wolfgang, Associate Professor, HDR, University of Innsbruck, *Rapporteur*
- Grosshans Frédéric, Chargé de recherche au CNRS, HDR, Sorbonne Université, *Co-encadrant*
- Markham Damian, Chargé de recherche au CNRS, HDR, Sorbonne Université, *Directeur de thèse*
- Murao Mio, Professor, University of Tokyo, *Rapporteure*
- Perdix Simon, Directeur de recherche Inria-Mocqua, Loria
- Potop-Butucaru Maria, Professeure, Sorbonne Université

Abstract

The field of quantum networks is currently a major area of investigation in quantum technologies. Research is ongoing at all levels. On the theorical level, to characterize what a quantum network is and to define appropriate figures of merits. On the implementation level, to define the protocol specifications which should be applied to global networks. On the concrete level, to actually build quantum networks. One of the simplest acts of quantum communication, the distribution of a single bipartite entangled state, has been highly studied as it is a simple problem to characterize, simulate and implement. It is also useful for a prominent quantum network application: the secured distribution of a cryptographic key. However, the use of quantum networks goes far beyond. A realistic quantum network theory should take into account the multiple simultaneous distributions which will happen over global networks. A complete quantum network theory should take into account the distribution of multipartite entangled states as they are useful for many quantum information applications, such as secret sharing. Thus, the use of quantum networks to their full extent implies the need to study the simultaneous distribution of multipartite states over quantum networks. In this manuscript, we report on several works of progress in the domain. We first study the recycling of previously distributed resources in the asymptotic regime by the use of entanglement combing and quantum state merging. Then, we study and solve the problem of a fundamental network bottleneck by using a particular formalism used across quantum information, the matrix product state formalism. Using this result, we characterize the distribution of quantum states using the tensor network formalism. We also characterize a broad class of classical distribution protocols using this formalism. We use this similarity to compare the distribution of classical correlations over classical networks to a the distribution of quantum state over quantum networks. We show the existence of a classical protocol which implies the existence of a quantum one but not the converse. We also build protocols to distribute specific classes of states over quantum networks such as graph states and GHZ states by using the graph state formalism and a bit of graph theory. Finally, we implement the previous protocols in a more realistic setting and participate in the elaboration of multipartite features for a quantum network simulator: QuISP. We also aimed to popularize and disseminate the notions of quantum information to a broad audience. We report on the creation of a video game based on quantum optics, adding to the existing popularization ludography. To develop it, we used several mechanisms known in the game-based learning literature and will test its impact on the broad audience in

the next few months. We hope these results will be beneficial to the quantum network theory, for both research and diffusion to the public.

Dedication and acknowledgements

Il y a trop de personnes à qui je souhaiterais dédier ce manuscrit. En fait, j'aimerais le dédier toutes les personnes qui m'ont aidés et soutenus jusqu'à ce jour. La liste est longue, je suis bien entouré. Je vais quand même essayer de donner un condensé : Papa, Maman, Marion, Tata, Tonton, Silvia, Pac Taï (Maxime), Mehdi, M. Iglesias, Loïc, Tintin (Clément), Florian, Senework, Nicolas, Thomas, François, Gaël, Quentin, Lucas, Étienne, Antoine, Robert, Léo, Raja, Nathan, Damian et Frédéric. Un remerciement particulier à ces personnes pour m'avoir aidé et supporté à un moment ou à un autre de mon parcours.

J'aimerais également remercier plus globalement toute l'équipe du groupe d'information quantique du LIP6, un groupe extra que je ne peux que conseiller. Nous étions un groupe de doctorants arrivés tous a peu près en même temps et ce fut un plaisir d'évoluer (et de manifester parfois) à vos côtés. J'espère que tout ira bien pour vous et qu'on se recroisera. Je voudrais également repréciser l'importance de mes maître de thèse Damian Markham et Frédéric Grosshans, c'est aussi grâce à eux que j'ai pu terminer cette thèse.

J'espère que ceux ou celles qui liront ce manuscrit prendront quand même un peu de plaisir et apprendront quelques choses en passant.

Vous savez, le diplôme, ça sert simplement à constituer une espèce de valeur marchande du savoir [...]. Tous les gens qui passent un diplôme savent pratiquement que ça ne sert à rien, qu'il n'y a pas de contenu, que c'est vide. Mais ceux qui n'ont pas passé le diplôme, c'est ceux là qui donnent un sens plein au diplôme. Et le diplôme, moi je crois qu'il est fait précisément pour ceux qui ne l'ont pas.

Michel Foucault

Table of Contents

Introduction

The PhD journey is a long one. You learn that *to research* is actually a combination of quite the number of verbs: to write, read, explain, think, argue, network, speak, cry, rewrite, reread and rewrite. And assuming you get the lessons, finally learning the ropes and becoming a more-or-less acceptable part of the scientific community. Assuming. There is still this recurring awkward moment, this dreaded occurrence when meeting new faces. They learn of your occupation and innocently ask the cursed question: "So, what's your topic?". The best choice is to evade the question; crush their hopes of learning something accurate and exciting about what you are working on and go back to the usual awkward silence that should stand between unrelated people. If you are in high-spirit – and have an hour or two in front of you – you can try another approach and start explaining. However, you have to go back a long long way and start with the beginning of quantum physics. You can start with some generalities about how quantum physics was a revolution in and of itself, how what we call the *classical* description of events was not sufficient anymore. Then, you can start enumerating the differences between the intuitive classical conceptions of the world and the counter intuitive quantum ones such as the superposition of states (referencing both the Schrödinger cat and the Stern-Gerlach experiment may be a good idea), the superposition explanation leading to a quick lecture about the existence of entanglement and can be accompanied with a story about the Einstein-Podolski-Rosen paradox [37], finally exposing that the quantum theory is non-local. Explain the meaning of *non-local*. You can finish off with more advanced notions which will prove useful later as the no-cloning theorem [113], demonstrating you cannot create a machine copying quantum states and quantum teleportation [94]. If the listener is still here – and if there is still some light in their eyes –, you can take a sip and continue. Now it's time to go into information theory.

They will think it is easier since they should be familiarized with it – if you avoid referencing too much the Claude Shanon's 1948 paper [101]. Reference it just enough to sound really smart – you can explain what is a *bit*, the unit of information (everybody knows

what is a bit) – and go a bit deeper. You can start talking about concrete implementations of bits such as capacitors which can be charged or not, or small magnets with positive or negative polarisation – don't say polarisation, since you will use it later for photons.

Mark a pause.

If the listener did not connect the dots a this point, you may ask "And what if you were to encode this information on the quantum objects I spoke about before?", to which the reply would surely be, either "What if, indeed?" or a deafening silence. Nevertheless, this is the moment you start smiling, take a deep breath and say "Well, this is quantum information.".

One of the first papers trying to build a quantum information theory was published in 1976 [56] by Roman Stanisław Ingarden. Since then, applications of this theory accumulated, this is a part which may have more interest from your audience who, most of the time, will ask you what is the purpose, and declare that they need more concrete examples to understand. Time to bring out the big guns. Begin with quantum cryptography and the theorical sure-fireway to foil man-in-the-middle attacks to distribute secret keys [11] . Then, announce the end of the financial system by developing on the Shor's algorithm [103] – please don't say that it computes faster because all calculations are done in parallel. If they ask you whether we already have a quantum computer, you can answer "Yes!", as several projects for building quantum computers are in progress [93, 6]. Nevertheless, you can, and you will, focus again on the communication part: we have those applications to distribute quantum keys, to secret share among several participants [60]. This is great. However, those applications are useful between several geographically distant parties, and there is some sort of problem. These applications need to use very specific quantum states and the no-cloning theorem prevents us from distributing quantum information as we distribute classical ones since you cannot copy quantum information. You can end with "There is a need for a quantum network theory, a way to distribute quantum states over network, and this is what I'm doing : studying the distribution of quantum states over quantum networks." You could conclude here. However, you will choose to continue and say: "But, let us be a little more specific."
Actually, when this thesis started three years ago, results on bipartite distribution could easily be found [1]. The aim was to share maximally entangled pairs in order to perform quantum key distributions. However, a lot of the applications presented previously need multipartite entanglement [60, 42] and multipartite entanglement is much more

difficult to manipulate or characterize. Moreover, the use of a global network by multiple users implies that simultaneous requests of communication will arise [23]. In a quantum network, it involves the simultaneous distribution of several states uncorrelated to each others and so, the distribution of product states. However, resources for distribution will be limited over quantum networks, in terms of repeater stations, memories, ect. This lack of resource will create bottlenecks which will hinder the network capacity if one does not optimize over the available resources. We will see that enlarging the set used of quantum operations beyond quantum teleportation and bipartite distillation is a way to overcome those limitations. The study of quantum networks is currently a major investigation field in quantum technologies. Quantum networks have ongoing research on their theoretical characterization [110, 82, 21], the specifications of protocols to use them [32, 65] and the actual building of hardware [64, 70] to implement them. My aim was to develop protocols and ways to distribute multipartite entanglement while optimizing those distributions in the case of – more or less – real uses of the network, which is the main theme of this manuscript.

You already killed the mood a long time ago. Thus, you decide to take the pen you always have in one of your pocket, and write on the napking "We won't stop here, you need to understand! So, here is my plan:"
In Chapter 1 we will do a review on quantum information and cover the technical bases to understand every parts. In Chapter 2, we study the very first result I had, a theorical work about the asymptotic rate of conversion of one multipartite entangled state into another. In Chapter 3, we remove the asymptotic condition, we study a fundamental bottleneck scenario and develop technique based on classical networking technique and the tensor network formalism to decide whether a state is distributable over a given topology of network. In Chapter 4, we focus on graph states and show one of the first protocol to indeed distribute those graph states over arbitrary quantum networks, then we present the implementation of said protocol on a realistic quantum network simulation. We will then conclude and present a work on the popularization of quantum optics: OptiQraft, a game-based learning approach on the topic of multipartite quantum states manipulation.

Summary of results

- Meignant C., Markham D., & Grosshans F. (2019).
  Distributing graph states over arbitrary quantum networks.
  Physical Review A, 100(5), 052333.
- Streltsov A., Meignant C., & Eisert J. (2020).
  Rates of Multipartite Entanglement Transformations.
  Physical Review Letters, 125(8), 080502.
- Meignant C., Grosshans F., & Markham D. (2021).
  Classical-quantum network coding: a story about tensor.
  arXiv preprint arXiv:2104.04745.
- The following work is not a part of the manuscript
  Booth R. I., Kissinger A., Markham D., Meignant C., & Perdrix S. (2021).
  Outcome determinism in measurement-based quantum computation with qudits.
  arXiv preprint arXiv:2109.13810.

Chapter 1

Definitions and framework

This chapter introduces the theorical grounding needed to understand this manuscript. However, for the hurried and already informed reader, an indication of which introduction's sections should be imperatively be read and understood is given at the start of each chapter. Each section of this chapter could be skipped at first by a new reader with the exception of the last one which summarize the notations used in this manuscript and provides succinct definitions of essential objects. For the meticulous reader, the introduction breakdown as follow. Sec. 1.1 will go back to the very core of information theory by defining the objects in which we encode information. Sec. 1.2 will explain how we will manipulate those objects by introducing the general quantum operation formalism as well as the different classes of operations we will see in the manuscript. Sec. 1.3 will present both Shannon and Von Neumann entropies as well as their interpretation in a communication scenario. Sec. 1.4, will introduce the specific classes of multipartite states we will try to distribute over quantum networks. Finally, Sec. 1.5 will introduce the network setting, which will be the setting for most of this work. In this introduction, notions of classical information theory will be outlined in parallel to the quantum information theory's ones, each object and means of operation in the quantum setting mirroring one in the classical setting. This choice is made as there is a lot to learn from the comparison of the two setups – this comparison being one of the essential point of this manuscript and reaching its apex in Chapter 3 – as well as a willingness to be accessible to a reader from both an informatic or a quantum background lacking knowledge in the

other field.

1.1 Elementary definitions

In this section we introduce the very first elementary objects, notations and definitions of both classical and quantum information theory.

1.1.1 Classical information and communication

Communication setup

Since its introduction by Shannon in 1945 [101], information theory has developed at a terrifying pace and has also found applications in other fields such as computation [96], cryptography [105] or machine learning [46]. Here, we restrict ourselves – for the sake of synthesis – to the – not so small – angle of communication scenarios in both the classical and the quantum setup. We first define the most fundamental communication setup, a bipartite communication scenario involving an emitter and a receiver:

Definition 1.1 (Source, Sink)**.** *In a bipartite communication scenario, an emitter wants to transmit a message to a receptor. We will denote the emitter of the message as the source, usually noted S and we will denote the receptor of the message as the sink usually noted T.*

To formalize the definition of a message we need to introduce the most basic unit of information, the *bit*.

Definition 1.2 (a Bit)**.** *A bit is an object which can take only two values, 0 or 1. It is the minimal quantity of information which can be transmitted.*

A message is defined as the concatenation of several bits sent from a source to a sink. In a general setting, we will use bits of higher dimension. A "bit" of dimension d – an object which can take d different values – will be called a d-it. Whenever the dimension is not relevant, we call such an object a dit.

Messages and discrete random variables

Usually, the components of a message follow a specific kind of structure known to both the source and the sink. This structure can come from a pre-established convention such as the use of a known language or prior information about what is sent. We can model the

impact of prior information on the message structure by modeling messages as *random discrete variables*:

Definition 1.3 (Random discrete variables)**.** *We define a random discrete variable X as the couple $X := (O, P)$, where $O = \{x_1, \ldots, x_n\}$ is the set of all the possible outcomes and P is a function from O to $\mathbb{R}$ such that $P(x_i)$ is the probability for X to have the outcome x_i. We denote $P(x_i)$ as P_i when no ambiguity exists. P is a probability distribution and as such $\forall x_i \in O$, $P_i \geq 0$ and $\sum_{i=1}^{n} P_i = 1$.*

In the context of our communication scenario, a source might seek to optimize its communication costs and send as few bits as possible to the sink. We will see in Subsec. 1.3.1 the fundamental contribution of the Shannon theory: this quantity is the entropy of the associated random variable's distribution.

1.1.2 Quantum information and communication

Unit of information

Each of the previously defined notions has a quantum counterpart. We first define the quantum bit, a name which will be often shortened as *qubit*:

Definition 1.4 (Qubit)**.** *A qubit is the smallest bit of information in the quantum setup. It is a quantum object encoded on a Hilbert space $\mathcal{H}$ of dimension 2. We usually write qubits as the linear combination of two orthogonal vectors regarding the usual inner product of said Hilbert space:*

$$|\psi\rangle := \alpha\,|u\rangle + \beta\,|v\rangle \quad \textit{where} \quad |\alpha|^2 + |\beta|^2 = 1 \quad \textit{and} \quad \langle u|v\rangle = 0 \tag{1.1}$$

Note that we use the "bra-ket" notation, every element v of $\mathcal{H}$ is written as $|v\rangle$ and its corresponding element in the dual basis of $\mathcal{H}$ is written as $\langle v|$. The inner product of $|u\rangle$ and $|v\rangle$ is denoted as $\langle v|u\rangle$. As in the classical case, we can define objects of higher dimension. We call a qu*d*-it – or qudit whenever the dimension is not relevant – a quantum object encoded on a Hilbert space of dimension d. Mirroring the classical message, we define a pure quantum state as the concatenation of several qudits. Sometimes, we will need to use another representation called the density matrix. Density matrices are linear operators over a Hilbert spaces and serve for a more general description of quantum states. The density matrix associated to a pure state $|\psi\rangle \in \mathcal{H}$, is defined as $\psi := |\psi\rangle\langle\psi| \in \mathcal{L}(\mathcal{H})$. We also define the density matrices associated to mixed states:

Definition 1.5 (Mixed State)**.** *We define mixed state as the convex combination of several pure states:*

$$\rho = \sum_i c_i \left|\psi_i\right\rangle \left\langle\psi_i\right|, \tag{1.2}$$

with Tr $\rho = 1$*. We will usually represent them by a combination of orthonormal pure states* $|\phi_i\rangle$*, such as*

$$\rho = \sum_i \lambda_i \left|\phi_i\right\rangle \left\langle\phi_i\right| \tag{1.3}$$

Here, $|\phi_i\rangle$ *are the eigenvectors of* ρ *and* λ_i *are their respective eigenvalues.*

Note that several different convex combinations can represent the same mixed state. For example, taking two arbitrary states $|u\rangle$, $|v\rangle$ of dimension 2 and their orthogonal complements $|u^\perp\rangle$, $|v^\perp\rangle$, the mixed state $\rho = 1/2\left(|u\rangle\langle u| + |u^\perp\rangle\langle u^\perp|\right)$ can also be written as $\rho = 1/2\left(|v\rangle\langle v| + |v^\perp\rangle\langle v^\perp|\right)$

Notation in networks

We will now move to definitions and notations which will be used in the quantum networks setting but are not defined in direct analogy to previous classical definitions. We are studying states in the network setting. As such, the same state can be shared by different parties of said network – we will see in section 1.5 how we define networks. As each of these parties own a part of the state, we label said part with the name of the owner. For example, given a state $|\psi\rangle$ shared by three parties A, B and C, we write:

$$|\psi\rangle^{A,B,C} = \sum_{i_A,i_B,i_C=0}^{d_A,d_B,d_C} c_{i_A,i_B,i_C} \left|i_A\right\rangle^A \otimes \left|i_B\right\rangle^B \otimes \left|i_C\right\rangle^C \tag{1.4}$$

$$= \sum_{i_A,i_B,i_C=0}^{d_A,d_B,d_C} c_{i_A,i_B,i_C} \left|i_A i_B i_C\right\rangle^{ABC} \tag{1.5}$$

Each party X owning part of the state is associated to a Hilbert Space $\mathcal{H}_X$ of dimension d_X and $|\psi\rangle$ belong to the product space of those Hilbert spaces – formally, $|\psi\rangle \in \bigotimes_X \mathcal{H}_X$. We will sometime decompose a party A into several *subparties* A_1, A_2, ect.

Bipartite and Multipartite states

Pure quantum states shared by two parties have been heavily studied in quantum information – [87] and Sec. 2.1. We usually call *bipartite states* quantum states which are shared by two parties and *multipartite states* the ones shared by more than two. We also call a *bipartition* the partition of the parties into two subsets. A multipartite state

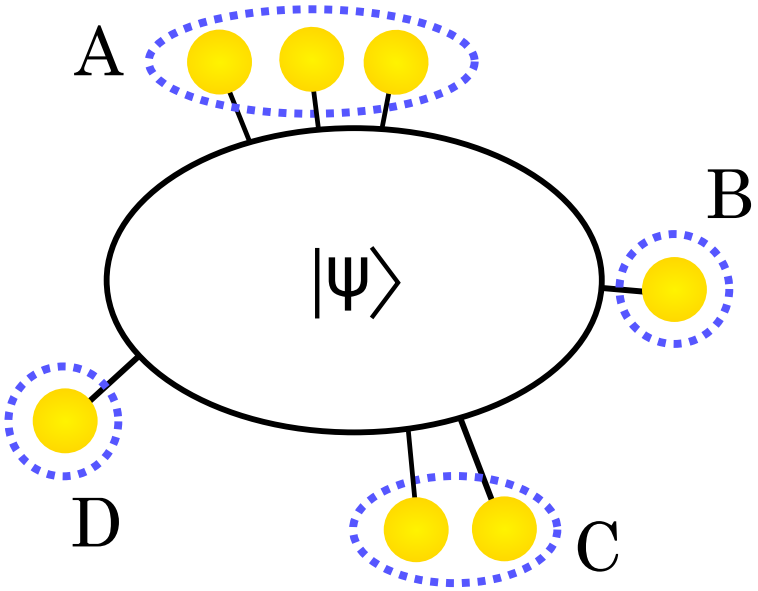

Figure 1.1: Pure states will be depicted as follow. Each of the blue dotted circle represent a subsystem owning part of the global state $|\psi\rangle$. Each yellow circle represent a qudit. A party can hold several qudits.

is considered bipartite regarding any of its bipartitions. As such, every result found on bipartite states can be readily applied on bipartions of multipartite states.

Entanglement

In some cases, a states can be written as a product of states regarding this partition. For example,

$$|\psi\rangle^{AB} = |00\rangle^{AB} + |01\rangle^{AB} + |10\rangle^{AB} + |11\rangle^{AB} = \frac{1}{2}\left(|0\rangle^{A} + |1\rangle^{A}\right) \otimes \left(|0\rangle^{B} + |1\rangle^{B}\right). \quad (1.6)$$

In this case, we say that $|\psi\rangle^{AB}$ is separable regarding the bipartition $\{\{A\},\{B\}\}$. If a state is not separable regarding a given partition. It is said to be *entangled*. Entanglement is one of our main resources for quantum networks as entanglement is necessary to perform quantum teleportation and various other tasks – see [12, 94] and last subsubsection of Subsec. 1.2.2.

Schmidt decomposition

Schmidt decomposition will not be used heavily in the main text. However, it will be of importance in Subsection 1.3.2 as a convenient way to describe any bipartite state and to visualize its entanglement.

Theorem 1.1 (Schmidt Decomposition)**.** *Let $|\psi\rangle^{AB}$ be a pure bipartite state. Assuming w.l.o.g. that $d_A \geq d_B$, we can find two orthonormal basis regarding the usual inner product of the vector's Hilbert space, $\{|u_i\rangle\}$ of $\mathcal{H}_A$ and $\{|v_j\rangle\}$ of $\mathcal{H}_B$ such that*

$$|\psi\rangle^{AB} = \sum_{i=1}^{d_B} c_i \, |u_i\rangle^A \otimes |v_i\rangle^B \tag{1.7}$$

where c_i are real positive scalars and are unique up to a reordering.

We have defined the necessary elementary objects needed for this thesis, we will now see which are the means to manipulate those objects.

1.2 Operating on information

We will see here how we manipulate bits and quantum state, with a heavy focus on quantum operations. We introduce here only the objects and definition which will be needed. A more exhaustive introduction to quantum operations can be found in [87].

1.2.1 Classical operations

Manipulation of bits and dits is quite straightforward in our setup. We consider that every party of a network can emit dits chosen from a classical distribution represented by any discrete random variable X. Given a message, we consider that every party can implement every deterministic operation which takes input in the set of all messages and output in the same set. However, for two distant parties A and B in a communication scenario, B cannot apply deterministic operations to the qudits owned by A and conversely. Nonetheless, A and B can share a *classical channel*, which would allow the transmission of classical informations:

Definition 1.6 (Classical Channel)**.** *Given two distant parties A and B, a classical channel of dimension d is an object which allows the communication from A to B or B to A of a single d-it. It can be directed and allows the transportation of a dit in only one direction, or it can be undirected and allows the transportation in any direction.*

Note that the term *distant* can refer to both geographical or temporal distance. In the second case, the channel would be a memory and parties A and B be the same party at different times. In those cases, the channel is obviously directed from the past to the future.

1.2.2 Quantum operations

We will use a variety of different operations to manipulate qudits. We will first see the definition of general quantum operations and then see more specific operations which will be of importance.

General Operations

Quantum operations are Trace Preserving Completely Positive maps [87] acting on the space of the linear operation over Hilbert spaces. Karl Kraus in 1983 [67] completely characterized such kind of operations. Any trace-preserving completely positive map $\Lambda : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ applied on a density matrix $\rho \in \mathcal{L}(\mathcal{H}_A)$ can always be written as

$$\Lambda(\rho) = \sum_i K_i \psi K_i^\dagger \tag{1.8}$$

where the $\{K_i\}_i \in \mathcal{L}(\mathcal{H}_\mathcal{A} \to \mathcal{H}_\mathcal{B})$ form a set of operators such that

$$\sum_i K_i^\dagger K_i = \mathbb{I}. \tag{1.9}$$

The elements of this set are called the Kraus operators and are the building block of purely quantum operations. We will now see more specific quantum operations which are the elementary operations to manipulate pure states.

Measurements

A general measurement in quantum mechanics pretty much boil down to the previously defined general operations. With the exception of distinguishing between the different possible outcomes of this operation. Let Λ be a measurement, characterized by the finite set of Kraus operator $\{K_i\}_i$, we call the measurement outcomes the positive semi-definite operator defined as $E_i := K_i^\dagger K_i$ for each Kraus operator. Measuring a state ρ with Λ, one reaches the outcome E_i with probability $\mathrm{Tr}(\rho E_i)$ and, in this case, modify the state as

$$\sigma_i := \frac{K_i \rho K_i^\dagger}{\mathrm{Tr}(\rho E_i)} \tag{1.10}$$

Unitary Operations

Supposing there is only one Kraus operator U, Eq. (1.9) implies that U is a unitary operator as it implies that $U^\dagger U = \mathbb{I}$. As unitary operations correspond to a change of basis [87], we will use both the terms "unitary operation" and "change of basis"

interchangeably. We will now present some preeminent unitary operations which will appear in this manuscript. First, the Pauli matrices:

$$\sigma_Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \sigma_X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_Y := \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \tag{1.11}$$

Those matrices are of extreme importance as they are one of the defining block of the stabilizer states, see Subsec. 1.4.2. Each of the Pauli matrice is diagonalizable, we will write its normalized eigenvectors corresponding to eigenvalues 1 and -1 as respectively $\{|0\rangle, |1\rangle\}$ for σ_Z, $\{|+\rangle, |-\rangle\}$ for σ_X and $\{|+_Y\rangle, |-_Y\rangle\}$ for σ_Y. As $\{|0\rangle, |1\rangle\}$ form an othornormal basis of the qubit space, we call a measurement in the X basis the measurement with Kraus operators $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. We define similarly a measurement in the Y or Z basis. The *Pauli group* is defined as $\mathcal{P}_1 :=< \sigma_X, \sigma_Z, \sigma_Y >$, which is the space generated by the Pauli matrices. Supposing we have n qubits, we can define a Pauli Group acting on each one of them. We define the n-Pauli group as the tensor product of those Pauli groups:

$$\mathcal{P}_n := \bigotimes_{i=1}^{n} \mathcal{P}_i. \tag{1.12}$$

The group of unitary operations which map the n-Pauli groups into themselves will be important to manipulate graph states. Such a set can be generated by matrices from the n-Pauli group itself and two other matrices. The first one, which can be applied on one qubit, is the Hadamard matrix, written in the $\{|0\rangle, |1\rangle\}$ basis as

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}. \tag{1.13}$$

It is the matrix which applies the change of basis from $\{|0\rangle, |1\rangle\}$ to $\{|+\rangle, |-\rangle\}$. The second one, is the controlled-Z operator. Shortened as CZ^{ST}, it is an operation which is applied on two qubits we call the source S and the target T. The CZ^{ST} operator applies a σ_Z operation on the target qubit if the source one is in the $|1\rangle^S$ state and the identity operation if the source one is in the $|0\rangle^S$ state. The CZ operator is represented in the $\{|00\rangle^{ST}, |01\rangle^{ST}, |10\rangle^{ST}, |11\rangle^{ST}\}$ basis as

$$\mathsf{CZ} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{1.14}$$

Actually, all Clifford operations can be constructed from a product of σ_X, σ_Z, H and CZ^{ST}, making it a complete set. Clifford operations are of capital importance in Measurement

Based Quantum Computation [16] or graph state distribution, see Chapter 4. In the network setting, every party possess one part of the state and can apply operation on solely its part of the state. We define the Local Unitary, LU – and respectively the Local Clifford, LC –, class of operations as the class of operations consisting of products of unitaries – respectively Cliffords – operators respecting the separation of the state into the different parties. The different classes of equivalence of the local classes of operations has been studied in [109], especially the question regarding the comparison of the LC and LU equivalence of graph states [115]. We will operate using LC operations in Chapter 4. Otherwise, we will often be interested in a larger class of operation.

LOCC

LOCC is an acronym which stands for Local Operations and Classical Communications. As already mentionned, we will investigate the transformations between quantum states shared by multiple distant parties. Each of those parties will be able to act quantumly on its part of the state, thus "Local Operations". However, in the quantum setting, distant parties will be able to communicate classically for free, thus "Classical Communications". Despite this pretty simple definition, LOCC has a very complicated structure and is difficult to find a simple mathematical closed form for it, see [27]. LOCC class of operations can be broken down as follows: we start from a state $|\psi\rangle^{A_1 \dots A_n}$ and one of the party, say A_j, perform a general measurement on its part of the state, broadcast the result of the measurement to the other parties which will apply unitary operations depending on the previous outcome. Then, another party, which can be the same, perform a measurement and so on. We say that a conversion from a state $|\psi\rangle$ to a state $|\phi\rangle$ is possible by LOCC if such a scheme can be done to deterministically implement the conversion.

Separable

Sometime, it can be simpler to consider separable operations: in terms of Kraus operators, we can write the separable operation SEP of a n-partite quantum state as

$$\mathrm{SEP}(\psi) = \sum_i K_i \psi K_i^\dagger \tag{1.15}$$

with

$$\sum_i K_i^\dagger K_i = \mathbb{I} \tag{1.16}$$

$$\text{and} \quad K_i = \bigotimes_{l=1}^{n} K_{i,l}. \tag{1.17}$$

Every LOCC operation is inside the set of separable operations – but, does not form the whole set [26] –, as such if an operation is not possible via Separable operations, it is not possible by LOCC, which is a good way to determine if a given conversion is possible via LOCC, since separable operations are far simpler mathematically.

SLOCC

Stochastic LOCCs form an even wider class of quantum communications and will be the main class of operations in Chapter 3. The operations so far implement *deterministic* transformation, meaning the conversion is done with probability 1. However, allowing the failure of a LOCC scheme and being satisfied to convert a state with at least a non-zero probability raise drastically the class' size. Stochastic LOCC form a set which includes the separable class of operations as any separable operation can be implemented by a SLOCC [27].

All the previously presented classes of operations can be sorted in a strictly inclusive hierarchy. We have that

$$\text{LC} \subsetneq \text{LU} \subsetneq \text{LOCC} \subsetneq \text{SEP} \subsetneq \text{SLOCC} \subsetneq \text{General Operations} \tag{1.18}$$

We will now see, the fundamental operations and objects which will allow the transmision of quantum information through a network.

Quantum channel

As in the classical case, we want to be able to transmit quantum states between distant parties. However, quantum information cannot be transmitted through classical channels [87], thus the need to define a quantum channel. Quantum channels are already defined in the quantum communication literature and are actually similar to the definition of a general operations. However, in our network setup, all our quantum channels will be considered perfect. Moreover, we will look at which distributions are possible under the LOCC class of operation, thus classical communications are not counted as resources in our protocols. In this context the Choi–Jamiołkowski isomorphism [28, 57] allows us to call a quantum channel of dimension d a maximally entangled pair – also called EPR pair in reference to the Einstein–Podolski–Rosen paradox [37] or Bell pair in reference to

the Bell inequality violated by those kind of state – of dimension d, written as

$$|\mathrm{EPR}^d\rangle^{AB} = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle^{AB}, \tag{1.19}$$

where we will drop the index d whenever $d = 2$.
In our setting, such a state is equivalent to a quantum channel of dimension d. Indeed, one can transmit a qudit from A to B by applying a quantum teleportation protocol [12].

Quantum teleportation protocol

We will use heavily the teleportation protocol in this manuscript. It is a LOCC protocol which perform the conversion from any state $|\psi\rangle^{A_1A_2} \otimes |\mathrm{EPR}^d\rangle^{A_3B}$ to the state $|\psi\rangle^{A_1B}$, with Hilbert space $\mathcal{H}_{A_2}$ of dimension d. In the particular case where $d = 2$. Alice will perform a joint measurement of the systems A_2 and A_3 in the EPR state basis which is given by the family of Kraus operators

$$\{\mathrm{EPR}, \sigma_X \mathrm{EPR} {\sigma_X}^\dagger, \sigma_Z \mathrm{EPR} {\sigma_Z}^\dagger, \sigma_Z \sigma_X \mathrm{EPR} {\sigma_X}^\dagger {\sigma_Z}^\dagger\} \tag{1.20}$$

where the Pauli operations are applied on A_3 and $\mathrm{EPR} := |\mathrm{EPR}\rangle^{A_2A_3} \langle\mathrm{EPR}|^{A_2A_3}$. Depending on the outcome, this operation project the state $|\psi\rangle^{A_1A_2} \otimes |\mathrm{EPR}^d\rangle^{A_3B}$ into the states $\left(\sigma_X{}^a \sigma_Z{}^b\right)^B |\psi\rangle^{A_1B}$ where a and b are the two bits giving the outcome of the measurement. Alice only has to send the two bits to Bob which will be able to correct the state by applying unitary operation on his part of the state.
This result can be readily extended to dimension d. One only has to find an orthogonal basis of unitary operators $\{U_i\}_{i\in\{1,\dots d^2\}}$ of dimension d such that $\mathrm{Tr}\left(U_i U_j^\dagger\right) = d\delta_{i,j}$. Indeed, the previous condition implies the family $\{U_i |\mathrm{EPR}^d\rangle\}$ is orthonormal as

$$\langle\mathrm{EPR}^d| U_j^\dagger U_i |\mathrm{EPR}^d\rangle = \delta_{i,j}. \tag{1.21}$$

Thus, the family of Kraus operators $\{U_i^{A_3} \mathrm{EPR}^d {U_i^{A_3}}^\dagger\}_{i\in\{1,\dots,d^2\}}$ is a complete general measurement. From there, after getting outcome i the state is given by $U_i^{B\dagger} |\psi\rangle^{A_1B}$. Alice has to transmit the outcome of the measurement to Bob. She has to send d d-its to do so. Bob will apply the appropriate correction U_i.

1.3 Measuring information

Given a communication between two parties, one may seek to minimize uses of the channels and ask, for example, the following questions: how many bits do I need to send

to transmit my message? Which states can I use for quantum communications and how can I quantify the amount of qubits I can send? We answer those two questions in this section.

1.3.1 The Shannon entropy

Definition 1.7. *Given a discrete random variable X, we define the Shannon entropy of the variable as*

$$H(X) = \sum_{i=1}^{n} P_i \log_2 \left(\frac{1}{P_i}\right) = -\sum_{i=1}^{n} P_i \log_2 P_i, \tag{1.22}$$

assuming $0 \log_2 0 = 0$.

This quantity is a cornerstone of the classical information theory. Indeed, in the fundamental scenario of a random variable X's communication, we can interpret this quantity as the quantity of bits needed to transmit without ambiguity which outcome was generated to another party [101]. Trying to get as close as possible to this theoretical minimum for objects such as written messages, images or videos is at the heart of every compression protocol. Another no-less-fundamental scenario, sometimes the sink possess some prior information about which outcome was generated by the source. This prior information can be modelized as a random variable Y correlated to X. The two random variables share a joint probability distribution defined by $P(x_i, y_j)$: the probability that X outcome is x_i and Y outcome is y_j. We also define the *conditional probability*:

Definition 1.8 (Conditional probability)**.** *Given two random variables X and Y, taking respectively value in the sets $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_m\}$ and sharing a probability distribution P. We define the conditional probability of X having outcome x_i knowing Y had outcome y_j as*

$$P(x_i|y_j) := \frac{P(x_i, y_j)}{P(y_j)}. \tag{1.23}$$

We may – and will – inquire about the quantity of bits we need to send given the sink possess a random variable Y which is correlated to the source random variable X. This quantity is defined as the *conditional entropy*:

Definition 1.9 (Conditional entropy)**.** *Given two random variables X and Y, each taking respectively value in the set $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_m\}$. We define the conditional entropy of X knowing Y as*

$$H(X|Y) = -\sum_{i,j=1}^{n,m} P(x_i, y_j) \log_2 P(x_i|y_j) = H(X, Y) - H(Y); \tag{1.24}$$

where $P(x_i, y_j)$ is the probability to have both outcomes x_i and y_j at the same time and $P(x_i|y_j)$ is the probability to have outcome x_i knowing we had outcome y_j.

The conditional entropy $H(X|Y)$ can be interpreted as the number of bits a source needs to transmit to a sink possessing a correlated random variable Y. We note that this quantity cannot be negative as it is a property which is not shared by its quantum counterpart.

1.3.2 The Von Neumann entropy and measuring entanglement

We introduced in Subsec. 1.1.2, the notion of the separability of states and entanglement. One simple way to determine whether a pure state $|\psi\rangle^{AB}$ is separable is to trace partially over one of the two Hilbert spaces sharing the state.

Definition 1.10 (Partial Trace)**.** *We define the partial trace on B over a state $|\psi\rangle^{AB}$ as*

$$\psi^A := Tr_B\ \psi^{AB} = \sum_i \langle b_i|\ \psi^{AB}\ |b_i\rangle \tag{1.25}$$

where $\{|b_i\rangle\}$ is a basis of the Hilbert space associated to party B. The result is called the reduced state of A.

If after tracing over B the state is still pure, then $|\psi\rangle^{AB}$ is separable regarding the birepartition $\{\{A\}, \{B\}\}$. We can go further by defining the Von Neumann entropy for quantum states.

Definition 1.11. *Given a mixed state ψ, we define the Von Neumann entropy as*

$$S(\psi) := -Tr\,\psi \log_2 \psi = -\sum_i \lambda_i \log_2 \lambda_i \tag{1.26}$$

where, as before, λ_i are the eigenvalues of ψ.

It is the quantum equivalent of the classical Shannon entropy, see Def. 1.7. Indeed, given a state $|\psi\rangle^{AB}$, the Von Neumann entropy of the reduced state of A quantifies the amount of qubits that have to be sent to transmit the part of the state owned by A to B – see Schumacher compression [99] . Moreover, for bipartite pure states, the Von Neumann entropy of the reduced state of each party is a good measure of entanglement [87]. As such, we will note the entanglement of a pure bipartite states as the local entropy of this state: the Von Neumann entropy of one of the party's reduced state,

$$E(|\psi\rangle^{AB}) := S(\psi^A). \tag{1.27}$$

1.3.3 Useful Properties of the Von Neumann entropy

The Von Neumann entropy will be one of the major tools of Chapter 2. In this section, we will review some interesting properties which will be used later. First, if ψ is the density matrix of a pure state $\psi = |\psi\rangle \langle\psi|$, then

$$S(\psi) = -\log_2(1) = 0. \tag{1.28}$$

As such, to know if a bipartite state $|\psi\rangle^{AB}$, is separable, we only need to compute the entropy of the partially traced state ψ^A, and see whether it is null.
Second property, for a pure state $|\psi\rangle^{AB}$,

$$S(\psi^A) = S(\psi^B), \tag{1.29}$$

this property is used heavily in Subsec. 2.2.3. It can be easily proved by Schmidt decomposing $|\psi\rangle^{AB}$ and computing both quantities. Third property, if a state is separable regarding one of its bipartitions, the Von Neumann entropy of the state is the sum of the two tensor product's terms entropy, i.e.

$$S(\psi^A \otimes \psi^B) = S(\psi^A) + S(\psi^B) \tag{1.30}$$

Another extremely used properties in Chapter 2, is the strong subadditivity of the entropy:

Lemma 1.1 (Strong subadditivity)**.** *Given a quantum state ψ^{ABC} shared by 3 parties, the following inequality is always true,*

$$S(\psi^{ABC}) + S(\psi^B) \leq S(\psi^{AB}) + S(\psi^{BC}). \tag{1.31}$$

If the state ψ^{ABC} is pure, this inequality reduces to a standard subadditivity inequality:

Corollary 1.1. *Given a quantum state ψ^{AC} shared by 2 parties, the following inequalities are always true,*

$$|S(\psi^A) - S(\psi^C)| \leq S(\psi^{AC}) \leq S(\psi^C) + S(\psi^A). \tag{1.32}$$

Last but not least among the properties, for a state ψ^{AB}, the local entropy of each party is invariant by local unitary operation. For U_A, a unitary operation acting on the part of the system own by A,

$$S(\psi^A) = S(U_A \psi^A U_A^\dagger). \tag{1.33}$$

Moreover, the entanglement of a pure states cannot increase through a LOCC protocol [86]. We will now see a big point of divergence between classical and quantum entropy.

1.3.4 Conditional entropy

As in the classical case, one can define the conditional Von Neumann entropy for a state ψ^{AB} as

$$S(\psi^{AB}, A|B) := S(\psi^{AB}) - S(\psi^{A}). \tag{1.34}$$

Since conditional Shannon entropy represented the number of bits that a source needed to transmit to a sink possessing a correlated random variable, one could follow a similar logic and deduce that conditional Von Neumann entropy should symbolize the amount of entanglement necessary to transport a part of a state shared by two parties where the receiving party already own partially said state. However, computing the conditional entropy of some states, for example the EPR pair, one finds

$$S(\mathrm{EPR}^{AB}, A|B) = S(\mathrm{EPR}^{AB}) - S(\mathrm{EPR}^{A}) = 0 - 1 = -1 \tag{1.35}$$

Does that mean we can increase entanglement by trying to transport a part of the states? We will give the solution latter in Subsec. 2.2.2. For now, we will present major classes of quantum states.

