Quantum Protocols involving Multiparticle Entanglement and their Representations in the zx-calculus.

Anne Hillebrand
University College
University of Oxford

A thesis submitted for the degree of
MSc Mathematics and the Foundations of Computer Science

1 September 2011

Acknowledgements

First I want to express my gratitude to my parents for making it possible for me to study at Oxford and for always supporting me and believing in me. Furthermore, I would like to thank Alex Merry for helping me out whenever I had trouble with `quantomatic`*. Moreover, I want to say thank you to my friends, who picked me up whenever I was down and took my mind off things when I needed it. Lastly I want to thank my supervisor Bob Coecke for introducing me to the subject of quantum picturalism and for always making time for me when I asked for it.*

Abstract

Quantum entanglement, described by Einstein as “spooky action at a distance”, is a key resource in many quantum protocols, like quantum teleportation and quantum cryptography. Yet entanglement makes protocols presented in Dirac notation difficult to follow and check. This is why Coecke nad Duncan have introduced a diagrammatic language for multi-qubit systems, called the red/green calculus or the ZX-calculus [23]. This diagrammatic notation is both intuitive and formally rigorous. It is a simple, graphical, high level language that emphasises the composition of systems and naturally captures the essentials of quantum mechanics. One crucial feature that will be exploited here is the encoding of complementary observables and corresponding phase shifts. Reasoning is done by rewriting diagrams, i.e. locally replacing some part of a diagram. Diagrams are defined by their topology only; the number of inputs and outputs and the way they are connected. This exemplifies the ‘flow’ of information.

For protocols involving multipartite entangled states, such as the Greenberger-Horne-Zeilinger and W-state, it will be shown that the ZX-calculus provides a relatively easy and more intuitive presentation. Moreover, in this representation it is easier to check that protocols are correct. Protocols that will be discussed in detail are quantum teleportation, quantum cryptography, leader election, superdense coding and quantum direct communication with multipartite entangled states.

Contents

List of Figures

Anyone who is not shocked by the quantum theory has not understood it.

Niels Bohr (1885-1962)

1 Introduction

The reader is assumed to be familiar with Dirac notation, for an introduction see [33].

1.1 Quantum vs. Classical

Quantum computing and information differ from classical computing and information in a few prominent ways. First, contrary to classical bits, not any arbitrary quantum state can be duplicated; the no cloning theorem [70] states that non-orthogonal states cannot be copied. Another key difference is the indistinguishability of non-orthogonal states. Unlike classical bits that are either 0 or 1, a qubit (qutrit etc.) can be any (normalised) complex vector. However, upon measurement a qubit collapses to one of the states in the measurement basis. So even though there are infinitely many possible qubits (qutrits etc.) they can only be distinguished if they are orthogonal. For example $|0\rangle$ and $|1\rangle$ can be identified.

Entanglement, described by Einstein as “spooky action at a distance”, is another resource that quantum computing has and classical computing lacks. When two ore more particles are entangled, their measurement outcomes are correlated, even when they are not physically together [70]. This is called non-locality [68, 71]. Entanglement is a key resource in many quantum protocols, like quantum teleportation [70] and quantum cryptography [7] and it is partly responsible for the exponential speedup in quantum computing [54].

1.2 Quantum Picturalism

Quantum protocols are usually described in Dirac notation. Though such a presentation works, it is low-level and therefore not a very intuitive formalism. For example, quantum teleportation was only discovered in 1993 [8], more than ten years after the idea of a quantum computer was introduced by Feynman [38]. The passage to an high level language was realized in [1], by relying on the compositional structure of monoidal categories. Corresponding intuitive presentations result in the form of quantum picturalism in [21, 22, 23, 28], which relies on the diagrammatic presentation of symmetric monoidal categories, tracing back to Penrose [72, 53, 77].

This diagrammatic notation is both intuitive and formally rigorous. It is a simple, graphical, high level language that emphasises the composition of systems and naturally captures the essentials of quantum mechanics. Because of this it has been described as "Kindergarten Quantum Mechanics" [21]. One crucial feature that will be exploited here is the encoding of complementary observables and corresponding phase shifts. Reasoning is done by rewriting diagrams, i.e. locally replacing some part of a diagram. Diagrams are defined by their topology only; the number of inputs and outputs and the way they are connected. This exemplifies the 'flow' of information. In this dissertation different quantum protocols are presented in the diagrammatic language called the ZX-calculus [22]. The ZX-calculus has been tested before on protocols such as teleportation and entanglement swapping, but it has never been applied on so many protocols involving multipartite entangled states. Furthermore, it was never applied on security protocols. Additionally, although some previous research has gone into the representation of the W-state, this representation was never used in relation to quantum protocols, as is done in this dissertation.

1.3 Quantomatic

In response to the development of the ZX-calculus researchers from Google, Edinburgh, Cambridge and Oxford have been developing a software tool called `quantomatic` to automate reasoning in the ZX-calculus [57] It is used in this dissertation to produce graphical proofs and check derivations.

It should be noted that `quantomatic` is still in its development stage. Being the first non-developer user of this software tool, part of the author's time was spent in developer meetings and a workshop to provide feedback and make suggestions.

1.4 Quantum teleportation

Quantum teleportation is one of the most striking phenomena in quantum computing. In quantum teleportation an unknown state is transmitted from the sender Alice to the receiver Bob without the propagation of the state through the intervening space. Instead, it is sent through a quantum channel, with the aid of some classical information. It was first presented in [8] with EPR pairs. Since then many protocols have followed [3, 17, 34, 29, 89, 67, 51, 91, 61, 79, 80, 20, 81]. In Chapter 5 and 7 the graphical representation of some teleportation protocols with the GHZ and W-state is explored [51, 45, 5, 74, 42].

1.5 Quantum Cryptography and Quantum Direct Communication

In this society it is becoming more and more important to be able to communicate privately. People don't want other people to be able to eavesdrop on the information being exchanged. There are a lot of classical cryptography protocols, but the most well-known and widely used is probably public key cryptography. The security of this protocol depends on the fact that there is no known classical algorithm that can factor a large prime in polynomial time [76]. The fact that Shor's factoring algorithm would be able to do just this, makes a lot of people afraid of the realisation of quantum computers [70]. Quantum mechanics however provides an even better alternative for classical cryptography: quantum key distribution (also called quantum cryptography) and quantum direct communication. Key distribution is not unknown in classical protocols; it was first introduced by Shamir in [78] in 1979. The advantage that quantum key distribution and quantum direct communication protocols have over classical systems is that eavesdropping is either not possible or can be detected easily. This is due to the no cloning theorem, uncertainty principle, indistinguishability of non-orthogonal states and non-locality of entanglement [70].

The first quantum key distribution protocol was proposed by Bennett and Brassard in [7] in 1984 and is generally referred to as the BB84 protocol. After that many other protocols have been proposed [37, 9, 6, 48, 66, 47, 69, 74, 20, 81]. In Chapter 5 and 7 the diagrammatic notation of some quantum key distribution protocols with the Greenberger-Horne-Zeilinger (GHZ) or the W-state is discussed [5, 45, 50, 32, 55]. The difference between quantum key distribution and quantum direct communication (QDC) is that for the latter secure communication can take place without first sharing a key to encrypt the message. The first QDC protocol with EPR pairs was proposed by Boström in 2002 and is generally referred to as the "Ping-Pong" protocol [12], though this has been proven to be insecure. [31, 14, 15]. In Chapter 6 and 8 QDC protocols with the GHZ and W-state are presented int he ZX-calculus [60, 59, 40, 90, 39, 46, 65, 16, 16, 84, 62, 64].

1.6 Some Definitions

These definitions will be used throughout the dissertation:

Definition 1. *A quantum protocol consists of two parts, the* **set of instructions** *and the* **desired behaviour***. The set of instructions are the things to be done to achieve the desired behaviour, i.e the goal of the protocol.*

Definition 2. *A quantum protocol is considered to be* **correct** *or* **valid** *if the set of instructions implies the desired behaviour.*

Definition 3. *The* **GHZ state** *and the* **W-state** *refer to* $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ *and* $|W_3\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$*, unless otherwise indicated.*

Definition 4. Measurement into the x-basis *gives outcome* $|x^+\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ *or* $|x^-\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$*.* **Measurement into the y-basis** *gives outcome* $|y^+\rangle = |i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$ *or* $|y^-\rangle = |-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$*.* **Measurement into the z-basis** *gives outcome* $|z^+\rangle = |0\rangle$ *or* $|z^-\rangle = |1\rangle$*.*

1.7 Outline

In Chapter 2 the necessary category theoretical background will be given. Then the diagrammatic language for Symmetric Monoidal categories will be introduced in Chapter 3. In Chapter 4 the red/green calculus will be explained, which will be used in later chapters to prove the correctness of quantum protocols. In Chapter 5 and 6 the graphical representation of quantum cryptography, superdense coding, teleportation and quantum direct communication with GHZ will be explored. In Chapter 7 and 8 the diagrammatic notation of leader election, key distribution, teleportation and quantum direct communication with W is described. In the final Chapter 9 teleportation of multiparticle states is presented in the ZX-calculus.

I would like to make a confession which may seem immoral: I do not believe absolutely in Hilbert space any more.

John Von Neumann
(1903-1957)

2 Monoidal Categories and other useful things

This chapter gives a brief category theory background, on which quantum picturalism is based. For more information see [27, 73, 58, 2, 28] or [22].

First the algebra of an autoshop will be discussed, then categories and monoids will be introduced. Thirdly, functors, natural transformations and adjoints will be reviewed and finally different kinds of monoidal categories will be explained.

2.1 Algebra, processes and broken cars

Consider an object of a certain type and call it A. Types of food could for example be a raw potato or a cooked carrot. Types of vehicles could be a red car or a blue motorcycle. Now let A be a red broken car and B be a red car in working order. There are several different ways to go from a broken car to a car in working order. You can for example bring the car to a workplace, call the AA or fix the car yourself. These are three different processes to go from one type A, red broken car, to another type B, red car in working order. These processes will respectively be called f, f_1 and f_2 and be represented by arrows. This gives

$$A \xrightarrow{f} B \qquad A \xrightarrow{f_1} B \qquad A \xrightarrow{f_2} B.$$

Now suppose the car needs to get a new colour; it was red before and and it needs to be blue. Let the process of spraying a car blue be denoted by g and a blue car in working order be C. Then $B \xrightarrow{g} C$ denotes the process to go from a red car in working order, to a blue car in working order. Doing g after f is called sequential composition and will be denoted by $\circ$. Note that when sequentially composing two processes, the process appearing on the right is applied first.

$$A \xrightarrow{g} B \xrightarrow{f} C = A \xrightarrow{g \circ f} C. \tag{2.1}$$

The process of doing nothing to an object in state X is denoted by $X \xrightarrow{1_X} X$. Naturally it follows that for any process w, $X \xrightarrow{w} Y$, $1_Y \circ w = w \circ 1_X = w$. Now imagine the red broken car in the shop. Of course it is not the only vehicle in the shop. Let D be a blue motorcycle in working order and let h, $D \xrightarrow{h} E$ be the process of giving a motorcycle new tires. Assuming there is more than one workman in the autoshop, these two processes can be done simultaneously. This is called parallel composition and will be denoted by $\otimes$. Thus

$$A \otimes D \xrightarrow{f \otimes h} B \otimes E. \tag{2.2}$$

Let k, $E \xrightarrow{k} F$ be the process of spraying a blue motorcycle red. If we sequentially compose this with h, the putting on of new tires, it can be parallel-composed with Eq. 2.2, to get

$$A \otimes D \xrightarrow{(g \circ f) \otimes (k \circ h)} C \otimes F. \tag{2.3}$$

However, parallel composing g and k gives $B \otimes E \xrightarrow{g \otimes k} C \otimes F$, sequentially composing this with Eq. 2.1 gives

$$A \otimes D \xrightarrow{f \otimes h} B \otimes E \xrightarrow{g \otimes k} C \otimes F = A \otimes D \xrightarrow{(g \otimes k) \circ (f \otimes h)} C \otimes F. \tag{2.4}$$

Sequential compositions can be seen as “after” and the parallel composition as “while” or “and”. Then obviously spraying a car red and a motorcycle blue after repairing the former and putting new tires on the latter, is the same as spraying the car red after repairing it and spraying the motorcycle red after putting new tires on. Thus

$$(g \circ f) \otimes (k \circ h) = (g \otimes k) \circ (f \otimes h). \tag{2.5}$$

This result is grounded in the properties of sequential composition and parallel composition. Such an intuitive notion of sequential composition and parallel composition, is what part of the diagrammatic language is based on. This collection of processes and types in the autoshop will be called **Autoshop**.

2.2 Groups, Vector Spaces and other Categories

A category is formally defined as Def. 5.

Definition 5. *A* ***category*** $\mathcal{C}$ *consists of*

1. *a collection of objects Ob($\mathcal{C}$), denoted by $A, B, C, ..$;*
2. *a collection Ar($\mathcal{C}$) of morphisms or arrows between the objects Ob($\mathcal{C}$), denoted by $f, g, h, ..$;*
3. *functions dom, cod: Ar($\mathcal{C}$) $\rightarrow$ Ob($\mathcal{C}$), assigning to each arrow f a domain dom(f) and a codomain cod(f). Arrow f with domain A and codomain B is written $f : A \rightarrow B$. For each pair of objects the set $\mathcal{C}(A, B) := \{f \in Ar(\mathcal{C}) | f : A \rightarrow B\}$ is defined, (sometimes referred to as hom(A, B)) and*

4. *for every three objects A, B and C, a binary operation $\mathcal{C}(A, B) \times \mathcal{C}(B, C) \to \mathcal{C}(A, C)$ called composition of morphisms; the composition of $f : A \to B$ and $g : B \to C$ is written as $g \circ f$ or gf (Some authors write fg or $f;g$ to keep things in the order in which they are applied; this will not be done here.),*

such that the following axioms hold:

1. *(associativity) if $f : A \to B$, $g : B \to C$ and $h : C \to D$ then $h \circ (g \circ f) = (h \circ g) \circ f$ and*
2. *(identity) for every object X, there exists an identity morphism $1_X : X \to X$ (or id_X), such that for every morphism $f : A \to B$, $1_B \circ f = f = f \circ 1_A$ holds.*

In the next section some examples of categories will be given.

2.2.1 Some examples of categories

A well known and often used example of a category is the category **Set**:

Example 1. ***Set*** *is the category of all sets and functions between sets as arrows. Composition is function composition and the identity arrow is the identity function.*

1. *Objects in* ***Set*** *are sets.*
2. *An arrow is a function $f : A \to B$ from set A to B.*
3. *The domain of function $f : A \to B$ is set A and the codomain is set B.*
4. *Composition of the functions $f : A \to B$ and $g : B \to C$ is the function $g \circ f : A \to C$.*

Furthermore composition of functions is associative and for mapping $f : A \to B$ and identity mapping $1_A : A \to A$, $1_A \circ f = f = f \circ 1_A$.

Another much used example is the category **Grp**, which is the category of all groups. For a formal definition of a group, the reader is referred to [44, 27, 2].

Example 2. ***Grp*** *is the category of all groups, with groups as objects, group-homomorphisms as arrows, function composition and identity functions. This is a category, because the composition of group-homomorphisms is a group-homomorphism and identity functions are group-homomorphisms too.*

Additionally, finite dimensional vector spaces over the field $\mathbb{K}$ form the category $\mathbf{FdVect}_{\mathbb{K}}$. For a formal definition of a vector space the reader is referred to [44, 27, 2].

Example 3. ***FdVect***$_{\mathbb{K}}$ *is the category of finite dimensional vector spaces over the field* $\mathbb{K}$*, with vector spaces over the field* $\mathbb{K}$ *as objects, linear maps as morphisms, function composition and identity functions. Two linear maps indeed form a new linear map and the identity functions are linear maps as well.*

Revisiting **Autoshop** from Sec. 2.1 will reveal that this is a category too.

Example 4. ***Autoshop*** *is the category of types and processes in the autoshop. The objects are different types of vehicles and the morphisms are the process to go from one type of vehicle to another. Composition of arrows is the composition of processes, which by its nature is associative. The identity is the process of doing nothing.*

Other examples include:

- **Top**: Category of small topological spaces and continuous maps as morphisms.
- **Mon**: Category of all monoids (see Def. 6) and monoid homomorphisms as arrows.
- **FdHilb**: Category of finite dimensional Hilbert spaces and linear maps as morphisms.
- **Pos**: Category of all partially ordered sets and order-preserving functions as arrows

Definition 6. *A* ***monoid*** $(M, \otimes, e)$ *is an underlying set* M *equipped with a binary operation* $- \otimes - : M \times M \to M$ *such that* $\forall x, y, z \in M$*,* $(x \otimes y) \otimes z = x \otimes (y \otimes z)$ *and a unit element* e*, such that* $\forall x \in M$*,* $e \otimes x = x = x \otimes e$*. A* ***monoid homomorphism*** *from* $(M, \otimes, e)$ *to* $(M', \otimes', e')$ *is a function* $f : M \to M'$ *such that* $f(e) = e$ *and* $f(x \otimes y) = f(x) \otimes' f(y)$*.*

For example $(\mathbb{N}, +, 0)$ and strings with string concatenation are monoids. Monoidal categories will play an important role later on.

2.2.2 Some finite examples: diagrams

There are also some interesting finite categories.

Example 5. *The category* ***0*** *has no objects or arrows, vacuously forfilling all conditions*

Example 6. ***1*** *is the category with one object* A *and one arrow: the identity arrow* 1_A*, satisfying the identity and associativity requirements. This category can be seen in Fig. 2.1 (a).*

Example 7. *The category* ***2*** *has two objects,* A *and* B*, two identity arrows,* 1_A *and* 1_B*, and one arrow,* $f : A \to B$*. It is easy to see that the associativity rules are satisfied. A diagrammatic representation can be seen in Fig. 2.1(b).*

$$\begin{tikzcd}
A \arrow[loop above, "1_A"]
\end{tikzcd}$$

(a)

$$\begin{tikzcd}
A \arrow[loop above, "1_A"] \arrow[r, "f"] & B \arrow[loop above, "1_B"]
\end{tikzcd}$$

(b)

$$\begin{tikzcd}
 & B \arrow[loop above, "1_B"] \arrow[dr, "g"] & \\
A \arrow[loop above, "1_A"] \arrow[ur, "f"] \arrow[rr, "h"'] & & C \arrow[loop above, "1_C"]
\end{tikzcd}$$

(a)

Figure 2.1: The categories **1**, **2** and **3** in order of appearance.

Example 8. *3 is the category with three objects, A, B and C, three identity arrows, $1_A, 1_B$ and 1_c, and three non-identity arrows, $f : A \to B$, $g : B \to C$ and $h : A \to C$ as can be seen in Fig. 2.1(c). As composition can only be defined in a single way, the associativity conditions are forfilled.*

2.3 Functors, Natural Transformations and Adjoints

Definition 7. *Let $\mathcal{C}, \mathcal{D}$ be categories. A **covariant functor** $F : \mathcal{C} \to \mathcal{D}$ is a map taking each object $A \in \mathcal{C}$ to an object $F(A) \in \mathcal{D}$. and each morphism $f : A \to B \in \mathcal{C}$ to a morphism $F(f) : F(A) \to F(B) \in \mathcal{D}$, such that $\forall A \in \mathcal{C}$ and composable arrows $f, g \in \mathcal{C}$ we have $F(1_A) = 1_{F(A)}$ and $F(g \circ f) = F(g) \circ F(f)$. A **contravariant functor** is one that maps objects to objects, but maps morphisms to morphisms going in the opposite direction, i.e. reverses all arrows.*

Definition 8. *An **opposite category** $\mathcal{C}^{op}$ of a category $\mathcal{C}$ is the category with the same objects as in $\mathcal{C}$, the same identities, but with all the morphisms reversed, such that $f^{op} \circ g^{op} = (g \circ f)^{op}$.*

$$\begin{tikzcd}
F(A) \arrow[r, "\eta_A"] \arrow[d, "F(f)"'] & G(A) \arrow[d, "G(f)"] \\
F(B) \arrow[r, "\eta_B"] & G(B)
\end{tikzcd}$$

Figure 2.2: A natural transformation.