1.4 Resource States

In this section, we review specific quantum states we will try to distribute over quantum networks in Chapter 3 and Chapter 4. Those states are resources for several quantum information applications, we will see which specifically.

1.4.1 GHZ states

GHZ states stand for Greenber-Horne-Zeilliger states as they form the generalization of EPR pairs to multipartite states. They present a kind of entanglement which goes beyond the bipartite one [112]. Formally, we can define a GHZ state over n qubits as:

$$|\mathrm{GHZ}_n\rangle^{A_1A_2\ldots A_n} := \frac{1}{\sqrt{2}}\left(|00\ldots0\rangle^{A_1A_2\ldots A_n} + |11\ldots1\rangle^{A_1A_2\ldots A_n}\right). \tag{1.36}$$

GHZ states can be defined as well over qu$d$-its as

$$|\mathrm{GHZ}_n^d\rangle^{A_1A_2\ldots A_n} = \frac{1}{\sqrt{d}}\sum_{i=1}^{d}|ii\ldots i\rangle^{A_1A_2\ldots A_n}. \tag{1.37}$$

We define the GHZ class of state as the set encompassing all the states which are LU equivalent to a GHZ state. This class is an important part of the quantum information

theory as they can be used in several kinds of schemes such as quantum secret sharing [69] and quantum metrology [36].

1.4.2 Graph States

We define the graph states as a subset of the stabilizer's class of state. A stabilizer state [48] over n qubits is a state which is stabilized – in other words, left invariant by application – by n independent elements of $\mathcal{P}_n$ excluding the trivial identity stabilizer. Graph states are defined from simple graph – a graph with only simple undirected edges and no self-loop –, as follow: each vertex is associated to a qubit of $|G\rangle$ and for each vertex $v \in V$, $|G\rangle$ is stabilized by

$$\sigma_X^v \prod_{u \in N_v} \sigma_Z^u, \tag{1.38}$$

where N_v is the neighbourhood of v. From this definition a description of graph states in terms of pure quantum states is deduced:

Definition 1.12 (Graph States)**.** *Let $G = (V, E)$ be a simple undirected graph, where V is the set of the graph's vertices and E is the set of the graph's edges. The graph state $|G\rangle$ is a multipartite state shared by the parties $v \in V$. We can construct the graph state $|G\rangle$ by initializing the state as the product of $|+\rangle^v$ states. Which is*

$$\bigotimes_{v \in V} |+\rangle^v \tag{1.39}$$

and apply a CZ *gate between v_i and v_j if and only if $\{v_i, v_j\} \in E$.*

In short, graph states can be depicted as a graph, each vertex of the graph representing a qubit and each edge a previous entangling interaction between said qubits. Note that, the graph states which are depicted as star graphs – graphs where only a single vertex is linked to all the others – or as complete graph – graphs in which every vertex is linked to all the others – are LU equivalent to the GHZ state, this will prove to be useful in Chapter 4. The prominence of graph states in a large number of applications, such as Measurement Based Quantum Computing [16], error corrections [9] or quantum metrology [102] makes it an inescapable type of state to study when one is looking for quantum states distribution protocols over quantum network, which is what we are doing specifically in Chapter 4. We can convert a graph state into another using only measurements in the X, Y and Z basis and a special operation called local complementation [48]. We will see each of these operations in Sec. 2.1.

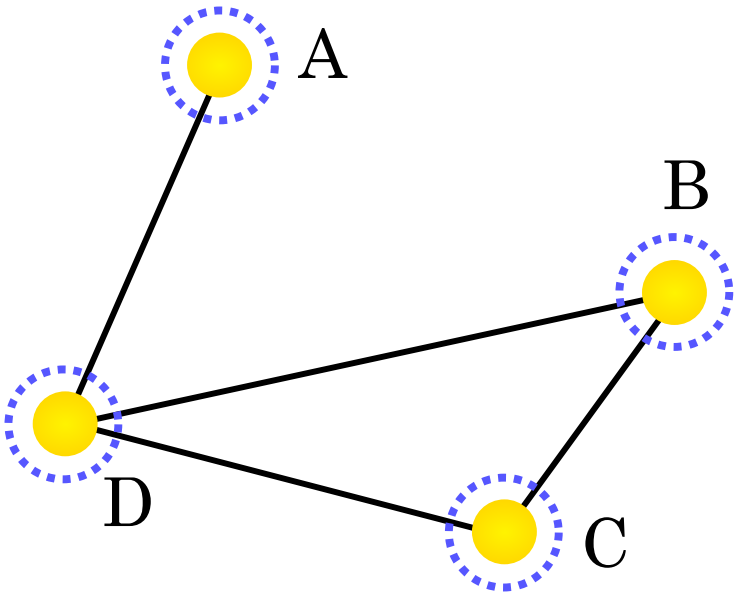

Figure 1.2: Representation of a graph state as a graph. Each node depicts a qubit and each edge depicts a CZ gate applied between the two qubits.

1.5 The network setting

We will finally see the global setting on which our protocols are based.

1.5.1 Networks definition

Whether it is classical or quantum, we model a network as a set of nodes v linked by perfect channels e allowing the exchange of (qu)dits of dimension d_e. Formally, the network is defined as the weighted graph $H = (V, E, D_E)$: V is the set of all nodes v, $E \subset V^2$ is the set of all channels e and D_E is the set of the channels' dimension d_e. For $v \in V$, we call N_v the neighbourhood of v which is the set of all nodes sharing a channel with v. As previously written, a classical channel of dimension d_e can pass a d_e-it and a quantum channel of the same dimension can pass a qud_e-it.
We wish to study which distribution tasks are possible over a given network. Distribution tasks are defined differently whether one consider the quantum or the classical setup: in the first case, the task is the distribution of a specific quantum state among the clients; in the latter case, it is a distribution of a discrete random variable over the network. To define a distribution task, we also need to know its set of clients, which are the nodes sharing the final correlation – either a quantum state or a classical random variable –

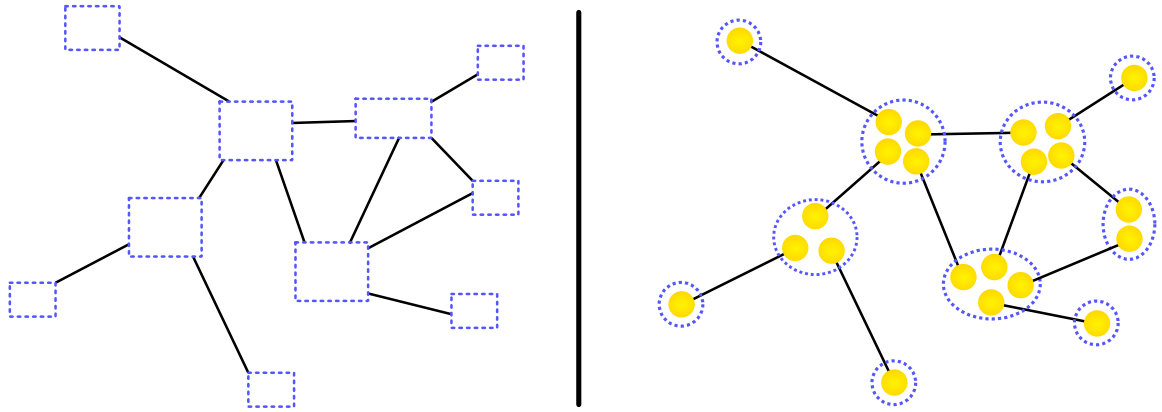

Figure 1.3: On the left, depiction of a classical network. Each blue dotted square is a classical node which can do classical arithmetic operations on its inputs and map the result to its outputs. Each edge is a perfect classical channel which can transmit one dit. On the right, depiction of a quantum network presenting the same topology. Each blue dotted circle is a node, which can apply arbitrary quantum operations on its qudits and send classical information to the other nodes. Each yellow circle is a qudit and is paired with another to form a maximally entangled pair, depicted as an edge between the two nodes. Each of these maximally entangled state can transmit one qudit.

after distribution. Without loss of generality[1], the leaves of the network – the nodes of degree 1 – will be the clients and we denote the set of all the network clients as $C \subset V$.

1.5.2 Routing through a network

In the classical setup, in order to perform the most fundamental communication – distributing information from a source to a sink – we can simply follow a path through the network, call it a route and calling the study of how to establish such a route, the study of routing. In an ideal world, one would want this path to be as short as possible, which led to the creation of several algorithms which could compute shortest paths or approximate shortest paths [47]. In the quantum setup, the equivalent objective is to transmit a qudit or to establish a maximally entangled pair between two clients of the system. This can be done using entanglement swapping, which is simply a quantum teleportation between two maximally entangled pairs. If this operation can be implemented on each intermediary node of the network, classical routing technique can be used to route information throught a quantum network. Some differences arise from the error correction part since quantum information cannot be cloned. However, we will focus on *multipartite communications*,

[1] A client leaf can be formally added for non-leaf clients, and non-client leaves can safely be ignored and removed from the network.

and what is coined by this term is the topic of the next subsection.

1.5.3 Multicast communication

As it happens, there are often more than two clients in most of the networks. Actually, there is a high chance for a network to have a huge number of clients and a non-negligible part of the networks' studies focus on large networks [5, 30]. In terms of communication, the multicast scenario happens when groups of clients wants to communicate together and want to share a service proposed by the network. In the classical setting, those clients could want to see the same match of football which is beyond a paywall or some clients could want to synchronize the streaming of a video to watch it at the same time. In the quantum setting we will analyze and distinguished 3 different scenarios, each one corresponding to one Chapter. First scenario, one group of clients wants to share several GHZ states to perform a secret sharing protocol or to share a graph state to perform distributed computations or trying to enhance the precision of some measure in quantum metrology. In this case, establishing EPR may not be the best solution. One could want to implement directly the specific operations needed to make a multipartite state grow inside the network. The routing here would be a bit different, one would need to find a minimal tree spanning all the clients which want to communicate, this question is treated in Chapter 4 and a solution is implemented on a quantum network's simulation. The second scenario arise from the fact that a network is a global public shared resource. If every clients wants to communicate between themselves at the same time, there might not be enough resources to satisfy everyone with routing. Managing simultaneous communications and controlling the possible resulting congestion is a necessary feature of a global network. We analyse and try to give means to analyze those distributions in Chapter 3. The third scenario concerns recycling of previously distributed resource. Entanglement is precious in quantum networks, how can one make at most use of it ? Can we convert a previous state into a new wanted one ? This is an answer we will reply to in the first Chapter of this manuscript, I named Chapter 2.

1.6 Notations

S: Source – the emitter – of the communication
T: Sink – the receptor – of the communication
A bit: The smallest unit of information, can take two values, 0 and 1

$X(O, P)$: random discrete variable with outcome O and probability distribution P
$\mathcal{H}$: Hilbert space
$\mathcal{L}(\mathcal{H})$: Space of linear operator over Hilbert space
$|\psi\rangle$: Pure quantum state
A qubit: A pure quantum state of dimension 2
ψ: The associated density matrix of $|\psi\rangle$
A party: An entity able to own several qudit on which it can perform quantum operation and is able to communicate classicaly with other party
Bipartite state: A state shared by two parties
Multipartite state: A state shared by several parties
Separable regarding a partition: A state which can be written as a product of state respecting the partition
Entangled state regarding a partition: A state which is not not separable regarding the partition
General Measurement: A set of Kraus operators $\{K_i\}$ giving outcome i with probability $\mathrm{Tr}(\rho E_i)$ and modify the measured state as $\sigma_i := \frac{K_i \rho K_i^\dagger}{\mathrm{Tr}(\rho E_i)}$
U: unitary operations
K_i: Kraus operators
σ_Z, σ_X, σ_Y: Pauli matrices
H: Hadamard matrix
CZ: Controlled-Z gate
LU: Local Unitary class of operation
LC: Local Clifford class of operation
LOCC: Local quantum Operation and free Classical Communication class of operation
SEP: Separable class of operation
SLOCC: Non-deterministic LOCC
$|\mathrm{EPR}^d\rangle$: A maximally entangled state of dimension d
Quantum Channel of dimension d: A state $|\mathrm{EPR}^d\rangle$ and two classical bits
$G = (V, E)$: Graph with vertices V and edges E
N_v: Neighbourhood of vertex v
$S(\psi^A)$: Von Neumann entropy of party A regarding the state ψ
$E(|\psi\rangle^{AB})$: Entanglement of the state $|\psi\rangle$
$S(\psi, A|B)$: Conditionnal entropy of A knowing B, regarding the state ψ
$|\mathrm{GHZ}_n^d\rangle$: Multipartite entangled state of dimension d, generalization of EPR pair to n-parties

$|G\rangle$: Graph state associated to the simple graph G
$H = (V, E, D_E)$: Network with nodes V, channels E and channels' dimension D_E
C: The set of the network's client. Also, leaf of the network.
Classical distribution task: Distributing a discrete random variable
Quantum distribution task: Distribution of a quantum state

Chapter 2

An asymptotic view on multipartite state distribution

I worked on the subject presented here with Alexander Streltsov[1] and Jens Eisert[2]. A part of it has been done before the beginning of my PhD but, the main part of the work was left incomplete and stayed in this state while I was finishing my master. Nevertheless, once I became a PhD candidate, we decided to revisit and complete the whole work. As a result, I visited Jens Eisert's institute, and was joined by Alexander Streltsov, for 3 months during which we collaborated. The resulting paper got accepted in Physical Review Letter [107] and we will present these results in the rest of this chapter.

Entanglement is a crucial resource for an important part of all quantum protocols; it is the major resource in quantum repeater networks as it is the main ingredient needed to perform quantum teleportation amongst other things[12, 94]. It is not surprising one of the earliest questions [10] in the field were "How can we transform one form of entanglement into another?" and "how can we switch from an entangled state into another?". The consequence being that the determination of the rate of conversion between bipartite states – we will see it in Subsec. 2.1.1 – is one of the earliest results of quantum information theory [10, 86]. However, the generalization of this result to multipartite states was left unsolved and is still on hold. This is a shame since creating entanglement

[1]Centre for Quantum Optical Technologies, Centre of New Technologies, University of Warsaw, Banacha 2c, 02-097 Warsaw, Poland

[2]Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany

is undeniably costly in quantum networks and one would want to use as much as possible of the available resources, specifically in networks featuring bottlenecks, which could be virtually any network if we increase the usage which is made of it. Building on these thoughts, it seemed imperative to us for previously distributed states to be reused as much as possible by converting them into desired resources rather than using more precious entanglement. Which is why we decided to tackle this old question one more time, trying to define more clearly what is the asymptotic rate of conversion between two arbitrary pure states. This section is ordered as follow: I first – in Sec. 2.1 – present the setup and the previously mentioned result concerning bipartite conversion as it readily gives an upper bound on the multipartite one. Then, I introduce – in Sec. 2.2 – the two major tools used in this paper: *quantum state merging* and *entanglement combing*. After that, I present – in Sec. 2.3 – a new lower bound on the conversion between tripartite pure states which outperforms any previously known bound. Finally, I generalize – in Sec. 2.4 – the result to $N+1$-partite states, where N is a whole number superior to 2.

2.1 Preliminaries

The most important notions used in this chapter are presented in Chapter 1 as:

- Quantum Operation, LOCC Subsec. 1.2.2
- Entanglement and Von Neumann entropy, Sec. 1.3

In this section, I will present the first major result concerning asymptotic conversion between bipartite pure states in Subsec. 2.1.1. Then, I will define formally the multipartite setup in Subsec. 2.1.2.

2.1.1 The bipartite case

The setup is the following: two geographically distant parties, Alice and Bob, share n copies of an entangled state. We can Schmidt decompose – see Subsec. 1.1.2 – each pair and write the i^{th} one as:

$$|\psi\rangle^{A_iB_i} = \sum_{j=0}^{d-1} \sqrt{p(j)}\, |j\rangle^{A_i} \otimes |j\rangle^{B_i}, \tag{2.1}$$

where each A_i is a subparty of Alice – see Subsec. 1.1.2; the same applies for each B_i and Bob.

The issue is that Alice and Bob are rather picky. They say the state $|\psi\rangle$ is only partially

entangled and, thus, would add noise to any qubit teleported thought them – it's true –, they would rather share copies of maximally entangled states such as EPR pairs to perform quantum teleportation with a near perfect fidelity. To that effect, they need to find a LOCC Λ such that $|\psi\rangle^{\otimes n}$, the initial state shared by them, is converted into as much as possible copies k of the maximally entangled state $|\text{EPR}\rangle$. We can measure the quality of the conversion protocol Λ by defining the rate of conversion R_Λ, which is the number k of state $|\text{EPR}\rangle$ extracted divided by the original number n of states $|\psi\rangle$.

$$R_\Lambda(|\psi\rangle^{\otimes n} \to |\text{EPR}\rangle^{\otimes k}) := \frac{k}{n}. \tag{2.2}$$

Of course, the aim is to find a Λ which maximize the amount of copies extracted . As such, we define the rate of conversion as

$$R(|\psi\rangle^{\otimes n} \to |\text{EPR}\rangle^{\otimes k}) := \sup_\Lambda R_\Lambda. \tag{2.3}$$

In their groundbreaking paper of 1996 [10], Charles Bennett et al. proved that in the asymptotic limit – taking the limit of having an infinite number n of copies –, we can find a LOCC such that the rate of conversion is determined by the sole bipartite entanglement measure – see Subsec. 1.3.2 of the state $|\psi\rangle$ as

$$R(|\psi\rangle \to |\text{EPR}\rangle) := \lim_{n\to\infty} R(|\psi\rangle^{\otimes n} \to |\text{EPR}\rangle^{\otimes k}) = E(|\psi\rangle) \tag{2.4}$$

The result was even stronger as the operation is completely reversible. Indeed, we can theorically distill from badly entangled pairs, but we can also dilute maximally entangled pairs without losing entanglement, the rate of conversion in this case is simply

$$R(|\text{EPR}\rangle \to |\psi\rangle) = \frac{1}{E(|\psi\rangle)}. \tag{2.5}$$

The rate of conversion between arbitrary states is fully computable using this reversible conversion from and into EPR as a medium operation. This leads to the following seminal result: the asymptotic rate of conversion between two pure states $|\psi\rangle$ and $|\phi\rangle$ is determined as

$$R(|\psi\rangle \to |\phi\rangle) = \frac{E(|\psi\rangle)}{E(|\phi\rangle)}. \tag{2.6}$$

This result makes the resource character of bipartite entanglement most manifest: the entanglement content is given simply by its content of maximally entangled states, and each form can be transformed reversibly into another and back.

2.1.2 Multipartite Setting

The situation is more complex when considering multipartite states. There are no measure which can describe as perfectly multipartite entanglement and research work is still ongoing to find a good operational measures [100]. Moreover, there is several kinds of maximally entangled states which cannot be transformed into one another by LOCC – or even SLOCC –, this prevents to find a resource state equivalent to the EPR state for the multipartite setting. For the tripartite case, there is two non-equivalent classes of states, the GHZ_3 class – see Subsec. 1.4.1 – and the class arising from the W state – $|W\rangle := \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$ –, which cannot be transformed into one another and back even by SLOCC [83]. For an even higher number of parties, the number of non-equivalent classes explodes [43]. As such, the rates which can be achieved when aiming at asymptotically transforming one N-partite state – where N is a whole number – into another with LOCC are far from clear. Several resource theories find a global setup from which we can find a resource characterization of multipartite entanglement [31, 15]. It is at the cost of considering a larger class than LOCC. However, the LOCC setup seems more relevant for a quantum network theory as it is the closest to a real networking setting. For these reasons, we decided to study the specific problem of finding the rate of asymptotic conversion between a given pair of states using LOCCs. In particular, we were interested in the optimally achievable asymptotic rate for this procedure, which we formally defined as the maximum rate of conversion when the number of initial copies goes to infinity,

$$R(|\psi\rangle \to |\phi\rangle) = \sup\left\{ r : \lim_{n\to\infty} \left(\inf_{\Lambda} \left\| \Lambda\left(|\psi\rangle^{\otimes n}\right) - |\phi\rangle^{\otimes \lfloor rn \rfloor} \right\|_1 \right) = 0 \right\}. \tag{2.7}$$

Here, Λ reflects a N-partite LOCC operation. When there is no ambiguity we will denote $R(|\psi\rangle \to |\phi\rangle)$ as R. The methods we developed were built upon and further developed the machinery of *entanglement combing*, which has been introduced and studied for general N-partite scenarios in [114] and is itself based on quantum state merging [51, 52], assisted entanglement of distillation [34, 104] and time-sharing – using resource states as different roles in the asymptotic protocol. We will introduce those notions in the next section through a brief outline.

2.2 Asymptotic entanglement manipulation

2.2.1 Entanglement of assistance

For a tripartite pure state $|\psi\rangle^{ABR}$, the assisted entanglement distillation is defined as the following setup. Alice and Bob want to communicate by using bipartite entangled state, however the only state they possess is entangled with a referee R. In order to extract bipartite entanglement between Alice and Bob, R will measure its part of state. For a given measurement Λ producing outcome $|\phi_i\rangle^{AB}$ with probability p_i, the average entanglement extracted between Alice and Bob is equal to

$$E_{\Lambda,|\psi\rangle} := \sum_i p_i S(\phi^A). \tag{2.8}$$

The entanglement of assistance is defined as the maximum over all the possible measurements of this quantity,

$$E_a(|\psi\rangle) := \sup_\lambda E_{\lambda,\psi}. \tag{2.9}$$

In [104], Smolin et al. proved the asymptotic entanglement of assistance defined as

$$E_a^\infty(|\psi\rangle) := \lim_{n\to\infty} \frac{1}{n} E_a(|\psi\rangle)^{\otimes n} \tag{2.10}$$

was equal to the minimum of the local entropy of Alice and Bob, i.e.

$$E_a^\infty(|\psi\rangle) = \min\{S(\psi^A), S(\psi^B)\} \tag{2.11}$$

This result will help us to prove Lemma 2.1.

2.2.2 State Merging

In the case the hurried reader did not read Sec. 1.3, I remind them quantum information can be negative. Indeed, if one evaluates the conditional entropy of an EPR pair $|\mathrm{EPR}\rangle^{AB}$, one finds

$$S(\mathrm{EPR}^{AB}, A|B) = S(\mathrm{EPR}^{AB}) - E(|\mathrm{EPR}\rangle^{AB}) = -1. \tag{2.12}$$

As explained in Section 1.3, the Von Neumann entropy is the quantum analogous of the Shannon entropy for classical information theory. As such, it can be interpreted as the minimal number of qubits needed to transmit a quantum state. Pursuing the analogy, the conditional Von Neumann entropy should be the minimal number of qubits needed to transmit part of quantum state to another party which already share a part of the very same quantum state. As such, what does mean a negative conditional entropy?

It was a big interpretative issue until the paper of Horodecki et al. [51] in which the authors managed to make sense of it by introducing the notion of *quantum state merging*. The setup is the following. A state $|\psi\rangle^{ABR}$ is a tripartite state shared by 3 parties, Alice, Bob and a Referee. Using only LOCC and previously shared entanglement – which will be used as a channel –, Alice has to transfer her part of the state to Bob, see Fig. 2.1 for a depiction of quantum state merging. The question is: how much entanglement is needed? This question is answered for the asymptotic regime in the cited paper: the asymptotic entanglement cost is equal to the very same conditional entropy.
In this setup, the operational meaning of the conditional entropy's negativity becomes clear. First, if the cost of the merging is null, it means no entanglement is necessary and only classical information has to be sent. Then, if the cost is strictly negative, not only we solely send classical information, but also, partial entanglement from the initial state $|\psi\rangle^{ABR}$ will remain between Alice and Bob after the merging. This entanglement will be available to use for further quantum communications between them. This leads to an increase of quantum communication resources at a rate of $r = -S(\psi^{AB}, A|B)$ EPR states between Alice and Bob and thus, a negative cost. The existence of this negative cost is at the heart of the entanglement combing.

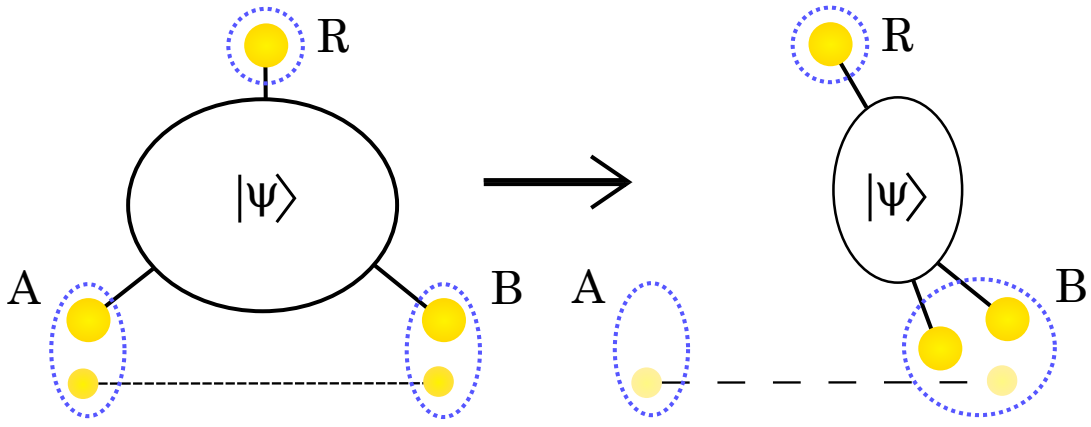

Figure 2.1: Depiction of the quantum state merging protocol. After the protocol, the part of the state previously owned by Alice is now owned by Bob. The dotted line symbolizes the pre-shared bipartite entanglement between Alice and Bob which can be used – or be increased – by the state merging protocol.

2.2.3 Entanglement Combing

Introduced in [114], entanglement combing is a useful tool to study asymptotic transformations. It is a LOCC protocol which converts any multipartite entangled state into a tensor product of bipartite states centered on one of the parties. The central party does not lose any entanglement regarding the rest of the system while the other parties are decorrelated from each other. This makes this protocol considered by its authors as being "lossless", at least concerning the entanglement of one party. Naming the central party as Alice and the other parties as Bobs, labeled from B_1 to B_N, we write the result of an entanglement combing as a tuple containing the amount of bipartite entanglement extracted from the process with each Bob. For a depiction of combing, see Fig. 2.2.
We will denote as E_i the amount of bipartite entanglement between Alice and the ith Bob after the combing, and so the resulting tuple as $F = (E_1, E_2, \ldots, E_N)$. As the local entanglement of Alice is left untouched and all the Bobs are decorrelated from each other, we can rewrite the property of the Von Neumann entropy concerning product state – see Subsec. 1.3.2 – as

$$\sum_{i=1}^{N} E_i = S(\psi^A), \tag{2.13}$$

where $|\psi\rangle$ is the initial state on which the combing is applied. As seen in the previous subsection, merging Bobs to Alice can lead to an increase of the bipartite entanglement. This phenomenon is at the heart of entanglement combing and allows the conversion to be made asymptotically without borrowing entanglement from external sources [114]. A very important result we will use in this work is the following theorem and concerns the

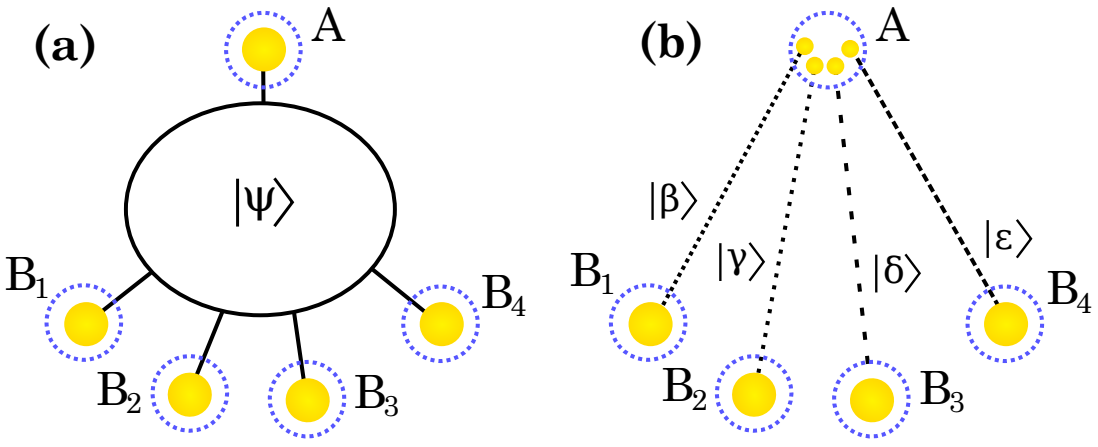

Figure 2.2: Depiction of the entanglement combing protocol. The state after the combing is the product of bipartite states between Alice and all the Bobs. Each one with entanglement E_i

set of achievable entanglement tuples:

Theorem 2.1 (Distribution of entangled pairs [114]). *The feasible set of different entanglement distributions in entanglement combing $F = (E_1, E_2, \ldots, E_N)$ for a given initial state $|\psi\rangle^{A,B_1,\ldots,B_N}$ is a polytope: it is the positive part of the convex polytope formed by the points given by merging the state's part of the N Bobs to Alice in different orders. Examples of such points can be found in Eq. (2.46) and Eq. (2.47).*

This result is given by an adequate use of the quantum state merging negative entropy and time-sharing. We will now see how we used those two tools to establishing our lower bound on the rate of asymptotic conversion.

2.3 The tripartite case

In this section, we focus on the tripartite case. Alice – labelled as A –, Bob – labelled as B – and Charlie – labelled as C – share an asymptotic number of a state $|\psi\rangle^{ABC}$ and wish to convert it into as many copies as possible of a state $|\phi\rangle^{ABC}$. In this section, we try to find lower and upper bounds on the asymptotic rate of conversion $R(|\psi\rangle^{ABC} \to |\phi\rangle^{ABC})$ between those two pure states. The study of this case already shows interesting results while providing clues on the methods which will be used on the $N+1$-partite case.

2.3.1 First observations

The upper bound given for the bipartite case in Eq. (2.6) already provides an upper bound on the tripartite case. Indeed, as made precise at the end of the "Bipartite and Multipartite states" paragraph Subsec. 1.1.2, every multipartite protocol – and so, every tripartite protocol – is bipartite regarding any of its bipartitions. As such, the optimal conversion rate using multipartite operations cannot exceeds the conversion rate given for bipartite conversion, and so,

$$R(|\psi\rangle^{ABC} \to |\phi\rangle^{ABC}) \leq \min\left\{\frac{S(\psi^A)}{S(\phi^A)}, \frac{S(\psi^B)}{S(\phi^B)}, \frac{S(\psi^C)}{S(\phi^C)}\right\}. \tag{2.14}$$

Whether this upper bound is achievable or not is mostly a case-by-case study and we know non-trivial conversions which achieve this upper bound and conversions which cannot. For example, if the desired final state $|\phi\rangle^{ABC}$ is a GHZ_3 the bound in Eq. (2.14) is known to be achievable whenever one of the reduced states ψ^{AB}, ψ^{BC} or ψ^{AC} is separable [104].

On the contrary, the following conversion

$$|\mathrm{GHZ}_3\rangle^{A_1B_1C_1} \otimes |\mathrm{GHZ}_3\rangle^{A_2B_2C_2} \to |\mathrm{EPR}\rangle^{A_1B_1} \otimes |\mathrm{EPR}\rangle^{A_2C_1} \otimes |\mathrm{EPR}\rangle^{B_2C_2}, \tag{2.15}$$

in which the parties aim to transform two GHZ states into EPR pairs which are equally distributed among all the parties, is known to be impossible to perform with unit rate [73]. However, computing the upper bound of Eq. (2.14), one finds that both states' local entropies are equal to 2 and finds the rate of conversion to be upper bounded as $R \leq 1$ which means the upper bound cannot be reached in this case.
Those examples suggest that the bound in Eq. (2.14) is a very rough estimate for general transformation and is saturated only for very specific sets of states – e.g. states with separable reduced states in the first example – having zero volume in the set of all pure states. However, we will see this is not the case: in the next section we compute a general lower bound for arbitrary conversion between pure states and show this lower bound is equal to the upper bound of Eq. (2.14) for a large family of states.

2.3.2 Establishing a lower-bound

As mentioned earlier, we will start from the result of entanglement combing described in Subsec. 2.2.3. In the specific tripartite setting, entanglement combing aims to transform the initial state $|\psi\rangle^{ABC}$ into a state of the form $|\mu\rangle^{A_1B} \otimes |\nu\rangle^{A_2C}$ with pure bipartite states $|\mu\rangle$ and $|\nu\rangle$. The following Lemma restates the results of combing in a form which will be suitable for our main theorem.

Lemma 2.1 (Conditions from tripartite entanglement combing)**.** *The transformation*

$$|\psi\rangle^{ABC} \to |\mu\rangle^{A_1B} \otimes |\nu\rangle^{A_2C} \tag{2.16}$$

is possible via asymptotic LOCC if and only if

$$E(|\mu^{A_1B}\rangle) + E(|\nu^{A_2C}\rangle) \leq S(\psi^A), \tag{2.17a}$$
$$E(|\mu^{A_1B}\rangle) \leq S(\psi^B), \tag{2.17b}$$
$$E(|\nu^{A_2C}\rangle) \leq S(\psi^C), \tag{2.17c}$$

Proof. The direct part of the statement is immediate. Indeed, if the transformation is possible, the left-side of the inequalities give the local entropy of respectively Alice, Bob and Charlie post-conversion, while the right ones give the pre-conversion's ones. Yet, LOCC protocols cannot increase the local entanglement of a state, see Subsec. 1.3.3,

making the direct statement a rewriting of the non-increasing local entropies under the action of a LOCC protocol. The transformation is not possible if any of the inequalities of the statement is violated.

We will show the converse statement, i.e., any pair of pure states $|\mu\rangle^{A_1B}$ and $|\nu\rangle^{A_2C}$ which fulfill the inequalities (2.17) can be obtained from $|\psi\rangle^{ABC}$ via LOCC in the asymptotic limit. Considering the local entropy of each party – $S(\psi^A)$, $S(\psi^B)$ and $S(\psi^C)$ –, we have to separate into 3 cases whether $S(\psi^A)$ is respectively superior to, inferior to or framed between the two other entropies. Depending on the case, we apply quantum state merging – Subsec. 2.2.2 – or assisted entanglement distillation – see Subsec. 2.2.1 – and use time-sharing between the different obtained protocols.

Case 1: $S(\psi^A) \geq S(\psi^B) \geq S(\psi^C)$**.** In this case, Bob can send his part of the state $|\psi\rangle$ to Alice by applying quantum state merging – Subsec. 2.2.2 and [52]. This procedure is possible by using asymptotic LOCC operations between Alice and Bob. Additionally, Alice and Bob gain EPR pairs at rate

$$-S(\psi^{ABC}, B|A) = S(\psi^A) - S(\psi^{AB}) = S(\psi^A) - S(\psi^C). \tag{2.18}$$

where in the second equality, we used the second property of the entropy regarding bipartite pure states: $S(\psi^{AB}) = S(\psi^C)$, see Subsec. 1.3.3 Eq. (1.29). The overall process, thus, achieve the transformation $|\psi\rangle^{ABC} \to |\mu\rangle^{A_1B} \otimes |\nu\rangle^{A_2C}$ with the bipartite states $|\mu\rangle$ and $|\nu\rangle$ having an entanglement of

$$\begin{aligned} E(|\mu^{A_1B}\rangle) &= S(\psi^A) - S(\psi^C), \\ E(|\nu^{A_2C}\rangle) &= S(\psi^C). \end{aligned} \tag{2.19}$$

Alternatively, Charlie can send his part of the state $|\psi\rangle$ to Alice, thus gaining EPR pairs at rate $S(\psi^A) - S(\psi^B)$.

$$\begin{aligned} E(|\mu^{A_1B}\rangle) &= S(\psi^B), \\ E(|\nu^{A_2C}\rangle) &= S(\psi^A) - S(\psi^B). \end{aligned} \tag{2.20}$$

In the next step we apply-time sharing, i.e., the first procedure is performed with probability p and the second with probability $(1-p)$ on the available copies of $|\psi\rangle$. In this way, we see that the transformation from $|\psi\rangle^{ABC}$ to $|\mu\rangle^{A_1B} \otimes |\nu\rangle^{A_2C}$ is possible for any pair of states $|\mu\rangle^{A_1B}$ and $|\nu\rangle^{A_2C}$ with entanglement values

$$\begin{aligned} E(|\mu^{A_1B}\rangle) &= p\left[S(\psi^A) - S(\psi^C)\right] + (1-p)S(\psi^B), \\ E(|\nu^{A_2C}\rangle) &= pS(\psi^C) + (1-p)\left[S(\psi^A) - S(\psi^B)\right]. \end{aligned} \tag{2.21}$$

By using subadditivity of von Neumann entropy – Cor 1.1 – and the second property on pure states – Eq. (1.29) –, it is straightforward to check that both

$$\begin{aligned} S(\psi^A) - S(\psi^C) &\leq S(\psi^B) \\ \text{and } S(\psi^A) - S(\psi^B) &\leq S(\psi^C) \end{aligned} \tag{2.22}$$

are true. Thus, for suitable choices of p, the quantities $E(|\mu^{A_1B}\rangle)$ and $E(|\nu^{A_2C}\rangle)$ can attain any values compatible with the conditions

$$E(|\mu^{A_1B}\rangle) + E(|\nu^{A_2C}\rangle) = S(\psi^A), \tag{2.23a}$$
$$E(|\mu^{A_1B}\rangle) \leq S(\psi^B), \tag{2.23b}$$
$$E(|\nu^{A_2C}\rangle) \leq S(\psi^C) \tag{2.23c}$$

and so can attain any value respecting the conditions of Eq. (2.17) as entanglement can always be decreased by the clever use of local measurements.
This completes the proof of Lemma 2.1 for Case 1.

Case 2: $S(\psi^B) \geq S(\psi^C) \geq S(\psi^A)$**.** In this case, Alice, Bob, and Charlie apply assisted entanglement distillation [34, 104] and Subsec. 2.2.1, with Charlie being the assisting party. This procedure, combined with teleportation, achieves the transformation with

$$\begin{aligned} E(|\mu^{A_1B}\rangle) &= \min\left\{S(\psi^A), S(\psi^B)\right\} = S(\psi^A), \\ E(|\nu^{A_2C}\rangle) &= 0. \end{aligned} \tag{2.24}$$

Alternatively, they can apply assisted entanglement distillation with Bob being the assisting party, thus achieving

$$\begin{aligned} E(|\mu^{A_1B}\rangle) &= 0, \\ E(|\nu^{A_2C}\rangle) &= \min\left\{S(\psi^A), S(\psi^C)\right\} = S(\psi^A). \end{aligned} \tag{2.25}$$

By applying time-sharing, we see that we can achieve the transformation with any states $|\mu\rangle^{A_1B}$ and $|\nu\rangle^{A_2C}$ fulfilling

$$E(|\mu^{A_1B}\rangle) = pS(\psi^A), \tag{2.26a}$$
$$E(|\nu^{A_2B}\rangle) = (1-p)S(\psi^A). \tag{2.26b}$$

As in Case 1, it implies the resulting entanglement can attain any value compatible with the conditions of Eq. (2.17) by choosing p adequately and measuring locally.
This completes the proof of Lemma 2.1 for Case 2.

Case 3: $S(\psi^B) \geq S(\psi^A) \geq S(\psi^C)$**.** Here, we will apply a combination of the protocols used in Case 1 and 2. In particular, Bob can send his part of the state $|\psi\rangle$ to Alice by quantum state merging, see Eq. (2.19). Alternatively, they can apply assisted entanglement distillation, see Eq. (2.24). By time-sharing, we obtain

$$\begin{aligned} E(|\mu^{A_1B}\rangle) &= S(\psi^A) - pS(\psi^C), \\ E(|\nu^{A_2C}\rangle) &= pS(\psi^C). \end{aligned} \tag{2.27}$$

By suitable choices of the probability p it is now possible to obtain any pair of states $|\mu\rangle^{A_1B}$ and $|\nu\rangle^{A_2C}$ such that

$$\begin{aligned} E(|\mu^{A_1B}\rangle) + E(|\nu^{A_2C}\rangle) &= S(\psi^A), \\ E(|\mu^{A_1B}\rangle) &\leq S(\psi^A), \\ E(|\nu^{A_2C}\rangle) &\leq S(\psi^C), \end{aligned} \tag{2.28}$$

which are equivalent to the conditions 2.17, since $S(\psi^A) \leq S(\psi^B)$. This completes the proof of Lemma 2.1 for Case 3. Note that any other case can be obtained from the above three cases by interchanging the role of Bob and Charlie. Thus, the proof of the Lemma is complete. □

Using this result, we are now in position to present a general lower bound on the transformation rate between tripartite pure states.

Theorem 2.2 (Lower bound for state transformations)**.** *For tripartite pure states shared by Alice, Bob and Charlie $|\psi\rangle^{ABC}$ and $|\phi\rangle^{ABC}$, the LOCC conversion rate is bounded from below as*

$$R\left(|\psi\rangle^{ABC} \to |\phi\rangle^{ABC}\right) \geq \min\left\{\frac{S(\psi^A)}{S(\phi^B)+S(\phi^C)}, \frac{S(\psi^B)}{S(\phi^B)}, \frac{S(\psi^C)}{S(\phi^C)}\right\}. \tag{2.29}$$

Proof. We prove this bound by presenting an explicit protocol achieving the bound, which is also summarized in Fig. 2.3. In the first step, the parties apply entanglement combing to perform the transformation

$$|\psi\rangle^{ABC} \to |\mu\rangle^{A_1B} \otimes |\nu\rangle^{A_2C} \tag{2.30}$$

in such a way that the following equalities are fulfilled for some $r \geq 0$,

$$E(|\mu^{A_1B}\rangle) = rS(\phi^B) \tag{2.31a}$$

$$E(|\nu^{A_2C}\rangle) = rS(\phi^C). \tag{2.31b}$$

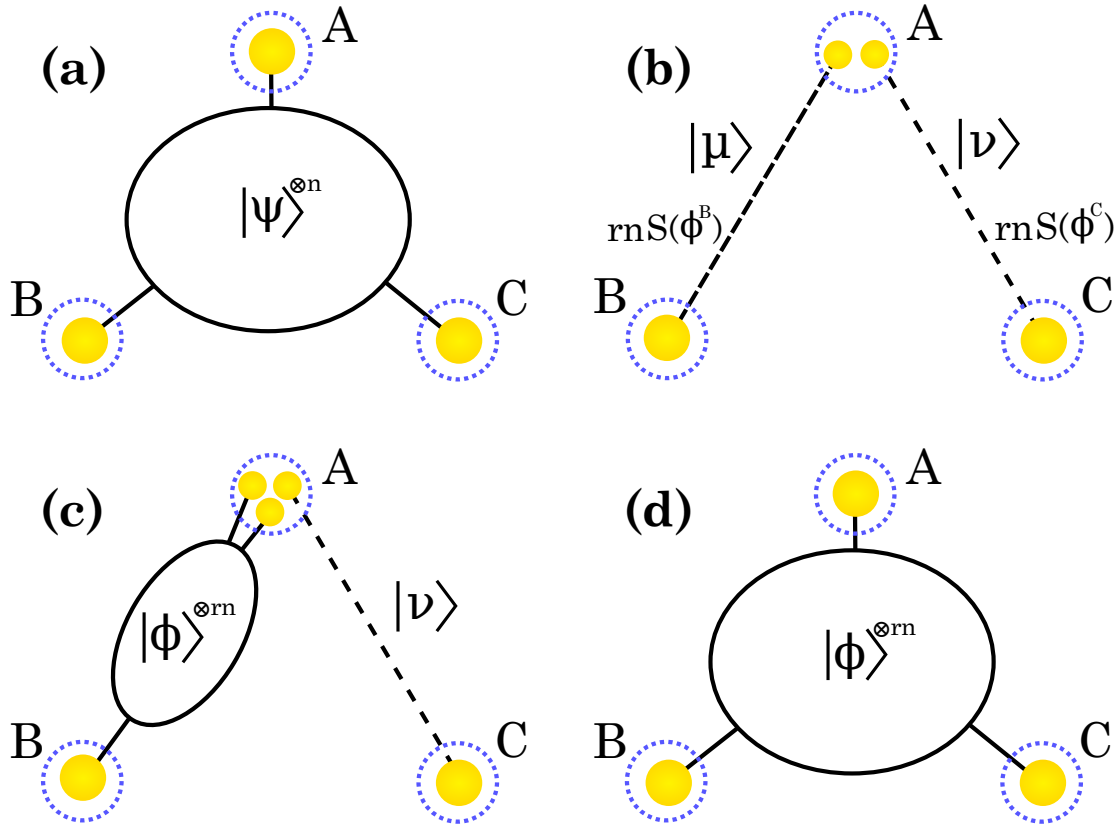

Figure 2.3: Conversion of a multipartite resource state $|\psi\rangle$ into the desired final state $|\phi\rangle$. The conversion is achieved via entanglement combing, i.e., via transforming the initial state $|\psi\rangle$ into singlets $|\mu\rangle$ and $|\nu\rangle$. One of the singlets is then converted into the desired final state $|\phi\rangle$. The remaining singlets are then used for teleporting the parts of $|\phi\rangle$ to the remaining parties.

The significance of this specific choice will become clear in a moment. In the next step, Alice and Bob apply LOCC for transforming the state $|\mu\rangle^{A_1B}$ into the desired final state $|\phi\rangle^{A_1A_3B}$. Since this is a bipartite LOCC protocol we can apply entanglement distillation such that the rate for this process is given by

$$\frac{E(|\nu^{A_1B}\rangle)}{S(\phi^B)} = r. \tag{2.32}$$

Note that due to Eqs. (2.31), this rate is equal to r. In a next step, Alice applies Schumacher compression [99] to the part of the state – labelled by A_3 – she will send to Charlie. The overall compression rate per copy of the initial state $|\psi\rangle^{ABC}$ is given by the rate of conversion r multiplied by the rate of compression $S(\psi^{A_3})$:

$$rS(\phi^{A_3}) = rS(\phi^C), \tag{2.33}$$

where in the last equality we relabeled to highlight this is the part which should be sent to Charlie. Once again, as can be seen in Eqs. (2.31), this rate interestingly coincides with the entanglement of the state $|\nu\rangle^{A_2C}$,

$$rS(\phi^C) = E(|\nu^{A_2C}\rangle). \tag{2.34}$$

This means we have the exact amount of entanglement necessary to transmit all the created copies. In a final step, Alice and Charlie distill the states $|\nu\rangle^{A_2C}$ into EPR pairs, and use them to teleport – see [12, 94] and last paragraph of Subsec. 1.2.2 – the compressed part ψ^{A_3} to Charlie. Due to Eq. (2.34), Alice and Charlie share exactly the right amount of entanglement for this procedure, i.e. , the process is possible with rate one and no entanglement is left over. In summary, the overall protocol transforms the state $|\psi\rangle^{ABC}$ into $|\phi\rangle^{ABC}$ at rate r.

To complete the proof, we will now show that r can be chosen such that

$$r = \min\left\{\frac{S(\psi^A)}{S(\phi^B)+S(\phi^C)}, \frac{S(\psi^B)}{S(\phi^B)}, \frac{S(\psi^C)}{S(\phi^C)}\right\}. \tag{2.35}$$

This can be seen directly by inserting the equations of the combing rate Eqs. (2.31) into the new form of the combing condition found in Lemma 2.1: Eqs. (2.17). In particular, the rate r can attain any value which is simultaneously compatible with the three inequalities

$$r \leq \frac{S(\psi^A)}{S(\phi^B)+S(\phi^C)}, \quad r \leq \frac{S(\psi^B)}{S(\phi^B)}, \quad r \leq \frac{S(\psi^C)}{S(\phi^C)}. \tag{2.36}$$

This completes the proof of the theorem. □

Of course, the value of the lower bound in Eq. (2.29) is heavily dependent on which party we choose to be the center of the combing – here, we chose Alice –. However, the procedure can be immediately generalized by interchanging the roles of the parties and computing the lower bounds:

$$R(|\psi\rangle^{ABC} \to |\phi\rangle^{ABC}) \geq \min\left\{\frac{S(\psi^B)}{S(\phi^A)+S(\phi^C)}, \frac{S(\psi^A)}{S(\phi^A)}, \frac{S(\psi^C)}{S(\phi^C)}\right\}, \tag{2.37}$$

$$R(|\psi\rangle^{ABC} \to |\phi\rangle^{ABC}) \geq \min\left\{\frac{S(\psi^C)}{S(\phi^A)+S(\phi^B)}, \frac{S(\psi^A)}{S(\phi^A)}, \frac{S(\psi^B)}{S(\phi^B)}\right\}. \tag{2.38}$$

The best bound is obtained by taking the maximum of Eqs. (2.29), (2.37) and (2.38).

2.3.3 Analysis of the result

We stress some important aspects and implications of this theorem. In Subsec. 2.3.1, we studied the conversion rate for some specific cases. In particular, we found an upper

bound in Eq. (2.14), we will now compare it to the newly found lower bound of Eq. (2.29) First observation, whenever the minimum in Eq. (2.29) is attained on the second or third entry – when $\frac{S(\psi^A)}{S(\phi^B)+S(\phi^C)} \geq \min\left\{\frac{S(\psi^B)}{S(\phi^B)}, \frac{S(\psi^C)}{S(\phi^C)}\right\}$ – the lower bound coincides with the upper bound in Eq. (2.14). This means that in all these instances the conversion problem is completely solved, giving rise to the rate

$$R(\psi^{ABC} \to \phi^{ABC}) = \min\left\{\frac{S(\psi^B)}{S(\phi^B)}, \frac{S(\psi^C)}{S(\phi^C)}\right\}. \tag{2.39}$$

As an example, consider the family of state vectors

$$|\psi\rangle^{ABC} = \cos\alpha\,|000\rangle + \sin\alpha\sin\beta\,|011\rangle + \sin\alpha\cos\beta\,|101\rangle\,, \tag{2.40}$$

for real α, β which we aim to convert into the GHZ state. The solid line in Fig. 2.4 shows our lower bound, taking the maximum of Eqs. (2.37), (2.38) and (2.29) as a function of α for $\beta = 1/2$, an arbitrary representative choice of value. The dashed line in Fig. 2.4 depicts the difference between the upper bound (2.14) and our lower bound. Note that the bounds coincide for a large parameter range of α, implying that our bound gives the exact conversion rate in these cases, different value of parameter β gives similar results. To the best of our knowledge, this outperforms any previously known bounds, such as the long-standing one of Smolin et al. [104] as they consider only one-way broadcasting protocols while ours is not limited to a particular class of LOCC.

Our results also shed new light on reversibility questions for tripartite state transformations. In general, a transformation $|\psi\rangle \to |\phi\rangle$ is said to be reversible if the conversion rates fulfill the relation

$$R(|\psi\rangle \to |\phi\rangle) = R(|\phi\rangle \to |\psi\rangle)^{-1}. \tag{2.41}$$

Let now $|\psi\rangle$ and $|\phi\rangle$ be two states for which the bound taking by choosing the best Alice in Theorem 2.2 is tight, e.g. $R(|\psi\rangle \to |\phi\rangle) = S(\psi^A)/S(\phi^A)$. Due to Eq. (2.14) it must be that

$$\frac{S(\psi^A)}{S(\phi^A)} \leq \frac{S(\psi^B)}{S(\phi^B)} \tag{2.42}$$

in this case. If this inequality is strict – which will be the generic case –, we obtain for the inverse transformation $|\phi\rangle \to |\psi\rangle$

$$R(|\phi\rangle \to |\psi\rangle) \leq \frac{S(\phi^B)}{S(\psi^B)} < \frac{S(\phi^A)}{S(\psi^A)} = R(|\psi\rangle \to |\phi\rangle)^{-1}, \tag{2.43}$$

where the first inequality follows from the upper bound of Eq. (2.14). These results show that those states which saturate the bound (2.14) do not allow for reversible

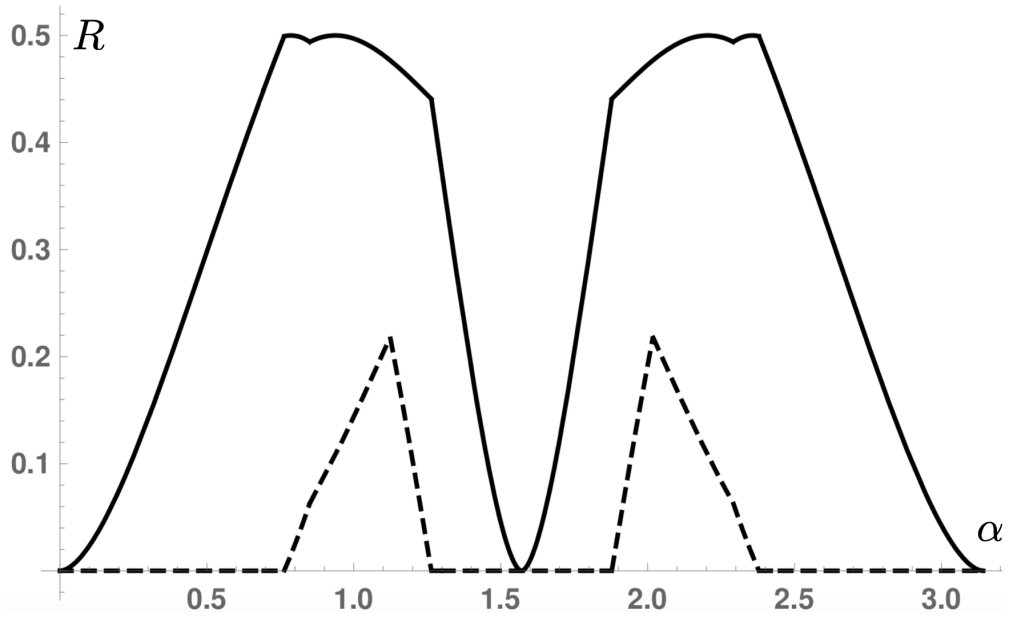

Figure 2.4: Lower bound for the conversion rate from the state vector $|\psi\rangle^{ABC}$ in Eq. (2.40) into a GHZ state, obtained by taking the maximum of Eqs. (2.29), (2.37) and (2.38) [solid line] and the difference between upper bound (2.14) and lower bound [dashed line] for $\beta = 1/2$.

transformations in the generic case. We will now comment on the limits of the approach presented here.

In particular, it is important to note that the lower bound in Theorem 2.2 is not optimal in general. This can be seen in the most simple way by considering the trivial transformation which leaves the state unchanged, i.e. , $|\psi\rangle^{ABC} \to |\psi\rangle^{ABC}$. Clearly, this can be achieved with unit rate $R = 1$. However, if we apply the lower bound in Theorem 2.2 to this transformation, we get $R \geq S(\psi^A)/[S(\psi^B) + S(\psi^C)]$. Due to subadditivity, it follows that our lower bound is in general below the achievable unit rate in this case.

We will now generalize the previous result to $N + 1$-partite states.

2.4 Generalization to multipartite states

In the discussion so far, we have focused on tripartite pure states. However, the presented tools can readily be applied to more general scenarios involving an arbitrary number of parties. In this more general setup the parties will be called Alice – A – and N Bobs – B_i – with $1 \leq i \leq N$. The aim of the process in this case is the asymptotic conversion of the $N + 1$-partite pure state $|\psi\rangle = |\psi\rangle^{AB_1 \ldots B_N}$ into the state $|\phi\rangle = |\phi\rangle^{AB_1 \ldots B_N}$.

The general idea for this procedure follows the same line of reasoning as in the tripartite

scenario discussed above. In the first step, entanglement combing is applied to the state $|\psi\rangle$, i.e., the transformation

$$|\psi\rangle \to |\mu_1\rangle^{A_1B_1} \otimes |\mu_2\rangle^{A_2B_2} \otimes \cdots \otimes |\mu_N\rangle^{A_NB_N} \tag{2.44}$$

with bipartite pure states $|\mu_i\rangle$. In the next step, Alice and the first Bob B_1 transform their state $|\mu_1\rangle^{A_1B_1}$ into the desired final state $|\phi\rangle$ via bipartite LOCC. In the final step, Alice applies Schumacher compression to the other parts of her state $|\phi\rangle$, and sends these parts to each of the remaining Bobs $B_2, \ldots, B_N$ by using the entanglement obtained in the first step of this protocol. As in the tripartite case, this protocol can be further optimized by interchanging the roles of the parties and applying time-sharing.

Theorem 2.3 (Lower bound for multipartite state conversion)**.** *For $N+1$-partite pure states $\psi^{AB_1\ldots B_N}$ and $\phi^{AB_1\ldots B_N}$, the LOCC conversion rate is bounded from below as*

$$R(\psi^{AB_1\ldots B_N} \to \phi^{AB_1\ldots B_N}) \geq \min_X \left\{ \frac{S(\psi^{AX})}{\sum_{B_i \notin X} S(\phi^{B_i})} \right\}, \tag{2.45}$$

where X denotes a subsystem of all Bobs, including the empty set.

The theorem is proven in Appendix A, we nevertheless give an explanation and outline of it. In the first step of the proof we will consider all possible ways to merge Bobs' parts of the state B_i with Alice. Since in the scenario considered here we have N Bobs, there are $N!$ different ways to achieve this, depending on the order of the Bobs in the merging procedure. We will first consider entanglement N-tuples $(E_1, \ldots, E_N)$, where E_i denotes the amount of entanglement shared between Alice and the i-th Bob after the merging procedure. For example, taking $N = 4$, merging first B_1, then B_2, then B_3 and finally B_4 to Alice will achieve the 4-tuple:

$$E_1 = S(\psi^A) - S(\psi^{AB_1}), \tag{2.46a}$$
$$E_2 = S(\psi^{AB_1}) - S(\psi^{AB_1B_2}), \tag{2.46b}$$
$$E_3 = S(\psi^{AB_1B_2}) - S(\psi^{AB_1B_2B_3}), \tag{2.46c}$$
$$E_4 = S(\psi^{AB_1B_2B_3}), \tag{2.46d}$$

while merging first B_3, then B_1, then B_4 and finally B_2 to Alice will achieve the 4-tuple:

$$E_1 = S(\psi^{AB_3}) - S(\psi^{AB_1B_3}), \tag{2.47a}$$
$$E_2 = S(\psi^{AB_1B_3B_4}), \tag{2.47b}$$
$$E_3 = S(\psi^A) - S(\psi^{AB_3}), \tag{2.47c}$$
$$E_4 = S(\psi^{AB_1B_3}) - S(\psi^{AB_1B_3B_4}). \tag{2.47d}$$

The aforementioned $N!$ merging procedures give rise to $N!$ N-tuples that we will denote as the entanglement extreme points. We note that some of the values E_i can be negative, implying that entanglement is consumed in this case. However, in the asymptotic regime, using time sharing on all the copies, a finite number of resource state can be consumed to create entanglement which will allow to perform those procedure without borrowing entanglement [114].
Proposition 2 of [114] guarantees that for any N-tuple $(E_1, \ldots, E_N)$ with the properties

- $\forall i \in \{1, \ldots, N\}$, $E_i \geq 0$,
- $(E_1, \ldots, E_N)$ is in the convex polytope spanned by the entanglement extreme points,

there exists an asymptotic LOCC protocol acting on the state $|\psi\rangle$ and distilling EPR pairs between Alice and each of the Bobs B_i at rate E_i. However, E_i is not the quantity which is relevant for the teleportation of ϕ^{B_i} to B_i. We are more interested into the rate at which we can send it. Which is why in the proof we do not consider the entanglement resulting from the combing process but the renormalized entanglement rates

$$R_i = \frac{E_i}{S(\phi^{B_i})}. \tag{2.48}$$

Using the above definition, we can define for each N-tuple $(E_1, \ldots, E_N)$ an N-tuple $(R_1, \ldots, R_N)$. We call *extreme points* the N-tuples obtained from the renormalization of the entanglement extreme points and we consider in the proof only the tuples $(R_1, \ldots, R_N)$. It is easily seen from the above condition on entanglement N-tuples that, if we find a distribution of rates $(R_1, \ldots, R_N)$ satisfying

- $\forall i \in \{1, \ldots, N\}$, $R_i \geq 0$,
- $(R_1, \ldots, R_N)$ is in the convex polytope spanned by the extreme points,

we will be able to achieve conversion from ψ to ϕ with rate

$$R(\psi \to \phi) \geq \min_i \{R_i\} \tag{2.49}$$

as the minimum rate of compression of reduced states ϕ^{B_i} is the limiting factor of our conversion protocol. Thus, in order to prove Eqs. (2.45), we will have to find in the convex set of the extreme points a point $(R_1, \ldots, R_N)$ such that

$$\min_i \{R_i\} \geq \min_{X \subset B_1, \ldots, B_N} \left\{ \frac{S(\psi^{AX})}{\sum_{B_i \notin X} S(\phi^{B_i})} \right\} =: m^{\psi,\phi}, \tag{2.50}$$

where X denotes a subset of the "all Bobs" set. For the sake of clarity, we denote the right-side lower bound as $m^{\psi,\phi}$ in the rest of the section.

We can now outline the end of the proof. In the first step we construct by applying time-sharing a set of points $(R_1, \ldots, R_N)$ satisfying $R_N \geq m^{\psi,\phi}$ from the extreme points. Obviously, the convex hull of these newly constructed points only contains rate distributions with the N^{th} coordinate greater than $m^{\psi,\phi}$. From our constructed points, we construct by convexity a new set of points $(R_1, \ldots, R_N)$ satisfying $R_{N-1} \geq m^{\psi,\phi}$. This leads to a set of points satisfying both $R_N \geq m^{\psi,\phi}$ and $R_{N-1} \geq m^{\psi,\phi}$. The procedure iterates with R_{N-2} until R_1. In this way, we will achieve a distribution $(R_1, \ldots, R_N)$ satisfying $\forall i \in \{1, \ldots, N\}, R_i \geq m^{\psi,\phi}$. Such a distribution will ensure conversion from ψ to ϕ with a rate of at least $m^{\psi,\phi}$, as claimed.

By using similar arguments as below Eq. (2.14), an upper bound to the conversion rate is found to be

$$R(\psi^{AB_1\ldots B_N} \to \phi^{AB_1\ldots B_N}) \leq \min_i \frac{S(\psi^{B_i})}{S(\phi^{B_i})}. \tag{2.51}$$

The bounds in Eqs. (2.45) and (2.51) coincide if the following equality holds true for some $1 \leq i \leq N$,

$$\frac{S(\psi^{B_i})}{S(\phi^{B_i})} = \min_X \left\{ \frac{S(\psi^{AX})}{\sum_{B_j \notin X} S(\phi^{B_j})} \right\}. \tag{2.52}$$

In those instances, Theorem 2.3 leads to a full solution of the conversion problem, and the corresponding rate is given by

$$R(\psi^{AB_1\ldots B_N} \to \phi^{AB_1\ldots B_N}) = \min_i \frac{S(\psi^{B_i})}{S(\phi^{B_i})}. \tag{2.53}$$

As in the tripartite case, the bound of Eq. (2.45) can be generalized by interchanging the roles of Alice and different Bobs. Previous analysis about the reversibility of state still hold, as well as the optimality of this bound over a large family of state. We show the computed bounds for the distillation of GHZ_4 from the 4-partite family of states

$$|\psi\rangle^{ABCD} = \cos\alpha\,|0000\rangle + \sin\alpha\,[\cos\beta\,|1001\rangle + \sin\beta\,(\cos\gamma\,|1100\rangle + \sin\gamma\,|1010\rangle)]\,, \tag{2.54}$$

for real α, β, γ. Figure 2.5 gives a visualization of the bounds' tightness for a large subset of this family.

2.5 Conclusion

The work presented in this chapter lead to a publication in PRL [107].

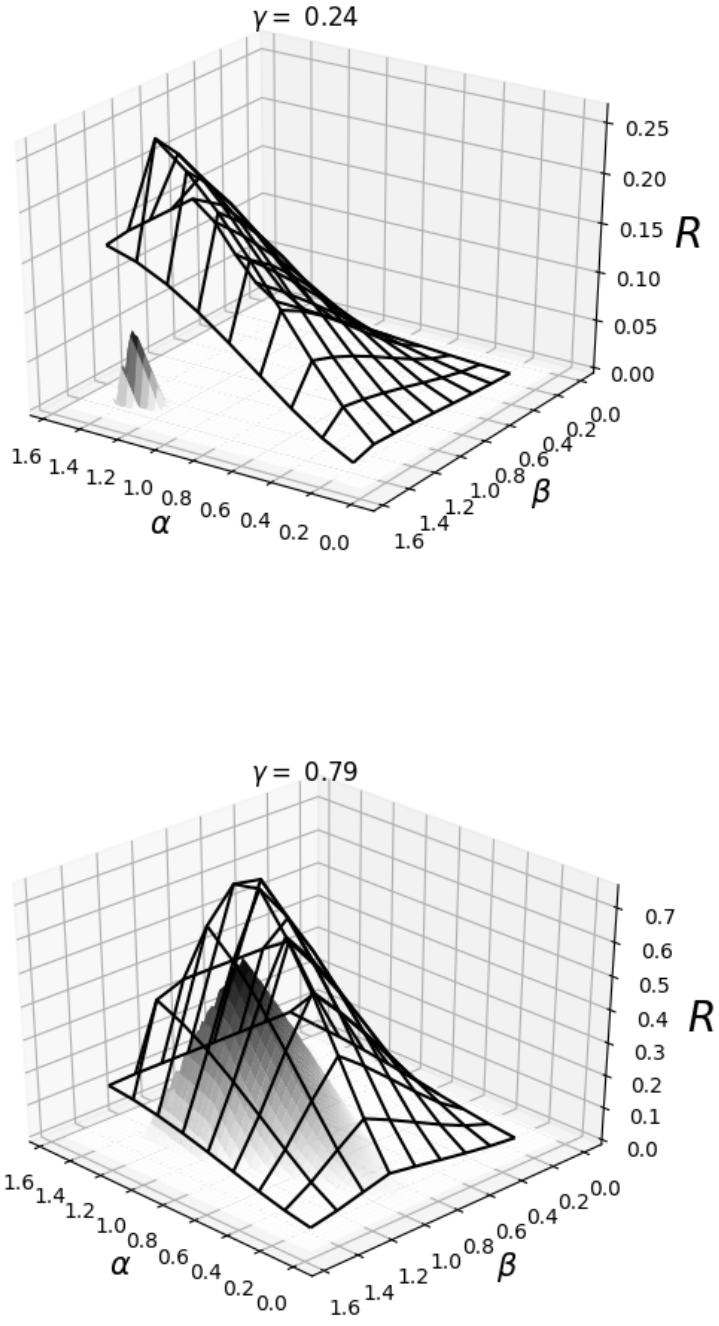

Figure 2.5: Upper bound [wireframe] and difference between upper and lower bound [plain surface drawing] for the conversion rate from the state vector $|\psi\rangle^{ABCD}$ in Eq. (2.54) into a GHZ state, obtained by taking the maximum of Eqs. (2.45), for two different values of γ. Even in the worst case, a large part of this family of state tighten the bound using our protocol.

In this work, we have reported substantial progress on asymptotic state transformation via multipartite local operations and classical communications, tackling an important long-standing problem which to large extent remained open since the early development of quantitative entanglement theory [13]. Similar techniques may also prove helpful in the study of other quantum resource theories different from entanglement, such as the resource theory of quantum coherence [106] and quantum thermodynamics [74, 55].

Yet, we are interested in the network setting. Concerning the topic of network's resource management, the significance of the established results on multipartite entanglement transformations hence lies in the way they help to understand how multipartite resources for protocols beyond point-to-point schemes in quantum networks can be prepared and manipulated. Here, multipartite entanglement is conceived to be created by local processes and bipartite transmissions involving pairs of nodes, followed by steps of entanglement manipulation, which presumably involve instances of classical routing techniques. The bounds above can be readily applied to the setting in which the preparation of smaller graph states has been successful [98], but from which larger GHZ states are still to be built up, without wanting to discard previously prepared steps. Specifically, our techniques lead to optimal GHZ distillation rates for various classes of pure states and the lower-bound can be computed easily for states of low-dimension, rendering them useful for any quantum information processing tasks relying on GHZ states. We hope that our established bounds provide meaningful guidance as to how to manage and recycle resources for quantum networks.

Nevertheless, the asymptotic picture is clearly not sufficient to study the distribution of states across a network. Indeed, on a concrete implementation of quantum networks, resources are limited, especially here and now in the early stage of their development. In the next chapter, we will study the single-shot setting, trying to optimize resources over quantum networks, the aim will not be to recycle previous resources but to manage the simultaneous use of the network by different users.

Chapter 3

Classical and quantum network coding

The time spent on what is presented in this chapter ended up being quite long. As often, it started with a small question: "Is it possible to distribute cross EPR pairs over a square-shaped repeater network?". A depiction of the distribution in effect can be found in Fig. 3.1. This question was already solved in the literature [3]. However, I did not find it at the time. We will review the differences between the two methods and results below. This question might seems simple but is linked to the concept of *network congestion* which is an important concept of the data networking theory. As already made precise, resources in networks are limited. For example, classical channels' transmission rate, routers' capacity of handling incoming connections and the rate at which we can produce reliable EPR pairs are all limited quantity in the network. In networks, a congestion may happen when a component – for example, a node or a channel – has to handle more information than it can process. This phenomenon can provoke several unfortunate events such as a delay in transmission, the loss of information – which can be dramatic for a quantum state – and in some cases, leads to the observation of a congestion collapse – a state of the network presenting extremely low performance. Overall, it provokes a reduction of the network's global efficiency. Of course, to prevent or solve such issues there is a simple and very universal solution used among other methods by several ISP – Internet Service Providers –: adding more communication resources,

raising drastically the capacity of the network's channels, more routers etc. It is an effective solution. However, there is reasons to believe that quantum communication resources will be costly in the years to come and quantum networks will not be as large as the classical internet network, even if we manage to build continental networks. A little bit of optimization will be always welcome. Especially given our specific era, it is essential to reduce energy/material costs as much as possible and we should capitalize on the fact that global quantum networks are still under development; it is still possible to design optimized quantum networks without having the tremendous cost of modifying a pre-established infrastructures. As such, studying the solving of bottlenecks without adding more resources is an interesting field of research which I think will be of interest in the years to come.

Whether it is classical or quantum, a cross distribution over a square network is quite a fundamental example of a bottleneck in network. We will see why and solve the issue in the quantum network setting in Sec. 3.1. Having resolved the square-cross problem – which we also refer to as the X-box game –, I saw that the problem was actually documented and solved using another approach [3] during. The result of Akibue et al. is focused on grid shaped quantum networks with quantum channels of dimension 2 they call *cluster networks*. Considering the left-side nodes of the grid as input nodes and the right-side ones as outputs, they studied which unitary operations were implementable by LOCC using the network. More formally, considering $|\psi\rangle$ as the input state, U as the implemented unitary operation and Λ as the LOCC performing the implementation:

$$\Lambda\left(|\psi\rangle\langle\psi| \otimes |\text{Network}\rangle\langle\text{Network}|\right) = U|\psi\rangle\langle\psi|U^{\dagger}. \tag{3.1}$$

Their specific proof concerning the X-Box game implied the knowledge of elaborate concepts such as the Kraus-Cirac decomposition and Kraus-Cirac number [66]. My approach is based on a similarity between Matrix Product States – MPS – [91] and distributions over cyclic networks, converting this problem as well as equivalent problems into a set of linear equations solvable using basic linear algebra. The methods used are readily extendable to distributions type not covered by Akibue et al. such as distribution over larger cyclic networks, cyclic networks with channels of dimension greater than 2 or to networks of arbitrary topology. It is the second result of this chapter.

Indeed, the resolution of the X-box game was only a first approach of a broader subject and led to a more global question: given a network, which are the possible distributions of quantum states beyond simple routing? Among the existing alternatives, we will focus on the quite well known network coding. We review the basics of classical network coding

and its quantum counterpart in Sec. 3.2. We will see that some questions are still left open concerning the latter. In order to study those questions, I present an extended version of quantum network coding, which represent the capabilities of quantum networks to solve distribution tasks and I show that the solving of a specific task is equivalent to the finding of a tensor's factorization in Sec. 3.3.
As a third result, in Sec. 3.4, I define an extended version of classical network coding and the class of distribution tasks it can solves in order to compare classical and quantum distribution. I show that both quantum network coding and classical network coding can be unified under the same tensor formalism, the difference being that quantum network coding allows the factorization to be done with tensors in $\mathbb{C}$ while for classical network coding it is restricted to non-negative tensors, tensor with coefficients in $\mathbb{R}^+$. I show a direct application of our formalism to find the minimal resources needed to perform simultaneous communication over a square shaped network. I conclude this chapter by giving an example of a distribution task achievable through quantum network coding while impossible with classical network coding, solving for the first time – to my knowledge – the converse of the problem arisen by Kobayashi et al. and expanding the extent of the full capabilities of quantum networks.
The most proeminent notions used in this chapter are presented in Chapter 1 as

- Operating quantum states and the – Stochastic – Local Operations and Classical Communications class of operation, Section 1.2
- Classical and quantum networking, Section 1.5

3.1 The Square-Cross problem (the X-Box Game)

We begin with the initial question, the solving of the distribution of cross EPR pair over a square network. The problem which allows me to develop the model presented in the next sections.

3.1.1 Setup and first attempts

We consider a square-shaped quantum network as in Fig. 3.1. The global state of the network is a product of EPR pairs we denote as

$$|\square\rangle := \frac{1}{4} \sum_{\alpha,\beta,\gamma,\delta=0}^{1} |\delta\alpha\alpha\beta\beta\gamma\gamma\delta\rangle^{A_1A_2B_1B_2C_1C_2D_1D_2} \tag{3.2}$$

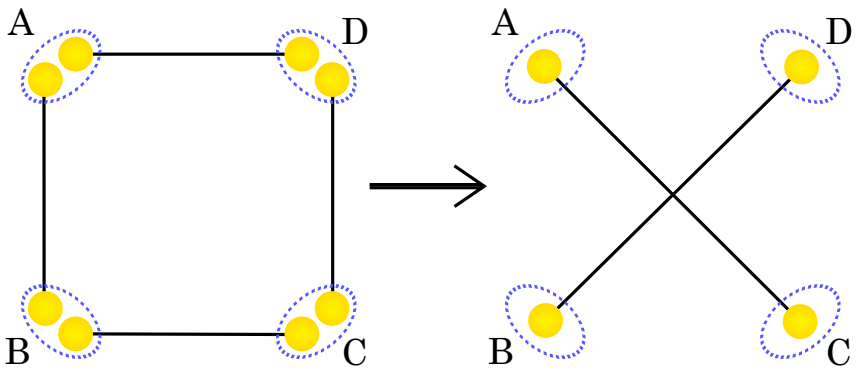

Figure 3.1: Depiction of the X-box game. On the left side, the initial square-shaped quantum network. On the right side, the two EPR pairs we want to distribute.

shared by 4 parties – A, B, C and D. The distribution task is to share two EPR pairs on this network, one between A and C, the other between B and D, as in Fig. 3.1. We remind the reader that a distribution task is defined as the use of the network to share a specific quantum state between the clients, see Subsec. 1.5.1. Here, we try to solve the so-called "X-box game" distribution task with a non-zero probability: we wish to find a SLOCC – Stochastic Local Operation and Classical Communication, see Subsec. 1.2.2 – protocol which distributes the state written as

$$|\times\rangle := \frac{1}{2}\sum_{\alpha,\beta=0}^{1} |\alpha\beta\alpha\beta\rangle^{ABCD}, \tag{3.3}$$

to the clients A, B, C and D. Using the knowledge acquired from the previous chapter, we can examine the value of entanglement of both the initial and finale state to decide whether or not there is enough entanglement to perform the distribution. Studying all the possible bipartitions, we compute

$$S(\square^{AB}) = S(\square^{AD}) = 2, \quad S(\square^{AC}) = 4 \quad \text{and, for each node } X,\ S(\square^{X}) = 2 \tag{3.4}$$

for the initial state and

$$S(\times^{AB}) = S(\times^{AD}) = 2, \quad S(\times^{AC}) = 0 \quad \text{and, for each node } X,\ S(\times^{X}) = 1 \tag{3.5}$$

for the final one. It is straightforward to see that, for all bipartition $\mathcal{P}$ we have

$$S(\square^{\mathcal{P}}) \geq S(\times^{\mathcal{P}}). \tag{3.6}$$

The results from the previous chapter do not prohibit the existence of a solution to the distribution task. A straightforward application of the bounds of Eqs. 2.29 and 2.51 gives

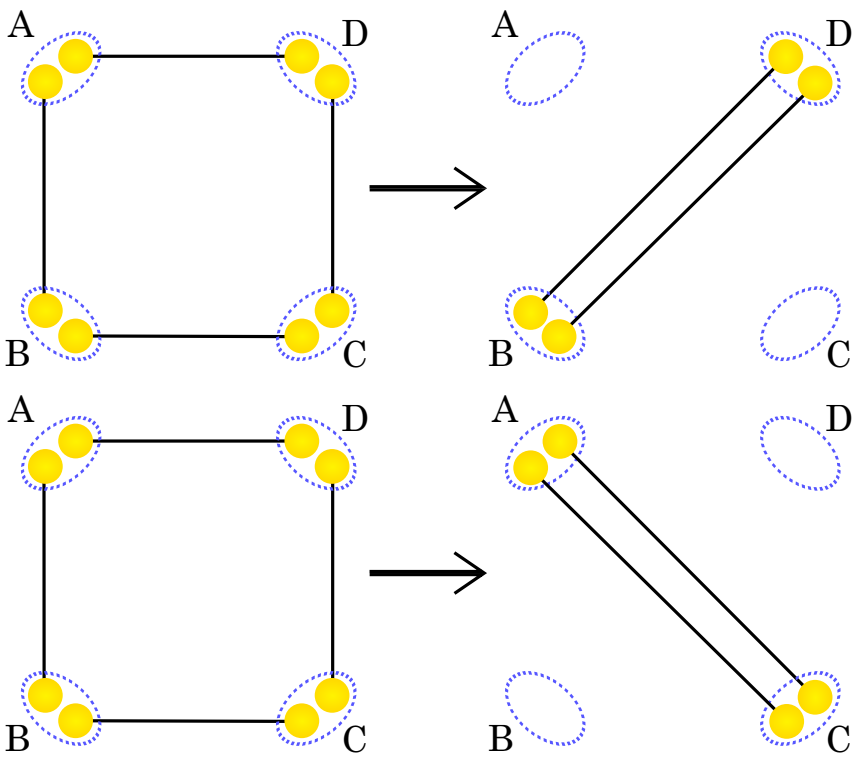

Figure 3.2: Depiction of the conversion of two square quantum networks into two cross of EPR pairs.

$\frac{1}{2} \leq R \leq 1$. But looking at each diagonal separately gives you a rate of 2 each time, which achieves a average rate of 1 by time-sharing, with an explicit asymptotic protocol. There is another explicit protocol which achieves the distribution. Indeed, if we possess multiple copies of the network the distribution is easily achieved. Indeed, one can take one copy and perform two entanglement swapping – see Subsec. 1.5.2 – to achieve two EPR pairs between A and C, then use another copy to establish two EPR pairs between B and D, see Fig. 3.2. Actually, we do not even need an asymptotic number of copies: if one possess 2 copies of the square network then conversion's rate is $R = 1$. Nevertheless, this tactic cannot work when the amount of initial state is reduced to an odd number of copies. The problem remains unsolved. We can extract from these first attempts another argument that this example is fundamental: in theory, we possess enough resources and by adjusting only slightly some parameters one can trivially solve the task; removing one link leads to a straightforward impossibility to perform the distribution, adding one trivialize it since a simple routing can perform it. This problem is really interesting as it sits between two easily solved problems, yet it is non-trivial to solve.

We found some traction to solve our problem using an already known tool from other

fields: the Matrix Product States representation.

3.1.2 Matrix Product State

How to characterize all the distribution tasks which can be performed over a square quantum network? The answer actually came from the Matrix Product State – MPS – representation [91]. In this formalism, we represent the coefficients of the state $|\psi\rangle$ as the trace of a product of matrices:

$$|\psi\rangle = \sum_{i_1,\dots,i_N=0}^{d_1-1,\dots,d_N-1} \mathrm{Tr}(\mathcal{M}^{i_1[1]} \dots \mathcal{M}^{i_N[N]}) \, |i_1,\dots,i_N\rangle^{C_1,\dots,C_N} \tag{3.7}$$

$$= \sum_{\{i_j\}} \mathcal{M}^{i_1[1]}_{\alpha_N,\alpha_1} \mathcal{M}^{i_2[2]}_{\alpha_1,\alpha_2} \dots \mathcal{M}^{i_N[N]}_{\alpha_{N-1},\alpha_N} \, |i_1,\dots,i_N\rangle^{C_1,\dots,C_N} \tag{3.8}$$

with $\mathcal{M}^{i_k[k]} \in \mathbb{C}^{D_k \times D_{k+1}}$, $D_{N+1} := D_1$ and we used the Einstein notation in the second line. This formalism is used in condensed matter physic among other fields [89] as it is a useful tool to study many-body systems [111]. For the purpose of this work, we will focus on a specific description of those MPSs: the valence bond picture. Matrix product states can be described as the output of the process of adding maximally entangled states of appropriate dimension D_i between each consecutive parties C_i and C_{i+1}, including one of dimension D_N between C_N and C_1, then measure the two qudits in each node to reduce the local dimension from $D_i.D_{i+1}$ to d_{C_i}. As the careful reader may have noticed, this depiction is extremely close to our setting for distributing quantum states over a cyclic network, such as the square. Hence come the motivation of using this formalism to study whether a distribution is achievable over the square quantum network.