Definition 9. *Let $\mathcal{C}, \mathcal{D}$ be categories and let F, G be functors from $\mathcal{C}$ to $\mathcal{D}$. A **natural transformation** $\eta : F \dot{\to} G$, is a function, which assigns to every object $A \in \mathcal{C}$ a morphism*

$\eta_A : F(A) \to G(A) \in \mathcal{D}$, such that for any morphism $f : A \to B \in \mathcal{C}$ the diagram in Fig. 2.2 commutes. If each component η_A of η is an isomorphism in $\mathcal{D}$, then η is a ***natural isomorphism****.*

2.4 Different kinds of Monoidal categories

A monoidal category is defined as follows:

Definition 10. *A monoidal category $\mathcal{C} = \{\mathcal{C}, \otimes, e, \alpha, \lambda, \rho\}$ is a category $\mathcal{C}$, a bifunctor $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$, an object $e \in \mathcal{C}$ and three natural isomorphisms α, λ, ρ such that*

1. *$\forall A, B, C \in \mathcal{C}, \alpha = \alpha_{A,B,C} : A \otimes (B \otimes C) \simeq (A \otimes B) \otimes C$ is a natural isomorphism and Fig. 2.3 commutes $\forall A, B, C, D \in \mathcal{C}$;*
2. *$\lambda = \lambda_A : e \otimes A \simeq a$ and $\rho = \rho_A = A \otimes e \simeq a$ are natural isomorphisms $\forall A \in \mathcal{C}$, such that Fig 2.4 commutes $\forall A, C \in \mathcal{C}$ and*
3. *$\lambda_e = \rho_e : e \otimes e \to e$ [58].*

$$\begin{tikzcd}
A \otimes (B \otimes (C \otimes D)) \arrow[d, "1 \otimes \alpha"] & (A \otimes B) \otimes (C \otimes D) \arrow[l, "\alpha"'] & ((A \otimes B) \otimes C) \otimes D \arrow[l, "\alpha"'] \\
A \otimes ((B \otimes C) \otimes D) \arrow[rr, "\alpha"] & & (A \otimes (B \otimes C)) \otimes D \arrow[u, "\alpha \otimes 1"']
\end{tikzcd}$$

Figure 2.3: Commuting diagram for a monoidal category.

$$\begin{tikzcd}
A \otimes (e \otimes C) \arrow[r, "\alpha"] \arrow[d, "1 \otimes \lambda"] & (A \otimes e) \otimes C \arrow[d, "\rho \otimes 1"] \\
A \otimes C \arrow[r, phantom, "="] & A \otimes C
\end{tikzcd}$$

Figure 2.4: Another commuting diagram for a monoidal category.

Furthermore, a strict monoidal category is a monoidal category for which the natural isomorphisms α, λ and ρ are identities.

Definition 11. *A* ***strict monoidal category*** *is a category $\mathcal{C}$ for which:*

1. *objects are associated with an associative bifunctor with a unit: ($\mathcal{C}$, $\otimes$,I), i.e.* $\forall A, B, C, \in \mathcal{C}$*,* $A \otimes (B \otimes C) = (A \otimes B) \otimes C$ *and* $I \otimes A = A = A \otimes I$*;*
2. *morphisms are associated with an associative bifunctor with a unit:* $\forall f : A \to B, g : C \to D \in \mathcal{C}$*,* $f \otimes g : A \otimes C \to B \otimes D \in \mathcal{C}$*, such that* $f \otimes (g \otimes h) = (f \otimes g) \otimes h$ *and* $1_I \otimes f = f = f \otimes 1_I$*;*
3. *when* $f' \circ f$ *and* $g' \circ g$ *are defined* $(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g)$ *and*
4. $\forall A, B \in \mathcal{C}$*,* $1_A \otimes 1_B = 1_{A \otimes B}$*.*

Theorem 1. *Every monoidal category is equivalent to a strict monoidal category [23, 58].*

However, (strict) symmetric monoidal categories will be considered mostly.

Definition 12. *A* ***(strict) symmetric monoidal category*** *is a (strict) monoidal category* $\mathcal{C}$ *in addition to a family of isomorphisms called symmetries* $\{A \otimes B \xrightarrow{\sigma_{A,B}} B \otimes A | A, B \in \mathcal{C}\}$*, such that* $\forall A, B \in \mathcal{C}$ $\sigma^{-1}_{A,B} = \sigma_{A,B}$ *and* $\forall A, B, C, D \in \mathcal{C}$ *and if* f, g *can be composed the diagram in Fig. 2.5 commutes, i.e. if* $\sigma_{C,D} \circ (f \otimes g) = (g \otimes f) \circ \sigma_{A,B}$*.*

$$\begin{tikzcd}
A \otimes B \arrow[r, "\sigma_{A,B}"] \arrow[d, "f \otimes g"'] & B \otimes A \arrow[d, "g \otimes f"] \\
C \otimes D \arrow[r, "\sigma_{C,D}"] & D \otimes C
\end{tikzcd}$$

Figure 2.5: A strict symmetric monoidal category

$$\begin{tikzcd}
A \arrow[r, "\rho_A"] \arrow[d, "1_A"] & A \otimes I \arrow[r, "1_A \otimes \eta_A"] & A \otimes (A^* \otimes A) \arrow[d, "\alpha_{A,A^*,A}"] \\
A & I \otimes A \arrow[l, "\lambda_A^{-1}"'] & (A \otimes A^*) \otimes A \arrow[l, "\epsilon_A \otimes 1_A"']
\end{tikzcd}$$

Figure 2.6: A commuting diagram for a compact category

Definition 13. *A* ***compact closed category*** $\mathcal{C}$ *is a symmetric monoidal category in which every object* $A \in \mathcal{C}$ *comes with another object* A^**, the* ***dual*** *of* A *and a pair of morphisms* $I \xrightarrow{\eta_A} A^* \otimes A$ *and* $A \otimes A^* \xrightarrow{\epsilon_A} I$*, respectively called* ***unit*** *and* ***counit****, such that Fig. 2.6 and 2.7 commute. [27]*

$$\begin{tikzcd}
A^* \arrow[r, "\lambda_{A^*}"] \arrow[d, "1_{A^*}"] & I \otimes A^* \arrow[r, "\eta_A \otimes 1_{A^*}"] & (A^* \otimes A) \otimes A^* \arrow[d, "\alpha^{-1}_{A^*,A,A^*}"] \\
A^* & A^* \otimes I \arrow[l, "\rho^{-1}_{A^*}"'] & A^* \otimes (A \otimes A^*) \arrow[l, "1_{A^*} \otimes \epsilon_A"']
\end{tikzcd}$$

Figure 2.7: Another commuting diagram for a compact category

Definition 14. *A* ***A dagger compact category*** *$\mathcal{C}$ is both a compact closed category and a dagger symmetric monoidal category, such that $\forall A \in \mathcal{C}, \epsilon_A = \eta_A \circ \sigma_{A,A^*}$. [27]*

Example 9. *The category* ***FdHilb*** *is a dagger compact category.*

Definition 15. *A* ***dagger symmetric monoidal category*** *is a symmetric monoidal category $\mathcal{C}$ which also has a dagger category structure such that $\forall f : A \to B, g : C \to D$, where $A, B, C \in Ob(\mathcal{C})$,*

1. $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger : B \otimes D \to A \otimes C$;
2. $\alpha^\dagger_{A,B,C} = \alpha^{-1}_{A,B,C} : (A \otimes B) \otimes C \to A \otimes (B \otimes C)$;
3. $\rho^\dagger_A = \rho^{-1}_A : A \otimes I \to A$;
4. $\lambda^\dagger_A = \lambda^{-1}_A : I \otimes A \to A$ *and*
5. $\sigma^\dagger_{A,B} = \sigma^{-1}_{A,B} : B \otimes A \to A \otimes B$.

α, λ, ρ and σ are the natural isomorphisms from the symmetric monoidal structure.

Definition 16. *A* ***strict dagger monoidal category*** *$\mathcal{C}$ is a strict monoidal category equipped with an involutive identity-on-objects contravariant functor $\dagger : \mathcal{C}^{op} \to \mathcal{C}$, such that $\forall A \in \mathcal{C}\ A^\dagger = A \quad , \forall f \in \mathcal{C}\ f^{\dagger\dagger} = f$ and $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$. Let $f^\dagger : B \to A$ be the* ***adjoint*** *of $f : A \to B$. A* ***strict dagger symmetric monoidal category*** *$\mathcal{C}$ is both a strict dagger monoidal category and a strict symmetric monoidal category, such that $\sigma^\dagger_{A,B} = \sigma^{-1}_{A,B}$.*

Definition 17. *An arrow $U : A \to B$ in a strict dagger monoidal category $\mathcal{C}$ is* ***unitary*** *if its inverse and adjoint are the same, i.e. if $U^\dagger = U^{-1}$*

These different kinds of monoidal categories will be used as a basis for the graphical calculus in Chapter 3.

A picture is worth a thousand words.

Proverb

3 Diagrammatic Language for Symmetric Monoidal Categories

In this chapter a diagrammatic language for symmetric monoidal categories (SMCs) is introduced. For a more complete and detailed explanation, see [27, 28, 21, 23] or [22].

A diagrammatic language for SMCs will be presented in the first section. This graphical calculus will be extended to Dagger Symmetric Monoidal Categories (†-SMCs) in the final section. At the end of this section it will be graphically shown that the teleportation protocol works.

3.1 Graphical Calculus for Symmetric Monoidal Categories

In this section the graphical calculus for symmetric monoidal categories will be introduced and its merits will be explained.

3.1.1 Characteristics of the graphical calculus for SMCs

In the graphical calculus all parts of a SMC have a graphical counterpart that is both intuitive and informative. Additionally, its coherence properties are very often trivial or a tautology. Most importantly Theorem 2 holds, which states that equations in SMCs follow from the axioms of SMCs if and only if it is derivable in the graphical calculus.

3.1.2 Graphical counterparts of SMCs

The **identity** 1_I is the empty picture.

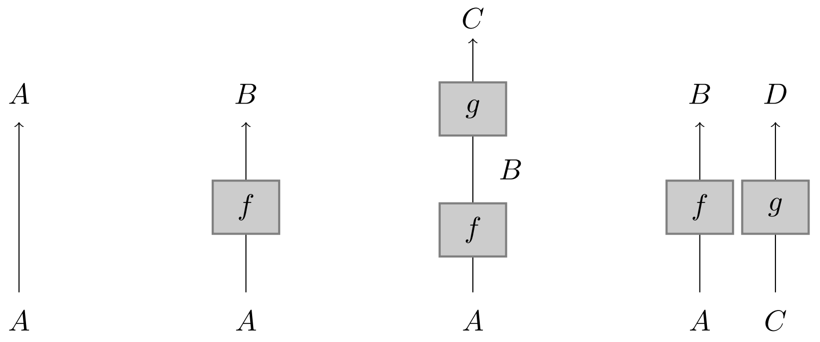
The **identity** 1_A for object $A \neq I$ is depicted as an arrow from A to A.

A **morphism** $f : A \to B$ is depicted as an arrow with a box from A to B.

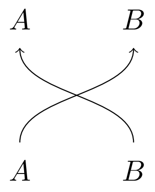
The **composition** $g \circ f$ of morphisms $f : a \to B$ and $g : B \to C$ is depicted by pasting g above f, connecting the output of f to the input of g.

The **tensor product** $f \otimes g$ of morphisms $f : A \to B$ and $g : C \to D$ is depicted by pasting g to the right of f.

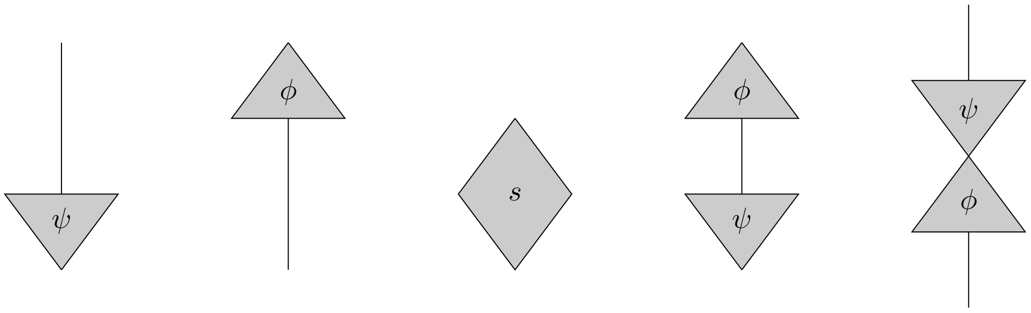
In order of appearance, identity 1_A, morphism $f : A \to B$, composition $g \circ f$ and $f \otimes g$:



Symmetry $\sigma_{AB} : A \otimes B \to B \otimes A$ is depicted as crossing wires:



The morphisms $|\psi\rangle : I \to A$, $\langle\phi| : A \to I$, $s : I \to s$, $\langle\phi \mid \psi\rangle : I \to s$ and $|\psi\rangle\,\langle\phi| : A \to I \to A$ are respectively depicted as



3.1.3 Properties of the graphical calculus

In this section some properties of the graphical calculus will be described.

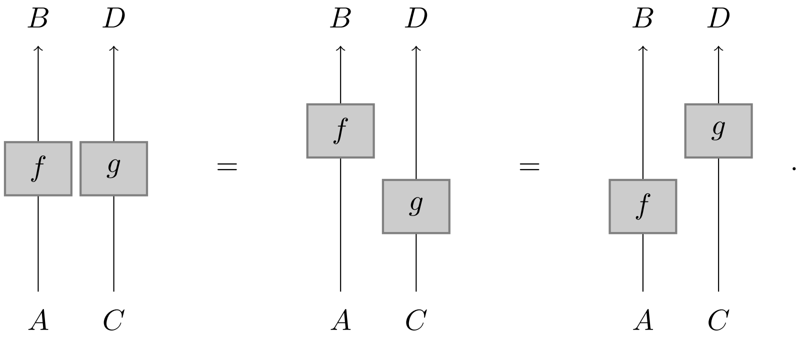
Definition 18. *An **isomorphism of diagrams** is a bijective correspondence between boxes and wires, which preserves the manner in which boxes and wires are connected. Equality of diagrams will be used to denote isomorphic diagrams.*

Theorem 2. *The graphical calculus for symmetric monoidal categories is such that an equational statement between formal expressions in the language of symmetric monoidal categories holds if and only if it holds up to an isomorphism of diagrams in the graphical calculus [52].*

For example

$$f \otimes g = (f \otimes 1_D) \circ (1_A \otimes g) = (1_B \otimes g) \circ (f \otimes 1_C), \tag{3.1}$$

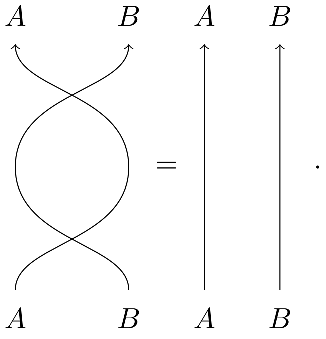
which holds in any strict monoidal category, is depicted as



The self-adjointness of symmetry on the other hand

$$\sigma_{B,A} \circ \sigma_{A,B} = 1_{A,B}, \tag{3.2}$$

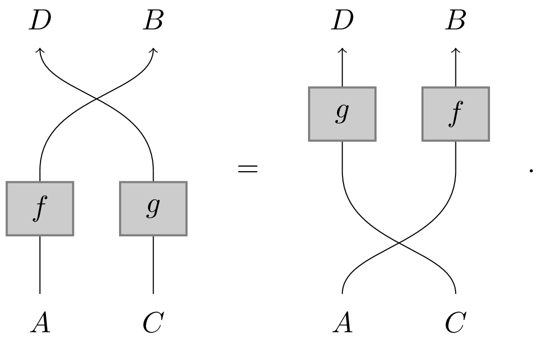
is easily depicted as



Finally the defining equation of symmetry

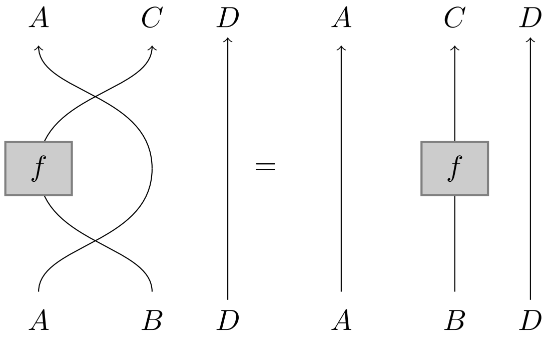
$$\sigma_{B,D} \circ (f \otimes g) = (g \otimes f) \circ \sigma_{A,C} \tag{3.3}$$

depicts as



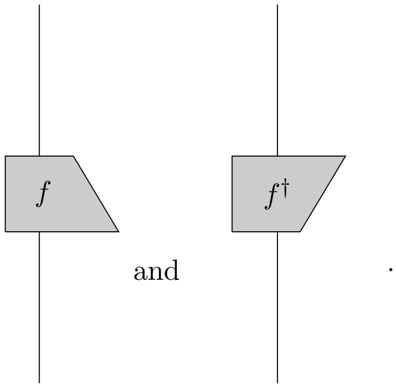
From this it can be deduced that boxes can "slide" along wires.

To rewrite a graph, parts of a graph are replaced on which a specific axiom applies. For example in $(\sigma_{CA} \circ (f_{B,C} \otimes 1_A) \circ \sigma_{AB}) \otimes 1_D$, the part $\sigma_{CA} \circ (f_{BC} \otimes 1_A) \circ \sigma_{AB}$ can be rewritten as $1_A \otimes f_{B,C}$, as long as inputs and outputs are connected to the corresponding inputs and outputs:



3.2 Graphical Calculus for Dagger Symmetric Monoidal Categories

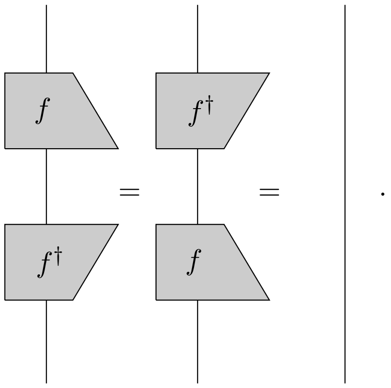
Theorem 2 extends to dagger symmetric monoidal categories (†-SMCs), as proven by Selinger in [77]. The adjoint is represented by vertical reflection. Now the boxes should be asymmetric. Morphisms $f : A \to B$ and $f^\dagger : B \to A$ are depicted as



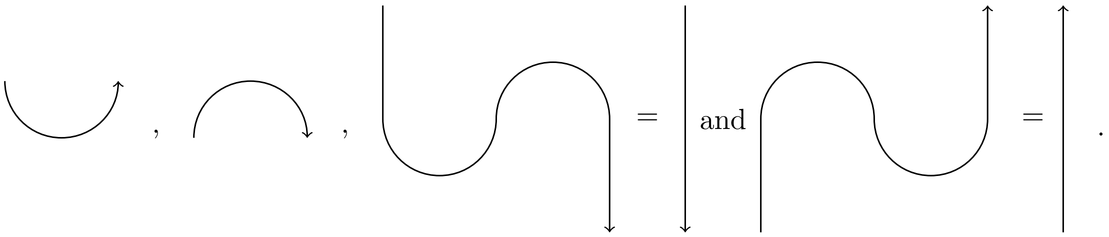
Furthermore

$$f \circ f^\dagger = f^\dagger \circ f = I \tag{3.4}$$

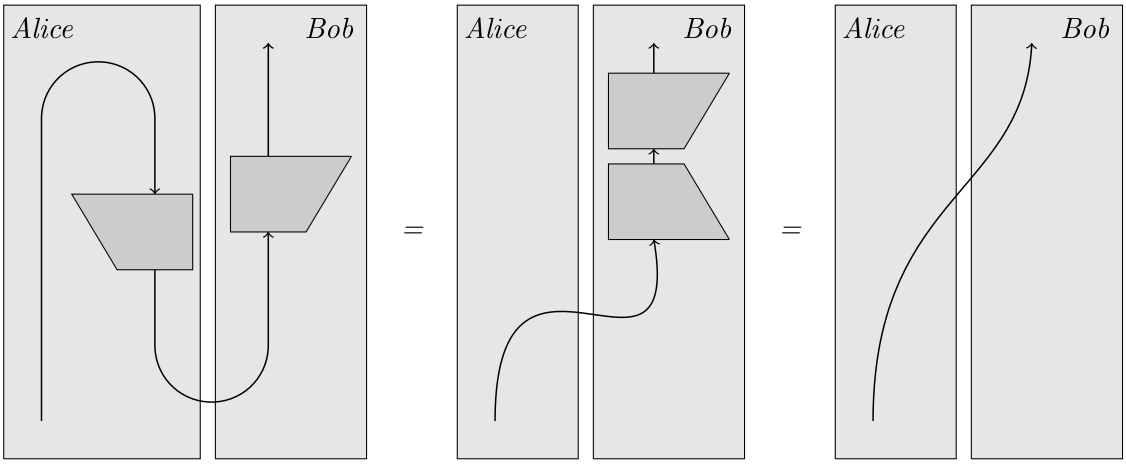
is



Moreover, the unit η_A (a cup) and co-unit ϵ_A (a cap) and their compositions $\eta_A \circ \epsilon_A$ and $\epsilon_A \circ \eta_A$ are



Example 10. *Taking Bell states as units composed with a unitary operation and Bell effects as co-units composed with a unitary operation, gives all the tools to display* ***Quantum Teleportation****. For a more elaborate description of the teleportation protocol see [70]. In the teleportation protocol, Alice and Bob teleport an unknown state from Alice to Bob by means of a shared Bell state, a Bell state measurement and a unitary operation. Now let the trapezium be the unitary operation involved. When sliding the unitary along the wire, it turns upside down and meets its adjoint. Eq. 3.4 states that they cancel each other out. So that part of the graph can be replaced. Composing a cup and a cap gives a straight line, so that part of the graph can be replaced as well. Now it has been shown graphically that the teleportation protocol works. The specifics are shown below.*



These are two very basic graphical language, but even rewriting with just these few axioms is quite powerful, as became clear in the previous example. This is the model that the ZX-calculus is based on. It works by the same principles, but is a little more elaborate. The ZX-calculus is described in Chapter 4.

Complementarity is when a red spider meets a green spider and its legs fall off.

Bob Coecke (1968-?)

4 The Red/Green Calculus

In this chapter the red/green calculus or the ZX-calculus is introduced. For a more thorough and complete presentation see [56, 24] or [23][1]. The highlights of these papers are explained here and expanded upon. Original work includes derivations of the basic rules and the graphical representation of measurement into different bases, $(-)i\sigma_y$ and the creation of entangled states.