Let us define more precisely the setting. In the following, we only consider MPSs where all matrices $\mathcal{M}^{i_k[k]}$ are square and of the same dimension: $\forall k, m \in \{1,\dots,N\}$, $D_k = D_m := D_\psi$. As shown in [91], we can represent any pure state $|\psi\rangle$ provided the describing matrices' dimension is large enough. However, we are interested by finding the description of states using the minimum possible dimension D_ψ and will refer to this minimum value as the bond dimension. Actually, for two arbitrary pure states $|\psi\rangle$ and $|\phi\rangle$, we can show the following necessary condition

Lemma 3.1. *If $|\psi\rangle$ can be converted into $|\phi\rangle$ via SLOCC, then the bond dimension D_ϕ of $|\phi\rangle$ must be smaller than or equal to D_ψ.*

Proof. Given two N-partite states shared by N locally distinct clients, $|\psi\rangle^{C_1,\dots,C_N}$ and $|\phi\rangle^{C_1,\dots,C_N}$. We suppose we can convert $|\psi\rangle$ into $|\phi\rangle$ via an SLOCC transformation. Such

a distribution is possible if and only if there exists a LOCC protocol with at least one branch achieving the distribution. Formally, if a SLOCC can convert $|\psi\rangle$ into $|\phi\rangle$, we can find a set of Kraus operators $\{K_i\}_{i\in 1,\dots,N}$ and $\lambda \in \mathbb{R}^{+*}$ such that

$$\bigotimes_i K_i \, |\psi\rangle^{C_1,\dots,C_N} = \lambda \, |\phi\rangle^{C_1,\dots,C_N} . \tag{3.9}$$

Equivalently, one can find a set of matrices $\{O_i\}_{i\in 1,\dots,N}$ such that

$$\bigotimes_i O_i \, |\psi\rangle^{C_1,\dots,C_N} = |\phi\rangle^{C_1,\dots,C_N} . \tag{3.10}$$

Trivially, the set of matrices $\{O_i\}_i$ can be converted into Kraus operators by a simple normalization.
We rewrite Eq. (3.10) in the MPS description using the bond dimension D_ψ:

$$\sum_{i_1,\dots,i_N=0}^{D_\psi} \bigotimes_{k=1}^{N} O_k^{i_k,j_k} \mathcal{M}^{j_1[1]}_{\alpha_N,\alpha_1} \dots \mathcal{M}^{j_N[N]}_{\alpha_{N-1},\alpha_N} \, |i_1 \dots i_N\rangle^{C_1,\dots,C_N} = |\phi\rangle \tag{3.11}$$

$$\sum_{i_1,\dots,i_N=0}^{D_\psi} \left(O_1^{i_1,j_1} \mathcal{M}^{j_1[1]}_{\alpha_N,\alpha_1}\right) \dots \left(O_N^{i_N,j_N} \mathcal{M}^{j_N[N]}_{\alpha_{N-1},\alpha_N}\right) |i_1 \dots i_N\rangle^{C_1,\dots,C_N} = |\phi\rangle \tag{3.12}$$

$$\sum_{i_1,\dots,i_N=0}^{D_\psi} \mathcal{N}^{i_1[1]}_{\alpha_N,\alpha_1} \dots \mathcal{N}^{i_N[N]}_{\alpha_{N-1},\alpha_N} \, |i_1 \dots i_N\rangle^{C_1,\dots,C_N} = |\phi\rangle , \tag{3.13}$$

where $\mathcal{N}^{i_k[k]} = O_k^{i_k,j_k} \mathcal{M}^{j_k[k]}$. Thus, we find an accurate MPS description of $|\phi\rangle$ using matrices of dimension D_ψ. As a consequence, the bond dimension of $|\phi\rangle$ is inferior to the bond dimension D_ψ. □

Armed with that knowledge, we can now rewrite our conversion problem. Finding a MPS representation of $|\square\rangle$ of bond dimension 2 is fairly straightforward. We take the matrices

$$\mathcal{M}^0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \mathcal{M}^1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \mathcal{M}^2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad \mathcal{M}^3 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{3.14}$$

and we have an effective MPS description of the square network as

$$|\square\rangle = \sum_{i_A,i_B,i_C,i_D=0}^{3} \mathrm{Tr}(\mathcal{M}^{i_A}\mathcal{M}^{i_B}\mathcal{M}^{i_C}\mathcal{M}^{i_D}) \, |i_A i_B i_C i_D\rangle . \tag{3.15}$$

This depiction is minimal since a description with a bond dimension 1 can only describe separable states. According to the previous assertions, if there is a SLOCC converting the square quantum network into a product of cross EPR, the bond dimensions of $|\times\rangle$

cannot exceed 2. Meaning the conversion is possible if and only if we can find 8 matrices in $\mathbb{C}^{2\times 2}$,

$$\begin{Bmatrix} \mathcal{A}^0 & \mathcal{B}^0 & \mathcal{C}^0 & \mathcal{D}^0 \\ \mathcal{A}^1 & \mathcal{B}^1 & \mathcal{C}^1 & \mathcal{D}^1 \end{Bmatrix} \tag{3.16}$$

to describe the state of Eq. (3.3),

$$|\times\rangle = \sum_{i_A,i_B,i_C,i_D=0}^{1} \mathrm{Tr}(\mathcal{A}^{i_A}\mathcal{B}^{i_B}\mathcal{C}^{i_C}\mathcal{D}^{i_D})\,|i_A i_B i_C i_D\rangle \tag{3.17}$$

Up to normalization, it means finding 8 matrices such that

$$\mathrm{Tr}(\mathcal{A}^{i_A}\mathcal{B}^{i_B}\mathcal{C}^{i_C}\mathcal{D}^{i_D}) = \delta_{i_A,i_C}\delta_{i_B,i_D} \tag{3.18}$$

The problem reduces to the resolution of a set of linear equations. In the next subsection, we will exploit the different symmetries of this set of equation to decide whether a solution exists.

3.1.3 Restricting the set of solutions

We want to find $\mathcal{A}^{i_A}$, $\mathcal{B}^{i_B}$, $\mathcal{C}^{i_C}$ and $\mathcal{D}^{i_D}$ in $\mathbb{C}^{2\times 2}$, which we represent as the solution set (3.16) obeying Eq. (3.18). We now look at several symmetries obeyed by the the set of solutions of Eq. (3.18), restricting the possible values of their 32 complex coefficients.

Matrix product families as bases. Firstly, the trace is a Hermitian form, it is an inner product on the space of all complex 2×2 matrices. As a consequence, Eq. (3.18) implies that each family of product of two consecutive matrices – $\{\mathcal{A}^{i_A}\mathcal{B}^{i_B}\}$, $\{\mathcal{B}^{i_B}\mathcal{C}^{i_C}\}$, $\{\mathcal{C}^{i_C}\mathcal{D}^{i_D}\}$ and $\{\mathcal{D}^{i_D}\mathcal{A}^{i_A}\}$ – is a base of $\mathbb{C}^{2\times 2}$. To prove this, let us instead suppose w.l.o.g. $\mathcal{A}^1\mathcal{B}^1$ is linearly dependent on the space generated by the family $\{\mathcal{A}^{i_A}\mathcal{B}^{i_B}\}$, meaning we can find a nontrivial set of coefficients $\{\lambda_{i_A,i_B}\}_{(i_A,i_B)\neq(1,1)}$ such that

$$\sum_{(i_A,i_B)\neq(1,1)} \lambda_{i_A,i_B}\mathcal{A}^{i_A}\mathcal{B}^{i_B} = \mathcal{A}^1\mathcal{B}^1, \tag{3.19}$$

we reach a contradicting statement as

$$\mathrm{Tr}(\mathcal{A}^1\mathcal{B}^1\mathcal{C}^1\mathcal{D}^1) = 1 \tag{3.20}$$

and

$$\sum_{(i_A,i_B)\neq(1,1)} \lambda_{i_A,i_B}\mathrm{Tr}(\mathcal{A}^{i_A}\mathcal{B}^{i_B}\mathcal{C}^1\mathcal{D}^1) = 0. \tag{3.21}$$

By cyclicity of the trace, the same can be said for each family of consecutive matrices.

Rank of the matrices. The second condition is all matrices have to be of rank 2. Indeed, if at least one of the describing matrices is of rank 1, no solution can be found. Supposing w.l.o.g $\mathcal{A}^0$ is of rank 1, we can write it as $\mathcal{A}^0 := |v\rangle\langle u|$ where $|u\rangle$ and $|v\rangle$ are vectors of $\mathbb{C}^2$. Eq. (3.18) becomes for $i_A = 0$:

$$\langle u\mathcal{B}^{i_B}|\,\mathcal{C}^1\,|\mathcal{D}^{i_D}v\rangle = 0 \tag{3.22}$$

where we used the notation $|\mathcal{X}^{i_X}w\rangle := \mathcal{X}^{i_X}\,|w\rangle$.
Clearly, $|D^0v\rangle$ and $|D^1v\rangle$ can be neither colinear nor nul since

$$1 = \langle u\mathcal{B}^0|\,\mathcal{C}^0\,|\mathcal{D}^0v\rangle \neq \langle u\mathcal{B}^0|\,\mathcal{C}^0\,|\mathcal{D}^1v\rangle = 0 \tag{3.23}$$

and

$$\langle u\mathcal{B}^1|\,\mathcal{C}^0\,|\mathcal{D}^1v\rangle = 1. \tag{3.24}$$

Since the same can be said for $\{|\mathcal{B}^{i_B}u\rangle\}$, we find that both 2-vector families are basis of $\mathbb{C}^2$. Associating this fact with Eq. (3.22), we deduce that $\mathcal{C}^1$ is the null matrix, which is impossible since $\mathrm{Tr}(\mathcal{A}^1\mathcal{B}^{i_B}\mathcal{C}^1\mathcal{D}^{i_B}) = 1$. As a consequence, all matrices used in the description have to be of rank 2, therefore invertible.

Further reduction showing there is no solution. We now focus on the set of linear equations set, we will reduce the number of free parameters of the solution and reach a contradiction for its existence. First, we use a simple symmetry, generic to the trace: for any invertible square matrix $M \in \mathbb{C}^{2\times2}$, we can replace the solution set (3.16) by

$$\begin{Bmatrix} \mathcal{A}^0 & \mathcal{B}^0M^{-1} & M\mathcal{C}^0 & \mathcal{D}^0 \\ \mathcal{A}^1 & \mathcal{B}^1M^{-1} & M\mathcal{C}^1 & \mathcal{D}^1 \end{Bmatrix}, \tag{3.25}$$

this transformation leaves the trace $\mathrm{Tr}(\mathcal{A}^{i_A}\mathcal{B}^{i_V}\mathcal{C}^{i_C}\mathcal{D}^{i_V})$ invariant. Using this symmetry with $M := \mathcal{B}^0$, we find there exist solutions of the form

$$\begin{Bmatrix} \mathcal{A}^0 & \mathbb{I} & \mathcal{C}^0 & \mathcal{D}^0 \\ \mathcal{A}^1 & \mathcal{B}^1 & \mathcal{C}^1 & \mathcal{D}^1 \end{Bmatrix}, \tag{3.26}$$

here and in the following, we will always – unless specified – abuse notations and still denote the matrices of the solution set as $\mathcal{X}^{i_X} \in \mathbb{C}^{2\times2}$ despite their change of values, as long as these values are free. Moreover, it is easy to check that, for $\alpha \in \mathbb{C}^*$ and $\lambda \in \mathbb{C}$,

$$\begin{Bmatrix} \mathcal{A}^0 & \mathcal{B}^0 & \mathcal{C}^0 & \mathcal{D}^0 + \lambda\mathcal{D}^1 \\ \mathcal{A}^1 & \alpha(\mathcal{B}^1 - \lambda\mathcal{B}^0) & \mathcal{C}^1 & \alpha^{-1}\mathcal{D}^1 \end{Bmatrix}, \tag{3.27}$$

is also solution thanks to symmetries of the solution set. In Eq. (3.26), taking $\alpha = 1$ and $\lambda = \mathrm{Tr}\ \mathcal{B}^1$, we find there must exist solution of the form

$$\begin{Bmatrix} \mathcal{A}^0 & \mathbb{I} & \mathcal{C}^0 & \mathcal{D}^0 \\ \mathcal{A}^1 & \mathcal{B}^1 & \mathcal{C}^1 & \mathcal{D}^1 \end{Bmatrix}, \tag{3.28}$$

with $\mathrm{Tr}\ \mathcal{B}^1 = 0$. Here, $\mathcal{B}^1$ being of rank 2, it is diagonalizable with non-null eigenvalues e and $-e$. As a consequence we can use (3.1.3) to inject matrices to diagonalize $\mathcal{B}^1$ then use symmetry (3.27) with $\alpha = e^{-1}$ and show any solution implies the existence of solutions of the form

$$\begin{Bmatrix} \mathcal{A}^0 & \mathbb{I} & \mathcal{C}^0 & \mathcal{D}^0 \\ \mathcal{A}^1 & Z & \mathcal{C}^1 & \mathcal{D}^1. \end{Bmatrix}, \tag{3.29}$$

where $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ is the usual Pauli matrix. However, using symmetry (3.27) again with $\alpha = 1/2$ and $\lambda = 1$, we can achieve a solution

$$\begin{Bmatrix} \mathcal{A}^0 & \mathbb{I} & \mathcal{C}^0 & \mathcal{D}^0 \\ \mathcal{A}^1 & \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) & \mathcal{C}^1 & \mathcal{D}^1, \end{Bmatrix}, \tag{3.30}$$

which is impossible since, as shown above, all the matrices used in the description should be invertible. Therefore, the existence of any solution to Eq. (3.18) leads to a contradiction, thus proving that the distribution of cross EPR pairs over a square quantum network of qubits is impossible, even through SLOCCs.

Extensions of this technique. The aim of this whole section, was not only to find the answer to this small but highly relevant question, but also to identify concepts and methods to solve the broader issue of characterizing which are the possible distributions over a quantum network. The use of MPSs can readily be expanded to cyclic networks of higher dimension – as we do later in Subsec. 3.4.1 – or larger networks. Moreover, we hope the link we made between MPSs and distributions over quantum networks will allow to apply the results of the MPS' field to the quantum network field as well as giving a network insight to the MPS field.

We will now expand this MPS technique to more general quantum networks using the tensor network formalism [89] in Sec. 3.3. But first, as already mentionned in the introduction, some techniques beyond routing already exist in the classical networking field and those methods inspired quantum networking scientists to create a whole new class of protocols. This is the subject of the next section.

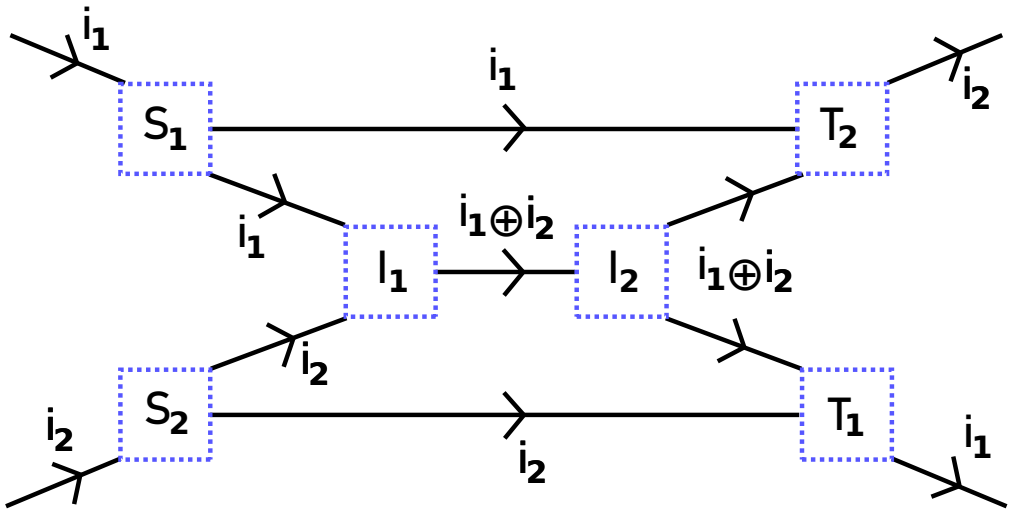

Figure 3.3: The butterfly network on which we want to implement a cross communication, each channel can only transmit one bit and channels are directed according to the arrows. The source S_1 wants to communicate a bit i_1 to the sink T_1, and the same applies to S_2, i_2 and T_2. Routing cannot work in this case. Indeed, the routing of one bit has to use the $I_1 \to I_2$ edge and the other source cannot use it anymore to reach the other sink. It can be solved easily with network coding as simply sending the addition modulo two of the two bits through the central node allow decoding at the sinks.

3.2 An introduction to classical and quantum network coding

A definition of quantum and classical networks and distribution tasks is given in Sec. 1.5.

3.2.1 Classical network coding

Introduced in [2], classical network coding arises naturally in the context of communication over networks. The main difference with routing is that intermediary nodes can perform arbitrary arithmetic operations before mapping the result of those operations to its output. Note that the class of network coding protocol contains all possible routing protocol as special cases where local computation is not performed. As such, the distributive capabilities of network coding protocols is at least as powerful as routing protocols. Actually, network coding outperform routing. This fact is well illustrated by the well known example of the butterfly network, shown on Figure 3.3. Network coding is already used in several network implementations [75], and is highly studied for noisy unreliable network such as wireless networks [90].

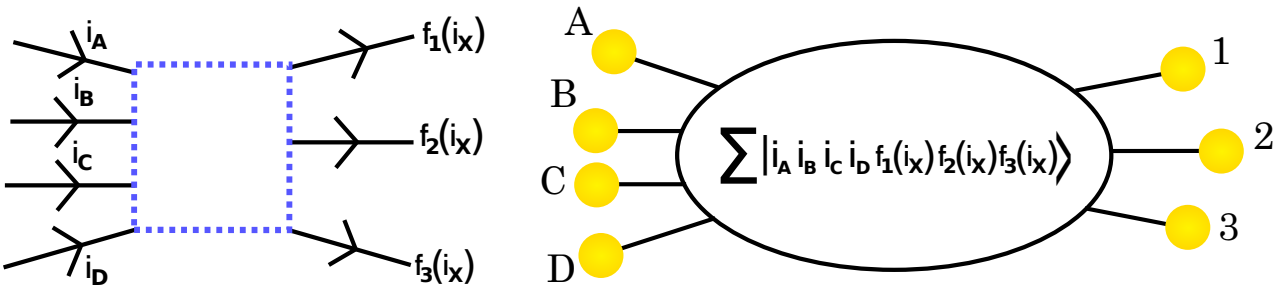

Figure 3.4: If the distribution on the classical network on the left side transforming the input i_X into $f_y(i_X)$ is doable on a network, the quantum state on right side can be distributed on a network having the same topology [62]

3.2.2 First quantum network coding and relation to classical

Kobayashi et al. [62] introduced a method of distribution they named quantum network coding. They proved that, for each classical network coding distribution protocol, one could construct a protocol using Local Operations and Classical Communications to distribute the corresponding quantum state over the quantum counterpart of the network, see Figure 3.4. A distribution over a classical network which, given inputs $i_1, \ldots, i_n$, outputs at the sinks the dits $f_1(i_1, \ldots, i_n), \ldots, f_m(i_1, \ldots, i_n)$ can be used to compute a LOCC to distribute the state $|\psi\rangle = \sum_{i_1,\ldots,i_n=0}^{d_1,\ldots,d_n} |i_1, \ldots, i_n, f_1, \ldots, f_m\rangle$ over the quantum version of the network – we dropped the explicit dependence of the output to the input for the sake of convenience. For an example on the butterfly network, see Fig. 3.5. The method is the following: at each node, the classical operation is simulated on the qudits inside it. Then, the qudits inside the network are measured in the reverse topological order of the classical protocol, which mean we start measuring the node which perform the last operation on the classical protocol then the penultimate and so on. They proved that each of those measures could be corrected if done in the correct order.

They left open the converse statement. Namely, the question of the existence of states which could be distributed by a LOCC quantum protocol while the equivalent classical network coding problem would have no solution. Our first example, the cross distribution over a square shaped network is indeed a nontrivial example of task impossible both quantumly and classically, hinting toward a validity of the converse statement. That was one of our motivations to study an extended version of quantum network coding to compare it to classical network coding and solve this open problem.

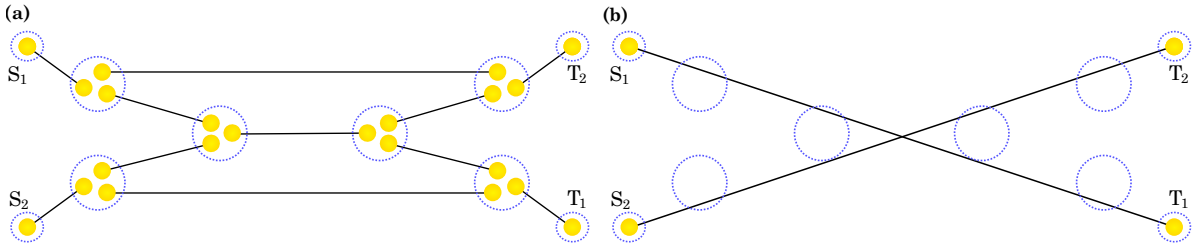

Figure 3.5: Depiction of the distribution of 2 EPR pairs over a butterfly network in the quantum setting. Here, the distribution of two bits in the classical protocol imply the existence of a LOCC protocol performing the distribution.

3.3 Stochastic network coding

Here, we study the full extent of quantum networks' distribution capability by extending the protocols to probabilistic ones and compare it *mutatis mutandis* to the classical one. Inspired by the previous description of a distribution in terms of MPSs, we have developed a new formalism based on tensor networks [38], a generalizations of MPSs to non linear topologies. Then, we show we can also reduce classical distributions over classical networks as tensor factorization. We will see in this framework the main difference is that classical network coding is only described with non-negative tensors. We will first present our version of quantum network coding adapted from the methods used in Sec. 3.1.

3.3.1 Quantum Network Coding

Let $H = (V, E, D_E)$ be a network in the quantum setting, and $C \subset V$ the set of clients. As each node $v \in V$ will own a part of a maximally entangled state for each incident edge, we label each qudit and denote the qudit belonging to edge e of node v as subsystem v_e. We describe the initial – unnormalized – state of the quantum network as

$$|H\rangle^V \propto \sum_{\overrightarrow{i_E}} \bigotimes_{e\in E} |i_e i_e\rangle^{v_e w_e} \tag{3.31}$$

where $\overrightarrow{i_E} := (i_e)_{e\in E}$. As written in Subsec. 1.5.1, distribution tasks correspond to the distribution of a pure state $|\psi\rangle^C$ shared among the clients in C. Such a task is possible over the network with nonzero probability if and only if one can find a Stochastic LOCC – SLOCC – protocol transforming $|H\rangle^V$ into $|\psi\rangle^C$. We extend the notion of *quantum network coding* to those non-deterministic protocols. The *stochastic* part is crucial as we wish to characterize the full set of states a quantum network can distribute with nonzero success probability. Formally, we will describe quantum distribution tasks target states

in the computational basis by

$$|\psi\rangle^C = \sum_{\overrightarrow{i_C}} \mathcal{T}^{\overrightarrow{i_C}} \bigotimes_{c\in C} |i_c\rangle^c \tag{3.32}$$

where $\overrightarrow{i_C} := (i_c)_{c\in C}$. Given a set of clients and a quantum network, we note we can fully characterize the quantum distribution task by a tensor $\mathcal{T}^{\overrightarrow{i_C}}$ with coefficients in $\mathbb{C}$. These coefficients are the ones of the target state $|\psi\rangle^C$, expressed in the computational basis. To extract the desired conditions for distribution, we first recall a necessary and sufficient condition for a SLOCC to distribute the state $|\psi\rangle^C$ on $|H\rangle^V$ [112]. As written in the proof of Lemma 3.1, such a distribution is possible if and only if there exists a LOCC protocol with at least one branch achieving the distribution. Formally, if a SLOCC can distribute $|\psi\rangle^C$ on $|H\rangle^V$, we can find a set of Kraus operators $\{K_v\}_{v\in V}$ and $\lambda \in \mathbb{R}^{+*}$ such that $\bigotimes_{v\in V} K_v |H\rangle^V = \lambda |\psi\rangle^C$. Equivalently, a SLOCC can distribute $|\psi\rangle$ on $|H\rangle$ if and only if there exists a set of matrices $\{M_v\}_{v\in V}$ such that:

$$\bigotimes_{v\in V} M_v |H\rangle^V = |\psi\rangle^C . \tag{3.33}$$

Trivially, the set of matrices $\{M_v\}_{v\in V}$ can be converted into Kraus operators by a simple normalization. Writing the action of the matrices M_v on the tensor representation, we deduce the following necessary and sufficient condition for a distribution task $\mathcal{T}^{\overrightarrow{i_C}}$ — as defined in eq. (3.32) — to be achievable over a quantum network.

Theorem 3.1. *Let $H = (V, E, D_E)$ be a quantum network, a distribution task $\mathcal{T}^{\overrightarrow{i_C}}$ is achievable by quantum network coding over the network if and only if $\mathcal{T}^{\overrightarrow{i_C}}$ can be factorized as*

$$\mathcal{T}^{\overrightarrow{i_C}} = \prod_{v\in V\setminus C} \mathcal{V}^{\overrightarrow{i_v}} \tag{3.34}$$

where each $v \in V$ is associated to tensor $\mathcal{V}^{\overrightarrow{i_v}} \in \mathbb{C}^{\times_{w\in N_v} d_{\{v,w\}}}$ and tensors are contracted along indices corresponding to shared edges.

Proof. This proof is similar to the one of Lemma 3.1. Let us suppose $|\psi\rangle^C$ is achievable by a SLOCC protocol. Since we are only interested by the existence of such a protocol and not its actual probability of success as long as it is non null, we may assume, without loss of generality, this SLOCC is the tensor product of successful single-dimensional projective measurements on all non-client nodes $V \setminus C$. More formally, for each node $v \in V \setminus C$, there exists an unnormalized bra

$$\langle \mathcal{V}_v| = \sum_{\overrightarrow{i_v}} \mathcal{V}_{\overrightarrow{i_v}} \langle \overrightarrow{i_v}| , \tag{3.35}$$

where $\mathcal{V}_{\overrightarrow{i_v}} \in \mathbb{C}$ for all $\overrightarrow{i_v} := (i_{v_e})_{e \in E v \in e}$ such that

$$|\psi\rangle^C = \left(\bigotimes_{v \in V \setminus C} \langle \mathcal{V}_v | \right) |H\rangle^V . \tag{3.36}$$

We then have

$$|\psi\rangle^C = \left(\bigotimes_{v \in V \setminus C} \sum_{\overrightarrow{i_v}} \mathcal{V}_{\overrightarrow{i_v}} \langle \overrightarrow{i_v} | \right) \left(\sum_{\overrightarrow{i_E}} \bigotimes_{e \in E} |i_e i_e\rangle^{v_e w_e} \right) \tag{3.37}$$

$$= \sum_{\overrightarrow{i_E}} \left(\bigotimes_{v \in V \setminus C} \sum_{\overrightarrow{i_v}} \mathcal{V}_{\overrightarrow{i_v}} \langle \overrightarrow{i_v} | \right) \left(\bigotimes_{e \in E} |i_e i_e\rangle^{v_e w_e} \right) \tag{3.38}$$

$$= \sum_{\overrightarrow{i_C}} \left(\bigotimes_{v \in V \setminus C} \sum_{\overrightarrow{i_v}} \mathcal{V}_{\overrightarrow{i_v}} \prod_{e \in E} \delta_{i_{w_e}}^{i_{v_e}} \right) \bigotimes_{c \in C} |i_c\rangle \tag{3.39}$$

$$= \sum_{\overrightarrow{i_C}} \prod_{v \in V \setminus C} \mathcal{V}^{\overrightarrow{i_v}} \bigotimes_{c \in C} |i_c\rangle , \tag{3.40}$$

where in the last line, we sum implicitly over repeated indices and the product is along the edges. By identification, we observe the requested equality:

$$\mathcal{T}^{\vec{i_v}} = \prod_v \mathcal{V}^{\vec{i_v}} \tag{3.41}$$

Conversely, if the equality is verified we can extract projective operators distributing $|\psi\rangle$ by chosing the bras along Eq. (3.35). □

This theorem is the generalization of the MPS factorization to tensor networks [89] factorization. This theorem is already a useful tool in order to study distributions over quantum networks. For example, a special case of it was already used to solve the square-cross problem in Sec. 3.1. We will use it in a specific way: to compare the classical and quantum network setting and try find a quantum distribution with no classical equivalent.

3.3.2 Stochastic Classical Network Coding

In order to be able to compare fairly the quantum and classical settings, we now adapt the formalism developed above to classical network coding. In a classical distribution task, clients are partitioned between the inputs – the sources $S \in C$ – and the outputs – the sinks $T \in C$ – of the network. In the literature [63, 49], network coding protocols are typically deterministic, i.e. each input $\vec{i} := (i_c)_{c \in S}$ at the sources always yields a specific

output $\vec{o} := (i_c)_{c\in T}$ at the sinks. However, we consider here the more general case of stochastic network coding; these protocols are probabilistic and, like the SLOCCs studied in the previous question, can abort with non zero probability. Formally, a distribution task is defined by a set of probabilities, for each input $\vec{i}$, the network outputs $\vec{o}$ with conditional probability $p(\vec{o}|\vec{i})$ and the protocol abort with probability $1-\sum_{\vec{o}} p(\vec{o}|\vec{i})$. We gather all probability in a tensor $\mathcal{T}^{\vec{i},\vec{o}} = p(\vec{o}|\vec{i})$ with real positive coefficients. As the sets of sources and sinks form together a partition of the set of clients, $\mathcal{T}^{\vec{i},\vec{o}}$ can be written as the tensor $\mathcal{T}^{\vec{i_C}}$, similarly to the description of quantum distribution tasks as tensors in Eq. (3.32). One can therefore define a classical and a quantum distribution task using the same formalism. The fact that classical tensor is restricted to real non-negative coefficients while the quantum one can also have negative and complex coefficients is the only formal difference between the two types of task.

Using this tensor formalism, we characterize necessary and sufficient conditions for a distribution task to be achievable over a given classical network. We can extend a bit the previous definition. Indeed, multiplying $\mathcal{T}$ by a strictly positive scalar $\lambda \in \mathbb{R}^{+*}$ will only alter the general probability of failure without changing the correlation between inputs and outputs. As a consequence, we deem a distribution task $\mathcal{T}$ is achievable on a classical network when there exists a λ strictly positive such that $\lambda\mathcal{T}$ is achievable.

How does one implement a stochastic classical network coding to perform a distribution task? The answer is quite straightforward: in a network coding setup, each node waits inputs $\vec{i_v}$, then performs an arithmetical operation such that it outputs $\vec{o_v}$ with probability $p_v(\vec{o_v}|\vec{i_v})$. As before, we regroup the probability table in tensor $\mathcal{V}^{\vec{i_v},\vec{o_v}} = p_v(\vec{o_v}|\vec{i_v})$. We can compute the tensor given by two nodes sharing a link: let v and w be two nodes of the network such that some outputs of v are inputs of w. We call $\vec{i_v}$ the inputs of v, $\vec{j}$ the inputs of w which are output of v, $\vec{o_v}$ the other outputs of v, $\vec{i_w}$ the inputs of w which are not output of v and, finally, $\vec{o_w}$ the outputs of w. The probability to input $(\vec{i_v},\vec{i_w})$ and output $(\vec{o_v},\vec{o_w})$ is given by:

$$p(\vec{o_v},\vec{o_w}|\vec{i_v},\vec{i_w}) = \sum_{\vec{j}} p_v(\vec{o_v},\vec{j}|\vec{i_v}).p_w(\vec{o_w}|\vec{j},\vec{i_w}) \tag{3.42}$$

The tensor relation becomes relevant here, grouping the probability table p in a tensor $\mathcal{P}^{\vec{o_v},\vec{o_w},\vec{i_v},\vec{i_w}} = p(\vec{o_v},\vec{o_w}|\vec{i_v},\vec{i_w})$, we can rewrite the previous equation as a contraction of tensors:

$$\mathcal{P}^{\vec{o_v},\vec{o_w},\vec{i_v},\vec{i_w}} = \mathcal{V}^{\vec{o_v},\vec{j},\vec{i_v}}\mathcal{W}^{\vec{o_w},\vec{j},\vec{i_w}} \tag{3.43}$$

where we used the Einstein notation to sum implicitly over repeated indices. Note that, among other things we introduced a causality in the classical distribution. This is a

difference with the quantum setting. The interested reader can find a study exploring the relationship between quantum distribution, classical distribution and causal order in [4]. So, each stochastic classical network coding is an assignation to each node v of a non-negative tensor $\mathcal{V} \in \mathbb{R}^{+\times_{w\in N_v} d_{\{w,v\}}}$, where there is an index for each incident channel and of the dimension of said channel. The distribution task associated to the assignation is the contraction of those tensors along the network's edges. Everything is set for the subsequent theorem:

Theorem 3.2. *Let $H = (V, E, D_E)$ be a classical network, a distribution task $\mathcal{T}^{\vec{i_c}}$ is achievable by a stochastic classical network coding over the network if and only if $\mathcal{T}^{\vec{i_c}}$ can be factorized as*

$$\mathcal{T}^{\vec{i_c}} = \prod_{v\in V} \mathcal{V}^{\vec{i_v}} \tag{3.44}$$

where each $v \in V$ is associated to tensor $\mathcal{V}^{\vec{i_v}} \in \mathbb{R}^{+\times_{w\in N_v} d_{\{v,w\}}}$ and tensors are contracted along indices corresponding to shared edges.

3.4 Comparison of classical and quantum network coding

As the main difference here is that classical network coding is only described with non-negative tensors. In order to keep the comparison between the quantum and the classical task meaningful, we restrict the distribution tasks we consider in the quantum setup to ones which are described by non-negative tensors. The class of state arising from this condition is the so-called quantum subset state [44], which encompasses all the states which can be written using non-negative real coefficients in the computational basis, up to local unitary operations. It is a broad class of states containing, among other things, highly relevant states for quantum applications the GHZ states, any bicolorable graph states as well as the W states – see Subsec. 2.1.2 for a definition of the W state on 3 qubits. By considering both theorems 3.1 and 3.2, we extract the following theorems

Theorem 3.3. *Any distribution task $\mathcal{T}$ achievable on a network by a stochastic classical network coding protocol is achievable on the corresponding quantum network by a quantum network coding protocol.*

Theorem 3.4. *The converse is not true.*

Theorem 3.3 is an extension of the result of [62], we first present its proof Theorem 3.3.

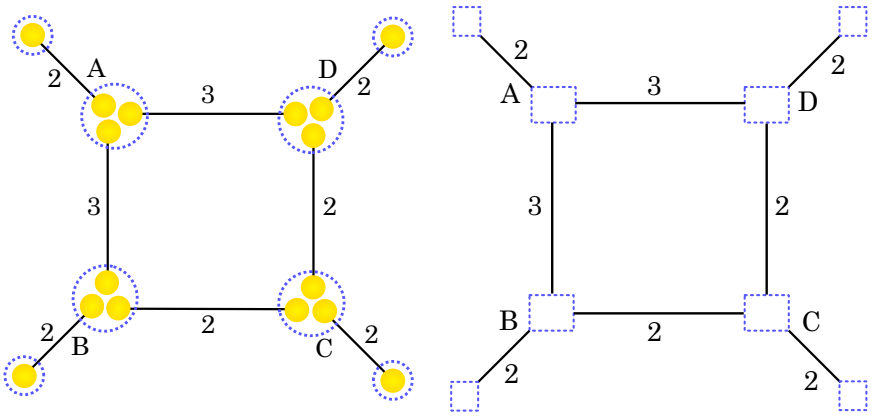

Figure 3.6: Depiction of the new network in both the quantum and classical settings. Both the top and the left channel are of dimension 3, the other two remain of dimension 2.

Proof. The implication from classical to quantum is the direct consequence of both Theorems 3.1 and 3.2: if a tensor is factorizable along the network topology in $\mathbb{R}^+$, the tensor is factorizable in $\mathbb{C}$ since $\mathbb{R}^+ \subset \mathbb{C}$. □

The proof of Theorem 3.4 is given in Subsec. 3.4.2, by a counter example, but let us first look at a direct application of Theorem 3.3.

3.4.1 Achieving cross binary EPR pairs on a square network with two ternary channels

We will see a direct application of Theorem 3.3. Let H be a classical network defined by the graph depicted on Figure 3.6, it an extension of the XBox game of Sec. 3.1. We choose A, B, C and D as the clients. The correlation we wish to implement is the following: we wish that A and C share a bit and that B and D share another uncorrelated bit. If we choose A and B as sources and C and D as sinks – a role's distribution expected if we look for cross distribution over the network –, no classical protocol can perform this distribution with probability 1. As can be seen in Figure 3.8, the direction we have to impose to be able to cross communicate implies that two bits have to be sent through a channel of dimension smaller than 4, which is impossible. However, choosing A as the only source and the other clients as sinks, there is a protocol to perform this distribution with probability 1, as can be seen in Figure 3.7.

We can extract from the classical protocol a quantum protocol allowing for the distribution of states $|\psi\rangle = |\text{EPR}\rangle^{AC} \otimes |\text{EPR}\rangle^{BD}$ on the quantum network. The protocol is the

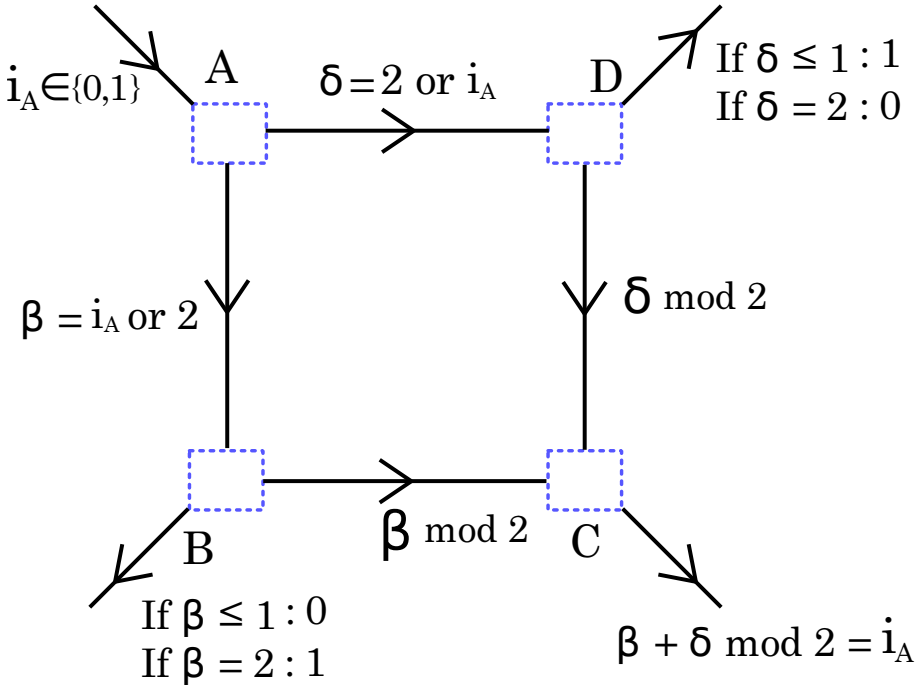

Figure 3.7: Classical scheme from which we can extract a LOCC to distribute cross binary EPR pairs across a square network. There is one source and 3 sinks here, the source will randomly decide which path will take i_A and send 2 through the other channel. This choice allow to broadcast two information in the network: i_A and which path was taken. This allows the establishment of the wanted correlation, i.e. the sharing of two independant bits, one between A and C, the other between B and D.

following, A creates locally the – unnormalized – state,

$$|002\rangle^{A,A_1,A_2} + |020\rangle^{A,A_1,A_2} + |112\rangle^{A,A_1,A_2} + |121\rangle^{A,A_1,A_2} \tag{3.45}$$

then keep the qubit labeled as A, sends the qutrit A_1 to B and send A_2 to D using quantum teleportation. We label the qutrit received by B as B_A and the one received by D as D_A. B generates one new qubit $|0\rangle^B$, then applies the unitary which achieves the transformation

$$\begin{aligned} |00\rangle^{B_A,B} &\to |00\rangle^{B_A,B} \\ |10\rangle^{B_A,B} &\to |10\rangle^{B_A,B} \\ |20\rangle^{B_A,B} &\to |21\rangle^{B_A,B}. \end{aligned}$$

B send the subsystem labeled as B_A to C and keep the other, we will label the received subsystem as C_B. Similarly, D generates one new state $|0\rangle^D$ and applies the unitary

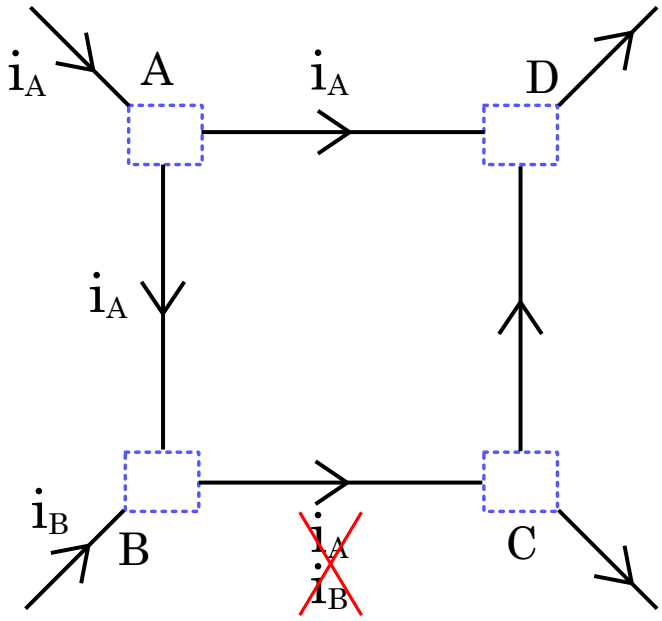

Figure 3.8: Cross communication of bits is impossible to do classically with probability 1 over this ternary network. Indeed, two bits of information have to go from the left side to right side and two bits have to be exchanged between the top and the bottom this impose the orientation of the channels. However, such choice of channels' direction involves that two bits have to pass into a channel of dimension strictly smaller than 4, which is impossible.

which achieves the transformation

$$\begin{aligned} |00\rangle^{D_A,D} &\to |01\rangle^{D_A,D} \\ |10\rangle^{D_A,D} &\to |11\rangle^{D_A,D} \\ |20\rangle^{D_A,D} &\to |20\rangle^{D_A,D} . \end{aligned}$$

D send the subsystem D_A to C, we label the received subsystem as C_D. At this step of the protocol, the – unnormalized – state is the following

$$|000\rangle^{ABD} |02\rangle^{C_BC_D} + |011\rangle^{ABD} |20\rangle^{C_BC_D} + |100\rangle^{ABD} |12\rangle^{C_BC_D} + |111\rangle^{ABD} |21\rangle^{C_BC_D} \quad (3.48)$$

Finally, C measures both subsystems C_B and C_D with the following – unnormalized – sub-family of Kraus operators

$$K_x = |0\rangle^C \langle 02|^{C_BC_D} + |1\rangle^C \langle 12|^{C_BC_D} + (-1)^x |0\rangle^C \langle 20|^{C_BC_D} + (-1)^x |1\rangle^C \langle 21|^{C_BC_D} . \quad (3.49)$$

We do not describe the whole family since this sub-family can be completed directly with Kraus operators K such that the probabilities of the associated outcomes are null. We eventually correct the phase by applying a Z operator on B achieving the wanted

distribution. We previously proved the impossibility of a cross distribution over a square network with link of dimension 2. Applying theorem 3.3, we show that cross distribution of qubits is achievable using ternary channels and we go further by showing a LOCC exists, which means the operation can succeed with probability one, a feat that cannot be achieved with classical network coding. This show that using ternary channels over quantum networks leads to a superiority into solving qubit bottleneck issues.

3.4.2 Superiority of quantum network coding

We now prove Theorem 3.4, and show that the question left-open by Kobayashi et al. [62] can be answered negatively. As shown in Theorem 3.1, distributing $|\psi\rangle$ means finding a factorization of $\mathcal{T}$ in the field $(\mathbb{C}, +, \cdot)$, while achieving the probability table $p(\vec{o}|\vec{i})$ by a stochastic classical network coding protocol is equivalent to the finding of a factorization of $\mathcal{T}$ in the semiring $(\mathbb{R}^+, +, \cdot)$. A counterexample – a tensor $\mathcal{T}$ and a network G such that $\mathcal{T}$ can be factorized in $\mathbb{C}$ and not in $\mathbb{R}^+$ – suffices to prove Theorem 3.4. We exhibit below such a counterexample, based on the noisy typewriter channel well known in classical information theory [101]. This is a channel defined on a finite alphabet $(a_0, \ldots, a_n)$ which transmits, with probability $1/2$ each, either the input letter or the next letter in the alphabet. Here, $n = 4$ and the alphabet is $0, 1, 2, 3$ the channel gives the following correlation table:

$$\mathcal{T} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}. \tag{3.50}$$

Viewed as a quantum network distribution task, it becomes up to normalization

$$|\psi\rangle = \sum_{j=0}^{3} |j\rangle \otimes (|j \oplus 1\rangle + |j\rangle), \tag{3.51}$$

where $\oplus$ denotes addition modulo 4.
The network we examine is composed of a single channel shared by two clients. We know the minimum dimension necessary to distribute $|\psi\rangle$ is the rank of matrix $\mathcal{T}$, which is 3.

We can find two matrices $C \in \mathbb{C}^{4\times3}$ and $F \in \mathbb{C}^{3\times4}$ such that $\mathcal{T} = CF$, as shown below

$$C = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \tag{3.52}$$

$$F = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \tag{3.53}$$

Therefore, the 4-dimensional noisy typewriter channel can be compressed with nonzero success-probability in a ternary quantum channel.

Is the same feat achievable by a ternary classical channel? In other words, can we find two matrices of the same dimension in $\mathbb{R}^+$ which factorize $\mathcal{T}$? We denote the i^{th} row of C as $\overrightarrow{c_i}$ and the j^{th} column of F as $\overrightarrow{f_j}$. If C and F factorize $\mathcal{T}$, then $\mathcal{T}^{i,j} = \overrightarrow{c_i}.\overrightarrow{f_j}$.

First observation, a row of C cannot be proportional to an other. Indeed, for all couples $\overrightarrow{c_i}$ and $\overrightarrow{c_j}$ of distinct rows, we can find a column $\overrightarrow{f_k}$ of F such that

$$\overrightarrow{c_i}.\overrightarrow{f_k} = 1 \tag{3.54a}$$

$$\text{and } \overrightarrow{c_j}.\overrightarrow{f_k} = 0. \tag{3.54b}$$

This fact will prove to be decisive later. Then, by definition of the problem, all the vectors are non-negative and show therefore an interesting property we can exploit: two non-negative orthogonal vectors are disjoints. For example, in our case $\overrightarrow{c_1}.\overrightarrow{f_3} = \mathcal{T}_{13} = 0$ implies that whenever the j^{th} component of the row vector $\overrightarrow{c_1}_j$ is non-null, $\overrightarrow{f_3}_j$ must be null. Since $\overrightarrow{c_1}$ is orthogonal to two non-colinear vectors – $\overrightarrow{c_1}.\overrightarrow{f_3} = 0$ and $\overrightarrow{c_1}.\overrightarrow{f_4} = 0$ – in a space of dimension 3, all the coefficients of $\overrightarrow{c_1}$ but one are null. Since the same can be said for each $\overrightarrow{c_i}$, the family $\{\overrightarrow{c_1}, \overrightarrow{c_2}, \overrightarrow{c_3}, \overrightarrow{c_4}\}$ is formed of 4 single coordinates vector in a space of dimension 3. Which implies two of them must be proportional which is impossible according to Eqs. 3.54. This factorization is therefore not achievable in $\mathbb{R}^+$: we cannot compress the 4 state noisy typewriter channel in a classical ternary channel, even stochastically. This task is therefore only achievable in a quantum setting, but not in a classical one.

3.5 Conclusion

The research presented here has been pre-published in arXiv [79] and is currently submitted to the journal Quantum.

In this chapter, we studied 3 different issues: the solving of a simple but fundamental bottleneck issue, the characterization of states which could be distributed on a quantum network, the comparison between classical distributions and quantum distributions. We developed here a new formalism to study those questions. This formalism is capable of finding previously known results in a more simple way, such as the impossibility to perform a cross distribution over a square shaped quantum network. It is also useful to find new results, such as the possibility for quantum networks to perform the previously considered cross distribution using ternary channel. A feat classical network coding cannot perform with probability one, this demonstrates the superiority of using ternary channel on quantum networks in order to solve bottleneck issues on the network. Moreover, in this formalism, showing the fundamental difference between stochastic quantum and classical network coding became simple as they were reduced as factorization of tensor in different sets. Exposing a quantum distribution of a quantum subset states with no classical equivalent was reduced to the problem of finding a matrix with a non-negative rank superior to its rank, answering in part the question left open by Kobayashi et al. [62] Moreover, by direct association, we can relate some classical protocol with a non-zero probability to succeed with their quantum equivalent, having the same probability of success. We have good hope that those results can benefit to the research about resource management over quantum networks and help to design optimized quantum networks.

CHAPTER 4

Distributing graph states over quantum networks

The work presented in this chapter contains in its first part the very first published research output of this PhD. It can be found *Phys. Rev. A* as "Distributing graph states over arbitrary quantum networks" [80]. This study was my first approach in order to design a single-shot distribution protocol and is also one of the last I have worked on, since I currently collaborate with Rodney Van Meter[1,2] and several members of the Keio university: Michał Hajdušek[3], Naphan Benchasattabuse[3] and Takahiko Satoh[1,4], to apply this distribution protocol to their quantum network simulator: QuISP available here[5] [78]. As a consequence, this chapter is divided in two major parts, I will first – in Sec. 4.1 and Sec. 4.2 – present the protocol as it was designed, then – in Sec. 4.3 – its more concrete implementation in the QuISP simulator.

At the heart of this work lies the distribution of GHZ states and graph states. For the reader unfamiliar with any of these two class of states or the graph formalism, the needed notions are exposed in Sec. 1.4. Our aim is to work on the general case of a

[1]Keio University Quantum Computing Center, Yokohama 223-8522, Japan

[2]Faculty of Environment and Information Studies, Keio University Shonan Fujisawa Campus, Fujisawa 252-0882, Japan

[3]Graduate School of Media and Governance, Keio University Shonan Fujisawa Campus, Fujisawa 252-0882, Japan

[4]Graduate School of Science and Technology, Keio University, Yokohama 223-8522, Japan

[5]https://aqua.sfc.wide.ad.jp/quisp_website/

single-shot graph state distribution protocol – i.e. to distribute a single copy of the state we wish to distribute – and to establish first cost metrics based on the consumption of maximally entangled pairs and the time needed to communicate. Since the publication of our protocol [80], those cost metrics have been studied and improved [40, 19]. The result of this research was a fairly simple multipartite protocol which gave glimpses of what could be done for multipartite distributions. We find two important features in our protocol, the choice of which graph state the clients build can be made post-distribution by using simple one qubit measurements and the protocol is optimal in terms of the number of EPR pairs consumed.
An open challenge was still to describe it with enough details to be able to simulate it. This part was on hold until a workshop in Japan in February 2020 which allowed me to meet Rodney Van Meter; discussions led to a collaboration which had and still has two objectives. First, adapting our protocol to the RuleSet setting used in QuISP. Second, adapting their simulator to multipartite communications, adding the necessary backbone for these protocols to be implemented.
I will first present in Sec. 4.1 some necessary theorical tools which have not been introduced yet. In this case, it will be a short introduction to the graphical manipulation of graph states and the links between those and physical operations. Then, I will describe and study the protocol to distribute GHZ state and arbitrary graph states over arbitrary quantum networks [80] in Sec. 4.2. Finally, I will introduce the RuleSet formalism and present the new concrete protocol designed for simulation using QuISP in Sec. 4.3.

4.1 Preliminaries

The main notions used in this chapter are presented in Chapter 1 as:

- Local Clifford class of operation in Subsec. 1.2.2
- Resource states in Sec. 1.4
- Networking in Sec. 1.5

As previously written, the first part of the work presented in this article is based on the graphical representation of operations and measurements of graph states. Indeed, several physical operations on a graph states $|G\rangle$ can be depicted as graph operations on the associated graph G, up to local corrections which we will neglect here and until the concrete implementation part in Sec. 4.3. In particular, we will use three elementary graph operations as building blocks for our protocols [108, 18]:

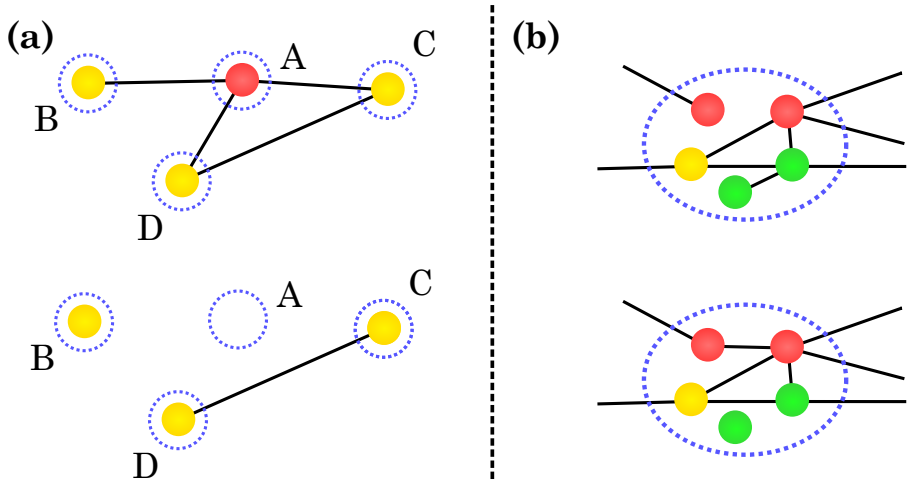

Figure 4.1: In (a) the qubit belonging to A is measured in Z destroying said qubit and removing the associated edges from the graph. In (b) two CZ are applied, one between the two top red qubits leading to an edge addition, and one between the two bottom green ones leading to an edge deletion.

- Vertex deletion. This operation removes one vertex and all the associated edges from the graph. Physically, it is implemented by the Pauli measurement of the relevant qubit in the Z basis, see (a) of Fig. 4.1
- Edge addition – or deletion. By applying a controlled-Z operation between two qubits belonging to the same node, we either delete or create an edge between them, depending whether they are adjacent or not; see (b) of Fig. 4.1.
- Local complementation on a vertex. This graph operation inverts the sub-graph induced by the neighborhood N_D of the concerned vertex D. It is implemented by applying the relevant operation to the qubits of $D \cup N_D$, described by the quantum unitary operator $U_D^\tau := e^{-i\frac{\pi}{4}X_D} \bigotimes_{M\in N_D} e^{i\frac{\pi}{4}Z_M}$ acting on $|G\rangle$, see Fig. 4.2.

Other useful, if non-elementary, operations, are the measurement of a qubit in either the Y or the X basis. A measurement in the Y basis corresponds graphically to a local complementation followed by the removal of the measured vertex. To see this, we note that the local complementation operations implement a basis change from Z to a Y on the concerned vertex. A measurement in the X basis is a bit trickier to represent, we need to choose an arbitrary neighbour of the measured qubit, we label n_X, and do in succession a local complementation on n_X, measure the qubit in Y and apply a local complementation on n_X again [48]. Note that the graphical transformation and associated operation are equivalent up to some local unitary operation, a so-called "correction", which depends on the outcome of the measurement. For example, if a Z measurement of a vertex v gives

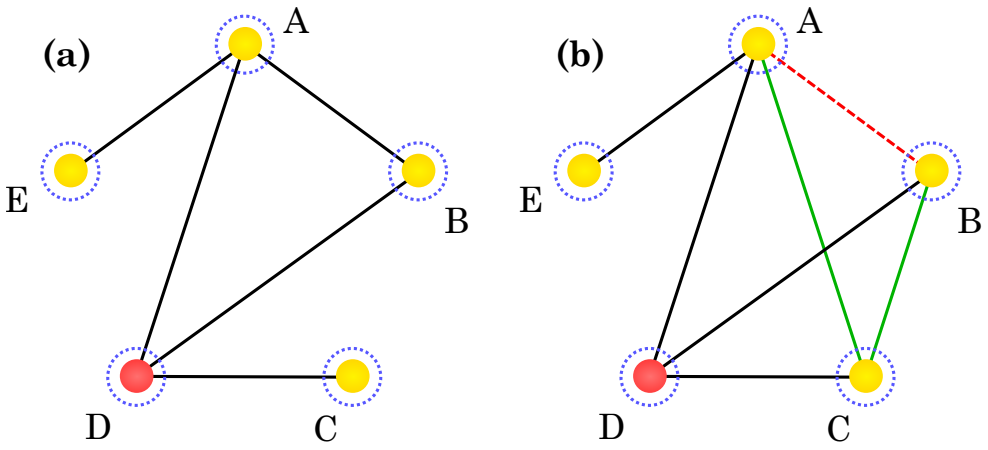

Figure 4.2: Example of the application of local complementation applied on node D. The physical operation associated is written as $U_D = e^{-i\frac{\pi}{4}X_D} \otimes e^{i\frac{\pi}{4}Z_A} \otimes e^{i\frac{\pi}{4}Z_B} \otimes e^{i\frac{\pi}{4}Z_C}$. (a) and (b) are respectively the graph state's represention before and after the local complementation: we observe the removal of the edge between A and B and the addition of two edges between both the pairs (A, C) and (B, C)

the outcome 0, no correction hast to be applied; but if it gives the outcome 1, then a σ_Z correction has to be applied to each neighbour of v. We will neglect corrections until the implementation part. As an example, Figure 4.3 shows how entanglement swapping along a line of repeaters [98, 1, 92] can be depicted graphically with the above tools. The essential observation here is that a Bell measurement is equivalent to performing a CZ-gate followed by two single qubit Y-measurements.
Using wisely the previous graphical rules, we designed a GHZ state distribution protocol which allows for an arbitrary graph state distribution.

4.2 GHZ and Graph states distribution

4.2.1 GHZ states distribution

The setup is the following: several clients of the network want to share a GHZ state across a given quantum network $H = (V, E, D_E)$ in which every channel is of dimension 2. As previously written in Subsec. 1.4.2, the complete graph state – the graph state depicted by a complete graph – is LU equivalent to a GHZ state. Ergo, in our setup, where local unitary operations can be freely performed, distributing this graph state means distributing a GHZ state. This is why we design a protocol which aims at distributing a complete graph state over the network. Note that the protocol presented here will differ

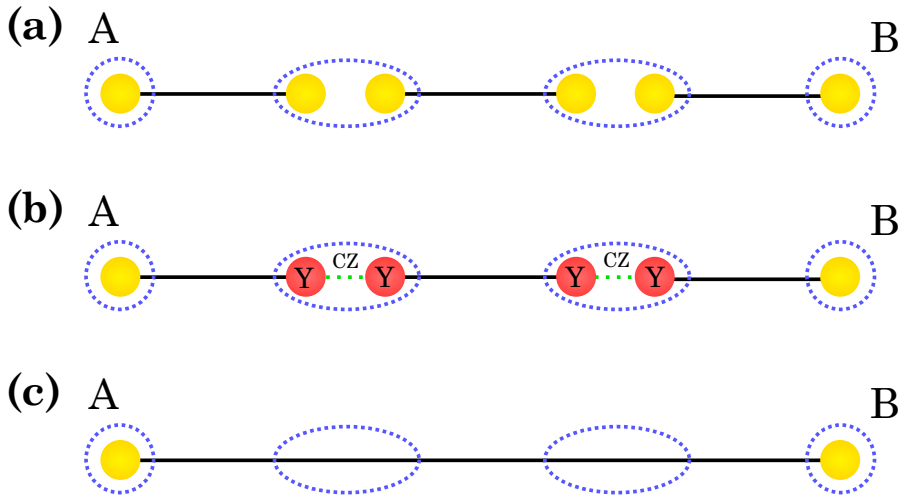

Figure 4.3: Graphical representation of the quantum repeater protocol. Starting from a repeater line, we apply CZ and two measurements in the Y basis at each repeater to obtain an EPR pair between the end nodes.

from the one we presented in [80]. Indeed, in our article, we distribute a star graph while here we distribute a complete graph. It does not change anything to the result but it helped to track needed corrections for the QuISP implementation.

A useful primitive: the clique expansion

We define below the procedure of clique extension, which is also be represented in Fig. 4.4, together with its effects over the graph's representation.
A clique of a graph G is defined as a complete subgraph of G. Let us observe the application of an X measurement to a qubit at the conjunction of two otherwise disjoint cliques. Let n_X be an arbitrary neighbour of the central qubit c, a local complementation of n_X will transform the clique owning both n_X and c into a sub-star centered on n_X as the subgraph induced by the neighbourhood of n_x is a complete graph. Then, the Y measurement of c will first remove all edges between the qubits of the remaining clique as they form a complete subgraph in the neighbourhood of c and, since the two cliques are disjoint, link all those qubits to n_X. This operation achieves a star graph encompassing all the initial qubits but c – which was measured and thus removed from the graph state depiction – and centered on n_X. Finally, the last local complementation of n_X will transform this star graph into a complete graph. This procedure and the effect over the graph's representation can be found in Fig. 4.4. We will use this property to make a clique grows through the network on which we want to distribute the GHZ state.

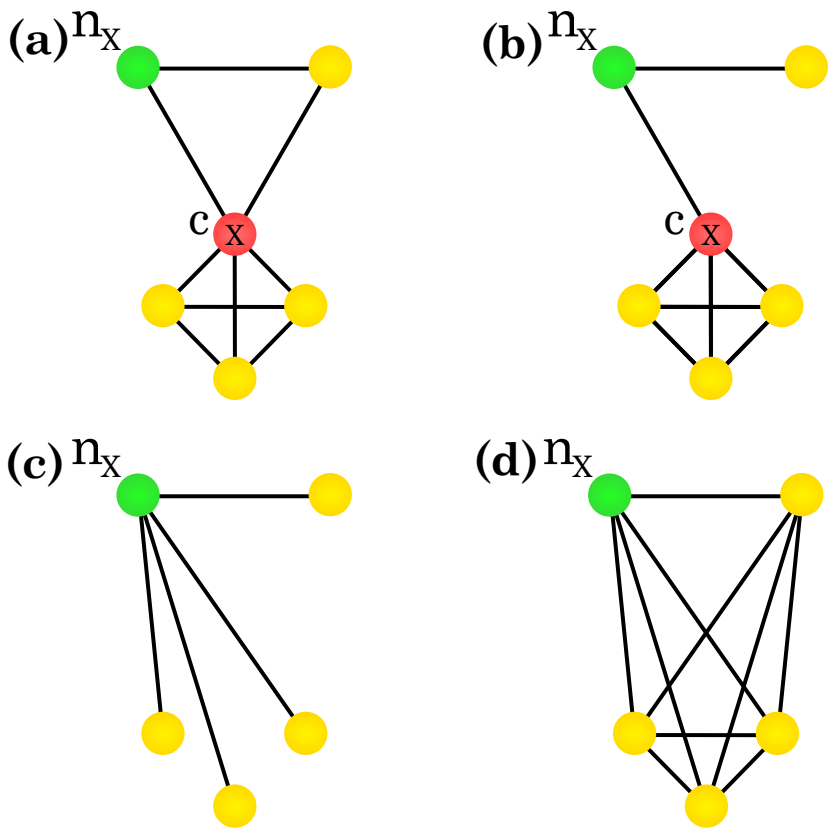

Figure 4.4: Here, c is the central red vertex and n_X the labeled green one. (a) is the initial graph state, c is a central node at the conjunction of 2 cliques of size 3 and 4 respectively. (b) is the state after the first local complementation on n_X, the edge between c and the last member of the clique is removed, the previous clique is transformed into a sub-star centered on n_X. (c) is the state after the Y measurement of c, the local complementation induced by the Y measurement erases the edges between nodes belonging to the other clique and link every one of them to n_X. (d) is the final state after the last local complementation on n_X, a new clique between all the presented qubits

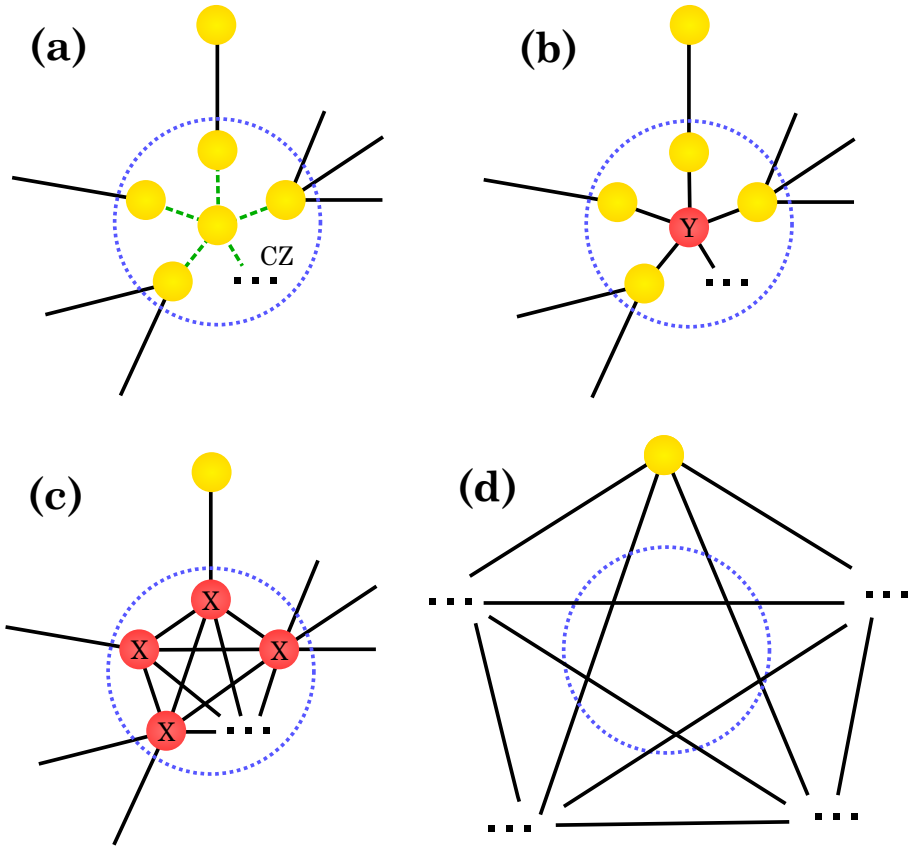

Figure 4.5: Depiction of the clique expansion, in the initial state, the network node is at the conjunction of several cliques, one for each of its neigbhour. In **(a)**, we added a central qubit and now perform CZ operations between it and the other qubits. In **(b)**, we measure the central qubit in the Y Basis resulting in a clique inside the node. In **(c)**, we measure all the other qubits in the X basis. **(d)** sequentially merging all the initial clique to the central one, finally achieving the clique expansion

The whole process relies on an operation we will call the *clique expansion* which acts on a node of the network as follow: if a node is at the conjunction of several cliques, this operation will merge all the cliques together in one larger clique. This operation is depicted in figure 4.5 and goes as follow

1. We add a qubit we initialize as $|+\rangle$ in the node, we call this qubit the central qubit
2. If the node is to be part of the final GHZ state, we add another qubit initialized as $|+\rangle$
3. We perform CZ operations between the central qubit and all the other qubits in the node – **(a)** in Fig. 4.5
4. We measure the central qubit in the Y basis – **(b)** in Fig. 4.5. At this point, all

qubits inside the node are at the conjunction of cliques as in Fig. 4.4 – **(c)** in Figure 4.5 to see a depiction.

5. We measure all the qubits of the node – but the one we may have added in step 2 – in the X basis. Each time we perform a measurement we are merging the central clique with another neighbouring clique. After the measures, all the cliques are merged together and we have achieved a clique between every neighbouring node.

A GHZ states distribution protocol

The clique expansion operation defined above will help us to share the complete graph state, across the full set of clients C. The first step is to find a minimal tree covering all the nodes of C – i.e. a subgraph connecting all the nodes in C with the minimum number of edges. The problem of finding such a tree is *the Steiner tree problem*, well-known in classical graph theory. Despite the full problem being NP-Hard [54], in the case we restrict – as we do – the network to an unweighted graph, the Steiner tree can be approximated in a polynomial time [97, 14]. And an approximated tree is sufficient, the Steiner tree is only a way to minimize entanglement consumption.

I would like too add here a remark on this previous work of mine [80]. We are dealing with networks, and one needs to adapt the Steiner tree algorithm to the constraint of the network. For example, by taking into account the likeliness of a congestion happening as it can be done in the classical setting [58]. Those congestion would add some weight to the tree as some edges are more likely to induce a waiting time on the distribution and so change the result of the algorithm. Actually, we may find some differences between the resulting Steiner tree in a classical and a quantum setting. Indeed, we proved in Chapter 3 some quantum distributions are possible with a non-zero probability while impossible in the classical setting, as such the congestion in the quantum setting may be of a different kind and the weight resulting from the simultaneous computation of several Steiner trees over the network may be impacted by these newly opened possibilities and would necessitate a work of its own.

Nevertheless, in this chapter we focus on a single distribution over the network and we assume we already know at least one Steiner tree for the given distribution, see Fig. 4.6 for a Steiner tree defined on our example network. In the implementation part of Sec. 4.3, we will use a concrete algorithm to approximate a minimal tree over the network. Now, we will distribute the GHZ state over the Steiner tree. We simply explore the tree and apply the clique expansion subprotocol with the exploration's current node effectively making a clique grows over the tree. An example of this process is depicted in Fig. 4.7.

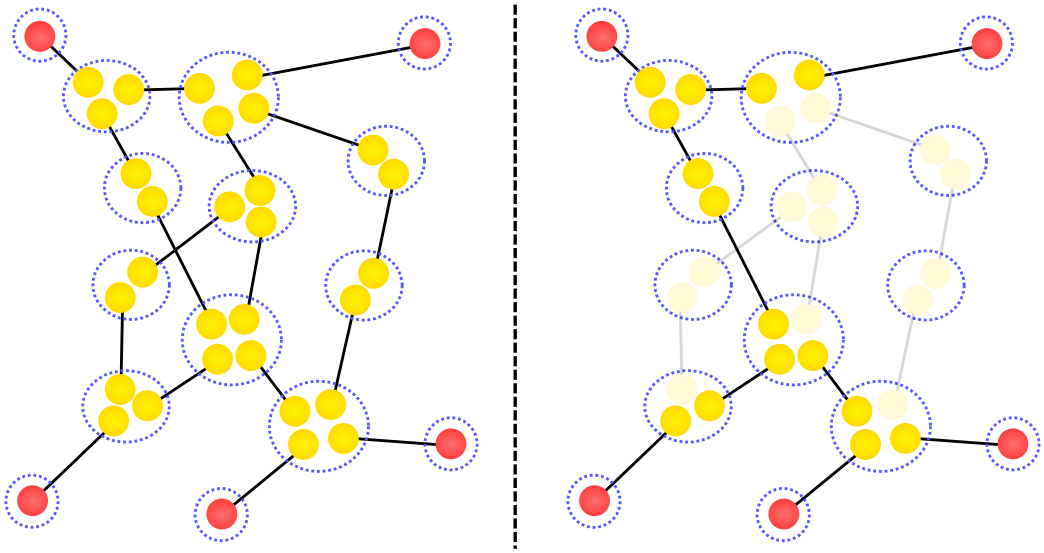

Figure 4.6: Example of a Steiner tree for a set of clients C. The nodes of C are represented by red colored leaves of the network. The left figure depicts the original network. On the right figure, the non-transparent parts depict the associated Steiner tree for the set C.

The number of EPR pairs consumed in this process is equal to the number of edges in the tree, which by definition is – almost – the minimum possible number for the – approximate – Steiner tree. Since clique expansion requires local operations to each node and the same Clifford operations at each time step, these commute and can all be done in one step, with a single step of correction afterwards [17]. Knowing which corrections to apply after distributing a GHZ state on the network is a question of interest we will study in Sec. 4.3. For now, we will use this specific protocol to discuss the distribution of arbitrary graph states.

4.2.2 Graph states distribution

We now show how to generalize the previous approach to distribute an arbitrary graph state over a set C of known clients of the network. The procedure will be to distribute a specific resource graph state: the edge-decorated complete graph. The edge-decorated complete graph is a complete graph on which we added a an intermediary node at each edge. See the left-side of Fig. 4.8 to see an edge-decorated complete graph for 5 nodes. From this graph state, nodes can construct any graph state by measuring each edge-qubit in either the Z basis or the Y basis, as represented in Figure 4.8. This graph is already used in [95] for a similar goal, with a protocol to distribute it in a different context. We present here a new approach to its distribution, adapted to our setting. We will also

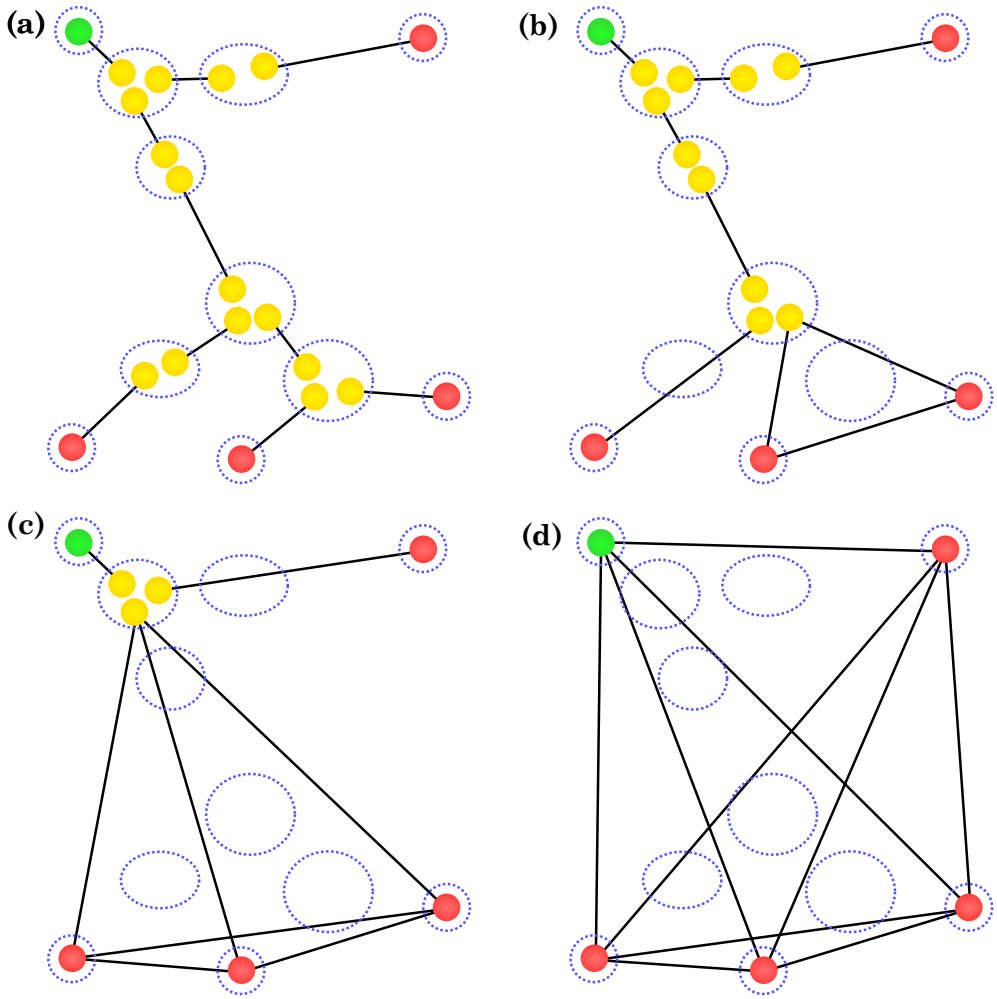

Figure 4.7: Complete distribution of a a GHZ state using successive clique expansion. We separated the clients leaves between a green top left client and the other red ones. The reason for this separation can be found in the concrete implementation part, see Sec. 4.3. Here we start from red leaves and gradually reach the green one by expanding the cliques along the way.

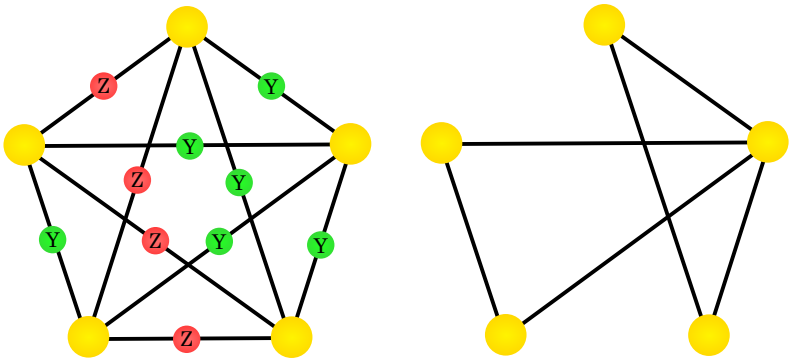

Figure 4.8: The edge-decorated graph can be projected into any graph state by measuring its edge-qubits. We can distribute it as a resource to generate arbitrary graph states. We measured each green node in the Y basis and each red node in the Z basis.

compute and optimize its cost in term of resources. We consider the consumption of EPR pairs and also introduce a notion of time. Indeed, we consider that at each time step the entanglement of the network is replenished and we will count the number of time steps which are necessary to distribute said states. The protocol to distribute the edge-decorated complete graph follows directly from multiple applications of the GHZ state distribution: we consider the set C of the k clients – k being the number of clients. The first step is solving the Steiner tree problem on the network for the k nodes. We distribute a k-GHZ state starting from one arbitrary client c_1, then we apply a local complementation on c_1 such that we switch the graphical representation of the distributed GHZ state to a star graph centered on the client. In order to have the Steiner tree for the set $C \setminus \{c_1\}$, we remove vertices from the tree. Then, we choose a second client c_2 to distribute a $(k-1)$-GHZ state. This procedure iterates until the distribution of a final EPR pair between the two last nodes of C. As seen in Fig. 4.9, the resulting graph state is locally equivalent to the edge-decorated dotted graph. Some optimizations are possible if the final graph state is a known quantity before the distribution. We call G the graph representing the graph state to distribute $|G\rangle$. We search to extract from G a star subgraph S_1 of maximum size. We distribute the GHZ state associated to S_1 using the GHZ state distribution protocol. Then we iterate with $G \setminus S_1$ and so on until $\bigcup S_i = G$. In its general form, the protocol presented is strictly independent from the network topology and from the wanted graph state which can be decided post-distribution. To evaluate the efficiency of this protocol, we compared it to the consumption of a pathological expensive case: the case of a line network where we each node is paired with its opposite and the aim is to distribute a EPR pair between them – see Fig. 4.10. If

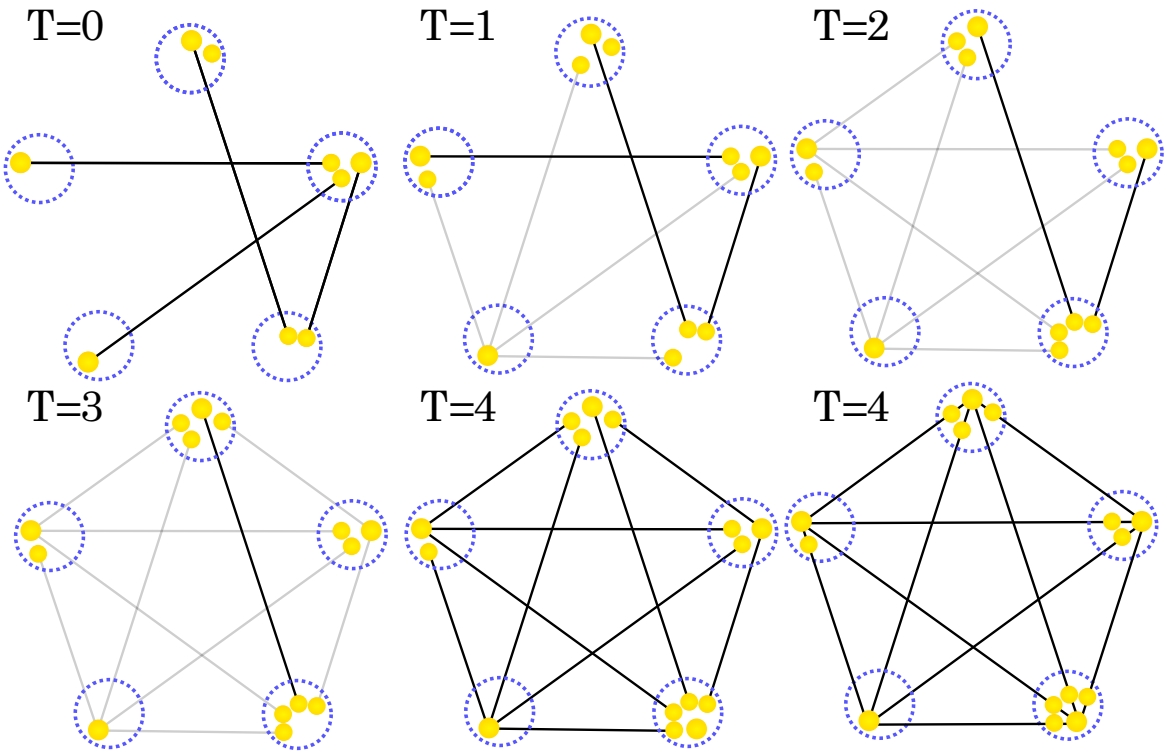

Figure 4.9: Distribution of the edge-decorated graph of size 5 from a Steiner Tree starting with at $T = 0$. At the end of step $T = i$, a star graph is shared centered on c_i, then vertex i is ignored in the following steps. Finally, the last step some local CZ operations are done to generate the desired edge-decorated graph state.