First the different components of the ZX-calculus will be explained, then the basic rules and some derivations are presented. Thirdly, measurement into different bases is described. Finally some useful facts are given.

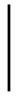
4.1 Components of the zx-calculus

The ZX-calculus consists of components joined by wires, like an electrical circuit. Its components are the following:

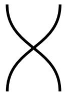
1. Z-vertices (green dots), labeled by an angle $\alpha \in [0, 2\pi)$, called the phase, with any number of inputs and or outputs, zero included.
2. X-vertices (red dots), complementary to the Z-vertices, labeled by a phase, also with any number of inputs, including none.
3. H-vertices (yellow squares labeled with an H), which represent Hadamard gates. They have exactly one input and one output.
4. $\sqrt{D}$-vertices (black diamonds), which represent scalars. These don't have any inputs or outputs.

The Hilbert space interpretation of these components is as as follows:

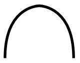
[1] Pictures from this paper are included with permission of the author.



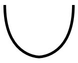
$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$



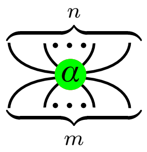
$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$



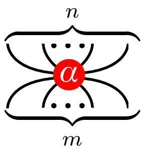
$$= |00\rangle + |11\rangle$$



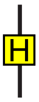
$$= \langle 00| + \langle 11|$$



$$:: \begin{cases} \overbrace{|0\ \dots\ 0\rangle}^{n} & \mapsto & \overbrace{|0\ \dots\ 0\rangle}^{m} \\ |1\ \dots\ 1\rangle & \mapsto & e^{i\alpha}\,|1\ \dots\ 1\rangle \\ \text{others} & \mapsto & 0 \end{cases}$$

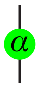


$$:: \begin{cases} \overbrace{|+\dots+\rangle}^{n} & \mapsto & \overbrace{|+\dots+\rangle}^{m} \\ |-\dots-\rangle & \mapsto & e^{i\alpha}\,|-\dots-\rangle \\ \text{others} & \mapsto & 0 \end{cases}$$

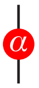


$$= \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

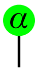
$$= \sqrt{2}$$



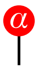
$$= Z_1^1(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$



$$= X_1^1(\alpha) = e^{-i\alpha/2} \begin{pmatrix} \cos\frac{\alpha}{2} & i\sin\frac{\alpha}{2} \\ i\sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} \end{pmatrix}$$



$$= |0\rangle + e^{i\alpha}\,|1\rangle$$



$$= \cos\tfrac{\alpha}{2}\,|0\rangle + i\sin\tfrac{\alpha}{2}\,|1\rangle$$

And the definition of adjoints and inner products:

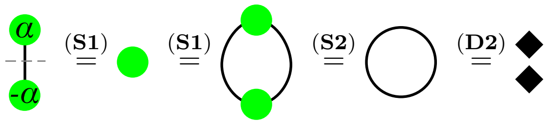
Definition 19. *Let $\mathfrak{D} : m \to n$ be a diagram; then its adjoint, $\mathfrak{D}^\dagger : n \to m$, is a diagram constructed by reflecting $\mathfrak{D}$ in the horizontal axis, and negating all the phases which occur in $\mathfrak{D}$.*

Definition 20. *Let $\mathfrak{A} : 0 \to n$ be a diagram and $\mathfrak{B} : 0 \to n$. Note that these form a n-qubit state in Hilbert space. Their inner product*

$$\langle \mathfrak{A} \mid \mathfrak{B} \rangle = \mathfrak{A}^\dagger \circ \mathfrak{B}\,.$$

is defined as the adjoint of $\mathfrak{A}$ composed with $\mathfrak{B}$, resulting in a diagram without any inputs or outputs; a complex scalar.

Example 11. *The inner product of $Z_1^0(\alpha)$ with itself can be computed in this fashion.*



The result is 2 because in the graphical calculus normalisation is left out.

4.2 The Rules

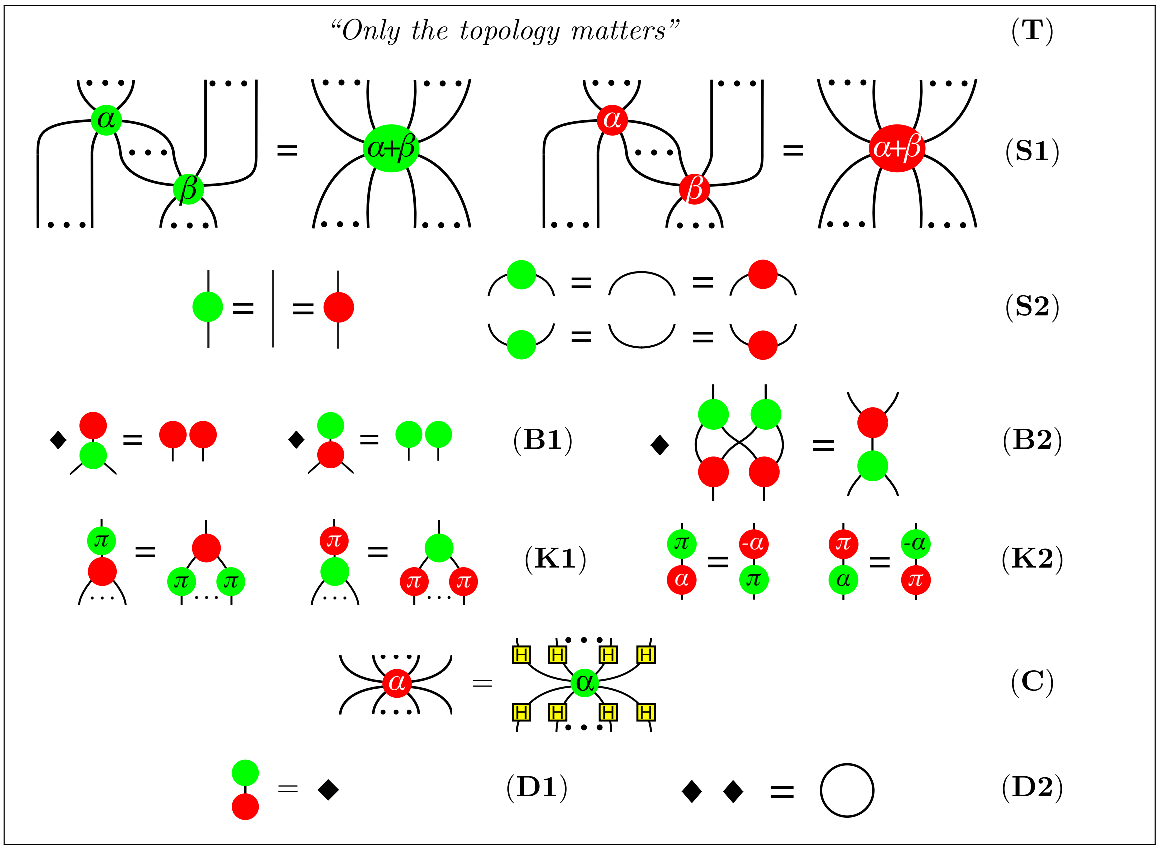


Figure 4.1: Basic Rules for the ZX-calculus

4.2.1 Quantomatic

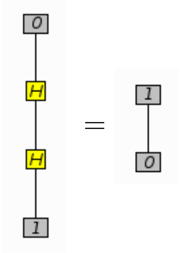
From now on all the pictures (except Fig. 4.1) are made with `quantomatic` [57], a software tool for reasoning with the ZX-calculus. Different rule sets can be loaded into `quantomatic`. One can then input a graph and see what rewrites are possible with the loaded rules. Download and installation instructions can be found at `http://sites.google.com/site/quantomatic/home`.

In `quantomatic` red and green dots are displayed as red and green dots, with their phase in a box of corresponding colour underneath the vertex. Hadamard gates are displayed as yellow boxes with an *H* in them. Finally, inputs and outputs are displayed as grey boxes with a number in it, called boundary vertices. `Quantomatic` does not distinguish between inputs and outputs; they look the same and are numbered with the same counter. E.g. a diagram with one input and one output would have one boundary vertex with the number zero and one with the number one in it.

4.2.2 Basic Rules

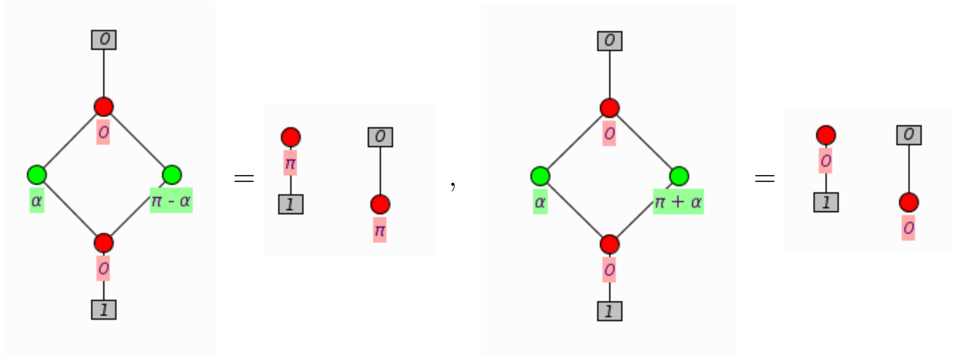
Derivations in the Red/Green-calculus are done mostly by a few simple rules, outlined in Fig. 4.1. Note that **T** does not mean that the topology is always preserved; other rules might change this completely. Informally **T** can be seen as “yanking” the wires, making sure the number of inputs and outputs is preserved and the way they are connected.

The self-adjointness of the Hadamard gate can be inferred by doubly applying (**C**), but will be treated as a separate rule:



(**H**)

An addition to these rules has been made by Kissinger in [56] and Coecke and Edwards in [24]. These two related rules that are called $|0\rangle$- and $|1\rangle$- supplementarity were found by solving a matrix equation in [56] and by means of the underlying algebraic structure in [24].



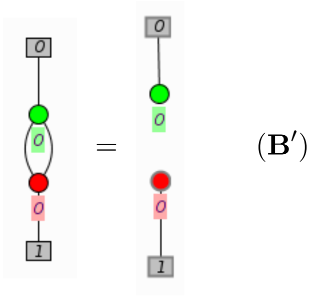
(**E**) .

From now on scalars will be left out for sake of simplicity. Note also that `quantomatic` does not include scalars in the rewrites.

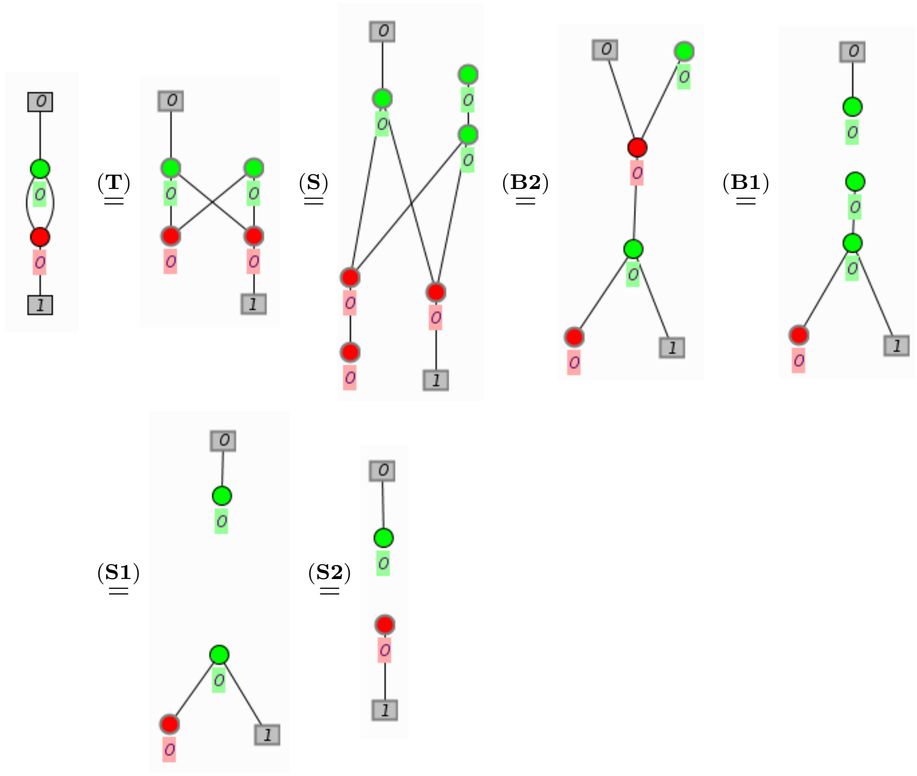
4.2.3 Some useful derivations from the Basic rules

Some useful rules can be derived from the basic rules.

Lemma 3 (Hopf law).



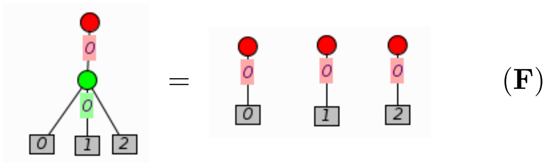
Proof.



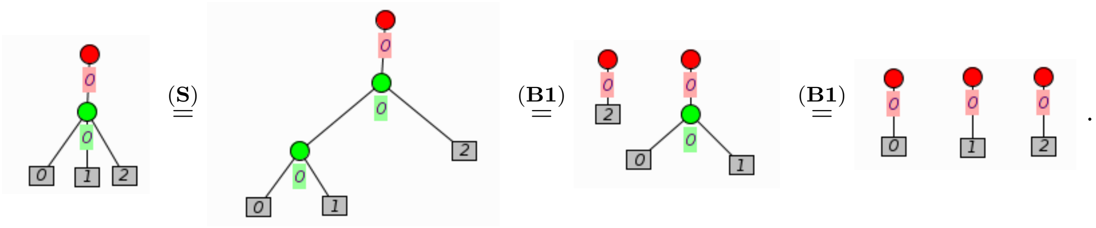
(4.1)

□

Lemma 4.



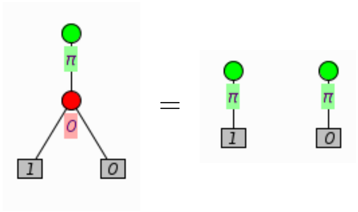
Proof.



(4.2)

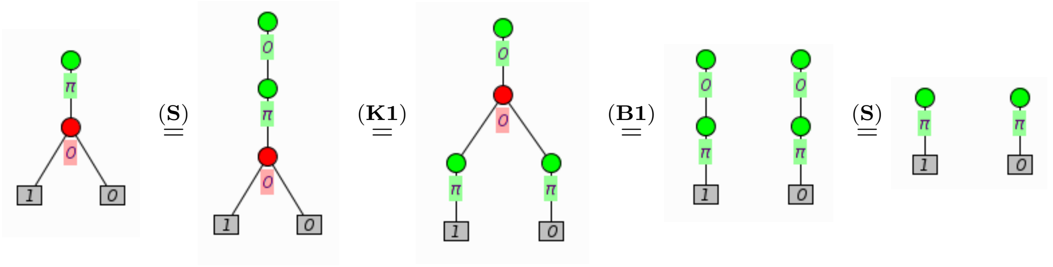
□

Lemma 5.



(**M**)

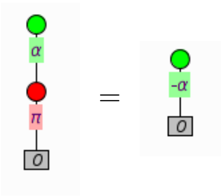
Proof.



(4.3)

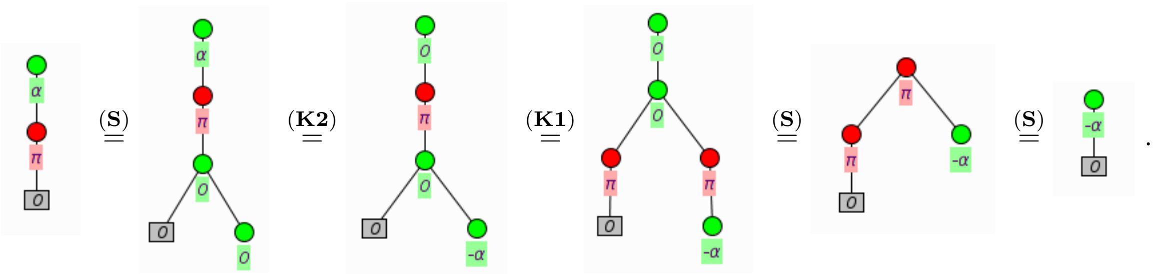
□

Lemma 6.



(**A**)

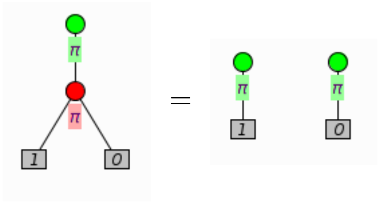
Proof.



(4.4)

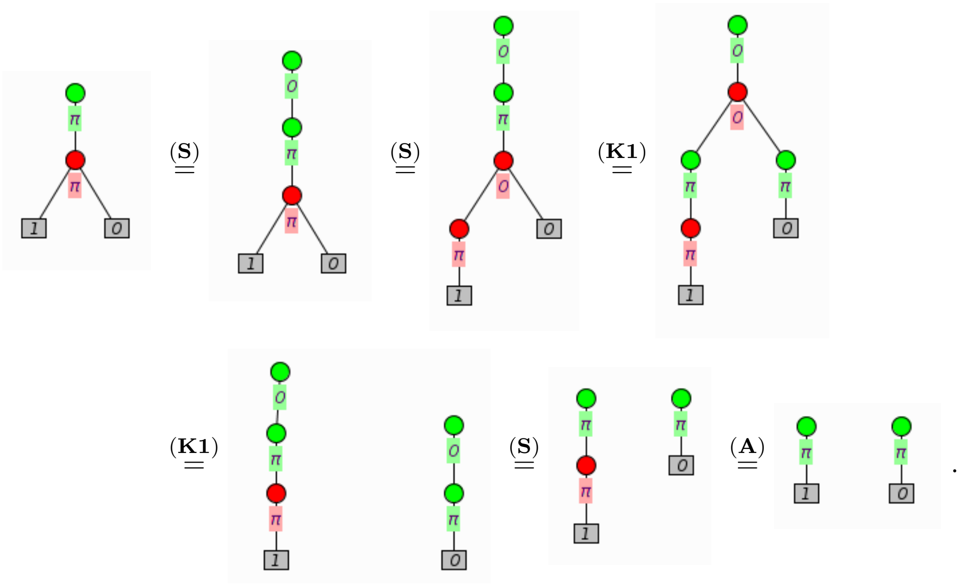
□

Lemma 7.



(**Z′**)

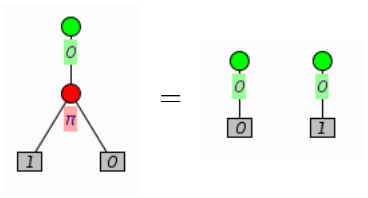
Proof.



(4.5)

□

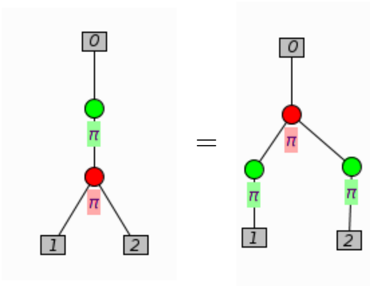
Lemma 8.



(**Z**)

Proof. As Lemma 7. □

Lemma 9.



(**K′**)

Proof. As Lemma 7. □

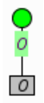
Note that each of these rules naturally also works with the colours reversed. These derivations can be loaded as rules in `quantomatic` [57], to make the simplifications of the diagrams faster. These rules will be used throughout this dissertation and be referenced by name, rather than by lemma.

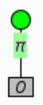
4.3 Measurements into different bases

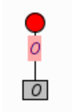
A quantum state can be measured into different bases. In this section the x-, y- and z-measurements will be explained in addition to Bell state measurements.

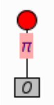
4.3.1 Measurements into the x- and z-basis

Measurements or "effects" into the x- and z-basis can be derived by the Hilbert space interpretation of points. $|+\rangle$ $(|x^+\rangle)$ and $|-\rangle$ $(|x^-\rangle)$ and $|0\rangle$ $(|z^+\rangle)$ and $|1\rangle(|z^-\rangle)$ are represented as



$= |+\rangle$


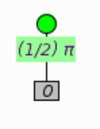
$= |-\rangle$


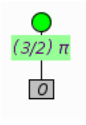
$= |0\rangle$


$= |1\rangle$. (4.6)

4.3.2 Measurements into the y-basis

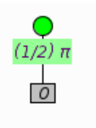
Another measurement basis is the y-basis. $|i\rangle = |y^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$ and $|-i\rangle = |y^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$, which can be found with the Hilbert space interpretation mentioned earlier. Then

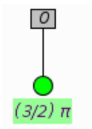
$|y^+\rangle =$


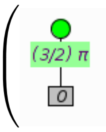
$|y^-\rangle =$


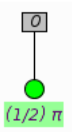
. (4.7)

Note that unlike $|x^\pm\rangle$ and $|z^\pm\rangle$, $|y^\pm\rangle$ is not its own adjoint. Instead we have:

$\langle y^+| = \Bigg($


$\Bigg)^\dagger =$


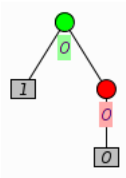
$\langle y^-| = \Bigg($


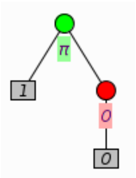
$\Bigg)^\dagger =$


. (4.8)

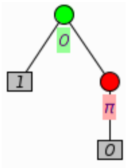
4.3.3 Measurements into the Bell Basis

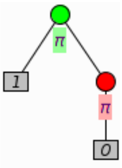
The four Bell states look as follows:

$|\phi^+\rangle =$


$= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ $|\phi^-\rangle =$


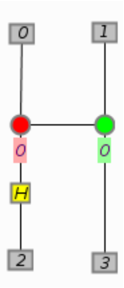
$= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ (4.9)

$|\psi^+\rangle =$


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


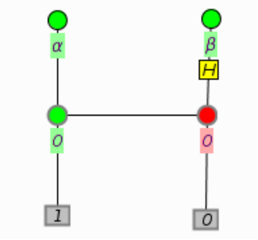
$= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$ (4.10)

Note that they are their own adjoints, so flipping from a cap to a cup and vice versa, will not change the phases. When doing a Bell state measurement, one of the four Bell states is obtained. The circuit to measure into the Bell basis is [23, 13]

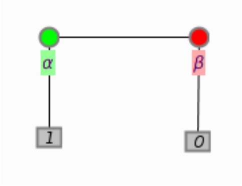


, (4.11)

which gives two qubits in the z-basis. Turning the circuit upside down and plugging two states in the z-basis, we obtain for $\alpha, \beta \in \{0, \pi\}$



$\overset{(\mathbf{S}),(\mathbf{C})}{=}$



,

which results in one of the four Bell states by Eq. 4.9 and 4.10.

4.4 Some useful facts

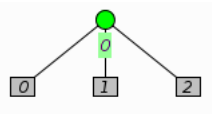
In this section some facts are presented, that will be needed later on.

4.4.1 The GHZ state

The GHZ state is one of the only two SLOCC-inequivalent classes of tripartite entanglement [35]. SLOCC-inequivalent means inequivalent under Stochastic Local Operations and Classical Communication, i.e. one cannot be turned into the other by means of stochastic local operations (unitaries and or measurements) and classical communication. GHZ is defined as $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, or as the map

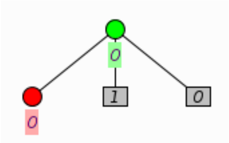
$$GHZ :: \begin{cases} |0\rangle \mapsto |00\rangle \\ |1\rangle \mapsto |11\rangle \, . \end{cases}$$

Graphically it is represented as [23]

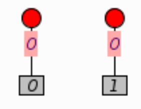


. (4.12)

Plugging $|0\rangle$ and $|1\rangle$ gives

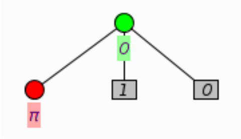


$\overset{(\mathbf{B1})}{=}$

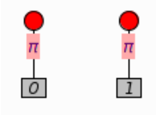


$= |00\rangle$ (4.13)

and



$\overset{(\mathbf{Z}')}{=}$



$= |11\rangle\,,$ (4.14)

as required.

4.4.2 The W-state

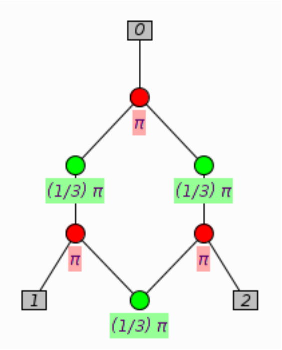
The class of W-states is SLOCC-inequivalent to the class of GHZ states [35]. The W-state is defined as

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle),$$

or as the map [56]

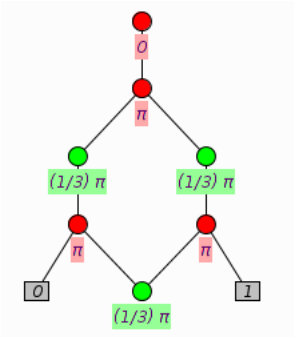
$$W :: \begin{cases} |0\rangle \mapsto |01\rangle + |10\rangle \\ |1\rangle \mapsto |00\rangle\,. \end{cases}$$

Considering this map, the W-state can be graphically represented as [56]

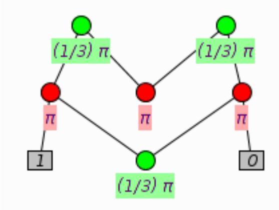


. (4.15)

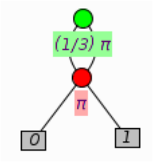
This graphical representation shows the robustness of the W-state; due to the pairwise entanglement, after tracing out one of the qubit, there is still the possibility of bipartite entanglement, as opposed to the GHZ state, which is fully separable when any of the qubits is traced out. Plugging $|0\rangle$ in Eq. 4.15 gives



$\overset{(\mathbf{S1})}{=}$

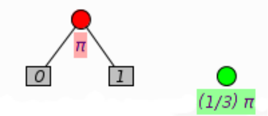


$\overset{(\mathbf{K2}),(\mathbf{S})}{=}$



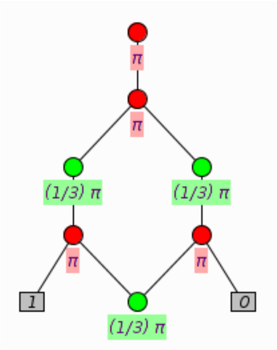
(4.16)

$\overset{(\mathbf{B'})}{=}$

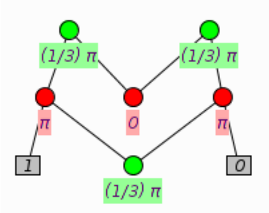


$= |01\rangle + |10\rangle\,,$ (4.17)

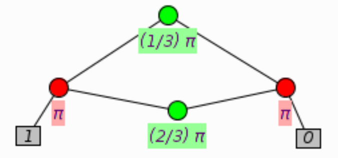
as expected. Plugging $|1\rangle$ in Eq. 4.15 gives



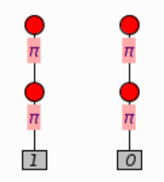
$\overset{(\mathbf{S1})}{=}$



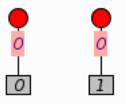
$\overset{(\mathbf{S})}{=}$



$\overset{(\mathbf{E})}{=}$

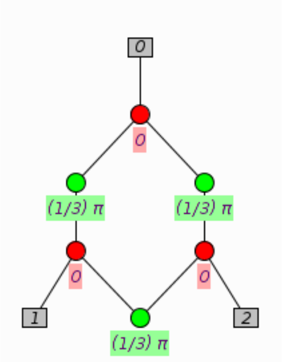


$\overset{(\mathbf{S1})}{=}$



$= |00\rangle\,,$ (4.18)

as required. Similarly one can define the opposite state $|W_{op}\rangle = \frac{1}{\sqrt{3}}(|110\rangle + |101\rangle + |011\rangle)$. Graphically this is

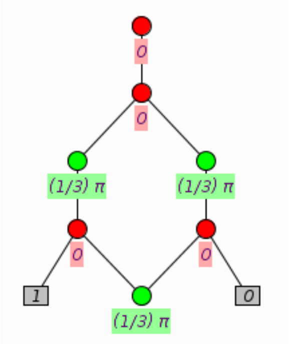


. (4.19)

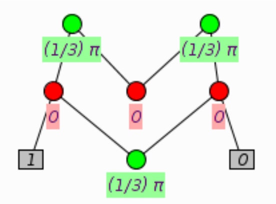
The mapping is

$$W :: \begin{cases} |0\rangle \mapsto |11\rangle \\ |1\rangle \mapsto |10\rangle + |01\rangle \,. \end{cases} \qquad .$$

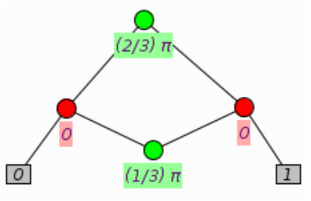
And plugging gives



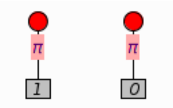
$\overset{(\mathbf{S1})}{=}$



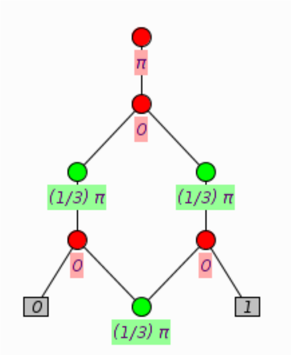
$\overset{(\mathbf{S})}{=}$



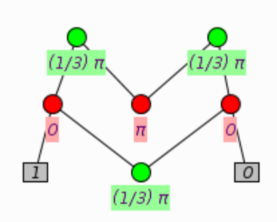
$\overset{(\mathbf{E})}{=}$



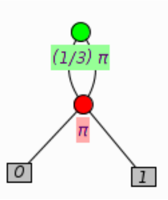
$$= |11\rangle \,, \tag{4.20}$$



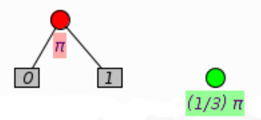
$\overset{(\mathbf{S1})}{=}$



$\overset{(\mathbf{S})}{=}$



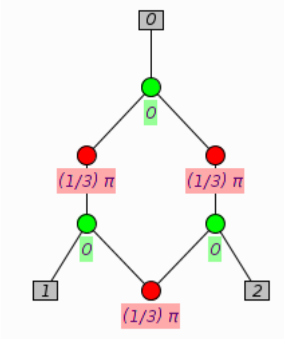
$\overset{(\mathbf{E})}{=}$



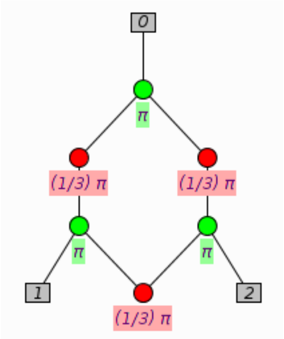
$$= |10\rangle + |01\rangle \,, \tag{4.21}$$

as expected. Likewise one can find the graphical representation of $|W_+\rangle = \frac{1}{\sqrt{3}}(|++-\rangle + |+-+\rangle + |-++\rangle)$ and $|W_-\rangle = \frac{1}{\sqrt{3}}(|--+\rangle + |-+-\rangle + |+--\rangle)$ as

$|W_+\rangle =$



$|W_-\rangle =$

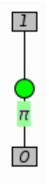


.

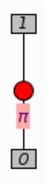
4.4.3 Pauli-Matrices

By the Hilbert space interpretation of the ZX-calculus one can obtain the Pauli-Z and Pauli-X matrices:

$\sigma_z =$



$= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \sigma_x =$

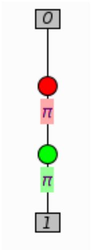


$= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$

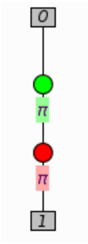
Considering the measurement bases from the previous section, another way to derive the Pauli-matrices is by considering their behaviour. The Z-matrix can be derived by considering its behaviour with respect to the x- and y- basis. The σ_z-matrix flips points in both x- and y-basis from plus to minus and vice versa. Because this constitutes adding π to the green phase, it follows that σ_z can be represented by $Z_1^1(\pi)$. In an equal fashion for σ_x and the z-basis; σ_x flips the z-basis from one to the other and can thus be represented by $X_1^1(\pi)$.

Once the Pauli-X and Z matrices are known, it is easily deduced that $i\sigma_y = \sigma_z \times \sigma_x = Z \circ X$ and $-i\sigma_y = \sigma_x \times \sigma_z = X \circ Z$ are compositions of X_1^1 and Z_1^1.

$i\sigma_y =$



$= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad -i\sigma_y =$



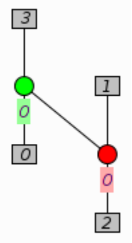
$= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$

4.4.4 Controlled Not gate

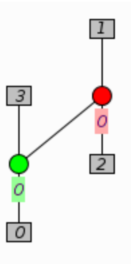
Another useful tool is the Controlled Not gate. There are two ways to deduce the graphical representation of this gate. The first one is by looking at its matrix representation and deducing it from there. Secondly it can be done by looking at its behavioural specifications.

The Controlled Not gate is defined as follows:

CNOT $=$

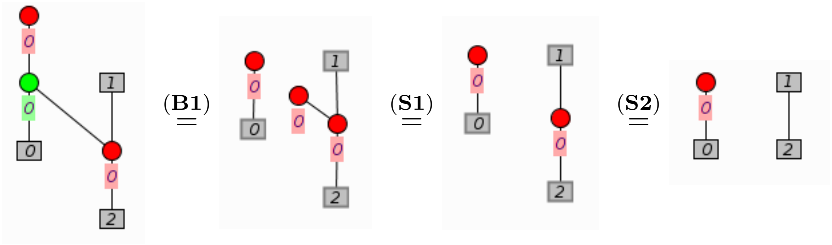


$=$



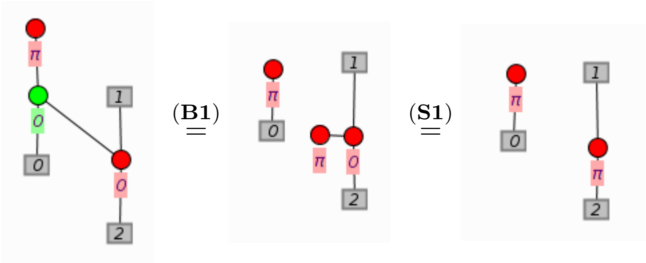
$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{4.22}$$

In a controlled not gate the target qubit (boundary vertex 1) is negated if the control input (boundary vertex 3) is $|1\rangle$. It is left unchanged when the target qubit is $|0\rangle$. The control qubit is always left unchanged. The process of checking the behaviour of an operator by means of inputs is called plugging. For input $|0\rangle$ one has



. (4.23)

So in this case both inputs stay unchanged. For input $|1\rangle$ one has



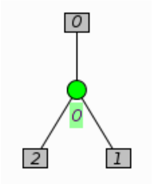
, (4.24)

which leaves the first input unchanged and negates the target input as required.

4.4.5 Using the Controlled Not gate to create EPR pairs

Lemma 10. *Let* $|\psi_a\rangle = a\,|0\rangle + b\,|1\rangle$*, where* $|a|^2 + |b|^2 = 1$*. Then*

$$\mathbf{CNOT}(|\psi_a\rangle \otimes |0\rangle) = a\,|00\rangle + b\,|11\rangle = \tag{4.25}$$

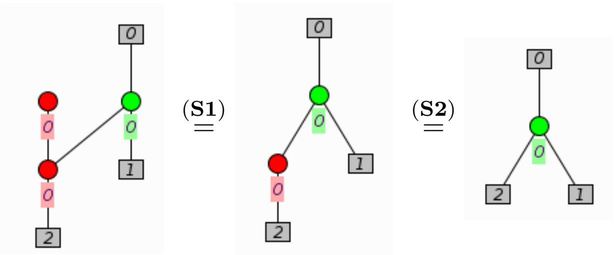


.

Proof.

$$\begin{aligned}\mathbf{CNOT}(|\psi_a\rangle \otimes |0\rangle) &= \mathbf{CNOT}(a\,|00\rangle + b\,|10\rangle)\\ &= \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}\begin{pmatrix} a\\ 0\\ b\\ 0\end{pmatrix} = \begin{pmatrix} a\\ 0\\ 0\\ b\end{pmatrix} = a\,|00\rangle + b\,|11\rangle\end{aligned}$$

$$= \tag{4.26}$$



.

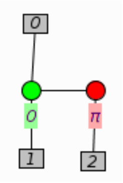
□

Corollary 11. *If* $|\psi_a\rangle = |+(-)\rangle$, *then*

$$\mathbf{CNOT}(|\psi_a\rangle \otimes |0\rangle) = \left|\phi^{+(-)}\right\rangle. \tag{4.27}$$

Lemma 12. *Let* $|\psi_a\rangle$ *be defined as before. Then*

$$\mathbf{CNOT}(|\psi_a\rangle \otimes |1\rangle) = a\,|01\rangle + b\,|10\rangle = \tag{4.28}$$

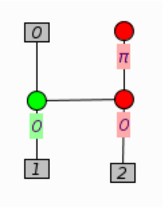


.

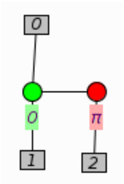
Proof.

$$\begin{aligned}\mathbf{CNOT}(|\psi_a\rangle \otimes |1\rangle) &= \mathbf{CNOT}(a\,|01\rangle + b\,|11\rangle)\\ &= \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0\\ a\\ 0\\ b \end{pmatrix} = \begin{pmatrix} 0\\ a\\ b\\ 0 \end{pmatrix} = a\,|01\rangle + b\,|10\rangle\end{aligned}$$

$$= \tag{4.29}$$



$$\overset{(\mathbf{S1})}{=}$$



□

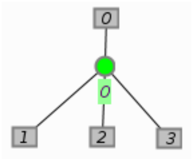
Corollary 13. *If* $|\psi_a\rangle = |+(-)\rangle$, *then*

$$\mathbf{CNOT}(|\psi_a\rangle \otimes |1\rangle) = \left|\psi^{+(-)}\right\rangle. \tag{4.30}$$

4.4.6 Using the Controlled Not gate to create GHZ-like states

Lemma 14. *Let* $|\psi_a\rangle$ *be defined as before. Then*

$$\mathbf{CNOT}_{13}(\mathbf{CNOT}_{12}(|\psi_a\rangle_1 \otimes |0\rangle_2 \otimes |0\rangle_3)) = a\,|000\rangle + b\,|111\rangle = \tag{4.31}$$



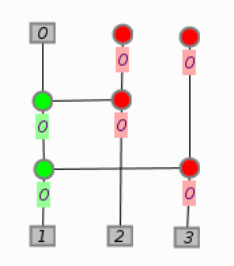
.

Proof.

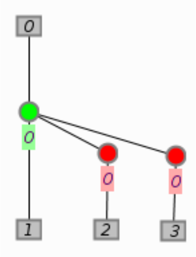
$$\mathbf{CNOT}_{13}(\mathbf{CNOT}_{12}(|\psi_a\rangle_1 \otimes |0\rangle_2 \otimes |0\rangle_3)) = \mathbf{CNOT}_{13}(a\,|000\rangle + b\,|110\rangle)$$

$$= a\,|000\rangle + b\,|111\rangle \tag{4.32}$$

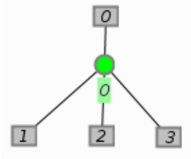
$=$



$\overset{(\mathbf{S1})}{=}$



$\overset{(\mathbf{S2})}{=}$

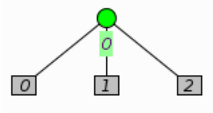


$.$ (4.33)

□

Corollary 15. *If $|\psi_a\rangle = |+\rangle$, then*

$\mathbf{CNOT}_{13}(\mathbf{CNOT}_{12}(|\psi_a\rangle_1 \otimes |0\rangle_2 \otimes |0\rangle_3)) = |GHZ\rangle =$



$.$ (4.34)

Quantum Cryptography is like computing all over again. We cannot possibly tell what the implications may be.

Andrew Hilton, director of CSFI

5 Quantum protocols with GHZ

Different Quantum protocols involving the GHZ and GHZ like states are presented in this chapter. Although the protocols discussed in this chapter are not new themselves, they have never been presented in the ZX-calculus before. Moreover, the ZX-calculus provides and alternative and new way to prove the correctness of these protocols.

First secret key sharing is presented, then quantum secret state sharing. Next the teleportation of EPR is described and finally superdense coding is presented.

5.1 Secret Key Sharing with GHZ

In this section the secret key sharing protocol as described in [45] will be represented in the ZX-calculus. Sometimes this is also called Quantum Cryptography. In the Secret key Sharing protocol Alice shares a key with two or more other people, in such a way that they have to cooperate to retrieve it. This section is broken up in two parts. First, Secret Key sharing with three people will be discussed. Then it will be extended to a protocol with four people. The protocol with four people has never before been discussed in so much detail.

5.1.1 Secret Key Sharing with three people

Suppose Alice, Bob and Charlie each have one particle from a GHZ triplet. Secret Key Sharing can be achieved with the following protocol:

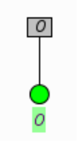
1. Each chooses at random whether to measure their particle in the x- or y-direction and publicly announce this direction.
2. If it is a valid combination of directions, Bob and Charlie can cooperate to obtain the measurement result of Alice, which will be the key. For the combinations see Table 5.1.

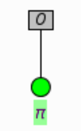
		Alice			
		$\langle x^+\rvert$	$\langle x^-\rvert$	$\langle y^+\rvert$	$\langle y^-\rvert$
Bob	$\langle x^+\rvert$	$\langle x^+\rvert$	$\langle x^-\rvert$	$\langle y^-\rvert$	$\langle y^+\rvert$
	$\langle x^-\rvert$	$\langle x^-\rvert$	$\langle x^+\rvert$	$\langle y^+\rvert$	$\langle y^-\rvert$
	$\langle y^+\rvert$	$\langle y^-\rvert$	$\langle y^+\rvert$	$\langle x^-\rvert$	$\langle x^+\rvert$
	$\langle y^-\rvert$	$\langle y^+\rvert$	$\langle y^-\rvert$	$\langle x^+\rvert$	$\langle x^-\rvert$

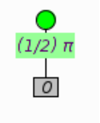
Table 5.1: This table shows Charlie's state, given Alice's and Bob's state.