		Protocol	Bound
N-GHZ	EPR	$N-1$	$N-1$
	T	1	1
Arbitrary Graph State	EPR	$\leq \frac{N(N-1)}{2}$	$\lfloor \frac{N}{2} \rfloor^2$
	T	$\leq N-1$	$\lfloor \frac{N}{2} \rfloor$

Table 4.1: Creation costs on a network of size N

one uses our general protocol, one finds a consumption of at most $\frac{N(N-1)}{2}$ EPR pairs and in $N-1$ time-steps. This upper bound is reached when all the network's nodes are part of the graph state. Both costs are equal up to a constant factor 2 to the cost of the pathological case – see Table 4.1. This was the actual end of this paper [80]. However, a meeting and discussions with Rodney Van Meter who leads AQUA, a team developing the quantum simulator QuISP, was a nice reason to read my old paper and

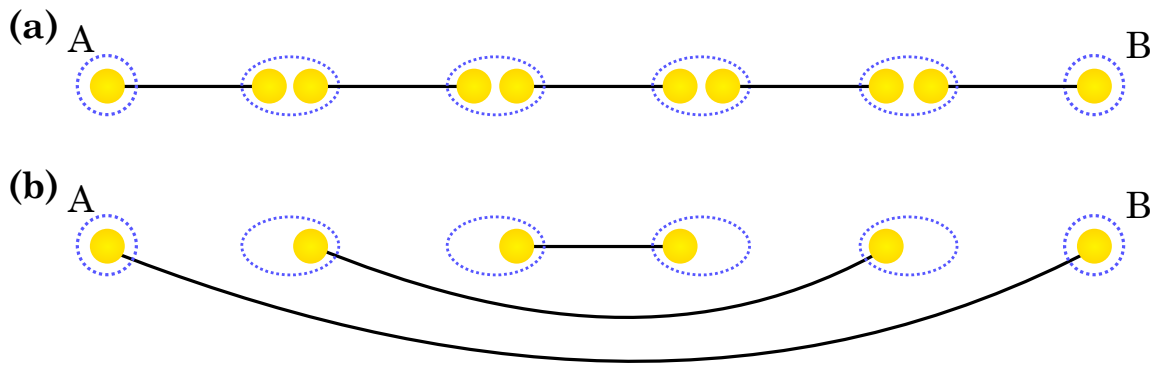

Figure 4.10: Depiction of an expensive case. We want to entangle each qubit with the opposite one over a line network. The upper subfigure is the initial state of the network and the lower one is the state of the network after distribution.

try to modify it enough in order for it to fit inside said simulator. The current result of my collaboration with the AQUA team is the topic of the next section.

4.3 Actual simulation of the GHZ state routing protocol

QuISP – Quantum Internet Simulation Package – is a quantum network simulator which aims at simulating large-scale physics-based quantum networks by simulating not only the quantum part of the quantum simulation but also the classical underlying network. The long-term plan of the AQUA team and the aim of such a tool is to study the emergent behaviours of large-scale networks such as *congestion collapse* – a behaviour resulting from a congestion which largely downgrade the communication capacity. Thus, being able to simulate a large variety of communication scenarios is an asset to test the behaviour of quantum networks under as much as possible conditions. I have contributed to QuISP by adding multipartite communication to the variety of existing scenarios. Indeed, at the time of writing, QuISP only supports bipartite communications, the distribution of maximally entangled pairs by different means [84] across quantum networks. Our theoretical multipartite protocol can fit into QuISP as an elementary block for multipartite communication, a type of communication which may – and I believe it will – proves relevant for quantum networks in the years to come.
Adding the GHZ state distribution protocol into QuISP required not only adapting the protocol to the proposed architecture but also adapting some of the simulator's architecture to the protocol. Indeed, supporting multipartite communications requires

some modification on the routing protocols and the underlying classical packet structure. Nevertheless, before dwelling into the implementation, I will first detail some critical aspects of the QuISP implementation. First, the QuISP protocols of communication are actually RuleSet based [77]. We will see the definition of this concept and what it meant for us trying to work with it in Subsec. 4.3.1. Second, in Subsec. 4.3.2 we will see important components of the QuISP network's nodes, in particular the QNIC – Quantum Network Interface Card – as they proved relevant for both the classical routing and the implementation of quantum operations. We will outline the practical routing algorithm used to approximate a Steiner Tree in order to route the information through the network in Subsec. 4.3.3 and describe which corrections are required at the end of the distribution in Subsec. 4.3.4. Finally, in Subsec. 4.3.1, we will detail the new RuleSet distribution protocol based on the previous GHZ state distribution protocol.

4.3.1 Introduction to RuleSets

A RuleSet [77] is set of rules each node needs to follow to achieve the desired task. It is an object which is formed of one or several Rules each holding a Condition and an Action. A Condition is formed of several Clauses, each one being a conditional statement concerning a resource such as "sharing a maximally entangled state with node x", when a Clause is met, it *locks* the resource which means the resource cannot be used by other Clauses. An Action is a sequence of operations, such as "Measuring qubit z in the X basis", it is where swapping and distillation operations are encoded. The node will perform the Action if and only if all the Clauses' condition are met.
In our case, the Action will be the clique expansion operation described in Subsec. 4.2.1 and the Clauses will be made to assure the existence of enough maximally entangled states – not already used by other protocols – and secure those resources. If a RuleSet is formed of several Rules, resources which have been used in the previous Rule are used as resources in the current one. The interest of using RuleSets lies in the synchronization between the different nodes which are part of the process. For a given transmission, the initiator of the transmission will send a RuleSet to every node which is part of the path – establishing the the tree is the aim of another protocol which will be outlined in 4.3.3 – taking into account the order in which those operations have to be executed. For example, looking to establish a maximally entangled pair between two distant nodes of the network while guarantying a given fidelity, one can distribute a RuleSet in which the intermediate nodes will wait until they share a maximally entangled pair with a specific partner and a specific fidelity. This clause will be satisfied only when the swapping of other nodes made

the two partners to share a maximally entangled pair with a high-enough fidelity. As a consequence, classical information walks the tree only twice: during the communication setup phase where a client initiates a connection – tries to find another specific client – and during the RuleSet distribution phase. No further inter-node communication is necessary since all the computations to synchronize the Actions are done at the initiator's node. To see a Ruleset, see Subsec. 4.3.5.

4.3.2 Quantum network nodes

Let us look at a more precise description of the module allowing quantum communication in QuISP's implementation of quantum nodes. Given a quantum network $H = (V, E, D_E)$ and $v \in V$ a node of this network, for each incident channel e to v, there is a QNIC – Quantum Network Interface Card – which will handle quantum communications, receiving, storing and sending photons. Each QNIC is physically linked one of the QNIC of the node sharing e with v. Those interfaces can contains Bell State analysers [81] or entangled photon pair sources, both these instrument being necessary in order to establish entangled pairs of photons between the two QNICs. They are also doted with solid state quantum memories to store the generated entanglement. One QNIC can only support one communication protocol at a time. A fact which will prove important in the routing phase.

4.3.3 Routing step

Our concrete GHZ state distribution protocol is asymmetric as we split the clients sharing the final GHZ state into one listener L and n clients forming – in an abuse of notation – the set C. See Fig. 4.6 for a depiction of a network. The listener's role is to wait for incoming connections from the other clients and, when an enough number of connections is reached, to generate a RuleSet for each node which is part of the communication and to distribute those RuleSets accross the network. Of course, the first step in all good communication protocol is to establish a path between all the participants. As previously mentioned, finding the Steiner tree over an arbitrary network is a NP hard problem [54]. Moreover, one cannot expect any node of the network to possess the full network map and to compute such a tree especially if one considers dynamic networks which change their topology over time.
In the QuISP simulator, routing is implemented by the mean of routing tables. If a given node S wants to reach another node T, S can look through its routing table to know

not the best path but the best next hop in order to reach T. More specifically, given T's address, S knows which of its neighbours is the best to reach to be the next node in the path. This type of routing can achieve shortest paths depending on how the routing table were computed, for example by initially computing the shortest path between each couples of node and keeping only the first step. Here, we will suppose the routing tables are sets such that the routing tables give shortest paths – it is currently implemented as such in QuISP – and we will use said routing scheme to establish a tree. For a given set of clients C and one listener L. In the connection setup phase, L put itself in listening mode waiting for a given amount of time and/or of connections. The clients try to reach L using the standard routing of the network resulting in the establishment of a shortest path between each client c and L. At each hop of the path the current node's address as well as which QNIC is used are added to the classical message. That way, whenever L reaches one of its listening termination condition, it knows all the different paths used by each clients c. From this information, L can compute a tree spanning C and L by fusing the different shortest path. Since each of those paths is a shortest path between a client c and L, this forms a simple approximation of the Steiner tree.
We then enter the RuleSet distribution phase in which the listener will send several classical messages containing the corresponding RuleSets throught the tree. Every time a node receives its RuleSet it will reserve the QNIC used by this communication to prevent other communication protocol to use those resources. This contrasts with the bipartite communication protocol currently implemented in QuISP where QNICs are reserved during the connection setup, thus preventing their use for several simultaneous incoming connections. Our order change solves this problem.
Some precisions regarding terminologies which will be used in the next section, the RuleSets are designed such that the distribution protocol is done over a directed tree. The root node of this tree is the listener and the directions flow to the terminal leaves which are the clients. In this directed tree, we call *children* of a node the nodes which can be accessed from the node using the directed edges and we call the *parent* of the node the only node above it in the hierarchy. We call the *parent qubit* of a node v the qubit in the parent node sharing – at least initially – a maximally entangled pair with v. In the depiction of the Steiner tree of Fig. 4.11 we have labeled nodes by their depth in said tree as the distribution will start from the deepest node and gradually go up. In this example, the first node to act will be the nodes labeled by 4 then 3 and so on. Before outlining the rules, we will study and make precise which corrections will be required at the end of the protocol.

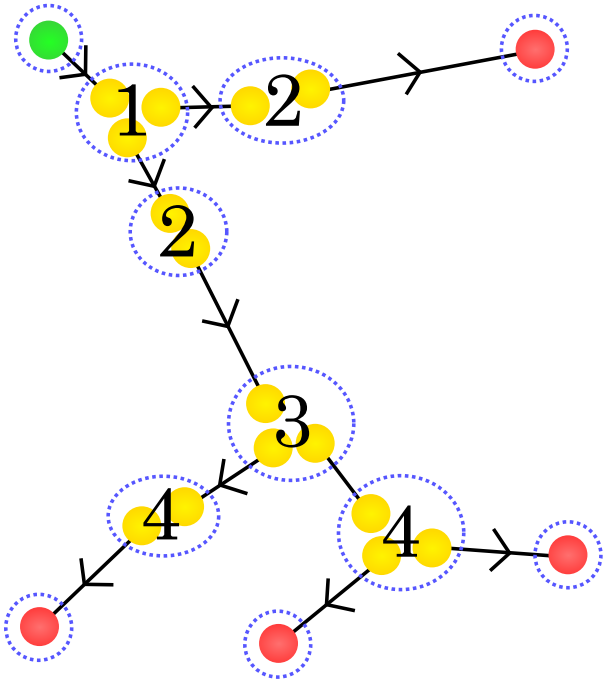

Figure 4.11: The directed Steiner tree according to the choice of a Listener – the top-left node. Each of the node is labeled by its depth in the tree.

4.3.4 Corrections and errors

As mentioned at the end of Subsec. 4.2.1, the order in which the operations are performed does not influence the final corrections. Nevertheless, we need to track which corrections are adequate at the end depending on the intermediate results. We will choose a specific order of operations and track step-by-step the accumulation of the required corrections on the clients' qubit and the listener one – the other qubits of the tree being measured and thus not needing any correction. We will follow the order of operation shown in Fig. 4.7, we first perform clique expansion on the deepest nodes of the tree and gradually go up, towards the Listener. As a consequence, when examining the specific order of operations inside a node, we will face the same setup: the node will share a GHZ state with its children which are clients and an EPR pair with its parent – you can once again observe this fact in Fig. 4.7. Table 4.2 displays the required correction depending on the measurement done and the measurement outcome. We denote a measurement in the Y basis with outcome m as $P_{y,m}$ and a measurement in the X basis as $P_{x,m}$.

For a given node, we follow the order of operations depicted in Subsec. 4.2.1 and in Fig. 4.5. The CZ operations do not induce any required correction. After measuring the

Measure of qubit v with result m	$P_{y,m}$	$P_{x,m}$
Correction if $m = 0$	$\sqrt{-i\sigma_Z}^{N_v}$	$\sqrt{i\sigma_Y}^{n_X}\sigma_Z^{N_v \setminus (n_X \cup N_{n_X})}$
Correction if $m = 1$	$\sqrt{i\sigma_Z}^{N_v}$	$\sqrt{-i\sigma_Y}^{n_X}\sigma_Z^{N_{n_X} \setminus (v \cup N_v)}$

Table 4.2: Correction required after a measurement in the Y or the X basis. Note that, as previously seen, n_X is an arbitrary neighbour of the measured qubit. In the rest of the text we choose n_X as the parent qubit of the measured qubit.

central node in the Y basis with a result m_c, all the neighbouring qubits have to be corrected as $\sqrt{(-1)^{\overline{m_c}} i\sigma_Z}$, where for a bit b, $\overline{b} = b \oplus 1$ is its negation. Note that we do not correct at this step but we wish to apply our next Actions on the corrected graph state. As a consequence, all the subsequent measures will be modified by their commutation relation with the required correction.

We now measure the qubit linked to the parent node in the Y basis with a result m_p. However, this measurement does not commute with the previous correction on the qubit. Actually, calling $P_{y,m} := |m_y\rangle \langle m_y|$ the measurement in the Y basis with outcome m and $P_{x,m'}$ the analogous operation for the X basis, we have that

$$P_{y,m}\sqrt{(-1)^{\overline{m_c}} i\sigma_Z} = \sqrt{(-1)^{\overline{m_c}} i\sigma_Z} P_{x,m\oplus m_c}, \tag{4.1}$$

according to [48]. Taking this into account, the Y measurement actually project the uncorrected state in the X basis – which is the projection done in the theoretical protocol – on the state $|(m_p \oplus m_c)_x\rangle$. We remember that the graph state resulting from a X measure depends – up to LC operations – on the choice of a neighbour n_X. We choose here and for all the subsequent X measurements n_X as the parent qubit of the node. The actually performed X measurement induces a required correction of $\sqrt{(-1)^{\widetilde{m_p}} i\sigma_Y}$ on the parent qubit and a required correction of $(\sigma_Z)^{\widetilde{\overline{m_p}}}$ on the other qubits of the node. This correction σ_Z does not commute with the subsequents X measurements which will be performed on the other qubits. It changes the result of the measurement as

$$P_{x,m}(\sigma_Z)^{m'} = (\sigma_Z)^{m'} P_{x,m\oplus m'} \tag{4.2}$$

From there, the Y measurement of each of the other qubit labeled by the associated edge e in the node with result m_e will do an effective X measurement with result

$$\widetilde{m_e} := m_e \oplus m_c \oplus \widetilde{\overline{m_p}} = m_e \oplus m_c \oplus \overline{m_p \oplus m_c} = \overline{m_e \oplus m_p}. \tag{4.3}$$

This measurement will finally add a required correction of $(\sigma_Z)^{\widetilde{\overline{m_e}}} = (\sigma_Z)^{m_e \oplus m_p}$ to the clients which are children of e. A required correction $\sqrt{i\sigma_Y}$ is also accumulated on the

parent qubit, but this correction commutes with the Y measurement. We can ignore it since it will not affect the subsequent Y measurements of this qubit unless the current node is the unique neighbour of the listener. If it is the case, a required correction of

$$\sqrt{(-1)^{\widetilde{m_p}} i\sigma_Y} \prod_e \sqrt{(-1)^{\widetilde{m_e}} i\sigma_Y} \tag{4.4}$$

is accumulated. Now that we have made precise which information will have to be stored and sent at the end of the communication, we can now outline the rules distributed to the nodes of the network in order to perform the distribution. We distinguish 4 different sets of rules: one for the Listener, one for the clients, one for the unique neighbour of the listener and the last for the remaining nodes.

4.3.5 Rules

Rules for the intermediary nodes

Rule 1 Clauses:

1. For each leaving edge e , we denote by C_e the set of clients which are children of e. The node needs to share a GHZ state with all the C_e
2. The node need to share an EPR pair with its parent.

Rule 1 Actions:

1. Generate a new stationary qubit unentangled to anyone in state $|+\rangle$
2. Perform a CZ operation between this new stationary qubit and each resource
3. Measure every qubit in the node in Y basis. We note m_p the result of the measurement of the qubit entangled with the parent and m_{C_e} the result of the measurement for the qubit which is part of the multipartite resource shared with C_e
4. Store a bit for each leaving edge $b_{C_e} := m_p \oplus m_{C_e}$

Rule 2 Clause:

1. Wait for one classical bit b_P from the parent

Rule 2 Actions:

1. For each leaving edge $e = [u, v]$, where u is the current node, sends $b_P \oplus b_{C_e}$ to v

Rule for clients

Clauses:

1. Wait for one classical bit b_P from its parent
2. Sharing a multipartite resource with the Listener and all other clients

Action:

1. Perform $\sigma_Z^{b_P}$ on its part of the resource.

Rule for the listener

Clauses:

1. Wait for two classical bits from from its only child. We label the two bits as b_0 and b_1
2. Sharing a multipartite resource with all the clients

Action:

1. Perform $\sqrt{i\sigma_Y}^{b_0.2+b_1}$ on its part of the resource.

Rule for the unique neighbour of the Listener

Clauses:

1. For each leaving edge e , we denote by C_e the set of clients which are children of e. The node needs to share a GHZ with all the C_e
2. The node needs to share an EPR with its parent.

Actions:

1. Generate a new stationary qubit unentangled to anyone in $|+\rangle$
2. Perform a CZ operation between this new stationary qubit and each resource
3. Measure every qubit in the node in the Y basis. We note m_p the result of the measurement for the qubit part of the EPR with the parent and m_{C_e} the result of the measurement for the qubit which is part of the multipartite resource shared with C_e.
4. For each leaving edge $e = [u, v]$, where u is the current node, sends $m_p \oplus m_{C_e}$ to v.

5. Sum mod 4 all the results of the measurements but the one of the stationary qubit as $(-1)^m$ – resulting in 1 for a result of 0 and -1 else – and sends the two resulting bits to the Listener. The two resulting bits allows to transmit the operation the Listener need to perform to correct the accumulation of $\sqrt{i\sigma_Y}$ of Eq. (4.4).

To implement those rules, it is necessary to change a bit the internal machinery of the QuISP simulation as we need to add multipartite resource states in the RuleSet machinery. However, it allows for GHZ states purification [35] at each step in order to ensure a GHZ state distribution as pure as possible.

4.3.6 Implementation done so far

For now, we implemented another set of rule which only check and reserve enough EPR pairs to form the tree and perform the clique expansion in one step. This type of greedy algorithm can make us loose everything if only one operation fails during the distribution which is very likely to happen but it represented a good first step to the future implementation of the distribution of multipartite entangled state over quantum networks.

4.4 Conclusion

We have presented two protocols to distribute respectively GHZ states and arbitrary graph states. Both of these theorical procotols can be readily applied on networks of any topology. Moreover, these protocols are close to optimal in terms of the number of steps T required and the number of Bell pairs consumed in the worst case. The model we used is naturally quite simplified, and there were many possibilities for trade-offs and improvements even within it and while some were exploited [19, 40], others are still lingering. Firstly, we note that the number of steps, T, does not necessarily represent time – for example, if nodes are allowed to share $N(N-1)$ Bell pairs, then everything can be done in one physical time step. One then has a potential trade-off between how parallel the uses of the quantum channel can be, and the use of quantum memory. Indeed, in terms of memory, one may tweak the steps in our protocol so as to paralelize as much as possible – with a little thought, one can see one only needs two qubits of memory per EPR pair vertex per node at any step. Furthermore, our optimality is for the worst case topology and state, for a given graph state and topology one may do much better as can be seen for example in our protocol for the GHZ state. The advantage for our scheme is

that it gives a method, and a bound, which works for all states and topologies with the same efficiency.

Although satisfying, this result was nonetheless incomplete. A protocol as simple as this one could be implemented and – for all the reason already supplied – should be implemented as a building block for quantum networks. A meeting in February 2020 with the AQUA team allowed me to fill this ambition. We have worked and are still working to bring quantum networks simulation to a new level, the multipartite distribution level. We found ways to accommodate the protocol to the simulator and the simulator to the protocol, each of them benefiting from the other. A first version is already implemented and the full version will certainly be released in a not-so-distant future. From there, the addition of GHZ states purification [35] and the arbitrary graph state distribution should not be too far fetched. Finally giving a strong multipartite feature to QuISP and, I hope, to the quantum networking field.

Popularization, conclusion and outlooks

We have reached the end of the exposure of the research works done during this thesis, but not yet the end of this manuscript. As part of my Phd, I also have worked on popularization of quantum mechanics, which I expose briefly in the next section, which is followed by the more traditional conclusion and outlook sections.

Popularization

As mentioned throughout this manuscript, quantum information's applications and quantum networks' implementations are currently being achieved in a real setting. Actual quantum information hardware – such as quantum key distribution boxes – are now available for sale, quantum networks and quantum computers are currently being developed at several distinct geographical locations [64, 70, 93, 6]. Observing the quick-paced development and the actual amount of funding[6] being injected in quantum information technologies, one may hypothesize that a non-negligible part of tomorrow's technologies would be quantum based and may be used by a broad audience. This is why I decided to focus a part of my PhD time on the creation of video games in order to introduce scientific notions to diverse types of public. First, by developing a small smartphone application to help students learning the very basics of matrix multiplication[7]. Then, and this is the topic of this small section, by starting the development of a game – OptiQraft – focusing on the creation and manipulation of boson-like particles.
I started OptiQraft[8] with the help and support of Ganaël Roeland[9], Léo Colisson[10], Raja

[6] For example, https://www.oezratty.net/wordpress/2021/decoder-annonce-plan-quantique-francais/
[7] findable here https://play.google.com/store/apps/details?id=com.TataInC.AppLUMA, does not work on all smartphones
[8] https://tatawanda.itch.io/optiqraft?secret=tefOExsixZwnRKSUSeBFhp9w4
[9] Laboratoire Kastler Brossel, Sorbonne Université, CNRS, ENS-PSL Research University, Collège

Yehia[10], and Robert Booth[10,11] for the newly created QICS[12]. Credit goes to Thomas Marchadour for the interface design and character design. I personally led this team, designed the game and implemented the core functionalities.

Game-based learning is an angle I wanted to explore since learning the existence of a whole scientific community studying the so-called *serious games* and their impact on learning [85, 61]. One of the most interesting features of game-based learning lies in the increased engagement and motivation it can induce on a learner through several mechanisms, such as the use of achievements and leaderboard [22, 59] or by giving a narrative enjoyable context [29]. A game can also be made to tailor the need of each specific student whether it is by the virtue of its difficulty as one cannot progress through a game if the previous notion are not acquired – reproducing the *scaffolded instruction* technique [8] – or by detecting which learning style corresponds to the student [39]. Mixed results were observed depending on several parameters such as the the audience tested and the mechanism being tested, some research displaying excellent results [25] and some displaying disappointing results going as far as a drawback [45]. Nevertheless, data on game-based learning is still lacking [33, 76] and we hope to contribute to the growing of the data set. Moreover, game-based learning could be a necessary and appealing tool to introduce the general audience to the at-first-sight – and second and third – confusing quantum concepts.

Of course, this idea is far from being brand-new; games which exploit high-level physics already exist – we can cite Velocity Raptor[13] as a game based on the special relativy behaviour of fast moving objects. As for quantum physics, there are already quite a respectable number of games which focus on the explanation. Two other major game are similar to our game. The first one is the well-named *The quantum game* – you can find at `http://play.quantumgame.io` – which focus on the wave description of a quantum state and aims to give an accurate description of the impact of the phase on quantum optics experiments. A new version is currently being developed at `https://quantumflytrap.com`. The second one is the also-appropriately-named *Quantum odyssey* [88]. This game is focused on quantum computation and aims to give visual understanding of quantum circuits. We chose a different approach from those two games and focused on the behaviour of several boson-like particles over the depiction of a realistic quantum

de France, 4 place Jussieu, Paris F-75252, France

[10]LIP6, Faculty of Science and Engineering, Sorbonne Université, CNRS, F-75005 Paris, France

[11]LORIA CNRS, Inria Mocqua, Université de Lorraine, F-54000 Nancy, France

[12]Quantum Information Center Sorbonne, https://qics.lip6.fr

[13]`https://testtubegames.com/velocityraptor.html`

optics table. This choice allowed us to capture boson effects such as the Hong–Ou–Mandel effect [50], not present in the two previous games. We expect this game to be a great addition to the current ludography of quantum games. A more accurate description of the game as well as the game-based learning mechanisms we used to design the game can be found in Appendix B.

Diffusion and prospect

At the time of writing, the game is featured on two different science popularization events: the "Fête de la science" and the "Festives", both are organised by Sorbonne University. The audience will be able to freely access the game and members of the team will be present to accompany the players. Our aim is to test the the learning impact on the public. We plan to, at least, build a questionnaire to be filled before and after the test. The goal is to have an assessment of whether or not the experience proved to be successful. I am also in discussion with Mathieu Muratet[14,15] from the MOCAH team of the LIP6. He is a researcher specialized into the study of the usage of "serious-games" as an educating tool, he already helped me on the matrices' application project. I think from this collaboration can emerge a way to contribute to the determination of which mechanisms are relevant to teach quantum physic and vulgarize knowledge to the general audience.

[14]Sorbonne Université, CNRS, LIP6, F-75005 Paris, France
[15]INS HEA, 92150 Suresnes, France

Conclusion

The PhD journey is indeed a long one. Yes, by the time you finished your explanation everyone will have left, leaving you speaking alone in front of empty chairs. So don't do that. Still, while the owner of the bar tries to kick you out because it is past closure time, you can conclude.

Quantum networks has been a topic of interest in recent years, and promises to continue that way in the years to come. I focused during those three years on general multipartite distribution over quantum networks. The studies I carried out analysed different kinds of setting and different kinds of multipartite distribution. I first studied the problem of recycling previously distributed quantum states for further operations. The problem was reduced to finding the asymptotic rate of conversion between multipartite entangled states. Together with Alexander Strelstov and Jens Eisert, we computed a new theoretical lower-bound optimal for a large family of conversion. We showed our lower-bound was an improvement over a long-standing previous one and we used it to find families of states presenting optimal GHZ state distillation rate. Then, I studied the full extent of the distribution possibilities over quantum networks. With my advisors Frédéric Grosshans and Damian Markham, we started by analysing a simple bottleneck problem: the distribution of cross EPR pairs over a square-shaped quantum network. We solved it using the Matrix Product State formalism. Then, we generalized the method to develop a formalism inspired from the tensor network formalism. This generalization gave rise to necessary and sufficient conditions to distribute quantum states over quantum networks given by the factorizability of tensors along the network topology. Finally, we showed this formalism encompasses stochastic classical distributions as well, the difference being a classical distribution is possible if and only if a tensor factorization exists using non-negative tensors while a quantum distribution can use complex tensors. We used the previous result to show that every stochastic classical distribution protocol had a quantum equivalent and gave as example the solving of the previous cross EPR pairs distribution by using 2 ternary channels. We also used the formalism to show there existed quantum network coding protocols with no classical equivalent. This last theorem solving, in part, a question left open by Kobayashi, Le Gall et al. [62]. The final result was divided in two parts. First, a theoretical protocol studying the distribution of GHZ states and graph states using the graphical tool box offered by the graph state formalism. We report a near optimal protocol in terms of time and the number of EPR states consumed. Later, we began to work in collaboration with Rodney Van Meter and the AQUA team to

adapt the protocol to QUISP[16], the quantum network simulator they are developing. This collaboration has achieved a first simulation of a GHZ state distribution protocol and is still ongoing at the time of writing. Finally, with Ganaël Roeland, Léo Colisson and Raja Yeha, we focused on the dissemination of knowledge by working on a game about quantum optics. We tried to popularize the behaviour of light by challenging the player to manipulate boson-like particles. Several known to game-based mechanism were included in the creation process. We hope to have results in the months to come. I also have good hope that the sum of those results can benefit to the research about resource management over quantum networks, by helping to design optimized quantum networks and by communicating about the quantum information technologies to a broad audience.

Outlook

This work does not take into account any kind of error whether it is inside the quantum channels or from other sources. However, a realistic quantum networking theory should take into account the unreliability of some part of the network. As a consequence, a question does linger: how to translate the previous results in a non-perfect setting? This would be next obvious step.
Another lacking point, I focused mainly on discrete quantum information, and the study of quantum networks in the discrete variable setting. However, quantum information with continuous variable is also an important part of the quantum information theory. Quantum networks in a continuous variable setting are already studied [24] and to investigate this setting is my next objective. I currently work on a continuous variable protocol to distribute quantum state based on a previous result of Arzani et al. [7]. In this work, we use secret sharing and perform arbitrary passive linear operations on inputted EPR pairs to distribute them to the nodes of the network.
Last missing result from this manuscript, I have started to implement the GHZ state distribution protocol over a simulation of quantum networks. I hope the next step would be to implement it on a real quantum network.

Last Words

This section marks the end of the manuscript. I hope this work will allow the quantum networks field to progress as a whole and gain a better understanding of how to handle

[16] https://github.com/sfc-aqua/quisp/

multipartite resources over quantum networks.

APPENDIX A

Proof of the lower bound for asymptotic conversion between multipartite states

In this Appendix we prove Theorem 2.3. We will rewrite it here for the sake of convenience

Theorem A.1 (Lower bound for multipartite state conversion)**.** *For $N+1$-partite pure states $\psi^{AB_1\ldots B_N}$ and $\phi^{AB_1\ldots B_N}$, the LOCC conversion rate is bounded from below as*

$$R(\psi^{AB_1\ldots B_N} \to \phi^{AB_1\ldots B_N}) \geq \min_X \left\{ \frac{S(\psi^{AX})}{\sum_{B_i \notin X} S(\phi^{B_i})} \right\}, \tag{A.1}$$

where X denotes a subsystem of all Bobs, including the empty set.

A.1 Main proof

Here, we present the proof of Theorem 2.2. The ideas presented in the following generalize the proof of Theorem 2.2 for tripartite pure state conversion. In particular, starting with the $N+1$-partite state $\psi = \psi^{AB_1\ldots B_N}$, we will apply entanglement combing [114] on Alice and all other parties (here referred to as "all the Bobs"), aiming to get bipartite entanglement between Alice and each of the parties B_i. If E_i denotes the entanglement

between Alice and i-th Bob after this procedure, the rate for state conversion from ψ to $\phi = \phi^{AB_1\ldots B_N}$ is bounded below as

$$R(\psi \to \phi) \geq \min_i \left\{ \frac{E_i}{S(\phi^{B_i})} \right\}. \tag{A.2}$$

To achieve conversion at rate $\min_i \left\{ E_i / S(\phi^{B_i}) \right\}$, Alice locally prepares the state $\phi^{A\tilde{A}_1\ldots\tilde{A}_N}$, applies Schumacher compression [99] to the registers $\tilde{A}_i$, and distributes them among the Bobs by using entanglement which has been combed in the previous procedure. In the rest of this section, we will show that combing can achieve an N-tuple of singlet rates $(E_1, \ldots, E_N)$ such that

$$\min_i \left\{ \frac{E_i}{S(\phi^{B_i})} \right\} \geq \min_X \left\{ \frac{S(\psi^{AX})}{\sum_{B_i \notin X} S(\phi^{B_i})} \right\}, =: m^{\psi,\phi} \tag{A.3}$$

where X denotes a subset of all the Bobs. When there is no ambiguity, we will denote $m^{\psi,\phi}$ simply by m.

In the first step of the proof we will consider all possible ways to merge Bobs' parts of the state B_i with Alice. Since in the scenario considered here we have N Bobs, there are $N!$ different ways to achieve this, depending on the order of the Bobs in the merging procedure. We will first consider entanglement N-tuple $(E_1, \ldots, E_N)$, where E_i denotes the amount of entanglement shared between Alice and i-th Bob after the merging procedure. For example, taking $N = 4$, merging first B_1, then B_2, then B_3 and finally B_4 to Alice will achieve the 4-tuple:

$$E_1 = S(\psi^A) - S(\psi^{AB_1}), \tag{A.4a}$$
$$E_2 = S(\psi^{AB_1}) - S(\psi^{AB_1B_2}), \tag{A.4b}$$
$$E_3 = S(\psi^{AB_1B_2}) - S(\psi^{AB_1B_2B_3}), \tag{A.4c}$$
$$E_4 = S(\psi^{AB_1B_2B_3}), \tag{A.4d}$$

while merging first B_3, then B_1, then B_4 and finally B_2 to Alice will achieve the 4-tuple:

$$E_1 = S(\psi^{AB_3}) - S(\psi^{AB_1B_3}), \tag{A.5a}$$
$$E_2 = S(\psi^{AB_1B_3B_4}), \tag{A.5b}$$
$$E_3 = S(\psi^A) - S(\psi^{AB_3}), \tag{A.5c}$$
$$E_4 = S(\psi^{AB_1B_3}) - S(\psi^{AB_1B_3B_4}). \tag{A.5d}$$

The aforementioned $N!$ merging procedures give rise to $N!$ N-tuples, which we will name the "entanglement extreme points". We note that some of the values E_i can be

negative, implying that entanglement is consumed in this case. Proposition 2 of Ref. [114] guarantees that for any N-tuple $(E_1, \ldots, E_N)$ with the properties

1. $\forall i \in \{1, \ldots, N\}$, $E_i \geq 0$,
2. $(E_1, \ldots, E_N)$ is in the convex polytope spanned by the entanglement extreme points,

there exists an asymptotic LOCC protocol acting on the state ψ and distilling singlets between Alice and each of the Bobs B_i at rate E_i. In the following, we are interested in the renormalized entanglement rates

$$R_i = \frac{E_i}{S(\phi^{B_i})}, \tag{A.6}$$

see also Eq. (A.2). We can define for each N-tuple $(E_1, \ldots, E_N)$ an N-tuple $(R_1, \ldots, R_N)$. We will consider from now on only the tuples $(R_1, \ldots, R_N)$, which will also be called "rate distributions". We will call "extreme points" the rates distribution defined from the entanglement extreme points. It is easily seen from previous combing condition and Eq. (A.2) that, if we find a distribution of rates $(R_1, \ldots, R_N)$ satisfying

1. $\forall i \in \{1, \ldots, N\}$, $R_i \geq 0$,
2. $(R_1, \ldots, R_N)$ is in the convex polytope spanned by the extreme points,

we will be able to achieve conversion from ψ to ϕ with rate

$$R(\psi \to \phi) \geq \min_i \{R_i\}. \tag{A.7}$$

In order to prove Eq. (A.3), we will find in the convex set of the extreme points a point $(R_1, \ldots, R_N)$ such that

$$\min_i \{R_i\} \geq \min_X \left\{ \frac{S(\psi^{AX})}{\sum_{B_i \notin X} S(\phi^{B_i})} \right\}. \tag{A.8}$$

We rewrite here the outline of the proof: in the first step we will construct by convexity a set of points $(R_1, \ldots, R_N)$ satisfying $R_N \geq m^{\psi,\phi}$ from the extreme points. We note that the convex set of these newly constructed points will only contain rate distributions with N^{th} coordinate superior to $m^{\psi,\phi}$. From our constructed points, we will construct by convexity a new set of points $(R_1, \ldots, R_N)$ satisfying $R_{N-1} \geq m^{\psi,\phi}$. This will lead to a set of point satisfying both $R_N \geq m^{\psi,\phi}$ and $R_{N-1} \geq m^{\psi,\phi}$. The procedure will continue with R_{N-2} until R_1. In this way, we will achieve a distribution $(R_1, \ldots, R_N)$ satisfying $\forall i \in \{1, \ldots, N\}, R_i \geq m^{\psi,\phi}$. Such a distribution will ensure conversion from ψ to ϕ with

a rate of at least $m^{\psi,\phi}$, as claimed.

First step. Each of the extreme points is the result of merging the Bobs to Alice in different order. Thus, we can associate each extreme point to a permutation σ on the set $\{1,\dots,N\}$. We denote the set of all permutations by $\mathcal{S}_N$. Moreover, $\sigma(k)=l$ means that B_l is the k^{th} Bob merged to Alice. It implies that,

$$\begin{aligned} R^{\sigma}_{\sigma(k)} = R^{\sigma}_{l} &= \frac{S(\psi^{AB_{\sigma(1)}\dots B_{\sigma(k-1)}}) - S(\psi^{AB_{\sigma(1)}\dots B_{\sigma(k-1)}B_l})}{S(\phi^{B_l})} \\ &= \frac{S(\psi^{AY^{\sigma}_{k-1}}) - S(\psi^{AY^{\sigma}_{k-1}B_l})}{S(\phi^{B_l})}, \end{aligned} \tag{A.9}$$

where we used the notation $Y^{\sigma}_{k}=\{B_{\sigma(1)},\dots,B_{\sigma(k)}\}$.
Our next observation is that we can group the $N!$ extreme points in $(N-1)!$ sets of N points. In the following, we denote by c_{N-i} the permutations defined for $i\in\{0,\dots,N-1\}$ as

$$c_{N-i}(k) = k,\ \forall k\in\{1,\dots,N-i-1\}, \tag{A.10a}$$

$$c_{N-i}(N-i) = N, \tag{A.10b}$$

$$c_{N-i}(k) = k-1,\ \forall k\in\{N-i+1,\dots,N\}. \tag{A.10c}$$

Consider now a distribution $(R^{\sigma}_1,\dots,R^{\sigma}_N)$ with $\sigma(N)=N$, i.e., B_N merged in N^{th} position. We form a set by grouping together the N distributions $(R_1^{\sigma\circ c_{N-i}},\dots,R_N^{\sigma\circ c_{N-i}})$. In term of merging order, the distribution $\sigma\circ c_{N-i}$ give rise to the following ordering:

1. For $k<N-i$, $B_{\sigma\circ c_{N-i}(k)}=B_{\sigma(k)}$ is merged in position k,
2. For $k=N-i$, $B_{\sigma\circ c_{N-i}(N-i)}=B_N$ is merged in position $N-i$,
3. For $N\geq k>N-i$, $B_{\sigma\circ c_{N-i}(k)}=B_{\sigma(k-1)}$ is merged in position k.