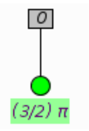
Note that if Charlie measures in the $x(y)$-basis when her state is in a $y(x)$-state, she will not be able to retrieve any information about the state.

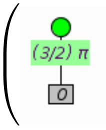
Lemma 16. *The secret sharing protocol as outlined above is a correct protocol.*

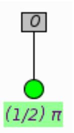
Proof. The protocol is correct, if Table 5.1 can be reproduced by means of the graphical language. Let Alice's measurement result be A and Bob's B. Remember that $\langle x^+| =$ 

, $\langle x^-| =$ 

, $\langle y^+| = \Big($ 

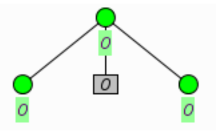
$\Big)^\dagger =$ 

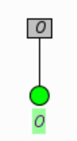
and $\langle y^-| = \Big($ 

$\Big)^\dagger =$ 

.

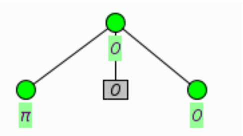
For $A = B = \langle x^+|$

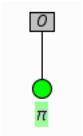


$=$ 

$= \langle x^+| .$ (5.1)

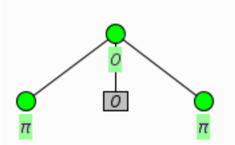
For $A = \langle x^+|$ and $B = \langle x^-|$ and also for $A = \langle x^-|$ and $B = \langle x^+|$

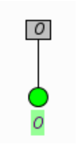


$=$ 

$= \langle x^-| .$ (5.2)

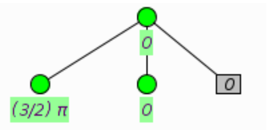
For $A = B = \langle x^-|$

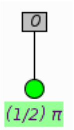


$=$ 

$= \langle x^+| .$ (5.3)

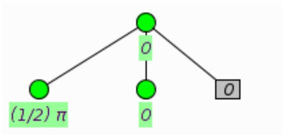
For $A = \langle x^+|$ and $B = \langle y^+|$ and also for $A = \langle y^+|$ and $B = \langle x^+|$



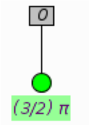
$=$ 

$= \langle y^-| .$ (5.4)

For $A = \langle x^+|$ and $B = \langle y^-|$ and also for $A = \langle y^-|$ and $B = \langle x^+|$

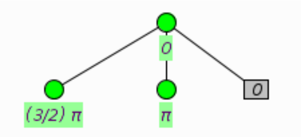


$=$

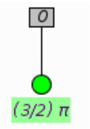


$$= \langle y^+|\,. \tag{5.5}$$

For $A = \langle x^-|$ and $B = \langle y^+|$ and also for $A = \langle y^+|$ and $B = \langle x^-|$

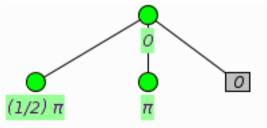


$=$

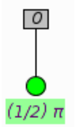


$$= \langle y^+|\,. \tag{5.6}$$

For $A = \langle x^-|$ and $B = \langle y^-|$ and also for $A = \langle y^-|$ and $B = \langle x^-|$

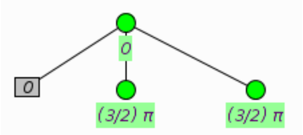


$=$

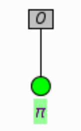


$$= \langle y^-|\,. \tag{5.7}$$

For $A = B = \langle y^+|$

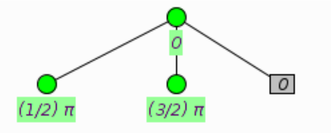


$=$

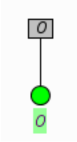


$$= \langle x^-|\,. \tag{5.8}$$

For $A = \langle y^+|$ and $B = \langle y^-|$ and also for $A = \langle y^-|$ and $B = \langle y^+|$

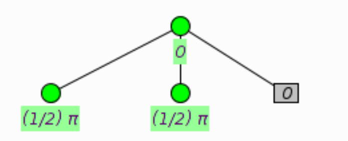


$=$

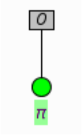


$$= \langle x^+|\,. \tag{5.9}$$

For $A = B = \langle y^-|$



$=$



$$= \langle x^-|\,. \tag{5.10}$$

Eq. 5.1 - 5.10 show that the set of instructions imply the desired behaviour and thus the validity of the protocol. □

5.1.2 Quantum Secret Sharing with four people

Suppose Alice, Bob, Charlie and Dan each have one particle from a four particle GHZ state. Quantum Secret Sharing can be achieved with the following protocol:

1. Each chooses at random whether to measure their particle in the x- or y- direction and communicates this information with Alice.

2. Alice decides whether the overall basis is usable and communicates all the chosen bases to the others. The only invalid basis is when three people measure in the same basis and just one other person in the other basis.
3. If it is a valid basis, Bob, Charlie and Dan can cooperate to obtain Alice's measurement result, by counting the number of minus states occurring in their measurement result.

Lemma 17. *The only invalid basis is when three people measure in one basis and one person measures in the other basis.*

Proof. There are three different possible measurement combinations. The first possibility is that everyone measures in the same basis. Three measurements will determine the final outcome. Once three measurements in the same basis are done, it is obvious that the result will be in the same basis, i.e. it will either be a combination of 0 and π, which by **S** and the adjoint of x will result in 0 or π, or it is a combination of $\pi/2$ and $3\pi/2$ which by **S** and the adjoint of y will result in $\pi/2$ or $3\pi/2$.

The second possibility is that two people measure in one basis and the others in the other basis. Considering three measurements to determine the final outcome again, gives two possibilities. Two x-bases and one y-basis or the other way around. The former is a pair of 0 and/or π and one $\pi/2$ or $3\pi/2$. Obviously **S** yields an outcome in the y-basis. The latter is a combination of a 0 or π and a pair of $\pi/2$ and/or $3\pi/2$. Naturally, **S** gives an outcome in the x-basis.

The final possibility is that three people measure in the same basis and the final person measures in the other basis. However, with the knowledge that three measurements determine the outcome of the final measurement we can conclude from the previous results, that in this case the final measurement will always be done in the opposite basis. Considering that measuring an x-outcome in the y-basis or vice versa will not provide one with any information about the state, it can only be concluded that this is an invalid overall basis. □

Lemma 18. *Overall, there is always an even number of minus states in the measurement outcomes of 4-GHZ if only measured in the x-basis.*

Proof. Let the x-outcomes be α, where $\alpha \in \{0, \pi\}$. Note that α is only equal to π when the outcome is minus. When everything is measured in the x-basis, by **S** and the adjoint of x the outcome $\gamma = \alpha_1 + \alpha_2 + \alpha_3 \pmod{2\pi}$. An odd number of π ($\langle x^-|$-outcomes) makes $\gamma = \pi$ ($\langle x^-|$). An even number of π ($\langle x^-|$) outcomes) gives $\gamma = 0$ ($\langle x^+|$). □

Lemma 19. *Overall, there is always an even number of plus states in the measurement outcomes of 4-GHZ if only measured in the y-basis.*

Proof. Let the y-outcomes be $\pi/2 + \beta$, where $\beta \in \{0, \pi\}$. Note that $\beta = \pi$ only when we obtain outcome $\langle y^+|$. By **S** and the adjoint of y the outcome $\gamma = \pi/2 + \beta_1 + \beta_2 + \beta_3 \pmod{2\pi}$. For an odd number of π ($\langle y^+|$), $\gamma = 3\pi/2$ ($\langle y^+|$). For an even number of π ($\langle y^+|$) $\gamma = \pi/2$ ($\langle y^-|$). □

Lemma 20. *Overall, there are is always an odd number of minus states in the measurement outcomes of 4-GHZ if two particles are measured in the x-basis and two in the y-basis.*

Proof. From previous results we know that any combination of two y-measurements and one x-measurement yields an outcome in the x-basis. By **S** and the adjoint of the x-basis deriving the final outcome is essentially adding up the angles of the other three outcomes. Now let the outcomes be defined as before. Then the final result $\gamma = \pi + \alpha + \beta_1 + \beta_2 \pmod{2\pi}$. Hence, whenever there is an odd number of π occurring $\gamma = 0$, yielding an outcome of $\langle x^+|$. To obtain an odd number of π, either just one α, β_1, β_2 is π, or all three of them are. If $\alpha = \pi$, then $\beta_1 = \beta_2$, which gives an even number of minus states in the y-measurement outcomes, and thus an odd overall number of minus states. If $\alpha = 0$, then $\beta_1 \neq \beta_2$, which gives an odd number minus states in the y-measurements and an odd overall number of minus states. For even numbers of π, $\gamma = \pi$, making the outcome $\langle x^-|$, which yields an odd number of minus states overall by similar logic as above.

On the other hand any combination of two x-measurements and one y-measurement will give an outcome in the y-basis. Setting the x- and y- outcomes as before, by **S** and the adjoint of y we obtain outcome $\gamma = \pi + \pi/2 + \alpha_1 + \alpha_2 + \beta \pmod{2\pi}$. Any odd number of π makes $\gamma = \pi/2$, i.e. $\langle y^-|$. If $\beta = \pi$ ($\langle y^+|$), then $\alpha_1 = \alpha_2$, making the overall number of minus states odd. If $\beta = 0$ ($\langle y^-|$), $\alpha_1 \neq \alpha_2$, which gives an odd overall number of minus states. An even number of π yields $\gamma = 3\pi/2$, i.e. outcome $\langle y^+|$. By similar logic as above it can be shown that this gives an odd overall number of minus states. □

Corollary 21. *Quantum Secret Sharing with 4-GHZ is a valid protocol.*

Proof. Lemma 17-20 show that if it is a valid overall basis, Alice's measurement outcome can be derived from the measurement outcomes of all the others. Note that less than three measurement outcomes, will not give any information on Alice's measurement outcome, still leaving both outcomes equally likely. Thus the set of instructions implies the desired behaviour. □

5.2 Quantum Secret State Sharing or Teleportation through GHZ

In this section the quantum secret state sharing protocol as described in [45, 5, 74] and [42] will be represented in the ZX-calculus. It will be shown that this representation yields the desired behaviour, which proves the correctness of the protocol. In the Secret State Sharing protocol Alice shares an arbitrary quantum state with two or more people in such a way that they have to cooperate to retrieve the state. If one person holds all the shares but Alice's share, this protocol can be seen as teleportation through GHZ. This is described in [55]. Assuming Alice Bob and Charlie share a tripartite GHZ state and Alice has the qubit to be teleported, the quantum secret state sharing protocol can be achieved as follows [45, 5, 74, 42]:

1. Alice makes a measurement in the Bell basis on both her qubits.
2. Bob makes a measurement on his particle in the x-basis.
3. Alice announces her measurement outcome. With this information and Bob's measurement outcome, Charlie knows which local operation to apply on his qubit in order to retrieve the quantum state. The local operations are summarised in Table. 5.2

		Alice			
		$\langle\Phi^+\rvert$	$\langle\Phi^-\rvert$	$\langle\Psi^+\rvert$	$\langle\Psi^-\rvert$
Bob	$\langle x^+\rvert$	I	σ_z	σ_x	$\sigma_x\sigma_z$
	$\langle x^-\rvert$	σ_z	I	$\sigma_x\sigma_z$	σ_x

Table 5.2: This table shows Charlie's local operation, given Alice's and Bob's measurement outcomes.

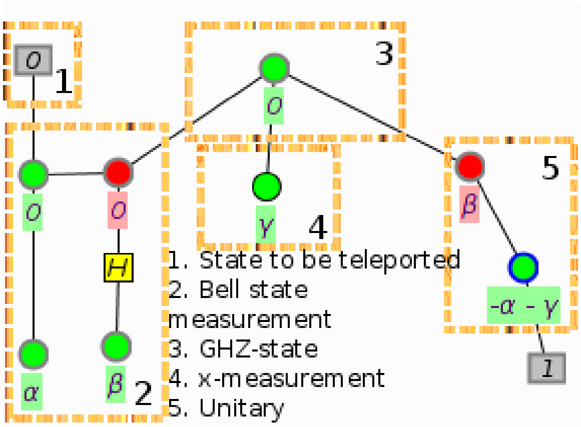


Figure 5.1: Graphical representation of the Quantum Secret State Sharing protocol.

α	β	γ	Bell State	x-state	local operation
0	0	0	$\langle\Phi^+\|$	$\langle x^+\|$	I
0	0	π	$\langle\Phi^+\|$	$\langle x^-\|$	σ_z
0	π	0	$\langle\Psi^+\|$	$\langle x^+\|$	σ_x
0	π	π	$\langle\Psi^+\|$	$\langle x^-\|$	$\sigma_x\sigma_y$
π	0	0	$\langle\Phi^-\|$	$\langle x^+\|$	σ_z
π	0	π	$\langle\Phi^-\|$	$\langle x^-\|$	I
π	π	0	$\langle\Psi^-\|$	$\langle x^+\|$	$\sigma_x\sigma_z$
π	π	π	$\langle\Psi^-\|$	$\langle x^-\|$	σ_x

Table 5.3: Eight possible outcomes of the quantum secret state sharing protocol. $\alpha, \beta, \gamma \in \{0, \pi\}$

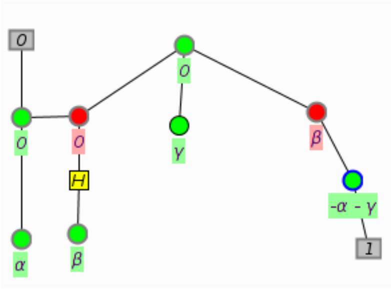
Lemma 22. *Fig. 5.1 is the graphical representation of the set of instructions of the Quantum Secret State Sharing protocol.*

Proof. This representation is obviously a qubit and a GHZ state tensored (box 1 and 3). This qubit and the first qubit of the GHZ state are measured in the Bell basis (box 2), yielding one of the four Bell states as an outcome. The second qubit in the GHZ state is measured in the x-basis (box 4). Then some local operations on the third qubit are performed, consisting of either σ_x, σ_z, none or both (box 5). All that is left to be shown is that different combinations of outcomes, yield the same local operations as in the description of the protocol. There are eight different combinations of outcomes for α, β and γ. In Table 5.3 they are all given together with their meaning. As can be seen, the last three columns reproduce Table 5.2 as expected.

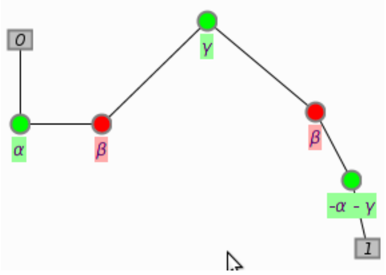
□

Lemma 23. *The quantum secret state sharing protocol is a correct protocol.*

Proof. Showing that for all the entries in Table 5.2 the graphical representation simplifies to a wire proves that the set of instructions implies the desired behaviour and thus the correctness of the protocol. The general representation from Fig. 5.1 can already be simplified:

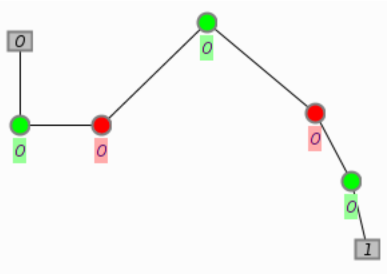


$\overset{(\mathbf{S}),(\mathbf{K2})}{=}$

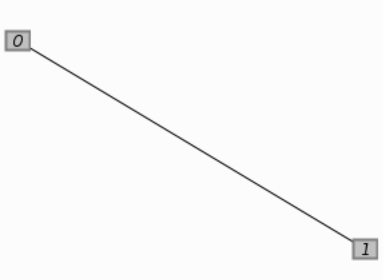


(5.11)

Then for $\alpha = \beta = \gamma = 0$

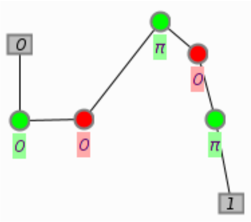


$$\overset{(\mathbf{S})}{=}$$

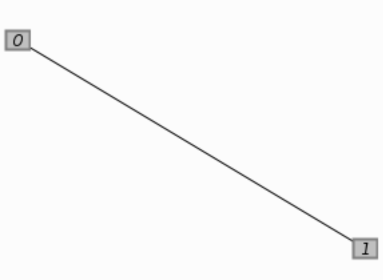


. (5.12)

For $\alpha = \beta = 0$ and $\gamma = \pi$

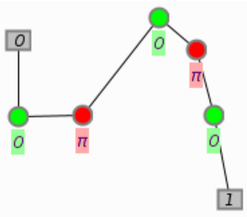


$$\overset{(\mathbf{S})}{=}$$

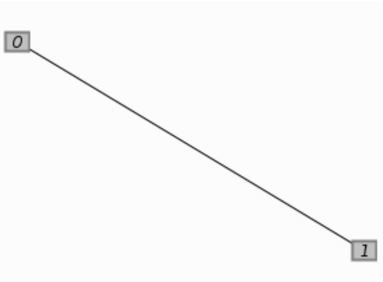


. (5.13)

For $\alpha = \gamma = 0$ and $\beta = \pi$

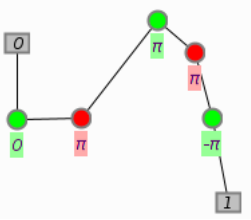


$$\overset{(\mathbf{S})}{=}$$

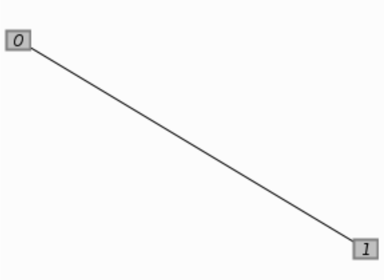


. (5.14)

For $\alpha = 0$ and $\beta = \gamma = \pi$

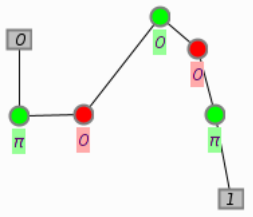


$$\overset{(\mathbf{S}),(\mathbf{C})}{=}$$

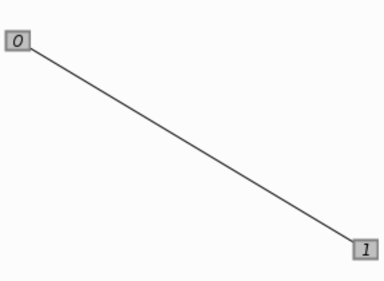


. (5.15)

For $\alpha = \pi$ and $\beta = \gamma = 0$

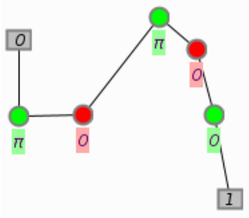


$$\overset{(\mathbf{S})}{=}$$

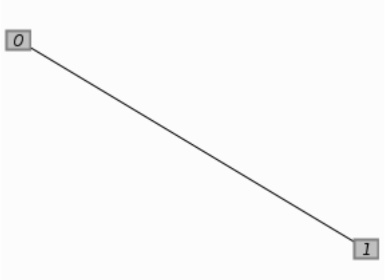


. (5.16)

For $\alpha = \gamma = \pi$ and $\beta = 0$

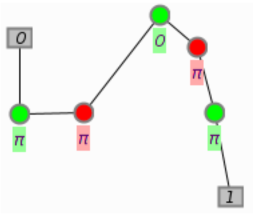


$\overset{(\mathbf{S})}{=}$

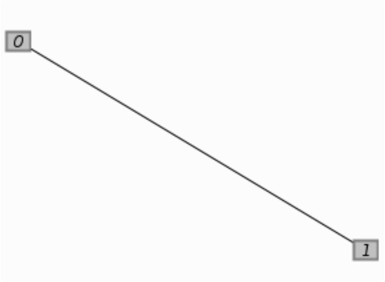


. (5.17)

For $\alpha = \beta = \pi$ and $\gamma = 0$

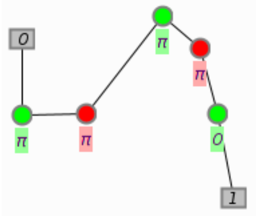


$\overset{(\mathbf{S})}{=}$

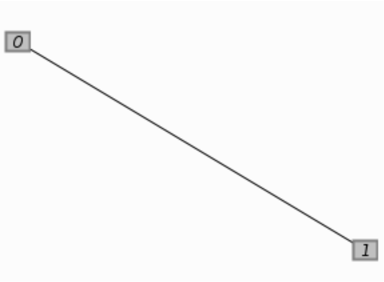


. (5.18)

For $\alpha = \beta = \gamma = \pi$



$\overset{(\mathbf{S}),(\mathbf{K2})}{=}$



. (5.19)

Eq. 5.12-5.19 imply the validity of the quantum secret state sharing protocol. □

5.3 EPR teleportation using GHZ

In the EPR teleportation protocol as described in [41, 51] Alice teleports the state $|\psi\rangle_2 = a\,|01\rangle + b\,|10\rangle$ to Bob and Charlie. In this section this protocol is presented in the red/green calculus. Moreover, it will be shown that these graphical representations yield the desired behaviour, proving the correctness of the protocol. This section is divided in two subsections. First the protocol will be transformed to the red/green calculus directly from its description. Second, the quantum circuit representation of the protocol will be written graphically.

5.3.1 Graphical presentation of EPR teleportation

In this subsection the EPR teleportation protocol from [41] will be written in the ZX-calculus directly from its description. EPR teleportation can be accomplished by the following protocol: Initially Alice, Bob and Charlie share a GHZ state (qubits 2, 3 and 4). Additionally

Alice has an entangled pair in the $|\psi\rangle_2 = a\,|01\rangle + b\,|10\rangle$ state (qubits 0 and 1), where $|a|^2 + |b|^2 = 1$. This is the state to be teleported. Alice has access to qubits 0, 1 and 2. Bob has qubit 3 and Charlie has qubit 4.

1. Alice performs a joint measurement on all three of her qubits, measuring qubit 0 in the x-basis and the qubits 1 and 2 in the Bell basis. She sends her outcomes to Bob and Charlie. There are 8 different outcomes she can get.
2. Based on the measurement outcomes, either Bob or Charlie perform local operations on their qubits. These combinations are summarised in Table 5.4.

Alice 1	Alice 2	Bob	Charlie	α	β	γ	Bob	Charlie
$\langle\Phi^+|$	$\langle x^+|$	σ_x	I	0	0	0	σ_x	I
$\langle\Phi^-|$	$\langle x^+|$	$i\sigma_y$	I	0	π	0	$i\sigma_y$	I
$\langle\Phi^+|$	$\langle x^-|$	$-i\sigma_y$	I	π	0	0	$-i\sigma_y$	I
$\langle\Phi^-|$	$\langle x^-|$	$-\sigma_x$	I	π	π	0	$-\sigma_x$	I
$\langle\Psi^+|$	$\langle x^+|$	I	σ_x	0	0	π	I	σ_x
$\langle\Psi^-|$	$\langle x^+|$	I	$-i\sigma_y$	0	π	π	I	$-i\sigma_y$
$\langle\Psi^+|$	$\langle x^-|$	I	$i\sigma_y$	π	0	π	I	$i\sigma_y$
$\langle\Psi^-|$	$\langle x^-|$	I	$-\sigma_x$	π	π	π	I	$-\sigma_x$

Table 5.4: The corresponding local operations that Bob and Charlie perform, given a measurement outcome of Alice. Additionally the corresponding phases of Fig. 5.2 are displayed.

Lemma 24. *Fig. 5.2 is the graphical representation of the set of instructions of the EPR teleportation through GHZ protocol.*

Proof. Box 1 is the state to be teleported by Lemma 12 and box two contains GHZ, the means of the teleportation. Box 3 represents a Bell state measurement and Box 4 a measurement into the x-basis. Box 5 and 6 are the corresponding unitaries that Bob and Charlie have to perform. Note that $-\sigma_x = \sigma_z\sigma_x\sigma_z$. In Table 5.4 it can be seen that these correspond to the correct unitaries. □

Lemma 25. *The EPR teleportation through GHZ protocol is correct.*

Proof. What needs to be shown is that for each measurement outcome and corresponding unitary operation, the diagram simplifies to the state to be teleported, which is the desired behaviour. For $\langle\Phi^+|$ and $\langle x^+|$ Bob applies σ_x, corresponding to $\alpha = \beta = \gamma = b_1 = b_3 =$

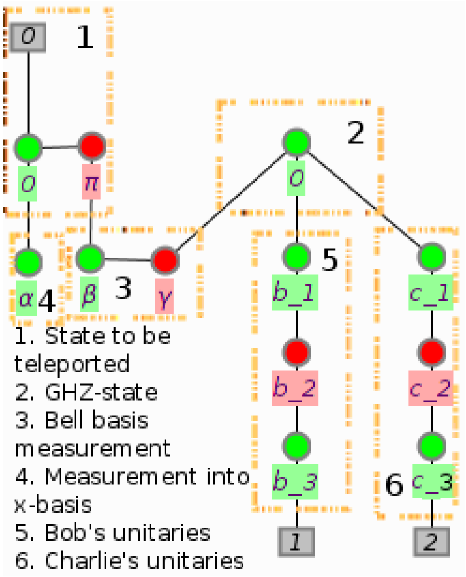
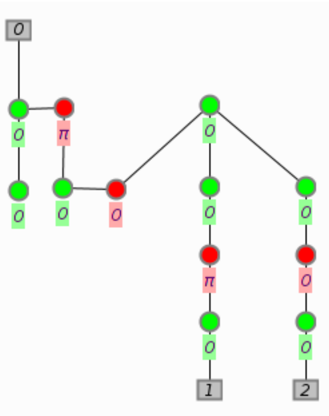
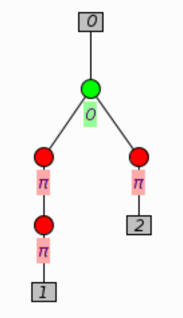


Figure 5.2: Graphical representation of the set of instructions of Teleportation of $a\,|01\rangle + b\,|10\rangle$ through GHZ protocol. $\alpha, \beta, \gamma \in \{0, \pi\}$, $b_1 = \beta, b_2 = \pi, b_3 = \alpha$ if $\gamma = 0$ and $c_1 = \alpha, c_2 = \pi, c_3 = \beta$ if $\gamma = \pi$.

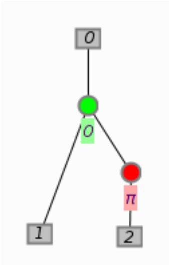
$c_1 = c_2 = c_3 = 0$ and $b_2 = \pi$



$\overset{(\mathbf{K1}),(\mathbf{S})}{=}$

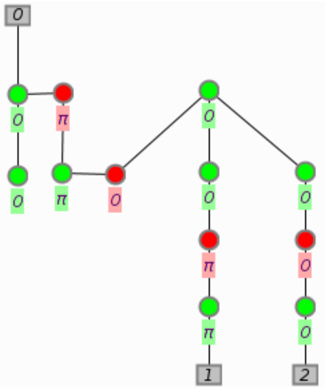


$\overset{(\mathbf{S})}{=}$

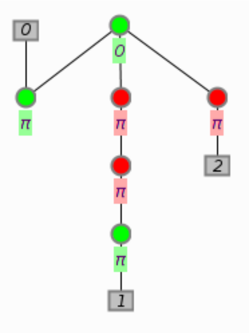


. (5.20)

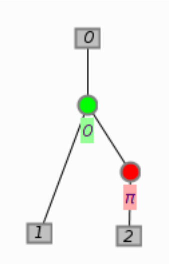
For $\langle\Phi^-|$ and $\langle x^+|$ Bob applies $i\sigma_y$, corresponding to $\alpha = \gamma = b_3 = c_1 = c_2 = c_3 = 0$ and $\beta = b_2 = b_3 = \pi$



$\overset{(\mathbf{K1}),(\mathbf{S})}{=}$

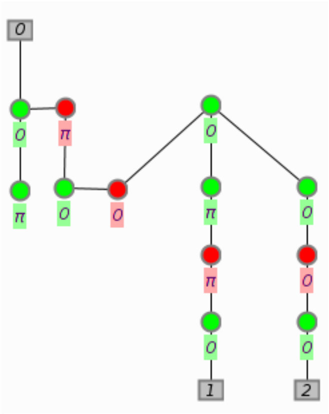


$\overset{(\mathbf{S})}{=}$

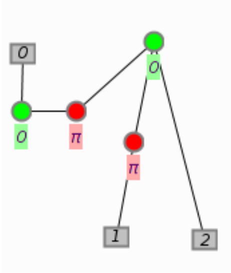


.

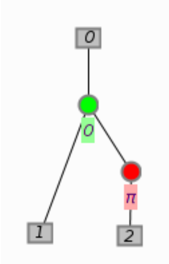
For $\langle\Phi^+|$ and $\langle x^-|$ Bob applies $-i\sigma_y$, corresponding to $\beta = \gamma = b_2 = c_1 = c_2 = c_3 = 0$ and $\alpha = b_1 = b_2 = \pi$



$\overset{(\mathbf{S})}{=}$

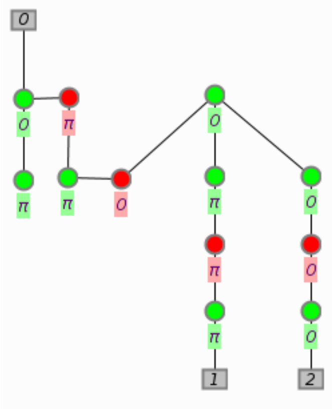


$\overset{(\mathbf{K1}),(\mathbf{S})}{=}$

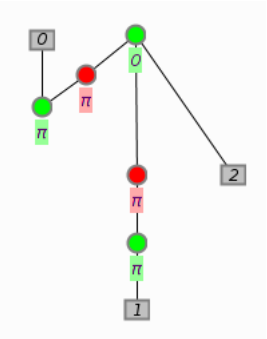


. (5.21)

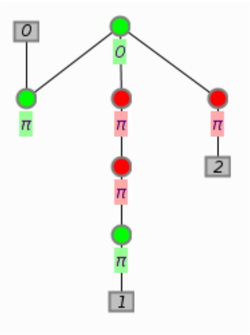
For $\langle\Phi^-|$ and $\langle x^-|$ Bob applies $-\sigma_x$, corresponding to $\gamma = c_1 = c_2 = c_3 = 0$ and $\alpha = \beta = b_1 = b_2 = b_3 = \pi$



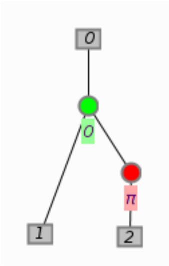
$\overset{(\mathbf{S})}{=}$



$\overset{(\mathbf{K1})}{=}$

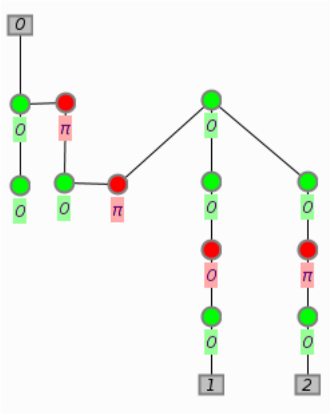


$\overset{(\mathbf{S})}{=}$

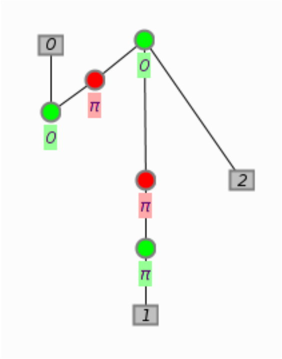


. (5.22)

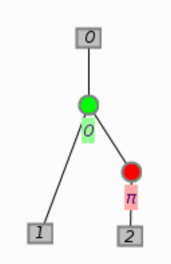
For $\langle\Psi^+|$ and $\langle x^+|$ Charlie applies σ_x, corresponding to $\alpha = \beta = b_1 = b_2 = b_3 = c_1 = c_3 = o$ and $\gamma = c_2 = \pi$



$\overset{(\mathbf{K1}),(\mathbf{S})}{=}$



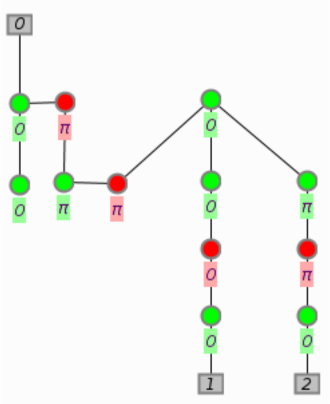
$\overset{(\mathbf{K1}),(\mathbf{S})}{=}$



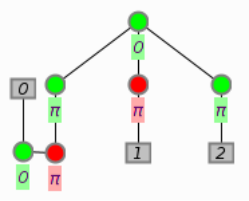
. (5.23)

For $\langle\Psi^-|$ and $\langle x^+|$ Charlie applies $-i\sigma_y$, corresponding to $\alpha = b_1 = b_2 = b_3 = c_1 = 0$ and

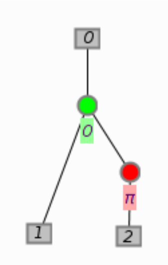
$\beta = \gamma = c_2 = c_3 = \pi$



$\overset{\mathbf{(K1)},\mathbf{(S)}}{=}$

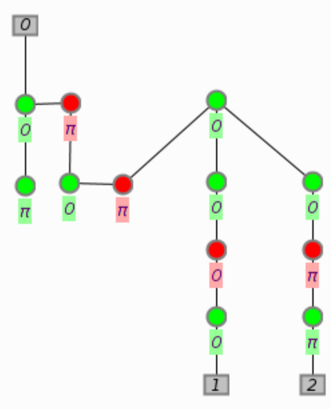


$\overset{\mathbf{(K1)},\mathbf{(S)}}{=}$

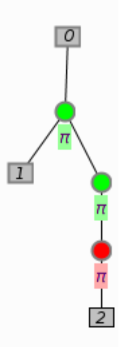


.

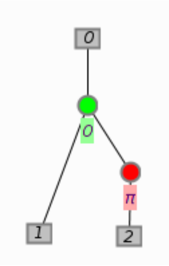
For $\langle\Psi^{+}|$ and $\langle x^{-}|$ Charlie applies $i\sigma_y$, corresponding to $\beta = b_1 = b_2 = b_3 = c_3 = o$ and $\alpha = \gamma = c_1 = c_2 = \pi$



$\overset{\mathbf{(S)}}{=}$

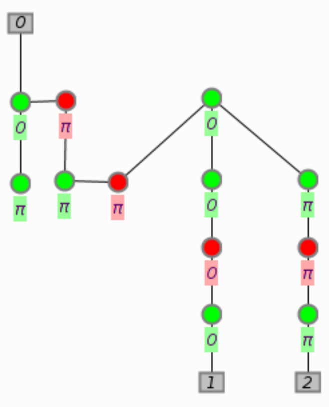


$\overset{\mathbf{(S)}}{=}$

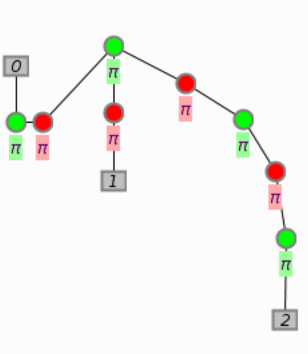


. (5.24)

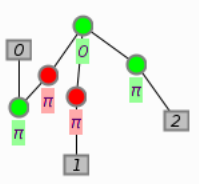
For $\langle\Psi^{-}|$ and $\langle x^{-}|$ Charlie applies $-\sigma_x$, corresponding to $b_1 = b_2 = b_3 = 0$ and $\alpha = \beta = \gamma = c_1 = c_2 = c_3 = \pi$



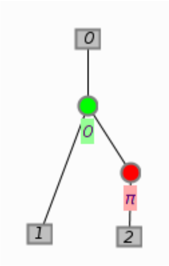
$\overset{\mathbf{(K1)},\mathbf{(S)}}{=}$



$\overset{\mathbf{(K2)},\mathbf{(S)}}{=}$



$$\overset{\textbf{(K1)},\textbf{(K2)},\textbf{(S)}}{=}$$



. (5.25)

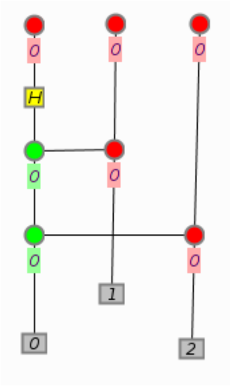
Eq. 5.20 - 5.25 imply the correctness of the protocol. □

5.3.2 Graphical presentation of EPR teleportation as a Quantum circuit

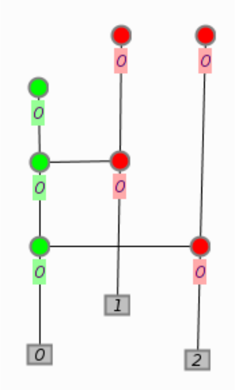
The EPR teleportation protocol can also be written as a quantum circuit [41]. In this subsection is will be shown that written in the red/green calculus, this circuit simplifies to the desired result.

Lemma 26. *The quantum circuit to create a GHZ state in [41] simplifies to GHZ.*

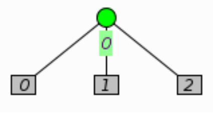
Proof.



$\overset{\textbf{(C)}}{=}$

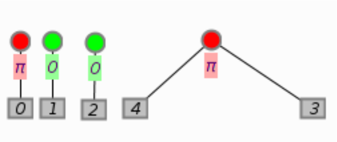


$\overset{\textbf{(S)}}{=}$



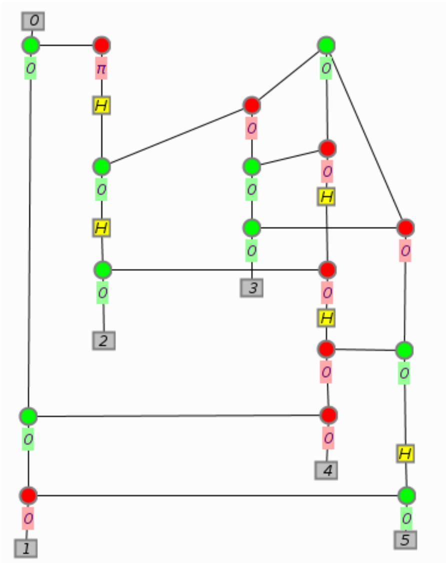
□

Lemma 27. *The network for teleportation of an EPR pair in [41] simplifies to*

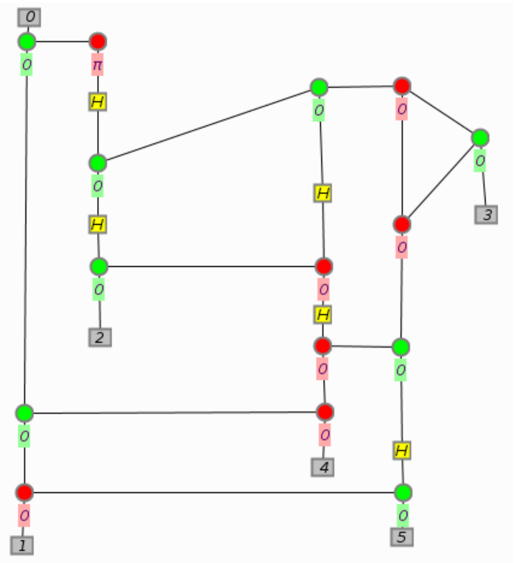


.

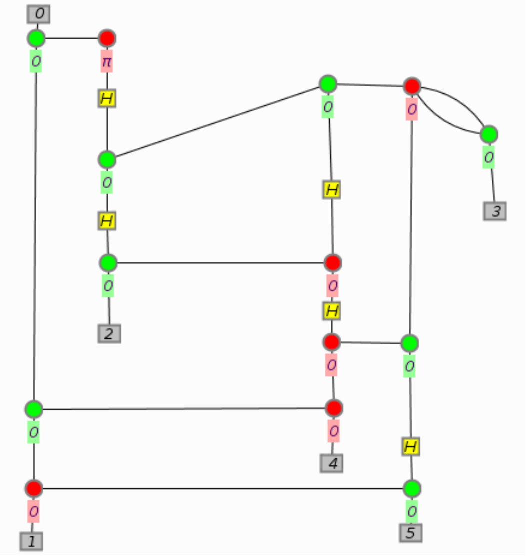
Proof. By Lemma 12, 26 and Cor. 15, the beginning of the network simplifies to $a\,|01\rangle + b\,|10\rangle$ as the state to be teleported and the GHZ state as a means to teleport the EPR-pair. Then the network can be written and simplified as follows:



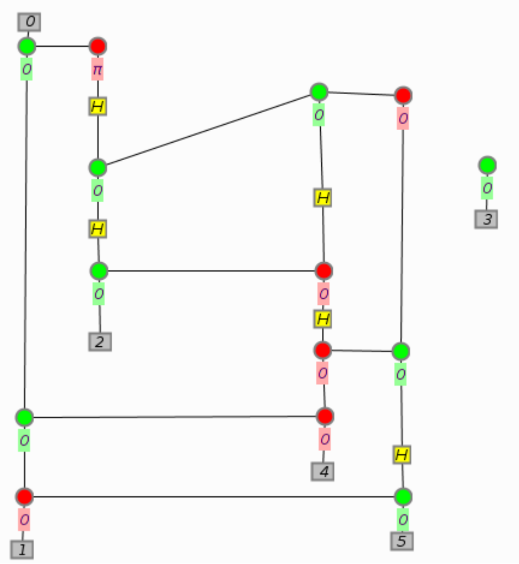
$\overset{(\mathbf{B2})}{=}$



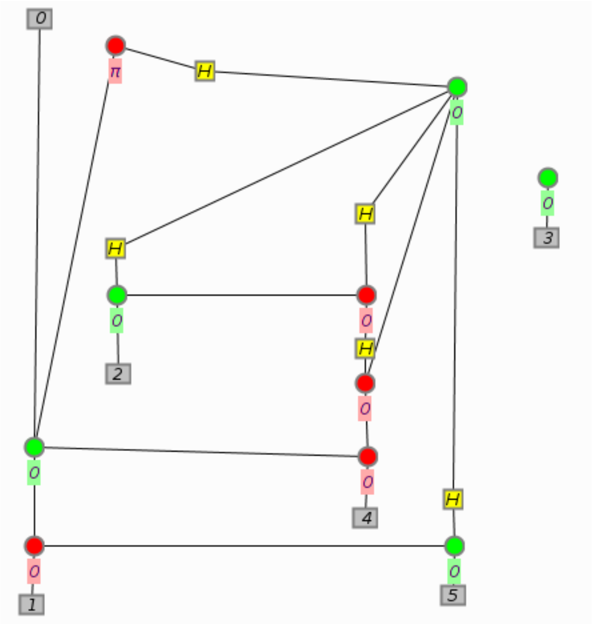
$\overset{(\mathbf{S1})}{=}$



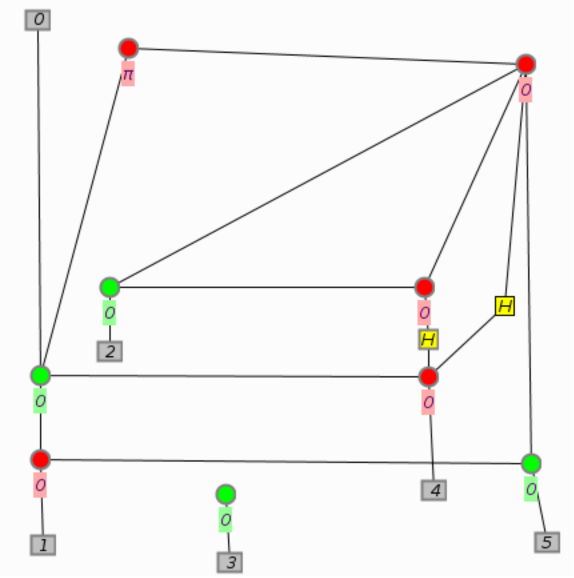
$\overset{(\mathbf{B'})}{=}$



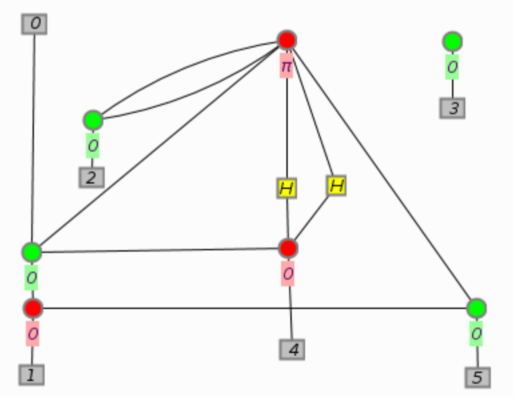
$\overset{(\mathbf{S1})}{=}$



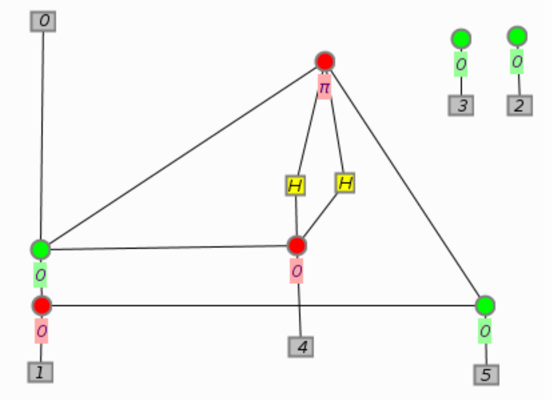
$\overset{(\mathbf{C})}{=}$



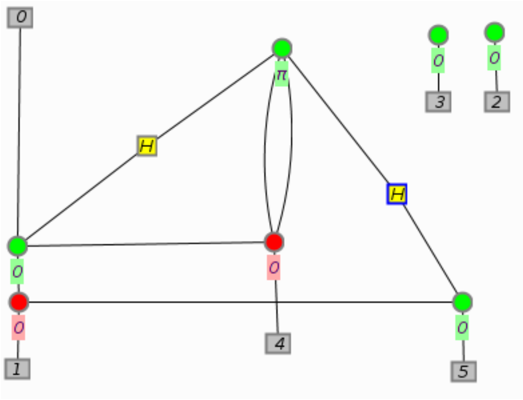
$\overset{(\mathbf{S1})}{=}$



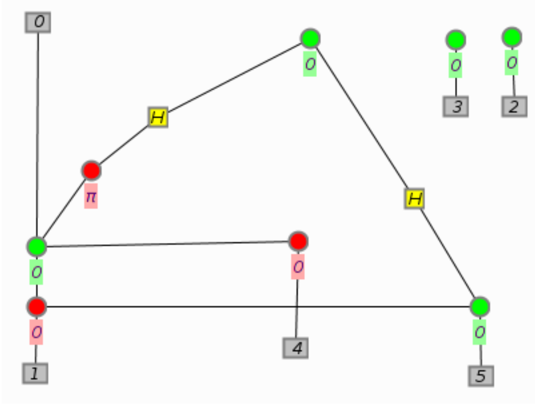
$\overset{(\mathbf{B'})}{=}$

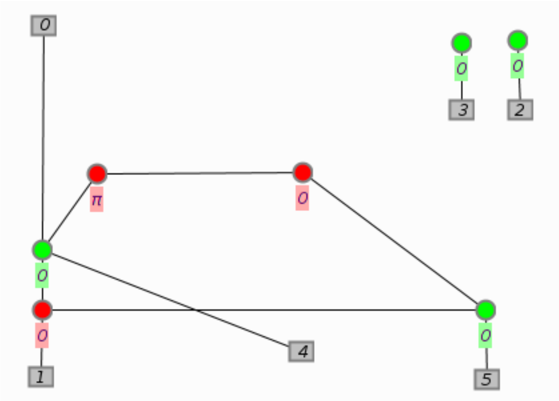


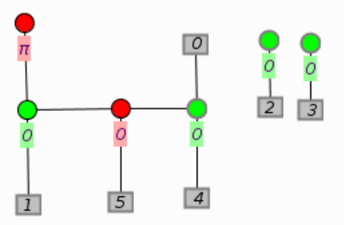
$\overset{(\mathbf{C})}{=}$

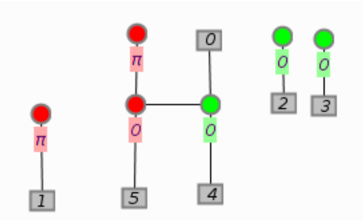


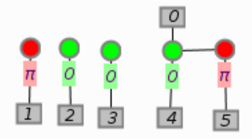
$\overset{(\mathbf{B'})}{=}$



$\overset{(\mathbf{C})}{=}$ 

$\overset{(\mathbf{B2})}{=}$ 

$\overset{(\mathbf{K1})}{=}$ 

$\overset{(\mathbf{S1})}{=}$ 

(5.26)

□

5.4 Superdense Coding with GHZ

As with Bell states, it is possible to transfer an amount of classical bits by transferring fewer qubits by means of different states in the GHZ class. When states in the GHZ class are used for super dense coding, two qubits need to be transfered in order to transfer three classical bits [18], and is therefore less efficient than superdense coding with Bell states, where two classical bits can be transferred by means of just a single qubit [70]. This section is divided up in five subsections. In the first subsection the steps of the protocol will be explained. In the second subsection the eight different states in the GHZ class will be presented. In the last three subsections it will be shown how, through measurement in the GHZ basis, these eight different states can be translated into three classical bits, proving the validity of the protocol.

5.4.1 Super Dense Coding with GHZ protocol

Provided Alice and Bob share $|GHZ\rangle$, such that the first qubit belongs to Bob and the other two qubits belong to Alice, the following protocol describes superdense coding with GHZ as in [18, 42]:

1. Alice applies a combination of $I, \sigma_x, i\sigma_y$ and σ_z on both her qubits, encoding one of eight distinguishable states in the GHZ class.
2. Alice transfers both her qubits to Bob.
3. Bob measures all three qubits in the GHZ basis, retrieving the state Alice encoded.

4. Bob translates the retrieved state to three classical bits.

5.4.2 Different GHZ states

There are eight different states in the GHZ class. One can go from one to the other by performing unitary single particle operations on two of the three particles. These unitary operations are $I, \sigma_x, i\sigma_y$ and σ_z. Though there are 16 different combinations of these operators on two qubits, only half of them generate distinguishable states [83] as can be seen by comparing the graphical representations in Table 5.5 and 5.6. In this section we will work with states in the standard form

$$|GHZ_{+ij}\rangle = \frac{1}{\sqrt{2}}(|0ij\rangle + |1\bar{i}\bar{j}\rangle), \tag{5.27}$$

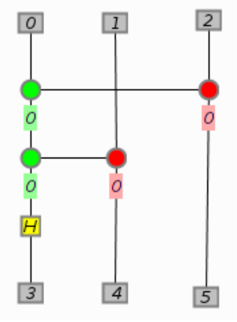
as in [30, 18], where $i, j \in \{0, 1\}$, $\bar{i} = 1 - i$ and $\bar{j} = 1 - j$.

5.4.3 Encoding a GHZ measurement outcome into classical bits

The encoding is as in [13]. After measurement, an output qubit is encoded as 0 if it is $|0\rangle$ and as 1 if it is$|1\rangle$. Every GHZ state gives three output bits. If the first output bit is 0, then there is an odd number of $|+\rangle$ in the basis, otherwise an even number. If the second output bit is 0, then the first two bits in the GHZ class state are the same, otherwise they are different. And finally, if the last output bit is 0, the the first and the last bit in the GHZ class state are the same. This encoding is displayed in Table 5.5.

5.4.4 Measurement into the GHZ basis

The circuit to measure into the GHZ basis is [13]



, (5.28)

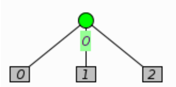
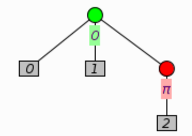
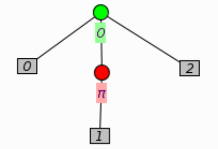
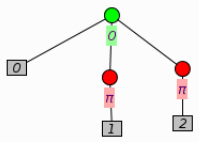
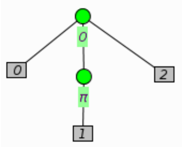
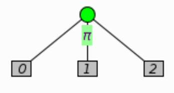
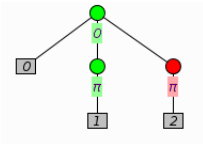
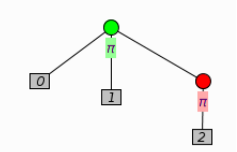
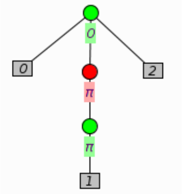
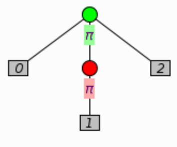
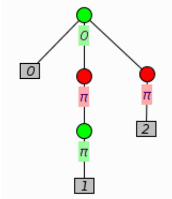
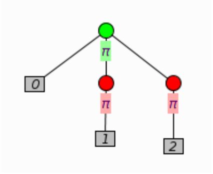
#	Binary	Standard Form (SF)	Unitaries	Graphical Representation
0	000	$\frac{1}{\sqrt{2}}(\|000\rangle + \|111\rangle)$	$I \otimes I$	
1	001	$\frac{1}{\sqrt{2}}(\|001\rangle + \|110\rangle)$	$I \otimes \sigma_x$	
2	010	$\frac{1}{\sqrt{2}}(\|010\rangle + \|101\rangle)$	$\sigma_x \otimes I$	
3	011	$\frac{1}{\sqrt{2}}(\|011\rangle + \|100\rangle)$	$\sigma_x \otimes \sigma_x$	
4	100	$\frac{1}{\sqrt{2}}(\|000\rangle - \|111\rangle)$	$\sigma_z \otimes I$	 $\overset{\textbf{(S)}}{=}$ 
5	101	$\frac{1}{\sqrt{2}}(\|001\rangle - \|110\rangle)$	$\sigma_z \otimes \sigma_x$	 $\overset{\textbf{(S)}}{=}$ 
6	110	$\frac{1}{\sqrt{2}}(\|010\rangle - \|101\rangle)$	$i\sigma_y \otimes I$	 $\overset{\textbf{(K2)}}{=}$ 
7	111	$\frac{1}{\sqrt{2}}(\|011\rangle - \|100\rangle)$	$i\sigma_y \otimes \sigma_x$	 $\overset{\textbf{(S)}}{=}$ 

Table 5.5: This table shows the eight different states in the GHZ class, their binary presentation, the unitaries that should be applied to the second and the third qubit to obtain this state from $|GHZ\rangle$ and finally their graphical representation.

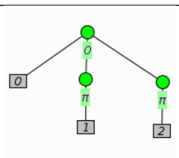
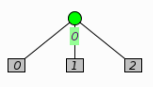
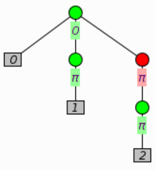
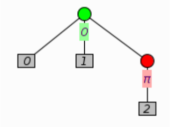
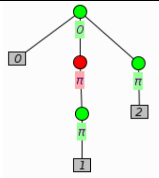
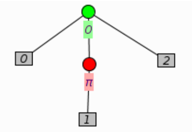
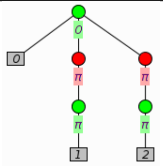
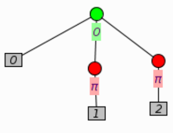
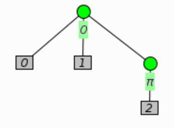
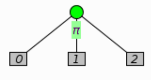
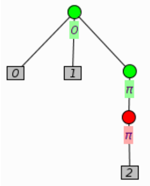
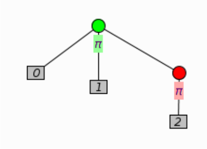
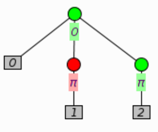
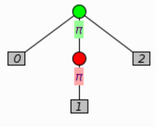
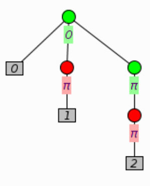
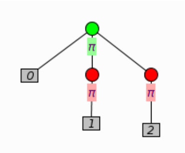
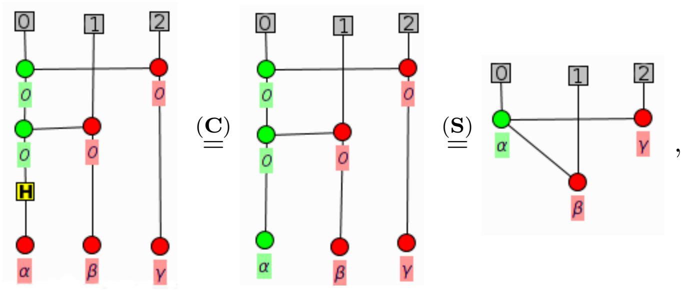
#	Binary	Alternative Form (AF)	Unitaries	Graphical Representation
0	000	$\frac{1}{\sqrt{2}}(\lvert 111\rangle + \lvert 000\rangle)$	$\sigma_z \otimes \sigma_z$	 $\overset{(\mathbf{S})}{=}$ 
1	001	$\frac{1}{\sqrt{2}}(\lvert 110\rangle + \lvert 001\rangle)$	$\sigma_z \otimes i\sigma_y$	 $\overset{(\mathbf{S}),(\mathbf{K2})}{=}$ 
2	010	$\frac{1}{\sqrt{2}}(\lvert 101\rangle + \lvert 010\rangle)$	$i\sigma_y \otimes \sigma_z$	 $\overset{(\mathbf{S}),(\mathbf{K2})}{=}$ 
3	011	$\frac{1}{\sqrt{2}}(\lvert 100\rangle + \lvert 011\rangle)$	$i\sigma_y \otimes i\sigma_y$	 $\overset{(\mathbf{S}),(\mathbf{K2})}{=}$ 
4	100	$\frac{1}{\sqrt{2}}(\lvert 111\rangle - \lvert 000\rangle)$	$I \otimes \sigma_z$	 $\overset{(\mathbf{S})}{=}$ 
5	101	$\frac{1}{\sqrt{2}}(\lvert 100\rangle - \lvert 001\rangle)$	$I \otimes i\sigma_y$	 $\overset{(\mathbf{S}),(\mathbf{K2})}{=}$ 
6	110	$\frac{1}{\sqrt{2}}(\lvert 101\rangle - \lvert 010\rangle)$	$\sigma_x \otimes \sigma_z$	 $\overset{(\mathbf{S})}{=}$ 
7	111	$\frac{1}{\sqrt{2}}(\lvert 100\rangle - \lvert 011\rangle)$	$\sigma_x \otimes i\sigma_y$	 $\overset{(\mathbf{S}),(\mathbf{K2})}{=}$ 

Table 5.6: This table shows the remaining states in the GHZ class, their binary presentation, the unitaries that should be applied to the second and the third qubit to obtain this state from $\lvert GHZ\rangle$ and finally their graphical representation.

which gives three qubits in the z-basis. Plugging states in the z-basis, we obtain for $\alpha, \beta, \gamma \in \{0, \pi\}$



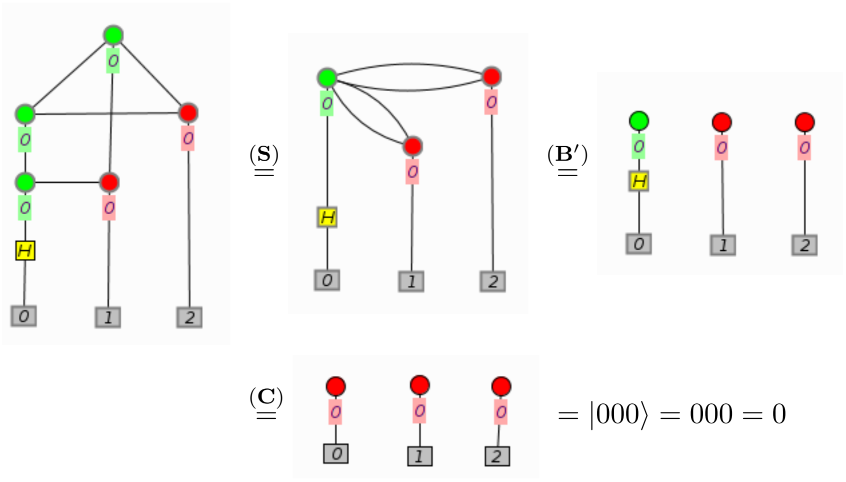
(5.29)

which results in one of eight states in the GHZ class by Table 5.5 and 5.6 if values for α, β and γ are set.

5.4.5 Validity of the protocol

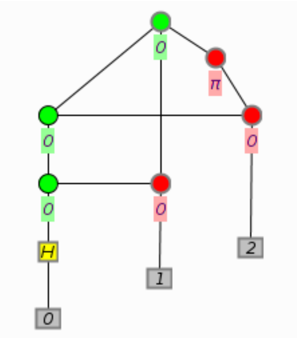
Lemma 28. *The encoding in combination with the GHZ measurement circuit in [13] makes for a valid Superdense Coding protocol*[1]*.*

Proof. Let $|0\rangle = 0$ and $|1\rangle = 1$ in classical bits. What needs to be shown is that for all eight states in the GHZ class, their measurement outcome is equal to their binary representation in Table 5.5.

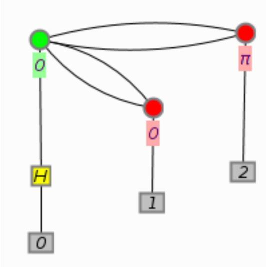


$= |000\rangle = 000 = 0$ (5.30)

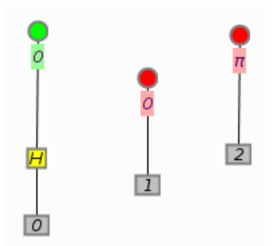
[1] Note that this encoding is different from [18, 42].