The distributions $\sigma\circ c_{N-i}$ are the distributions obtained by merging Bobs 1 to $N-1$ with the relative order given by σ. The only difference is the merging position of B_N. We can order this set by the value of the N^{th} coordinate. Indeed,

$$R^{\sigma}_N \geq R_N^{\sigma\circ c_{N-1}} \geq R_N^{\sigma\circ c_{N-2}} \geq \cdots \geq R_N^{\sigma\circ c_1}. \tag{A.11}$$

Note that $\sigma\circ c_N=\sigma$. For a proof of Eq. (A.11) in the general case see Sec. A.2. There are $(N-1)!$ distributions satisfying $\sigma(N)=N$. We have $(N-1)!$ ordered sets of size N. Observe that for all $\sigma\in S_N$ satisfying $\sigma(N)=N$,

$$R^{\sigma}_N = \frac{S(\psi^{AB_1\dots B_{N-1}})}{S(\phi^{B_N})} \in \left\{ \frac{S(\psi^{AX})}{\sum_{B_i\notin X} S(\phi^{B_i})} \right\}. \tag{A.12}$$

As a consequence,

$$R_N^\sigma \geq m^{\psi,\phi}. \tag{A.13}$$

Two situations can happen for each of the $(N-1)!$ sets. The first case is that $R_N^{\sigma\circ c_1} \geq m^{\psi,\phi}$. In this case, we can obtain the distribution $(R_1^{\sigma\circ c_1}, \ldots, R_{N-1}^{\sigma\circ c_1}, m^{\psi,\phi})$ from $(R_1^{\sigma\circ c_1}, \ldots, R_N^{\sigma\circ c_1})$ by simply reducing the entanglement between Alice and B_N.
The second case is that we can find i such that $R_N^{\sigma\circ c_{N-i}} \geq m^{\psi,\phi} > R_N^{\sigma\circ c_{N-i-1}}$. In this case, we can consider a convex combination of $R^{\sigma\circ c_{N-i}}$ and $R^{\sigma\circ c_{N-i-1}}$, in order to arrive at a resulting distribution $(R_1, \ldots, R_N)$ such that $R_N = m^{\psi,\phi}$. We also know easily the value of most of the two distribution's coordinates. Indeed,

1. For $k < N-i-1$, $c_{N-i-1}(k) = c_{N-i}(k) = k$, which gives

$$R^{\sigma\circ c_{N-i-1}}_{\sigma\circ c_{N-i-1}(k)} = R^{\sigma\circ c_{N-i-1}}_{\sigma(k)} = \frac{S(\psi^{AY^\sigma_{k-1}}) - S(\psi^{AY^\sigma_k})}{S(\phi^{B_{\sigma(k)}})}, \tag{A.14a}$$

$$R^{\sigma\circ c_{N-i}}_{\sigma\circ c_{N-i}(k)} = R^{\sigma\circ c_{N-i}}_{\sigma(k)} = \frac{S(\psi^{AY^\sigma_{k-1}}) - S(\psi^{AY^\sigma_k})}{S(\phi^{B_{\sigma(k)}})}. \tag{A.14b}$$

2. For $k = N-i-1$, $c_{N-i-1}(N-i-1) = N$ and $c_{N-i}(N-i-1) = N-i-1$,

$$R^{\sigma\circ c_{N-i-1}}_{\sigma\circ c_{N-i-1}(N-i-1)} = R^{\sigma\circ c_{N-i-1}}_{N} = \frac{S(\psi^{AY^\sigma_{N-i-2}}) - S(\psi^{AY^\sigma_{N-i-2}B_N})}{S(\phi^{B_N})}, \tag{A.15a}$$

$$R^{\sigma\circ c_{N-i}}_{\sigma\circ c_{N-i}(N-i-1)} = R^{\sigma\circ c_{N-i}}_{\sigma(N-i-1)} = \frac{S(\psi^{AY^\sigma_{N-i-2}}) - S(\psi^{AY^\sigma_{N-i-1}})}{S(\phi^{B_{\sigma(N-i-1)}})}. \tag{A.15b}$$

3. For $k = N-i$, $c_{N-i-1}(N-i) = N-i-1$ and $c_{N-i}(N-i) = N$,

$$R^{\sigma\circ c_{N-i-1}}_{\sigma\circ c_{N-i-1}(N-i)} = R^{\sigma\circ c_{N-i-1}}_{\sigma(N-i-1)} = \frac{S(\psi^{AY^\sigma_{N-i-2}B_N}) - S(\psi^{AY^\sigma_{N-i-1}B_N})}{S(\phi^{B_{\sigma(N-i-1)}})}, \tag{A.16a}$$

$$R^{\sigma\circ c_{N-i}}_{\sigma\circ c_{N-i}(N-i)} = R^{\sigma\circ c_{N-i}}_{N} = \frac{S(\psi^{AY^\sigma_{N-i-1}}) - S(\psi^{AY^\sigma_{N-i-1}B_N})}{S(\phi^{B_N})}. \tag{A.16b}$$

4. For $k > N-i$, $c_{N-i-1}(k) = c_{N-i}(k) = k-1$,

$$R^{\sigma\circ c_{N-i-1}}_{\sigma\circ c_{N-i-1}(k)} = R^{\sigma\circ c_{N-i-1}}_{\sigma(k-1)} = \frac{S(\psi^{AY^\sigma_{k-2}B_N}) - S(\psi^{AY^\sigma_{k-1}B_N})}{S(\phi^{B_{\sigma(k-1)}})}, \tag{A.17a}$$

$$R^{\sigma\circ c_{N-i}}_{\sigma\circ c_{N-i}(k)} = R^{\sigma\circ c_{N-i}}_{\sigma(k-1)} = \frac{S(\psi^{AY^\sigma_{k-2}B_N}) - S(\psi^{AY^\sigma_{k-1}B_N})}{S(\phi^{B_{\sigma(k-1)}})}. \tag{A.17b}$$

Only two coordinates differ in the distributions given by $\sigma \circ c_{N-i}$ and $\sigma \circ c_{N-i-1}$. As a consequence, the distribution resulting from their convex combination will be a distribution with N^{th} coordinate taking the value $m^{\psi,\phi}$, while the $\sigma(N-i-1)^{\text{th}}$ one assumes the value

$$\frac{S(\psi^{AY^\sigma_{N-i-2}}) - m^{\psi,\phi} S(\phi^{B_N}) - S(\psi^{AY^\sigma_{N-i-1}B_N})}{S(\phi^{B_{\sigma(N-i-1)}})}, \tag{A.18}$$

and $\forall k \in \{1,\dots,N-1\} \setminus \{N-i-1\}$, the k^{th} coordinate take the value $R^{\sigma\circ c_{N-i}}_{\sigma(k)}$. We will apply this procedure for each $\sigma \in \mathcal{S}_N$ with $\sigma(N) = N$. We associate the resulting distributions with the σ that gave rise to the distribution we used in the convex combination. The result are $(N-1)!$ distributions $(R^\sigma_1,\dots,R^\sigma_{N-1},m^{\psi,\phi})$ one for each permutation σ. For the given quantum state ψ equipped with the partitioning in A and $\{B_1,\dots,B_{N-1}\}$, we now define the function

$$S^\psi_2 : X \subset \{B_1,\dots,B_{N-1}\} \to \mathbb{R}^+_0 \tag{A.19}$$

that depends on subsets $X \subset \{B_1,\dots,B_{N-1}\}$, taking the values

$$S^\psi_2(X) := \begin{cases} S(\psi^{AX}) - m^{\psi,\phi} S(\phi^{B_N}), \\ \quad \text{if } \frac{S(\psi^{AX})-S(\psi^{AXB_N})}{S(\phi^{B_N})} < m(\psi,\phi), \\ S(\psi^{AXB_N}), \\ \quad \text{if } \frac{S(\psi^{AX})-S(\psi^{AXB_N})}{S(\phi^{B_N})} \geq m^{\psi,\phi}. \end{cases} \tag{A.20}$$

We can rewrite the coordinates of $(R^\sigma_1,\dots,R^\sigma_{N-1},m^{\psi,\phi})$ as a function of S^ψ_2.

1. For $k < N-i-1$, $R^{\sigma\circ c_k}_N < R^{\sigma\circ c_{k+1}}_N \leq R^{\sigma\circ c_{N-i-1}}_N < m^{\psi,\phi}$. As a consequence,

$$R^\sigma_{\sigma(k)} = \frac{S(\psi^{AY^\sigma_{k-1}}) - S(\psi^{AY^\sigma_k})}{S(\phi^{B_{\sigma(k)}})} \tag{A.21}$$

$$= \frac{S^\psi_2(Y^\sigma_{k-1}) - S^\psi_2(Y^\sigma_k)}{S(\phi^{B_{\sigma(k)}})}. \tag{A.22}$$

2. For $k = N-i-1$, $R^{\sigma\circ c_{N-i-1}}_N < m^{\psi,\phi} \leq R^{\sigma\circ c_{N-i}}_N$,

$$R^\sigma_{\sigma(N-i-1)} = \frac{S(\psi^{AY^\sigma_{N-i-2}}) - m^{\psi,\phi} S(\phi^{B_N}) - S(\psi^{AY^\sigma_{N-i-1}B_N})}{S(\phi^{B_{\sigma(N-i-1)}})} \tag{A.23}$$

$$= \frac{S^\psi_2(Y^\sigma_{k-1}) - S^\psi_2(Y^\sigma_k)}{S(\phi^{B_{\sigma(k)}})}. \tag{A.24}$$

3. For $N > k > N-i-1$, $m^{\psi,\phi} \leq R^{\sigma\circ c_{N-i}}_N \leq R^{\sigma\circ c_k}_N \leq R^{\sigma\circ c_{k+1}}_N$,

$$R^\sigma_{\sigma(k)} = \frac{S(\psi^{AY^\sigma_{k-1}B_N}) - S(\psi^{AY^\sigma_k B_N})}{S(\phi^{B_{\sigma(k)}})} \tag{A.25}$$

$$= \frac{S^\psi_2(Y^\sigma_{k-1}) - S^\psi_2(Y^\sigma_k)}{S(\phi^{B_{\sigma(k)}})}. \tag{A.26}$$

In summary, the have just presented first step of the procedure leaves us with $(N-1)!$ distributions $(R^\sigma_1,\dots,R^\sigma_{N-1},m^{\psi,\phi})$.

We introduce now generalized functions which will be used in the following steps. We define in a recursive way the functions S_j^ψ for $j \in \{1, \ldots, N\}$ by

$$S_j^\psi : X \subset \{B_1, \ldots, B_{N-j+1}\} \to \mathbb{R}_0^+, \tag{A.27a}$$

$$S_1^\psi(X) := S(\psi^{AX}), \tag{A.27b}$$

$$S_{j+1}^\psi(X) := \begin{cases} S_j^\psi(X) - m_j^{\psi,\phi} S(\phi^{B_{N-j+1}}), \\ \quad \text{if } \frac{S_j^\psi(X) - S_j^\psi(XB_{N-j+1})}{S(\phi^{B_{N-j+1}})} < m_j^{\psi,\phi}, \\ S_j^\psi(XB_{N-j+1}), \\ \quad \text{if } \frac{S_j^\psi(X) - S_j^\psi(XB_{N-j+1})}{S(\phi^{B_{N-j+1}})} \geq m_j^{\psi,\phi}. \end{cases} \tag{A.27c}$$

Moreover, $m_j^{\psi,\phi}$ is given as follows,

$$m_j^{\psi,\phi} := \min \left\{ \frac{S_j^\psi(X)}{\sum_{B_i \notin X} S(\phi^{B_i})}, X \subset \{B_1, \ldots, B_{N-j+1}\} \right\}. \tag{A.28}$$

We show in Sec. A.3 that all the function S_j satisfy strong subadditivity on the subsets of Bobs such that $\forall X \subset \{B_1, \ldots, B_{N-j+1}\}$ and for $B_l, B_m \notin X$,

$$S_j^\psi(XB_l) + S_j^\psi(XB_m) \geq S_j^\psi(XB_lB_m) + S_j^\psi(X). \tag{A.29}$$

Equipped with these tools, we are now ready to present the general $(j+1)^{\text{th}}$ step of the procedure, where we will make extensive use of the properties of R_i^σ and the generalized functions S_j^ψ and $m_j^{\psi,\phi}$ discussed above.

$(j+1)^{\text{th}}$ step. In the $(j+1)^{\text{th}}$ step, there are $(N-j)!$ distributions denoted as $(R_1^\sigma, \ldots, R_{N-j}^\sigma, m_j^{\psi,\phi}, m_{j-1}^{\psi,\phi}, \ldots, m^{\psi,\phi})$. One for each $\sigma \in \mathcal{S}_N$ with $\forall k \in \{N-j+1, \ldots, N\}$, $\sigma(k) = k$. For $k \in \{1, \ldots, N-j\}$, the coordinate's values are given by

$$R_{\sigma(k)}^\sigma = \frac{S_{j+1}(\psi^{AY_{k-1}^\sigma}) - S_{j+1}(\psi^{AY_k^\sigma})}{S(\phi^{B_{\sigma(k)}})}, \tag{A.30}$$

We will construct by convexity $(N-j-1)!$ distributions $(R_1, \ldots, R_{N-j-1}, m_{j+1}^{\psi,\phi}, \ldots, m^{\psi,\phi})$. We proceed as before and group distributions in $(N-j-1)!$ sets of $N-j$ distributions. We consider distributions associated with permutations σ verifying $\sigma(N-j) = N-j$. For $i \in \{0, \ldots, N-j-1\}$, we define the permutations,

$$c_{N-j-i}^{j+1}(k) = k, \forall k \in \{1, \ldots, N-j-i-1\}, \tag{A.31a}$$

$$c_{N-j-i}^{j+1}(N-j-i) = N-j, \tag{A.31b}$$

$$c_{N-j-i}^{j+1}(k) = k-1, \forall k \in \{N-j-i+1, \ldots, N-j\}, \tag{A.31c}$$

and we group the distributions $R^{\sigma\circ c^{j+1}_{N-j-i}}$. For the sake of clarity, we drop the superscript of the c permutations and we write $N_j := N - j$ for the rest of the proof. We arrive at a hierarchy in the coordinates N_j, i.e. (see Sec. A.2),

$$R^{\sigma\circ c_{N_j}}_{N_j} \geq R^{\sigma\circ c_{N_j-1}}_{N_j} \geq \cdots \geq R^{\sigma\circ c_1}_{N_j} \tag{A.32}$$

with

$$R^{\sigma\circ c_{N_j}}_{N_j} \in \left\{ \frac{S_{j+1}(X)}{\sum_{B_i\notin X} S(\phi^{B_i})} \right\}. \tag{A.33}$$

As a consequence,

$$R^{\sigma\circ c_{N_j}}_{N_j} \geq m_{j+1}. \tag{A.34}$$

As in the first step, if $R^{\sigma\circ c_1}_{N_j} \geq m_{j+1}$, then we can take the distributions $R^{\sigma\circ c_1}$ and reduce entanglement to achieve a distribution $(R^f_1, \ldots, R^f_{N_j-1}, m_{j+1}, \ldots, m)$. Else, we can find an i such that

$$R^{\sigma\circ c_{N_j-i}}_{N_j} \geq m_{j+1} > R^{\sigma\circ c_{N_j-i-1}}_{N_j}. \tag{A.35}$$

Again following the same ideas as in the first step, we take a convex combination of the two distributions $R^{\sigma\circ c_{N_j-i}}$ and $R^{\sigma\circ c_{N_j-i-1}}$. The values of all coordinates are given by

1. For $k < N - i - j - 1$, $c_{N_j-i-1}(k) = c_{N_j-i}(k) = k$, we obtain

$$R^{\sigma\circ c_{N_j-i-1}}_{\sigma\circ c_{N_j-i-1}(k)} = R^{\sigma\circ c_{N_j-i-1}}_{\sigma(k)} = \frac{S_{j+1}(\psi^{AY^\sigma_{k-1}}) - S_{j+1}(\psi^{AY^\sigma_k})}{S_{j+1}(\phi^{B_{\sigma(k)}})}, \tag{A.36}$$

$$R^{\sigma\circ c_{N_j-i}}_{\sigma\circ c_{N_j-i}(k)} = R^{\sigma\circ c_{N_j-i}}_{\sigma(k)} = \frac{S_{j+1}(\psi^{AY^\sigma_{k-1}}) - S_{j+1}(\psi^{AY^\sigma_k})}{S(\phi^{B_{\sigma(k)}})}. \tag{A.37}$$

2. For $k = N_j - i - 1$, $c_{N_j-i-1}(N_j - i - 1) = N$ and $c_{N_j-i}(N_j - i - 1) = N_j - i - 1$, we obtain

$$\begin{aligned} R^{\sigma\circ c_{N_j-i-1}}_{\sigma\circ c_{N_j-i-1}(N_j-i-1)} &= R^{\sigma\circ c_{N_j-i-1}}_{N_j} \\ &= \frac{S_{j+1}(\psi^{AY^\sigma_{N_j-i-2}}) - S_{j+1}(\psi^{AY^\sigma_{N_j-i-2}B_{N_j}})}{S(\phi^{B_{N_j}})}, \end{aligned} \tag{A.38}$$

$$\begin{aligned} R^{\sigma\circ c_{N_j-i}}_{\sigma\circ c_{N_j-i}(N_j-i-1)} &= R^{\sigma\circ c_{N_j-i}}_{\sigma(N_j-i-1)} \\ &= \frac{S_{j+1}(\psi^{AY^\sigma_{N_j-i-2}}) - S_{j+1}(\psi^{AY^\sigma_{N_j-i-1}})}{S(\phi^{B_{\sigma(N_j-i-1)}})}. \end{aligned} \tag{A.39}$$

3. For $k = N_j - i$, $c_{N_j-i-1}(N_j - i) = N_j - i - 1$ and $c_{N_j-i}(N_j - i) = N_j$, we obtain

$$\begin{aligned} R^{\sigma\circ c_{N_j-i-1}}_{\sigma\circ c_{N_j-i-1}(N_j-i)} =& R^{\sigma\circ c_{N_j-i-1}}_{\sigma(N_j-i-1)} && \text{(A.40)}\\ =& \frac{S_{j+1}(\psi^{AY^\sigma_{N_j-i-2}B_{N_j}}) - S_{j+1}(\psi^{AY^\sigma_{N_j-i-1}B_{N_j}})}{S(\phi^{B_{\sigma(N_j-i-1)}})}, \\ R^{\sigma\circ c_{N_j-i}}_{\sigma\circ c_{N_j-i}(N_j-i)} =& R^{\sigma\circ c_{N_j-i}}_{N_j} && \text{(A.41)}\\ =& \frac{S_{j+1}(\psi^{AY^\sigma_{N_j-i-1}}) - S_{j+1}(\psi^{AY^\sigma_{N_j-i-1}B_{N_j}})}{S(\phi^{B_{N_j}})}. \end{aligned}$$

4. For $k > N_j - i$, $c_{N_j-i-1}(k) = c_{N_j-i}(k) = k - 1$, we obtain

$$R^{\sigma\circ c_{N_j-i-1}}_{\sigma\circ c_{N_j-i-1}(k)} = R^{\sigma\circ c_{N_j-i-1}}_{\sigma(k-1)} = \frac{S_{j+1}(\psi^{AY^\sigma_{k-2}B_{N_j}}) - S_{j+1}(\psi^{AY^\sigma_{k-1}B_{N_j}})}{S(\phi^{B_{\sigma(k-1)}})}, \quad \text{(A.42)}$$

$$R^{\sigma\circ c_{N_j-i}}_{\sigma\circ c_{N_j-i}(k)} = R^{\sigma\circ c_{N_j-i}}_{\sigma(k-1)} = \frac{S_{j+1}(\psi^{AY^\sigma_{k-2}B_{N_j}}) - S_{j+1}(\psi^{AY^\sigma_{k-1}B_{N_j}})}{S(\phi^{B_{\sigma(k-1)}})}. \quad \text{(A.43)}$$

Again, only two coordinates differ between the distributions given by $\sigma \circ c_{N_j-i}$ and $\sigma \circ c_{N_j-i-1}$. As a consequence, the distribution resulting from their convex combination will be a distribution with a N_j^{th} coordinate of value $m^{\psi,\phi}_{j+1}$, a $\sigma(N_j - i - 1)^{\text{th}}$ coordinate of value

$$\frac{S^\psi_{j+1}(Y^\sigma_{N_j-i-2}) - m^{\psi,\phi}_{j+1}S(\phi^{B_{N_j}}) - S^\psi_{j+1}(Y^\sigma_{N_j-i-1}B_{N_j})}{S(\phi^{B_{\sigma(N_j-i-1)}})}, \quad \text{(A.44)}$$

and $\forall k \in \{1, \ldots, N_j - 1\} \setminus \{N_j - i - 1\}$, a k^{th} coordinate of value $R^{\sigma\circ c_{N_j-i}}_{\sigma(k)}$. As in the first step, from each permutation $\sigma \in \mathcal{S}_N$ with $\forall k \in \{N - j, \ldots, N\}, \sigma(k) = k$ we have a resulting distribution $(R^\sigma_1, \ldots, R^\sigma_{N_j-1}, m^{\psi,\phi}_{j+1}, \ldots, m^{\psi,\phi})$ that we label with σ. All the coordinate $R^\sigma_{\sigma(k)}$ can be rewritten in term of S^ψ_{j+2} such that

$$R^\sigma_{\sigma(k)} = \frac{S^\psi_{j+2}(Y^\sigma_{k-1}) - S^\psi_{j+2}(Y^\sigma_k)}{S(\phi^{B_{\sigma(k)}})}. \quad \text{(A.45)}$$

Following this procedure until step N, we find ourselves with the distribution $(m^{\psi,\phi}_N, m^{\psi,\phi}_{N-1}, \ldots, m^{\psi,\phi}_2, m^{\psi,\phi})$. It remains to be proven that $\forall j \in \{1, \ldots, N-1\}$, $m^{\psi,\phi}_{j+1} \geq m^{\psi,\phi}_j$. Taking an element of the set from which $m^{\psi,\phi}_{j+1}$ is the minimum: $S^\psi_{j+1}(X)/(\sum_{B_i \notin X} S(\phi^{B_i}))$, where X is a subset of $\{B_1, \ldots, B_{N_j}\}$, we will show it is greater or equal to every elements of the set from which $m^{\psi,\phi}_j$ is the minimum,

$$M^{\psi,\phi}_j := \left\{ \frac{S^\psi_j(Y)}{\sum_{B_i \notin Y} S(\phi^{B_i})}, Y \subset \{B_1, \ldots, B_{N_j+1}\} \right\}. \quad \text{(A.46)}$$

There are two cases:

1. If $S^{\psi}_{j+1}(X) = S^{\psi}_{j}(XB_{N_j+1})$, then

$$\frac{S^{\psi}_{j+1}(X)}{\sum_{B_i \notin X} S(\phi^{B_i})} = \frac{S^{\psi}_{j}(XB_{N_j+1})}{\sum_{B_i \notin Y} S(\phi^{B_i})} \in M^{\psi,\phi}_{j}. \tag{A.47}$$

   As a consequence,

$$\frac{S^{\psi}_{j+1}(X)}{\sum_{B_i \notin Y} S(\phi^{B_i})} \geq m^{\psi,\phi}_{j}. \tag{A.48}$$

2. If $S^{\psi}_{j+1}(X) = S^{\psi}_{j}(X) - m^{\psi,\phi}_{j} S(\phi^{B_{N_j+1}})$, we know that

$$\frac{S^{\psi}_{j}(X)}{\sum_{B_i \notin X} S(\phi^{B_i}) + S(\phi^{B_{N_j+1}})} \geq m^{\psi,\phi}_{j}. \tag{A.49}$$

   It implies directly that

$$\frac{S^{\psi}_{j}(X) - m^{\psi,\phi}_{j} S(\phi^{B_{N_j+1}})}{\sum_{B_i \notin X} S(\phi^{B_i})} \geq m^{\psi,\phi}_{j}. \tag{A.50}$$

Thus, recalling that via LOCC it is always possible to reduce bipartite entanglement between Alice and the Bobs, we can finally achieve the distribution $(m^{\psi,\phi}, \ldots, m^{\psi,\phi})$, and the proof of Theorem 3 is complete.

A.2 Proof of Eqs. (A.11) and (A.32)

To prove Eq. (A.32) we will show that $\forall i \in \{0, \ldots, N_j - 2\}$, $R^{\sigma \circ c_{N_j - i}}_{N_j} \geq R^{\sigma \circ c_{N_j - i - 1}}_{N}$. First, we need to remark that according to definition (A.31),

$$\begin{aligned} Y^{\sigma \circ c_{N_j-i}}_{N_j-i-1} &= \{B_{\sigma \circ c_{N_j-i}(1)}, \ldots, B_{\sigma \circ c_{N_j-i}(N_j-i-1)}\} \\ &= \{B_{\sigma(1)}, \ldots, B_{\sigma(N_j-i-1)}\} \\ &= Y^{\sigma}_{N_j-i-1}. \end{aligned}$$

Then rewriting explicitly the coordinates $R^{\sigma \circ c_{N_j-i}}_{N_j}$ and $R^{\sigma \circ c_{N_j-i-1}}_{N_j}$ we obtain

$$\begin{aligned} R^{\sigma \circ c_{N_j-i}}_{N_j} &= \frac{S^{\psi}_{j+1}(Y^{\sigma \circ c_{N_j-i}}_{N_j-i-1}) - S^{\psi}_{j+1}(Y^{\sigma \circ c_{N_j-i}}_{N_j-i-1} B_{N_j})}{S(\phi^{B_{N_j}})} \\ &= \frac{S^{\psi}_{j+1}(Y^{\sigma}_{N_j-i-1}) - S^{\psi}_{j+1}(Y^{\sigma}_{N_j-i-1} B_{N_j})}{S(\phi^{B_{N_j}})} \\ &= \frac{S^{\psi}_{j+1}(Y^{\sigma}_{N_j-i-2} B_{\sigma(N_j-i-1)}) - S^{\psi}_{j+1}(Y^{\sigma}_{N_j-i-2} B_{\sigma(N_j-i-1)} B_{N_j})}{S(\phi^{B_{N_j}})}, \end{aligned} \tag{A.51}$$

and

$$R_{N_j}^{\sigma\circ c_{N_j-i-1}} = \frac{S_{j+1}^{\psi}(Y_{N_j-i-2}^{\sigma\circ c_{N_j-i-1}}) - S_{j+1}^{\psi}(Y_{N_j-i-2}^{\sigma\circ c_{N_j-i-1}} B_{N_j})}{S(\phi^{B_{N_j}})} = \frac{S_{j+1}^{\psi}(Y_{N_j-i-2}^{\sigma}) - S_{j+1}^{\psi}(Y_{N_j-i-2}^{\sigma} B_{N_j})}{S(\phi^{B_{N_j}})}. \tag{A.52}$$

The "strong subadditivity" of Eq. (A.29) ensures that for all subsets Y,

$$S_{j+1}^{\psi}(YB_{\sigma(N_j-i-1)}) + S_{j+1}^{\psi}(YB_{N_j}) \geq S_{j+1}^{\psi}(YB_{\sigma(N_j-i-1)}B_{N_j}) + S_{j+1}^{\psi}(Y). \tag{A.53}$$

Eq. (A.32) follows directly from it, since Eq. (A.53) implies that

$$S_{j+1}^{\psi}(YB_{\sigma(N_j-i-1)}) - S_{j+1}^{\psi}(YB_{\sigma(N_j-i-1)}B_{N_j}) \geq S_{j+1}^{\psi}(Y) - S_{j+1}^{\psi}(YB_{N_j}). \tag{A.54}$$

It follows that $R_{N_j}^{\sigma\circ c_{N_j-i}} \geq R_N^{\sigma\circ c_{N_j-i-1}}$. Eqs. (A.11) are proven in the same manner.

A.3 Proof of Eq. (A.29)

Given that S_j^{ψ} satisfy strong subadditivity, we will show that $\forall X \subset \{B_1, \ldots, B_{N-j}\}$ and for $B_l, B_m \notin X$,

$$S_{j+1}^{\psi}(XB_l) + S_{j+1}^{\psi}(XB_m) - S_{j+1}^{\psi}(X) - S_{j+1}^{\psi}(XB_lB_m) \geq 0, \tag{A.55}$$

with S_{j+1}^{ψ} defined as in Eq. (A.27c).

For a given $X \subset \{B_1, \ldots, B_{N-j}\}$ and given $B_l, B_m \notin X$, each term of the inequality (A.55) can be rewritten using S_j^{ψ}. For all $Y \subset \{B_1, \ldots, B_{N-j}\}$, the value of $S_{j+1}^{\psi}(Y)$ depends on the value of $S_j^{\psi}(Y) - S_j^{\psi}(YB_{N_j+1})$. As a consequence, several cases arise depending on the value of the four following values,

$$A := \frac{S_j^{\psi}(X) - S_j^{\psi}(XB_{N_j+1})}{S(\phi^{B_{N_j+1}})}, \tag{A.56a}$$

$$B := \frac{S_j^{\psi}(XB_l) - S_j^{\psi}(XB_lB_{N_j+1})}{S(\phi^{B_{N_j+1}})}, \tag{A.56b}$$

$$C := \frac{S_j^{\psi}(XB_m) - S_j^{\psi}(XB_mB_{N_j+1})}{S(\phi^{B_{N_j+1}})}, \tag{A.56c}$$

$$D := \frac{S_j^{\psi}(XB_lB_m) - S_j^{\psi}(XB_lB_mB_{N_j+1})}{S(\phi^{B_{N_j+1}})}. \tag{A.56d}$$

From Eq. (A.29), we can deduce $A \leq B$, $A \leq C$, $B \leq D$ and $C \leq D$. We can assume without loss of generality that $B \leq C$. Thus,

$$A \leq B \leq C \leq D \tag{A.57}$$

and there is only five cases to examine $m_j^{\psi,\phi} < A$, $A \leq m_j^{\psi,\phi} < B$, $B \leq m_j^{\psi,\phi} < C$, $C \leq m_j^{\psi,\phi} < D$ and $D \leq m_j^{\psi,\phi}$. We will prove inequality (A.55) for each of these case.

1. $m_j^{\psi,\phi} < A$.
   We can rewrite the left-hand side of inequality (A.55) as

$$\begin{aligned} &S_{j+1}^{\psi}(XB_l) + S_{j+1}^{\psi}(XB_m) - S_{j+1}^{\psi}(X) - S_{j+1}^{\psi}(XB_lB_m) = \\ &\qquad S_j^{\psi}(XB_lB_{N_j+1}) + S_j^{\psi}(XB_mB_{N_j+1}) - S_j^{\psi}(XB_{N_j+1}) - S_j^{\psi}(XB_lB_mB_{N_j+1}). \end{aligned}$$

   According to Eq. (A.29),

$$S_j^{\psi}(XB_lB_{N_j+1}) + S_j^{\psi}(XB_mB_{N_j+1}) - S_j^{\psi}(XB_{N_j+1}) - S_j^{\psi}(XB_lB_mB_{N_j+1}) \geq 0. \tag{A.58}$$

   So the inequality is verified.
2. $A \leq m_j^{\psi,\phi} < B$.
   We can rewrite the left-hand side of inequality (A.55) as

$$\begin{aligned} &S_{j+1}^{\psi}(XB_l) + S_{j+1}^{\psi}(XB_m) - S_{j+1}^{\psi}(X) - S_{j+1}^{\psi}(XB_lB_m) = \\ &\qquad S_j^{\psi}(XB_lB_{N_j+1}) + S_j^{\psi}(XB_mB_{N_j+1}) - S_j^{\psi}(X) + \\ &\qquad\qquad m_j^{\psi,\phi} S(\phi^{B_{N_j+1}}) - S_j^{\psi}(XB_lB_mB_{N_j+1}). \end{aligned}$$

   According to Eq. (A.29), we know that the last equation's right side is larger than

$$S_j^{\psi}(XB_{N_j+1}) - S_j^{\psi}(X) + m_j^{\psi,\phi} S(\phi^{B_{N_j+1}}).$$

   The latter quantity is non-negative because $m_j^{\psi,\phi} \geq A$, showing the validity of the inequality.
3. $B \leq m_j^{\psi,\phi} < C$.
   Once again, we rewrite the left-hand side of the inequality (A.55):

$$\begin{aligned} &S_{j+1}^{\psi}(XB_l) + S_{j+1}^{\psi}(XB_m) - S_{j+1}^{\psi}(X) - S_{j+1}^{\psi}(XB_lB_m) = \\ &\qquad S_j^{\psi}(XB_l) + S_j^{\psi}(XB_mB_{N_j+1}) - S_j^{\psi}(X) - S_j^{\psi}(XB_lB_mB_{N_j+1}). \end{aligned}$$

   The "strong subbaditivity" of the function S_j^{ψ} gives rise to

$$S_j^{\psi}(XB_mB_{N_j+1}) - S_j^{\psi}(XB_lB_mB_{N_j+1}) \geq S_j^{\psi}(XB_{N_j+1}) - S_j^{\psi}(XB_lB_{N_j+1}), \tag{A.59}$$

and this implies that

$$S_j^{\psi}(XB_l) + S_j^{\psi}(XB_mB_{N_j+1}) - S_j^{\psi}(X) - S_j^{\psi}(XB_lB_mB_{N_j+1}) \geq S_j^{\psi}(XB_l) + S_j^{\psi}(XB_{N_j+1}) - S_j^{\psi}(X) - S_j^{\psi}(XB_lB_{N_j+1}).$$

Again, the "strong subbaditivity" of S_j^{ψ} allow us to conclude that the right-hand side is positive. Thus, inequality (A.55) is verified.

4. $C \leq m_j^{\psi,\phi} < D$.
   In this case, the rewriting gives,

$$S_{j+1}^{\psi}(XB_l) + S_{j+1}^{\psi}(XB_m) - S_{j+1}^{\psi}(X) - S_{j+1}^{\psi}(XB_lB_m) = S_j^{\psi}(XB_l) + S_j^{\psi}(XB_m) - m_j^{\psi,\phi}S(\phi^{B_{N_j+1}}) - S_j^{\psi}(X) - S_j^{\psi}(XB_lB_mB_{N_j+1}).$$

   D being superior to $m_j^{\psi,\phi}$ implies directly that

$$-S_j^{\psi}(XB_lB_mB_{N_j+1}) - m_j^{\psi,\phi}S(\phi^{B_{N_j+1}}) > -S_j^{\psi}(XB_lB_m).$$

   We can lower bound the right-hand side by

$$S_j^{\psi}(XB_l) + S_j^{\psi}(XB_m) - S_j^{\psi}(X) - S_j^{\psi}(XB_lB_m).$$

   Once again, the "strong subbaditivity" of S_j^{ψ} allows to conclude that the inequality (A.55) is true.

5. $D < m_j^{\psi,\phi}$.
   The last case is straightforward since the rewriting in term of S_j^{ψ} is

$$S_{j+1}^{\psi}(XB_l) + S_{j+1}^{\psi}(XB_m) - S_{j+1}^{\psi}(X) - S_{j+1}^{\psi}(XB_lB_m) = S_j^{\psi}(XB_l) + S_j^{\psi}(XB_m) - S_j^{\psi}(X) - S_j^{\psi}(XB_lB_m).$$

   In this case, the "strong subbaditivity" of Eq. (A.29) leads us directly to the conclusion that the inequality (A.55) is true.

In conclusion, the inequality (A.55) is verified for each possible case. Thus Eq. (A.29) is verified by induction.

Appendix B

OptiQraft: a game-based approach of quantum optics

B.1 Presentation of OptiQraft

B.1.1 Summary

We chose to develop this game as a *puzzle game* which is an enigma sort of game. Enigma and puzzle games reflect well the "learning" part and is a frequent choice for game based learning [88, 71, 68, 72]. Indeed, this progression mirrors the exercise progression already present in standard pedagogy as you progress through levels and can only go further if you managed to understand the previously introduced notion. The pitch of the game is quite simple. The game is cut into several levels. In each of these levels, the player is given one or several quantum states as inputs and have to produce a given output from those inputs. In order to win, the player has access to an optic table represented as a grid and several kinds of instruments: an emitter which can output a specific quantum state, mirrors, beamsplitters, measurers and dephasers, see Fig. B.1 for a depiction of the interface. The whole simulation follows a cycle logic, each spatial mode – see next subsection – on the quantum optic table will advance at the velocity of one case per cycle.

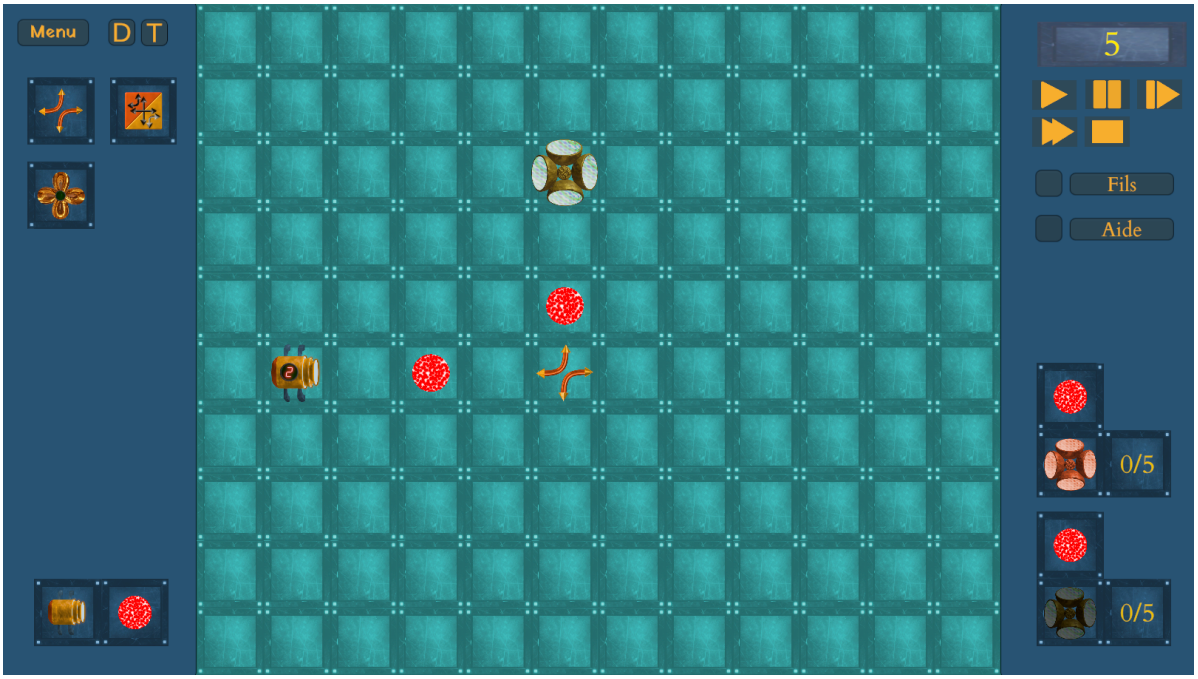

Figure B.1: Capture of the game interface, on the left panel you can find the available instruments. Instruments are placed on the grid on which spatial modes – depicted as colored circles – will move, one case per cycle. The cycles handling is done using the button at the top right of the screen

B.1.2 Set of states

We decided to play using the basic features of quantum optics. The particle which will be manipulated is a *faketon* – fauxton in French – an imaginary quantum particle presenting boson properties. We will label faketons' creation operator as $\hat{a}^\dagger$, a state can be equivalently described as a normalized sum of kets or as the normalized sum of the power of creation operators $a^\dagger$. Regarding the coefficients of the state, we decided for the sake of simplicity to restrict the set of phases which can be applied to the binary set -1 and $+1$ as it reduced the number of parameters we needed to describe. Finally, we allowed the state to be separated between several parties which will be the different spatial modes. As such, the states we manipulate in the game are written as

$$|\psi\rangle := \sum_{\{i_1,\dots,i_N\}} c_{i_1,\dots,i_N} \, |i_1,\dots,i_N\rangle^{M_1,\dots,M_N} \tag{B.1}$$

where M_j is the party representing the j^{th} spatial mode. Or using creation operators $a_j^\dagger$:

$$|\psi\rangle = \left(\sum_{\{i_1,\dots,i_N\}} \frac{c_{i_1,\dots,i_N}}{\sqrt{i_1!\dots i_N!}} (\hat{a}_1^\dagger)^{i_1} \dots (\hat{a}_N^\dagger)^{i_N} \right) |0,\dots,0\rangle^{M_1,\dots,M_N} , \tag{B.2}$$

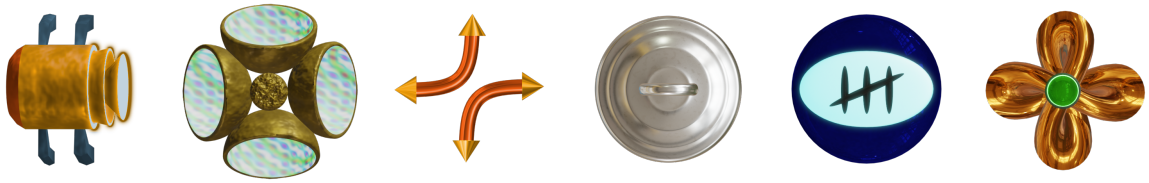

Figure B.2: Graphical representation of the instruments. In this order: emitter, collector, mirror, trash, measurer, dephaser

In both descriptions, the coefficients $c_{i_1,\ldots,i_N}$ form a set of real variable such that

$$\sum_{\{i_1,\ldots,i_N\}} c^2_{i_1,\ldots,i_N} = 1 \tag{B.3}$$

B.1.3 Instruments

We present here the different instruments which are used to manipulate quantum states, in the order in which we introduce them to the player. You can find the current graphical representation in Fig. B.2

Emitter

Emitters emit *packets* which are the game name for spatial modes. Each packet can be in a superposition of the number of faketons inside it. An emitter can emit several *linked* packets, which are entangled spatial modes such as the unnormalized

$$|01\rangle^{M_1M_2} + |10\rangle^{M_1M_2} \tag{B.4}$$

quantum state, in which a faketon is present in both packets at the same time. Their role is to be the input of quantum states into the simulation. The input states are fixed for each level.

Collector

As we introduced them in the game, collectors are non-physical instruments. They only accept a specific kind of states and know exactly which state they received without measuring it. Their role is to be the output of the created quantum state. We decided that collectors could accept only one packet at a time. As a consequence, in order to output a multipartite state, several collectors had to be placed each receiving only one packet. We made this choice to support the notion of a state being non-local.

Mirror

Mirrors change the direction of light, and thus they should change the direction of the packet. To make it understandable to everyone, mirrors are depicted as two arrows symbolizing the change of direction.

Trash

As the name suggests, those instruments trash any packet which enter. Trashes affect the entered packet by performing destructive measurement in the number of faketons – $\{|0\rangle, |1\rangle, \dots\}$ – basis and destroying it after.

Measurer

Those instruments also measure the inputted packet in the number of faketons basis. There are two differences with trashes: measurers can send a classical signal to other instruments depending on the result of the measurement and they perform a non-destructive measurement. If several packets enter at the same time, the packets are projected into the subspaces corresponding to the actual number of faketons which entered. For example, if two packets enter at the same time, they are projected into one of the following subspaces:

$$\{\{|00\rangle\}, \{|01\rangle, |10\rangle\}, \{|02\rangle, |11\rangle, |20\rangle\}, \dots\} \tag{B.5}$$

Dephaser

Dephasers as the name implies apply a -1 phase to every faketon which goes through them when they are activated. Labelling the input mode as $\hat{a}^\dagger$ and the output mode as $\hat{b}^\dagger$, activated dephasers apply

$$\hat{b}^\dagger = -\hat{a}^\dagger \tag{B.6}$$

They can be configured to be turned on and off periodically or they be controlled by a classical signal. In this case, each signal switches the dephaser's activation.

Beamsplitter

Beamsplitters were the most complex objects to explain as they were the cause of the interference phenomenon. Labelling the two input modes of the beamsplitter as $\hat{a}^\dagger$ and

Figure B.3: Graphical depiction of the beamsplitter. The arrows symbolize the reflection and the transmission of the input packet. The white arrow marks the reflection which will add a phase.

$b^\dagger$ and the two output modes as $\hat{c}^\dagger$ and $\hat{d}^\dagger$, we chose to implement the beamsplitter as the operation which change the basis of creation operators as:

$$\hat{c}^\dagger = \frac{1}{\sqrt{2}}\left(\hat{a}^\dagger + \hat{b}^\dagger\right) \tag{B.7a}$$

$$\hat{d}^\dagger = \frac{1}{\sqrt{2}}\left(\hat{a}^\dagger - \hat{b}^\dagger\right). \tag{B.7b}$$

As can be seen in Fig. B.3, we added two visual feedback when implementing the beamsplitter. The first one is the use of arrows to show the direction which can take an inputted faketon. Following the arrows, one can see both a reflection and a transmission. The second feedback is to represent the phenomenon of phase multiplication which ensues from Eq. (B.7b). Observing Fig. B.3, we can observe one of the arrow is white while the others are black. The white arrow depicts the -1 phase added when the faketon is being reflected by this face on the beamsplitter.

B.2 Representing information

We have to represent two types of information, a classical one which allows the communication between instruments and the quantum one we wish to manipulate.

B.2.1 Classical signals

It can be necessary to constrain the behaviour or some instruments to the result of a measurement. Classical signals will be emitted by the measure instrument if it is linked to an instrument which can receive such a signal. The classical signal and the quantum packets move at the same velocity since both are – in spirit – made of light. However, for the sake of simplicity, classical signal does not follow the grid and can thus take a shorter path than any packet.

B.2.2 Quantum states

We could not afford to write quantum states in the standard bra-ket formalism or as the sum of creation operators as those concepts involve the knowledge of linear algebra. As such, we formalized a graphical description of our subset of quantum states. In order to offer a suitable representation of quantum states in the previously described set – Subsec. B.1.2 –, we identified three key notions our representation needed to show: the superposition of states, the phase and the non-locality.

Superposition

We assumed a friendly introduction to quantum physics had to pass by the use of classical concepts, as they are the ones the general audience is familiarized with. We found the most interesting and relevant quantity to represent to be the probability of having a given number of faketons inside a given state. Indeed, this quantity is easily understandable from a classical point-of-view and it fitted well with the measurement instrument, allowing a player to predict to some extent the result of a measurement. This information had to be visible at all times, since it eased player's state manipulations – not that it do not necessarily improve the learning process [20]. As such, we chose packets to be represented as circles, we associated a color to each possible number of faketon inside the packet and we drew the probability to measure this number of faketon as the proportion on the circle representing the mode, see Fig. B.4. This is, in our opinion, a visual quick-to-assess description of the superposition of states.

Phase

The second notion we needed to represent was the phase. Adding the phase as a continuous quantity taking values on the unit circles was something too difficult to describe. We decided to settle on only two phases: 1 and -1, since it is the minimal set of phases

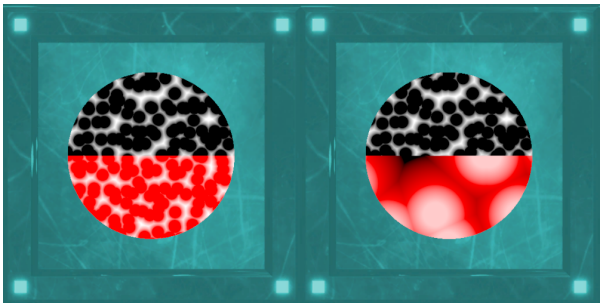

Figure B.4: On the left, a graphical description of the $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ state. The black color means there is no faketon and the red that there is one. On the right, a $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ state. Note that the phase applied to the right faketon induces a change of pattern.

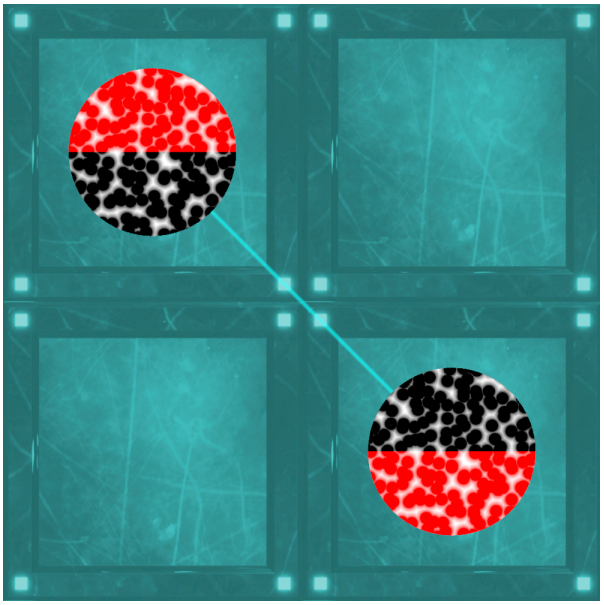

Figure B.5: Graphical representation of the $\frac{1}{\sqrt{2}}\left(|10\rangle^{A,B} + |01\rangle^{A,B}\right)$ state. The same portion represent the same ket. Here the faketon is either on the top left or on the bottom right.

needed to witness an interference phenomenon. We gave a different pattern but the same color to a phase-shifted state, resulting on the following representation: Fig. B.4.

Entanglement

The third notion and not the least was that a state can be present at several positions at the same time. To represent this phenomenon, we added a line between the packets belonging to the same states. To represent the joint probabilities, we color the same portion of the circle with the appropriate number of faketon, see Fig. B.5 for a represention.

Concessions

In order to maximize visual feedback, we added a full text description of the state in terms of phase and probability which appears when clicking on any of its packet. We also made small concessions to the gameplay. We stop the simulation and generate an in-game error if the superposition of states becomes too large or if the amount of a state's spatial modes exceeds a certain number, as it makes the reading of the states too difficult and it increases drastically the time of computation. We also added collision between spatial modes if they met outside a beamsplitter or a measurement instrument – while precising that in reality, photon do not collide – as it adds some challenge and increases the readability of a simulation.

B.3 Implementation and tutorial

B.3.1 Game design

Each of the quantum notions – superposition, phase, non-locality and interference – is a non-trivial notion we needed to introduce to the – supposed – non-informed player.

Level Progression

At the time of writing, levels have been divided into portions, each concerning a notion the player needs to acquire whether it is a gameplay notion or a physics notion. Each of these portion is comprised of mandatory levels which introduce the notion and optional ones which reuse already introduces notions in different contexts in order to support the assimilation of said notions. Following the notion of *scaffolded instruction* [8], the player cannot access a portion if the mandatory levels of the previous portion were not completed.

Scoring

We added a minimal leaderboard at the end of each level, it simply indicates where you are in terms of performances compared to the other players. The performance we compare are: the number of cycles to complete the level, the number of instruments use, and – since some instruments can be classically constrained to other – the number of classical threads used. In the spirit of [41, 53], adding a score incitement can drive some profiles to optimize the level and increase playing time.

Freedom

Lastly, we chose to give as much freedom as possible to the player into the placement of instruments and the handling of the optics table. In earlier levels, the instruments are already placed on the grid, then gradually players are given more and more freedom to place themselves. This will allow some tinkering of the quantum engine and to explore the non-intuitive action of instruments over quantum object. While some studies had this "freedom of choice" as a discussed criterion as can be seen in [33], there is, to my knowledge, no specific and isolated study of this mechanism.

B.3.2 Level Design

In addition of these game design choices we did level design choices to introduce notions one at a time.

Superposition and non-locality

The notions of superposition and non-locality have been introduced through the use of measurement. Showing the collapse of the superposition and the non-locality as well the probabilistic nature of those collapse give a visualisation of both phenomenon. We built levels where the use of measurers was mandatory by introducing a temporary object, a mirror which could rotate when receiving a classical signal. Thanks to this instrument, the player can distribute quantum states taking into account the local or non-local superposition of states. We made this object temporary as one of the later level is to make such an instrument using only beamsplitters, mirrors and a dephaser to build a Mach-Zehnder interferometer [116].

Phase

The notion of phase and the dephaser instrument were simply introduced by levels asking for dephased output, for example taking the left faketon of Fig. B.4 as input and the right one as output. We also had to explain that two states differing by a global phase where equals. This problem was solved in two different ways. First, we added a hot key to switch the global phase of the faketon needed by the collector which made accessible the two different representations of the same state. Second, by adding levels mimicking previous levels but with the addition of a global phase on the inputted quantum states. This allow the player to see the physics do not change when adding a global phase. We

hope a combination of those two techniques with the addition of tutorial texts give an understanding of the concept of global phase.

Beamsplitter and interference

The last but not least notions have been the introduction of both the beamsplitter and the phenomenon of interference. Concerning the beamsplitter, we introduced gradually the effect of the beamsplitter by forcing the direction in which the input packet has to enter which allow the player to observe gradually the effect of the beamsplitter on states. The first challenge has been to explain the differences between being "reflected or transmitted" and being "reflected and transmitted". We solved it by introducing non-locality before introducing the beamsplitter. In earlier levels, we show an emitter could input linked packets, such as two packets sharing one faketon as in Fig. B.5. As such, we had the player playing with the concept before introducing the beamsplitter.
Concerning the interference phenomenon, we introduce it in two steps. First, we ask for an operation to separate two faketons which are in the same packet. Normally, at this point, the player understood that half will be transmitted and the other half will be reflected. Then, we ask for the converse operation, using a beamsplitter to fuse two faketons into one packet. This operation produces a Hong-Ou-Mandel [50] effect which is not what is expected by the player at this point. We use the occasion to introduce the wave-particle duality of faketon and to explain the phenomenon of interference.
Last notion we introduce is the self-interference of a faketon with itself. For now, we culminate with the introduction of the Mach-Zehnder interferometer [116] and the way to use it as a rotating miror by adding a dephaser inside one of the branches as in Fig. B.6. We added a few number of levels using this mechanism to support the learning of the Mach-Zehnder including an animation-level showing the difference between the Mach-Zehnder interferometer and a "classical" one in which we track the faketon all along. Thanks to this animation-level, we can litterally show that if you allow the superposition to happen, the faketon always comes out in the same direction.

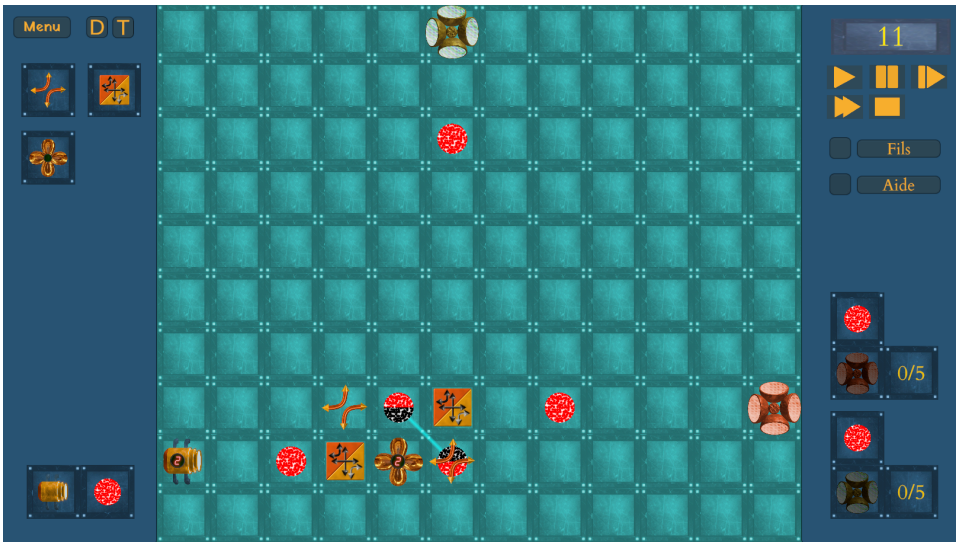

Figure B.6: Reproduction of a Mach-Zehnder interferometer in the game. With the Mach-Zehnder, the player is able to distribute quantum states between 2 different collectors.

Bibliography

[1] A. Acín, J. I. Cirac, and M. Lewenstein.
Entanglement percolation in quantum networks.
Nature Physics, 3(4):256–259, 2007.
URL https://www.nature.com/articles/nphys549.

[2] R. Ahlswede, N. Cai, S.-Y. Li, and R. W. Yeung.
Network information flow.
IEEE Transactions on information theory, 46(4):1204–1216, 2000.
URL http://www.inf.fu-berlin.de/lehre/WS11/Wireless/papers/CodAhlswede00.pdf.

[3] S. Akibue and M. Murao.
Network coding for distributed quantum computation over cluster and butterfly networks.
IEEE Transactions on Information Theory, 62(11):6620–6637, 2016.
URL https://arxiv.org/pdf/1503.07740.

[4] S. Akibue, M. Owari, G. Kato, and M. Murao.
Entanglement-assisted classical communication can simulate classical communication without causal order.
Physical Review A, 96(6):062331, 2017.
URL https://link.aps.org/pdf/10.1103/PhysRevA.96.062331.

[5] R. Albert and A.-L. Barabási.
Statistical mechanics of complex networks.
Reviews of modern physics, 74(1):47, 2002.
URL https://link.aps.org/pdf/10.1103/RevModPhys.74.47.

[6] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, et al.
Quantum supremacy using a programmable superconducting processor.

Nature, 574(7779):505–510, 2019.
URL https://www.nature.com/articles/s4158601916665.

[7] F. Arzani, G. Ferrini, F. Grosshans, and D. Markham.
Random coding for sharing bosonic quantum secrets.
Physical Review A, 100(2):022303, 2019.
URL https://link.aps.org/pdf/10.1103/PhysRevA.100.022303.

[8] P. L. Beed, E. M. Hawkins, and C. M. Roller.
Moving learners toward independence: The power of scaffolded instruction.
The Reading Teacher, 44(9):648–655, 1991.
URL https://www.jstor.org/stable/20200767.

[9] B. Bell, D. Herrera-Martí, M. Tame, D. Markham, W. Wadsworth, and J. Rarity.
Experimental demonstration of a graph state quantum error-correction code.
Nature communications, 5(1):1–10, 2014.
URL https://www.nature.com/articles/ncomms4658.pdf.

[10] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher.
Concentrating partial entanglement by local operations.
Physical Review A, 53(4):2046, 1996.
URL https://link.aps.org/pdf/10.1103/PhysRevA.53.2046.

[11] C. H. Bennett and G. Brassard.
Quantum cryptography: Public key distribution and coin tossing.
arXiv preprint arXiv:2003.06557, 2020.
URL https://arxiv.org/pdf/2003.06557.

[12] 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.
Physical review letters, 70(13):1895, 1993.
URL https://link.aps.org/pdf/10.1103/PhysRevLett.70.1895.

[13] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal.
Exact and asymptotic measures of multipartite pure-state entanglement.
Phys. Rev. A, 63:012307, Dec 2000.
doi:10.1103/PhysRevA.63.012307.

[14] P. Berman, M. Karpinski, and A. Zelikovsky.
1.25-approximation algorithm for steiner tree problem with distances 1 and 2.

In *Workshop on Algorithms and Data Structures*, pages 86–97. Springer, 2009. doi:10.1007/978-3-642-03367-4_8.

[15] F. G. Brandao and M. B. Plenio.
A reversible theory of entanglement and its relation to the second law.
Communications in Mathematical Physics, 295(3):829–851, 2010.
URL https://link.springer.com/content/pdf/10.1007/s00220-010-1003-1.pdf.

[16] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest.
Measurement-based quantum computation.
Nature Physics, 5(1):19–26, 2009.
URL https://www.nature.com/articles/nphys1157.

[17] D. Browne, E. Kashefi, and S. Perdrix.
Computational depth complexity of measurement-based quantum computation.
In W. van Dam, V. M. Kendon, and S. Severini, editors, *Theory of Quantum Computation, Communication, and Cryptography*, volume 6519 of *Lecture Notes in Computer Science*, pages 35–46, Berlin, Heidelberg, 2011. Springer, arXiv:0909.4673. doi:10.1007/978-3-642-18073-6_4.

[18] D. E. Browne and H. J. Briegel.
One-way quantum computation.
In D. Brußand G. Leuchs, editors, *Lectures on quantum information*, chapter 20. Wiley, 2007, arXiv:quant-ph/0603226. doi:10.1002/9783527618637.ch20.

[19] L. Bugalho, B. C. Coutinho, and Y. Omar.
Distributing multipartite entanglement over noisy quantum networks.
arXiv preprint arXiv:2103.14759, 2021.
URL https://arxiv.org/pdf/2103.14759.

[20] D. Burgos, C. Van Nimwegen, H. Van Oostendorp, and R. Koper.
Game-based learning and the role of feedback. a case study.
2007.
URL https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.107.2930.

[21] M. Caleffi.
Optimal routing for quantum networks.
IEEE Access, 5:22299–22312, 2017.

URL https://ieeexplore.ieee.org/iel7/6287639/6514899/08068178.pdf.

[22] V. Camilleri, L. Busuttil, and M. Montebello.
Social interactive learning in multiplayer games.
In *Serious games and edutainment applications*, pages 481–501. Springer, 2011.
URL https://www.academia.edu/download/32081821/978-1-4471-2161-9_23.pdf.

[23] R. L. Carter and M. E. Crovella.
Measuring bottleneck link speed in packet-switched networks.
Performance evaluation, 27:297–318, 1996.
URL http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.17.2405&rep=rep1&type=pdf.

[24] F. Centrone, F. Grosshans, and V. Parigi.
Cost and routing of continuous variable quantum networks.
arXiv preprint arXiv:2108.08176, 2021.
URL https://arxiv.org/pdf/2108.08176.

[25] D. Charles, T. Charles, M. McNeill, D. Bustard, and M. Black.
Game-based feedback for educational multi-user virtual environments.
British Journal of Educational Technology, 42(4):638–654, 2011.
URL https://bera-journals.onlinelibrary.wiley.com/doi/full/10.1111/j.1467-8535.2010.01068.x.

[26] A. M. Childs, D. Leung, L. Mančinska, and M. Ozols.
A framework for bounding nonlocality of state discrimination.
Communications in Mathematical Physics, 323(3):1121–1153, 2013.
URL https://link.springer.com/content/pdf/10.1007/s00220-013-1784-0.pdf.

[27] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter.
Everything you always wanted to know about locc (but were afraid to ask).
Communications in Mathematical Physics, 328(1):303–326, 2014.
URL https://link.springer.com/content/pdf/10.1007/s00220-014-1953-9.pdf.

[28] M.-D. Choi.
Completely positive linear maps on complex matrices.
Linear algebra and its applications, 10(3):285–290, 1975.

URL https://www.sciencedirect.com/science/article/pii/0024379575900750/pdf.

[29] M. C. Clark and M. Rossiter.
Narrative learning in adulthood.
New directions for adult and continuing education, 2008(119):61–70, 2008.
URL https://onlinelibrary.wiley.com/doi/pdf/10.1002/ace.306.

[30] R. Cohen and S. Havlin.
Complex networks: structure, robustness and function.
Cambridge university press, 2010.

[31] P. Contreras-Tejada, C. Palazuelos, and J. I. De Vicente.
Resource theory of entanglement with a unique multipartite maximally entangled state.
Physical review letters, 122(12):120503, 2019.
URL https://link.aps.org/pdf/10.1103/PhysRevLett.122.120503.

[32] A. Dahlberg, M. Skrzypczyk, T. Coopmans, L. Wubben, F. Rozpędek, M. Pompili, A. Stolk, P. Pawełczak, R. Knegjens, J. de Oliveira Filho, et al.
A link layer protocol for quantum networks.
In *Proceedings of the ACM Special Interest Group on Data Communication*, pages 159–173. ACM, 2019.
URL https://dl.acm.org/doi/pdf/10.1145/3341302.3342070.

[33] D. Dicheva, C. Dichev, G. Agre, and G. Angelova.
Gamification in education: A systematic mapping study.
Journal of Educational Technology & Society, 18(3):75–88, 2015.
URL https://www.academia.edu/download/36177791/ETS-Dicheva-Gamification-in-Education.pdf.

[34] D. DiVincenzo, C. Fuchs, H. Mabuchi, J. Smolin, A. Thapliyal, and A. Uhlmann.
Entanglement of assistance.
In *Quantum Computing and Quantum Communications*, volume 1509 of *Lecture Notes in Computer Science*, pages 247–257. Springer Berlin Heidelberg, 1999.
doi:10.1007/3-540-49208-9_21.

[35] W. Dür, H. Aschauer, and H.-J. Briegel.
Multiparticle entanglement purification for graph states.
Physical review letters, 91(10):107903, 2003.
URL https://link.aps.org/pdf/10.1103/PhysRevLett.91.107903.

[36] W. Dür, M. Skotiniotis, F. Froewis, and B. Kraus.
Improved quantum metrology using quantum error correction.
Physical Review Letters, 112(8):080801, 2014.
URL https://link.aps.org/pdf/10.1103/PhysRevLett.112.080801.

[37] A. Einstein, B. Podolsky, and N. Rosen.
Can quantum-mechanical description of physical reality be considered complete?
Phys. Rev., 47:777–780, May 1935.
doi:10.1103/PhysRev.47.777.

[38] G. Evenbly and G. Vidal.
Tensor network states and geometry.
Journal of Statistical Physics, 145(4):891–918, 2011.
URL https://link.springer.com/content/pdf/10.1007/s10955-011-0237-4.pdf.

[39] J. Feldman, A. Monteserin, and A. Amandi.
Detecting students' perception style by using games.
Computers & Education, 71:14–22, 2014.
URL https://www.sciencedirect.com/science/article/pii/S0360131513002625.

[40] A. Fischer and D. Towsley.
Distributing graph states across quantum networks.
arXiv preprint arXiv:2009.10888, 2020.
URL https://arxiv.org/pdf/2009.10888.

[41] P. Fotaris, T. Mastoras, R. Leinfellner, and Y. Rosunally.
Climbing up the leaderboard: An empirical study of applying gamification techniques to a computer programming class.
Electronic Journal of e-learning, 14(2):94–110, 2016.
URL https://files.eric.ed.gov/fulltext/EJ1101229.pdf.

[42] V. Giovannetti, S. Lloyd, and L. Maccone.
Quantum metrology.
Physical review letters, 96(1):010401, 2006.
URL https://link.aps.org/pdf/10.1103/PhysRevLett.96.010401.

[43] G. Gour and N. R. Wallach.
Classification of multipartite entanglement of all finite dimensionality.
Physical review letters, 111(6):060502, 2013.

URL https://link.aps.org/pdf/10.1103/PhysRevLett.111.060502.

[44] A. B. Grilo, I. Kerenidis, and J. Sikora.
Qma with subset state witnesses.
In *International Symposium on Mathematical Foundations of Computer Science*, pages 163–174. Springer, 2015.
URL https://arxiv.org/pdf/1410.2882.

[45] M. D. Hanus and J. Fox.
Assessing the effects of gamification in the classroom: A longitudinal study on intrinsic motivation, social comparison, satisfaction, effort, and academic performance.
Computers & education, 80:152–161, 2015.
URL https://www.sciencedirect.com/science/article/pii/S0360131514002000.

[46] P. Harrington.
Machine learning in action.
Simon and Schuster, 2012.

[47] P. E. Hart, N. J. Nilsson, and B. Raphael.
A formal basis for the heuristic determination of minimum cost paths.
IEEE transactions on Systems Science and Cybernetics, 4(2):100–107, 1968.
URL https://ieeexplore.ieee.org/abstract/document/4082128/.

[48] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Nest, and H.-J. Briegel.
Entanglement in graph states and its applications.
arXiv preprint quant-ph/0602096, 2006.
URL https://arxiv.org/pdf/quant-ph/0602096.

[49] T. Ho and D. Lun.
Network coding: an introduction.
Cambridge University Press, 2008.

[50] C.-K. Hong, Z.-Y. Ou, and L. Mandel.
Measurement of subpicosecond time intervals between two photons by interference.
Physical review letters, 59(18):2044, 1987.
URL https://link.aps.org/pdf/10.1103/PhysRevLett.59.2044.

[51] M. Horodecki, J. Oppenheim, and A. Winter.
Partial quantum information.

Nature, 436(7051):673–676, 2005.
URL https://www.nature.com/articles/nature03909.

[52] M. Horodecki, J. Oppenheim, and A. Winter.
Quantum state merging and negative information.
Communications in Mathematical Physics, 269(1):107–136, 2007.
URL https://link.springer.com/content/pdf/10.1007/s00220-006-0118-x.pdf.

[53] B. Huang and K. F. Hew.
Do points, badges and leaderboard increase learning and activity: A quasi-experiment on the effects of gamification.
In *Proceedings of the 23rd International Conference on Computers in Education*, pages 275–280, 2015.
URL https://www.researchgate.net/profile/Khe-Hew/publication/286001811_Do_points_badges_and_leaderboard_increase_learning_and_activity_A_quasi-experiment_on_the_effects_of_gamification/links/5665404708ae15e746333d22/Do-points-badges-and-leaderboard-increase-learning-and-activity-A-quasi-experim pdf.

[54] F. K. Hwang, D. S. Richards, and P. Winter.
The Steiner tree problem, volume 53 of *Annals of Discrete Mathematics*.
North Holland, 1992.

[55] P. Ćwikliński, M. Studziński, M. Horodecki, and J. Oppenheim.
Limitations on the evolution of quantum coherences: Towards fully quantum second laws of thermodynamics.
Phys. Rev. Lett., 115:210403, Nov 2015.
doi:10.1103/PhysRevLett.115.210403.

[56] R. S. Ingarden.
Quantum information theory.
Reports on Mathematical Physics, 10(1):43–72, 1976.
URL https://www.sciencedirect.com/science/article/abs/pii/0034487776900057.

[57] A. Jamiołkowski.
Linear transformations which preserve trace and positive semidefiniteness of operators.

Reports on Mathematical Physics, 3(4):275–278, 1972.

[58] K. Jansen and H. Zhang.
An approximation algorithm for the multicast congestion problem via minimum steiner trees.
2002.
URL http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.3.3628.

[59] K. M. Kapp.
The gamification of learning and instruction: game-based methods and strategies for training and education.
John Wiley & Sons, 2012.

[60] A. Keet, B. Fortescue, D. Markham, and B. C. Sanders.
Quantum secret sharing with qudit graph states.
Physical Review A, 82(6):062315, 2010.
URL https://link.aps.org/pdf/10.1103/PhysRevA.82.062315.

[61] B. Kim, H. Park, and Y. Baek.
Not just fun, but serious strategies: Using meta-cognitive strategies in game-based learning.
Computers & Education, 52(4):800–810, 2009.
URL https://www.sciencedirect.com/science/article/pii/S0360131508001954.

[62] H. Kobayashi, F. Le Gall, H. Nishimura, and M. Rötteler.
Perfect quantum network communication protocol based on classical network coding.
In *2010 IEEE International Symposium on Information Theory*, pages 2686–2690. IEEE, 2010.
URL https://arxiv.org/pdf/0902.1299.

[63] R. Koetter and M. Médard.
An algebraic approach to network coding.
IEEE/ACM transactions on networking, 11(5):782–795, 2003.
URL http://web.mit.edu/~medard/www/mpapers/aaatnetworkcoding.pdf.

[64] W. Kozlowski and S. Wehner.
Towards large-scale quantum networks.

In *Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication*, pages 1–7, 2019.
URL https://dl.acm.org/doi/pdf/10.1145/3345312.3345497.

[65] W. Kozlowski, S. Wehner, R. Meter, B. Rijsman, A. S. Cacciapuoti, M. Caleffi, and S. Nagayama.
Architectural principles for a quantum internet.
Internet Engineering Task Force, Internet-Draft draft-irtfqirg-principles-03, 2020.
URL https://datatracker.ietf.org/meeting/109/materials/slides-109-qirg-draft-irtf-qirg-principles-00.pdf.

[66] B. Kraus and J. I. Cirac.
Optimal creation of entanglement using a two-qubit gate.
Physical Review A, 63(6):062309, 2001.
URL https://link.aps.org/pdf/10.1103/PhysRevA.63.062309.

[67] K. Kraus, A. Böhm, J. D. Dollard, and W. Wootters.
States, effects, and operations: fundamental notions of quantum theory. lectures in mathematical physics at the university of texas at austin.
Lecture notes in physics, 190, 1983.

[68] M. J. Lee, F. Bahmani, I. Kwan, J. LaFerte, P. Charters, A. Horvath, F. Luor, J. Cao, C. Law, M. Beswetherick, et al.
Principles of a debugging-first puzzle game for computing education.
In *2014 IEEE symposium on visual languages and human-centric computing (VL/HCC)*, pages 57–64. IEEE, 2014.
URL https://www.researchgate.net/profile/Margaret-Burnett-2/publication/271545214_Principles_of_a_debugging-first_puzzle_game_for_computing_education/links/563ce8cb08aec6f17dd7e365/Principles-of-a-debugging-first-puzzle-game-for-computing-education.pdf.

[69] C.-H. Liao, C.-W. Yang, and T. Hwang.
Dynamic quantum secret sharing protocol based on ghz state.
Quantum information processing, 13(8):1907–1916, 2014.
URL https://link.springer.com/article/10.1007/s11128-014-0779-x.

[70] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, et al.
Satellite-relayed intercontinental quantum network.

Physical review letters, 120(3):030501, 2018.
URL https://link.aps.org/pdf/10.1103/PhysRevLett.120.030501.

[71] S. Lim, Y. Kim, and K. Kim.
A study on puzzle game-based learning content for understanding mandala.
International Journal of Advanced Culture Technology, 8(2):34–41, 2020.
URL https://www.koreascience.or.kr/article/JAKO202019854292307.pdf.

[72] C.-H. Lin and C.-M. Chen.
Developing spatial visualization and mental rotation with a digital puzzle game at primary school level.
Computers in Human Behavior, 57:23–30, 2016.
URL https://www.sciencedirect.com/science/article/pii/S0747563215302971.

[73] N. Linden, S. Popescu, B. Schumacher, and M. Westmoreland.
Reversibility of local transformations of multiparticle entanglement.
Quant. Inf. Proc., 4(3):241–250, 2005.
doi:10.1007/s11128-005-4608-0.

[74] M. Lostaglio, D. Jennings, and T. Rudolph.
Description of quantum coherence in thermodynamic processes requires constraints beyond free energy.
Nat. Commun., 6:6383, Mar. 2015.
doi:10.1038/ncomms7383.

[75] L. Lu, T. Wang, S. C. Liew, and S. Zhang.
Implementation of physical-layer network coding.
Physical Communication, 6:74–87, 2013.
URL https://www.sciencedirect.com/science/article/pii/S1874490712000213.

[76] M. Ludwig, S. Jablonski, A. Caldeira, and A. Moura.
Research on Outdoor STEM Education in the digiTal Age.
WTM-Verlag, Verlag für wissenschaftliche Texte und Medien, 2020.
URL https://www.researchgate.net/profile/Vale-Isabel-2/publication/342564965_Photography_A_Resource_to_Capture_Outdoor_Math/links/5f31a349a6fdcccc43bee725/Photography-A-Resource-to-Capture-Outdoor-Math.pdf.

[77] T. Matsuo.

Simulation of a dynamic, ruleset-based quantum network.
arXiv preprint arXiv:1908.10758, 2019.
URL https://arxiv.org/pdf/1908.10758.

[78] T. Matsuo, C. Durand, and R. Van Meter.
Quantum link bootstrapping using a ruleset-based communication protocol.
Physical Review A, 100(5):052320, 2019.
URL https://link.aps.org/pdf/10.1103/PhysRevA.100.052320.

[79] C. Meignant, F. Grosshans, and D. Markham.
Classical-quantum network coding: a story about tensor.
arXiv preprint arXiv:2104.04745, 2021.
URL https://arxiv.org/pdf/2104.04745.

[80] C. Meignant, D. Markham, and F. Grosshans.
Distributing graph states over arbitrary quantum networks.
Physical Review A, 100(5):052333, 2019.
URL https://link.aps.org/pdf/10.1103/PhysRevA.100.052333.

[81] M. Michler, K. Mattle, H. Weinfurter, and A. Zeilinger.
Interferometric bell-state analysis.
Physical Review A, 53(3):R1209, 1996.
URL https://link.aps.org/pdf/10.1103/PhysRevA.53.R1209.

[82] J. Miguel-Ramiro, A. Pirker, and W. Dür.
Genuine quantum networks with superposed tasks and addressing.
npj Quantum Information, 7(1):1–15, 2021.
URL https://www.nature.com/articles/s41534-021-00472-5.

[83] A. Miyake.
Classification of multipartite entangled states by multidimensional determinants.
Physical Review A, 67(1):012108, 2003.
URL https://link.aps.org/pdf/10.1103/PhysRevA.67.012108.

[84] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang.
Optimal architectures for long distance quantum communication.
Scientific reports, 6(1):1–10, 2016.
URL https://www.nature.com/articles/srep20463.

[85] M. Muratet, P. Torguet, J.-P. Jessel, and F. Viallet.
Towards a serious game to help students learn computer programming.

International Journal of Computer Games Technology, 2009, 2009.
URL https://www.hindawi.com/journals/IJCGT/2009/470590/.

[86] M. A. Nielsen.
Conditions for a class of entanglement transformations.
Physical Review Letters, 83(2):436, 1999.
URL https://link.aps.org/pdf/10.1103/PhysRevLett.83.436.

[87] M. A. Nielsen and I. Chuang.
Quantum computation and quantum information, 2002.

[88] L. Nita, N. Chancellor, L. M. Smith, H. Cramman, and G. Dost.
Inclusive learning for quantum computing: supporting the aims of quantum literacy using the puzzle game quantum odyssey.
arXiv preprint arXiv:2106.07077, 2021.
URL https://arxiv.org/pdf/2106.07077.

[89] R. Orús.
A practical introduction to tensor networks: Matrix product states and projected entangled pair states.
Annals of Physics, 349:117–158, 2014.
URL https://www.sciencedirect.com/science/article/pii/S0003491614001596.

[90] M. V. Pedersen, F. H. Fitzek, and T. Larsen.
Implementation and performance evaluation of network coding for cooperative mobile devices.
In *ICC Workshops-2008 IEEE International Conference on Communications Workshops*, pages 91–96. IEEE, 2008.

[91] D. Perez-Garcia, F. Verstraete, M. M. Wolf, and J. I. Cirac.
Matrix product state representations.
arXiv preprint quant-ph/0608197, 2006.
URL https://arxiv.org/pdf/quant-ph/0608197.

[92] S. Perseguers, J. I. Cirac, A. Acín, M. Lewenstein, and J. Wehr.
Entanglement distribution in pure-state quantum networks.
Physical Review A, 77(2):022308, 2008.
doi:10.1103/PhysRevA.77.022308.

[93] J. M. Pino, J. M. Dreiling, C. Figgatt, J. P. Gaebler, S. A. Moses, C. Baldwin, M. Foss-Feig, D. Hayes, K. Mayer, C. Ryan-Anderson, et al.
Demonstration of the qccd trapped-ion quantum computer architecture.
arXiv preprint arXiv:2003.01293, 2020.

[94] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein.
Advances in quantum teleportation.
Nature Phot., 9:641–652, 2015.
doi:10.1038/nphoton.2015.154.

[95] A. Pirker, J. Wallnöfer, and W. Dür.
Modular architectures for quantum networks.
New Journal of Physics, 20(5):053054, 2018.
doi:10.1088/1367-2630/aac2aa.

[96] M. Pohst and H. Zassenhaus.
Algorithmic algebraic number theory, volume 30.
Cambridge University Press, 1997.

[97] G. Robins and A. Zelikovsky.
Tighter bounds for graph steiner tree approximation.
SIAM Journal on Discrete Mathematics, 19(1):122–134, 2005.
doi:10.1137/S0895480101393155.

[98] E. Schoute, L. Mancinska, T. Islam, I. Kerenidis, and S. Wehner.
Shortcuts to quantum network routing.
arXiv preprint arXiv:1610.05238, 2016.
URL https://arxiv.org/pdf/1610.05238.

[99] B. Schumacher.
Quantum coding.
Phys. Rev. A, 51:2738–2747, Apr 1995.
doi:10.1103/PhysRevA.51.2738.

[100] K. Schwaiger, D. Sauerwein, M. Cuquet, J. I. de Vicente, and B. Kraus.
Operational multipartite entanglement measures.
Physical review letters, 115(15):150502, 2015.
URL https://link.aps.org/pdf/10.1103/PhysRevLett.115.150502.

[101] C. E. Shannon.
A mathematical theory of communication.

The Bell system technical journal, 27(3):379–423, 1948.
URL https://pure.mpg.de/rest/items/item_2383164/component/file_2383163/content.

[102] N. Shettell and D. Markham.
Graph states as a resource for quantum metrology.
Physical review letters, 124(11):110502, 2020.
URL https://link.aps.org/pdf/10.1103/PhysRevLett.124.110502.

[103] P. W. Shor.
Algorithms for quantum computation: discrete logarithms and factoring.
In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.
URL https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.123.5183&rep=rep1&type=pdf.

[104] J. A. Smolin, F. Verstraete, and A. Winter.
Entanglement of assistance and multipartite state distillation.
Phys. Rev. A, 72:052317, Nov 2005.
doi:10.1103/PhysRevA.72.052317.

[105] D. R. Stinson.
Cryptography: theory and practice.
Chapman and Hall/CRC, 2005.

[106] A. Streltsov, G. Adesso, and M. B. Plenio.
Colloquium: Quantum coherence as a resource.
Rev. Mod. Phys., 89:041003, Oct 2017.
doi:10.1103/RevModPhys.89.041003.

[107] A. Streltsov, C. Meignant, and J. Eisert.
Rates of multipartite entanglement transformations.
Physical Review Letters, 125(8):080502, 2020.
URL https://link.aps.org/pdf/10.1103/PhysRevLett.125.080502.

[108] M. Van den Nest, J. Dehaene, and B. De Moor.
Graphical description of the action of local clifford transformations on graph states.
Physical Review A, 69(2):022316, 2004.
doi:10.1103/PhysRevA.69.022316.

[109] M. Van den Nest, J. Dehaene, and B. De Moor.

Local unitary versus local clifford equivalence of stabilizer states.
Physical Review A, 71(6):062323, 2005.
URL https://link.aps.org/pdf/10.1103/PhysRevA.71.062323.

[110] R. Van Meter, T. Satoh, T. D. Ladd, W. J. Munro, and K. Nemoto.
Path selection for quantum repeater networks.
Networking Science, 3(1-4):82–95, 2013.
URL https://link.springer.com/content/pdf/10.1007/s13119-013-0026-2.pdf.

[111] T. B. Wahl, A. Pal, and S. H. Simon.
Efficient representation of fully many-body localized systems using tensor networks.
Physical Review X, 7(2):021018, 2017.
URL https://link.aps.org/pdf/10.1103/PhysRevX.7.021018.

[112] M. Walter, D. Gross, and J. Eisert.
Multipartite entanglement.
Quantum Information: From Foundations to Quantum Technology Applications, pages 293–330, 2016.
URL https://arxiv.org/pdf/1612.02437.

[113] W. K. Wootters and W. H. Zurek.
A single quantum cannot be cloned.
Nature, 299(5886):802–803, 1982.
URL https://www.nature.com/articles/299802a0.pdf.

[114] D. Yang and J. Eisert.
Entanglement combing.
Phys. Rev. Lett., 103:220501, Nov 2009.
doi:10.1103/PhysRevLett.103.220501.

[115] B. Zeng, H. Chung, A. W. Cross, and I. L. Chuang.
Local unitary versus local clifford equivalence of stabilizer and graph states.
Physical Review A, 75(3):032325, 2007.
URL https://link.aps.org/pdf/10.1103/PhysRevA.75.032325.

[116] K. Zetie, S. Adams, and R. Tocknell.
How does a mach-zehnder interferometer work?
Physics Education, 35(1):46, 2000.
URL https://iopscience.iop.org/article/10.1088/0031-9120/35/1/308/pdf.