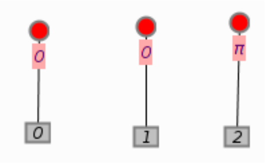
$\overset{(\mathbf{S})}{=}$



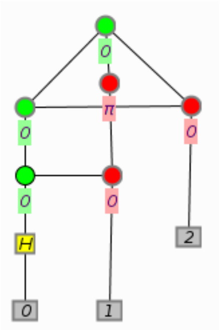
$\overset{(\mathbf{B}')}{=}$



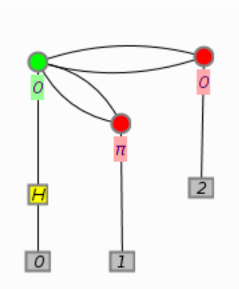
$\overset{(\mathbf{C})}{=}$



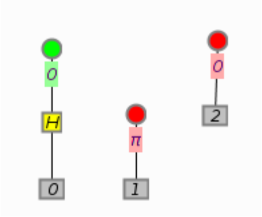
$$= |001\rangle = 001 = 1 \tag{5.31}$$



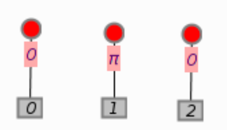
$\overset{(\mathbf{S})}{=}$



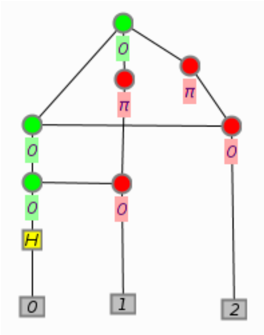
$\overset{(\mathbf{B}')}{=}$



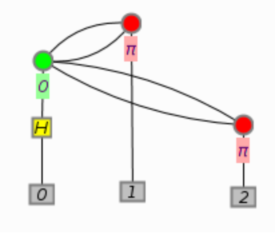
$\overset{(\mathbf{C})}{=}$



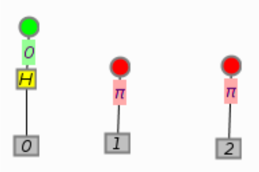
$$= |010\rangle = 010 = 2 \tag{5.32}$$



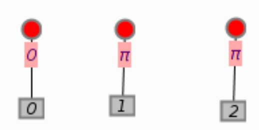
$\overset{(\mathbf{S})}{=}$



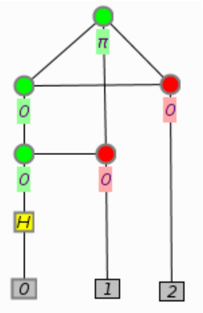
$\overset{(\mathbf{B}')}{=}$



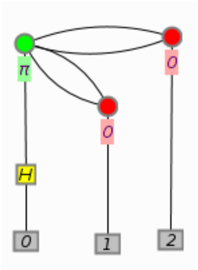
$\overset{(\mathbf{C})}{=}$



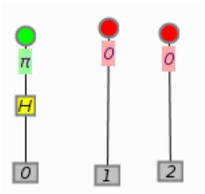
$$= |011\rangle = 011 = 3 \tag{5.33}$$



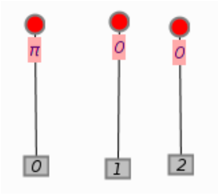
$\overset{(\mathbf{S})}{=}$



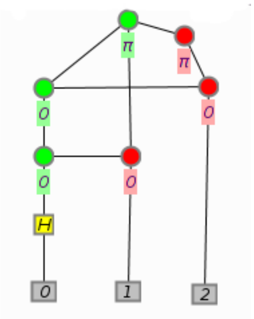
$\overset{(\mathbf{B'})}{=}$



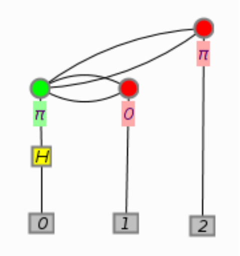
$\overset{(\mathbf{C})}{=}$



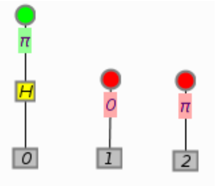
$$= |100\rangle = 100 = 4 \tag{5.34}$$



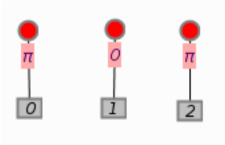
$\overset{(\mathbf{S})}{=}$



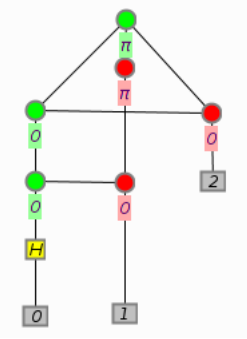
$\overset{(\mathbf{B'})}{=}$



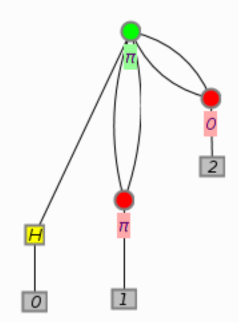
$\overset{(\mathbf{C})}{=}$



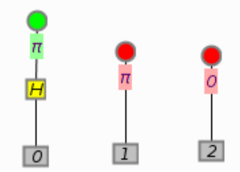
$$= |101\rangle = 101 = 5 \tag{5.35}$$



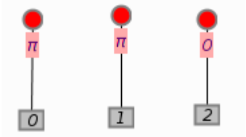
$\overset{(\mathbf{S})}{=}$



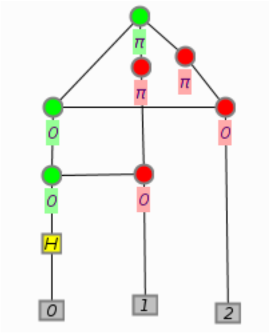
$\overset{(\mathbf{B'})}{=}$



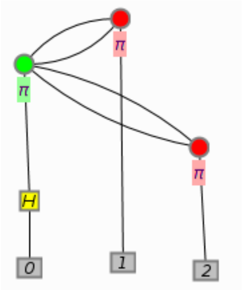
$\overset{(\mathbf{C})}{=}$



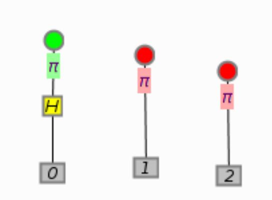
$$= |110\rangle = 110 = 6 \tag{5.36}$$



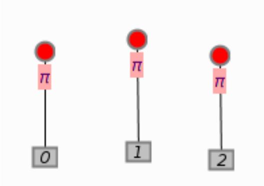
$\overset{(\mathbf{S})}{=}$



$\overset{(\mathbf{B'})}{=}$



$\overset{(\mathbf{C})}{=}$



$$= |111\rangle = 111 = 7. \qquad (5.37)$$

Eq. 5.30-5.37 imply the validity of the protocol. □

5.4.6 Superdense coding with N-GHZ

In a similar way superdense coding for N-GHZ states can be constructed. One of $\{I, i\sigma_y, \sigma_x, \sigma_z\}$ can be applied on the N^{th} qubit and one of $\{I, \sigma_x\}$ on qubit $2-(N-1)$ to encode 2^N different states. They can be distinguished with a measurement like the GHZ basis measurement [13].

[B]efore you so quickly label me a third party to the communication, just remember: I loved [Bob] first. We had something and [Alice] tore it away. She is the attacker, not me.

Eve on
http://xkcd.com/177/

6 Quantum Direct Communication Protocols with GHZ

In this chapter different Quantum Direct Communication (QDC) Protocols that make use of GHZ are presented. With quantum cryptography, Alice first shares a private key with the other participants, which they use to encrypt their secret message, so they can send it over a classical channel. With QDC protocols, Alice and the other participants can communicate safely, without generating a private key first. In principal, one can use every QDC protocol for quantum key distribution as well. All one has to do is, instead of encrypting the secret message, encrypt a random bit string. Note that this does not necessarily hold the other way around, since in quantum key sharing one does not always have control over the contents of the shared bit string.

As in classical cryptography, during QDC Alice tries to send a message to Bob, Charlie, . . . , Zach, depending on the number of participants in the protocol. Trent is a neutral third party, not involved in the communication itself. Finally Eve is an eavesdropper trying to intercept and/or disturb the secret message. In this context she is an evil quantum physicist, able to build all devices that are allowed by laws of quantum mechanics [60, 16, 76].

The protocols in this chapter have all been previously published. However they have never been organised in this way, i.e. different Quantum Direct Communication protocols together, that all involve GHZ states. Additionally they are now presented and analysed in the ZX-calculus instead of the original presentation in Dirac notation. Note that the ZX-calculus has never been applied to QDC protocols before.

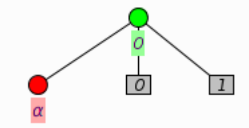
First eavesdropping with GHZ is explained, then QDC with GHZ. Next is QDC by rearranging particle orders, after which multi-step and multi-party QDC with GHZ will be presented. Then QDC with entanglement swapping is described. Finally QDC with Authentication, Improved QDC with authentication and Efficient QDC with Authentication will be explained.

6.1 Detecting Eavesdropping with GHZ

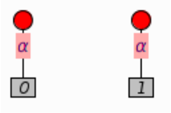
In this section it will be shown that when one qubit of $|GHZ\rangle$ is measured into the z- or x-basis, this determines the outcome of the other two qubits. If this correspondence is not there, there is an eavesdropper on the quantum channel. Specific attacks will be discussed in relation to the protocols.

Lemma 29. *When all three qubits of $|GHZ\rangle$ are measured in the z-basis, they will all have the same measurement outcome.*

Proof. Let $\alpha \in \{0, \pi\}$, then



$$\overset{\textbf{(B1)}/\textbf{(M)}}{=}$$

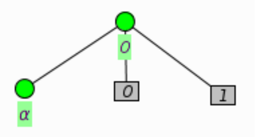


. (6.1)

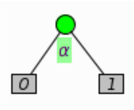
□

Lemma 30. *When one qubit of $|GHZ\rangle$ is measured into the x-basis, the other two qubits are either in the state $|\phi^+\rangle$ if the outcome is $|+\rangle$, or $|\phi^-\rangle$ if the outcome is $|-\rangle$.*

Proof. Let $\alpha \in \{0, \pi\}$, then



$$\overset{\textbf{(S1)}}{=}$$

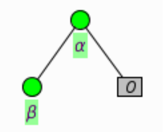


. (6.2)

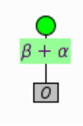
Which is $|\phi^+\rangle$ or $|\phi^-\rangle$. □

Lemma 31. *If all qubits of $|GHZ\rangle$ are measured into the x-basis, the second and third measurements will give the same outcome if the first outcome is $|0\rangle$ and opposite outcomes if the first outcome is $|1\rangle$.*

Proof. By Lemma 30, after one measurement the state is $|\phi^+\rangle$ or $|\phi^-\rangle$. Let $\alpha, \beta \in \{0, \pi\}$, then



$$\overset{\textbf{(S1)}}{=}$$



. (6.3)

Thus the results of the second and third measurements are the same if $\alpha = 0$ and opposite otherwise. □

6.2 Quantum secure direct communication with GHZ

In this section the Quantum Secure Direct Communication with GHZ protocol as described in [49] is presented. First it will be described for three people. Then it will be expanded to N people.

6.2.1 Three-party Quantum Secure Direct Communication with GHZ

Assuming Alice, Bob and Charlie want to communicate safely, this can be achieved in two stages [49]. First they check whether the quantum channel is safe:

1. Alice randomly prepares N GHZ states in one of the eight different GHZ states $|\Psi_i\rangle_{ABC}$, where A,B and C stand for Alice, Bob and Charlie respectively and $0 \leq i \leq 7$.
2. Alice sends Bob and Charlie their qubits.
3. Bob chooses an arbitrary subset M and randomly measures them in the z- or x-basis. He communicates which qubits he chose and their outcomes to Alice and Charlie classically.
4. Alice and Charlie measure their corresponding qubits in the same basis. Charlie communicates her results with Alice through a classical channel.
5. With the measurement outcomes and the sequence of GHZ states that Alice prepared, she can detect eavesdropping.

When they have established that the channel is safe, they proceed with direct communication using the remaining $K = N - |M|$ GHZ states.

1. Bob and Charlie perform I for bit 0 and $i\sigma_y$ for bit 1 on their qubits.
2. Bob and Charlie send their qubits to Alice.
3. Alice performs I for 00, σ_x for 01, $i\sigma_y$ for 10 and σ_z for 11 on her qubit.
4. She measures the entire GHZ state into the GHZ basis. She publishes her outcomes and the original GHZ states.
5. With this information and their own secret message, they can now deduce what secrets the other two encoded.

Lemma 32. *Fig. 6.1 is the graphical representation of the set of instructions of the three-party Quantum Secure Direct Communication with GHZ.*

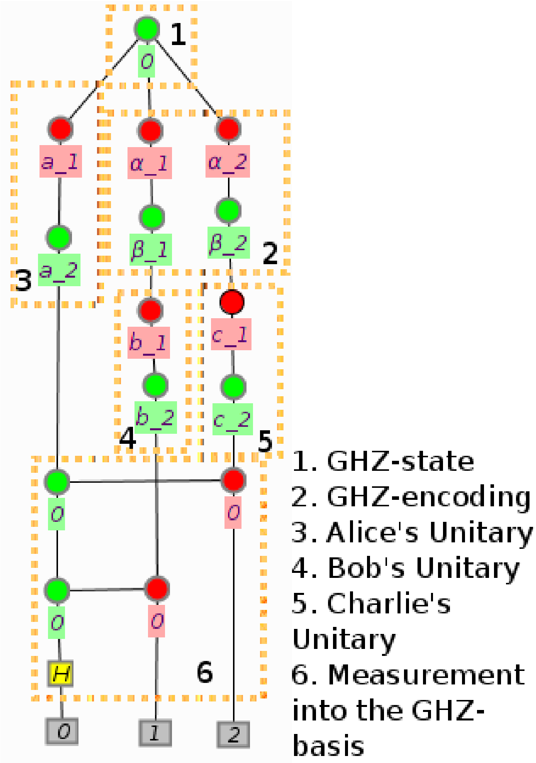


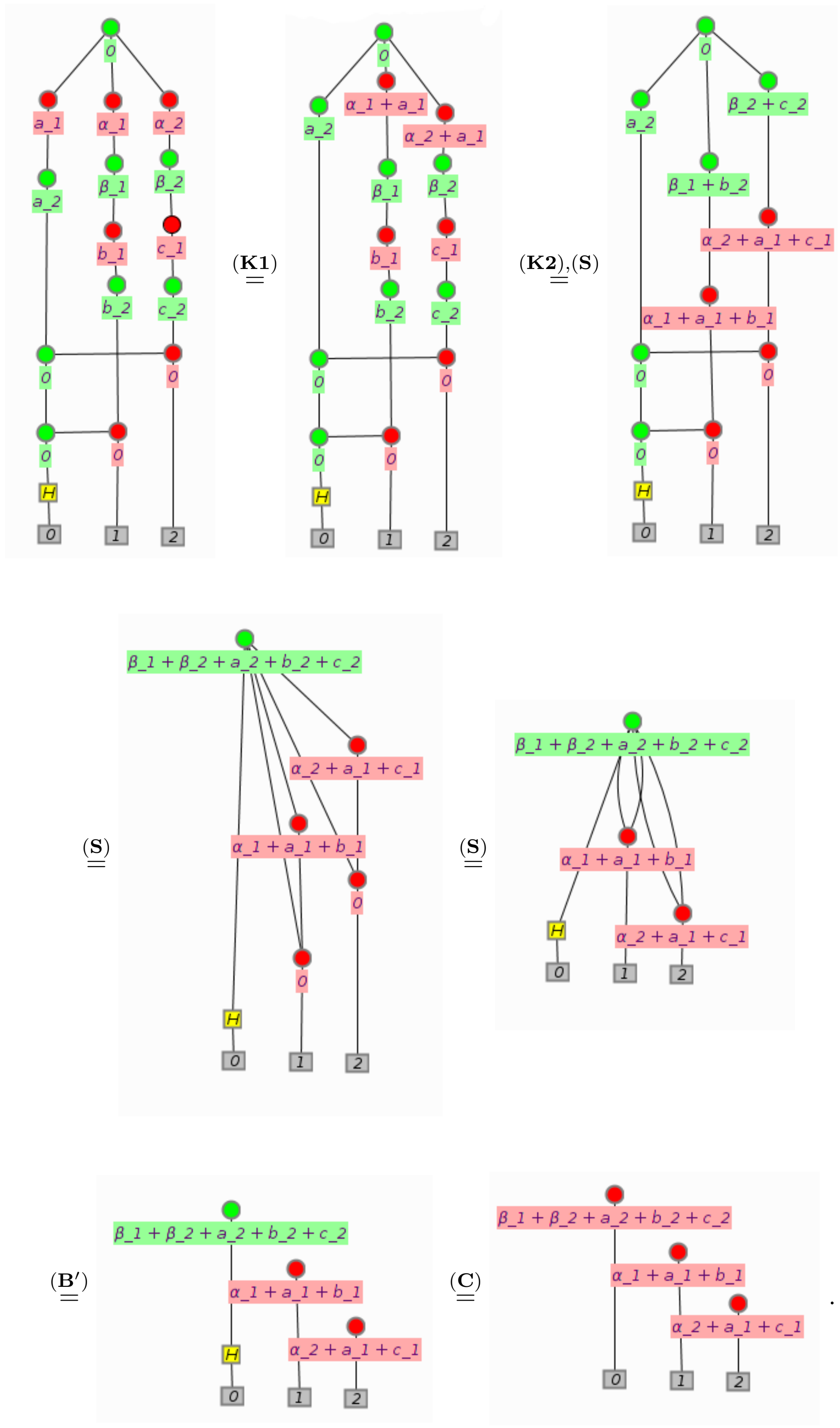
Figure 6.1: Graphical representation of the set of instructions of the three-party Quantum Secure Direct Communication with GHZ. $\alpha_1, \alpha_2, \beta_1, \beta_2$, a_1, a_2, b_1, b_2, $c_1, c_2 \in \{0, \pi\}$, $b_1 = b_2$ and $c_1 = c_2$.

Proof. Box 1 is a GHZ state. Box 2 is the encoding of the GHZ state into one of eight GHZ states by Table 5.5. Box 3 is Alice's unitary. Box 4 and 5 are Bob and Charlie's unitaries. Because $b_1 = b_2$ and $c_1 = c_2$ and $b_1, b_2, c_1, c_2 \in \{0, \pi\}$, this is either I or $i\sigma_y$. Finally, box 6 is measurement into the GHZ basis by Eq. 5.28. □

Lemma 33. *The three-party Quantum Secure Direct Communication with GHZ protocol is correct.*

Proof. By Lemma 32 Fig. 6.1 is the graphical representation of the set of instructions.

Simplification of this representation gives



. (6.4)

Now it is possible for all of them to solve for the phases of the other two. Let the measurement outcome be $\gamma_A, \gamma_B, \gamma_C$ for the values of qubit A, B and C respectively. Then

$$\gamma_A = a_2 + \beta_1 + b_1 + \beta_2 + c_1 \tag{6.5}$$

$$\gamma_B = a_1 + \alpha_1 + b_2 \tag{6.6}$$

$$\gamma_C = a_1 + \alpha_2 + c_2. \tag{6.7}$$

Alice can solve for b_2 and c_2 in Eq. 6.6 and 6.7. She then automatically knows the unitaries Bob and Charlie applied. Bob can solve for a_1 from Eq. 6.6. He can then plug this value into Eq. 6.7 to solve for c_2. He can use this information to solve for a_2 in Eq. 6.5. He now knows what unitaries Alice and Charlie have applied. Charlie can solve for a_1 in Eq. 6.7 and then plug this value into Eq. 6.6 to solve for b_2. If she uses all this information, she can solve for a_2 in Eq. 6.5. She now knows what unitaries Alice and Bob have applied to their qubits. Thus everyone can deduce what the secret message of the other two was, hence the protocol is correct. □

6.2.2 N-party Quantum Secure Direct Communication with GHZ

Assuming Alice, Bob, Charlie, ... and Zach want to communicate safely, this can be achieved in two parts [49]. First they check whether the quantum channel is safe:

1. Alice randomly prepares L GHZ states in one of the 2^N different GHZ states as in Sec. 5.4.6 $|\Psi_i\rangle_{ABC...Z}$, where A,B, C ... and Z stand for Alice, Bob, Charlie, ... and Zach respectively and $0 \leq i \leq 2^N$.
2. Alice sends Bob, Charlie, ... and Zach their qubits.
3. Bob chooses an arbitrary subset M and measures them in the z- or the x-basis randomly. He communicates which qubits and their outcomes to the others classically.
4. Alice, Charlie, ... and Zach measure their corresponding qubits in the same basis. Charlie, ... and Zach communicate their results with Alice through a classical channel.
5. With the measurement outcomes and the sequence of GHZ states that Alice prepared, she can detect eavesdropping.

When they have established that the channel is safe, they proceed with direct communication using the remaining $K = L - |M|$ GHZ states.

1. Bob, Charlie, ... and Zach perform I for bit 0 and $i\sigma_y$ for bit 1 on their qubits.
2. They send all their qubits to Alice.
3. Alice performs I for 00, σ_x for 01, $i\sigma_y$ for 10 and σ_z for 11 on her qubit.

4. She measures the entire GHZ state into the GHZ basis. She publishes her outcomes and the original GHZ states.
5. With this information and their own secret message, they can now all deduce the secrets the others encoded.

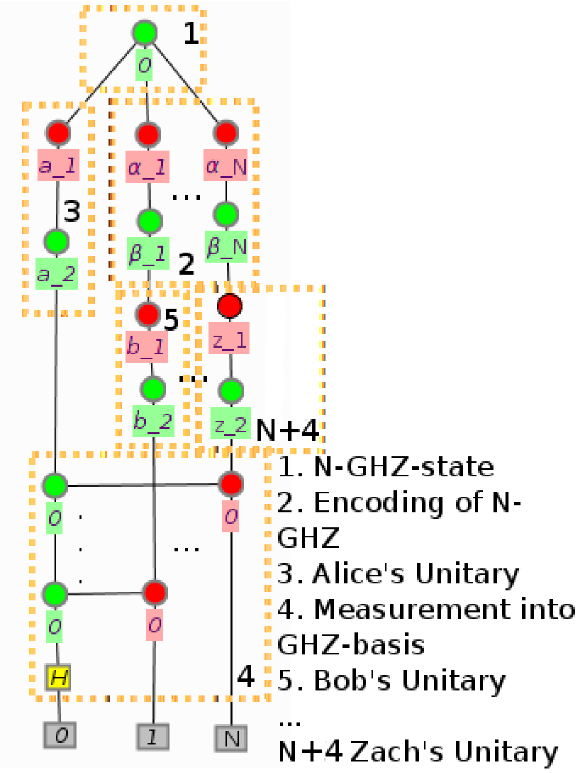


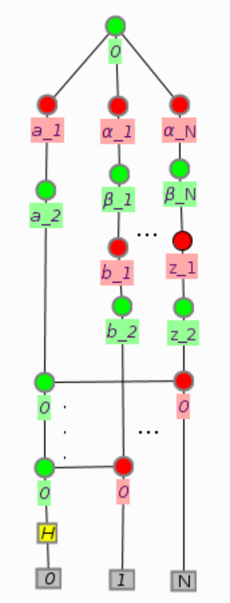
Figure 6.2: Graphical representation of the set of instructions of the N-party Quantum Secure Direct Communication using N-GHZ states. $\alpha_1, \ldots \alpha_N$,$\beta_1, \ldots \beta_N$, $a_1, a_2, b_1, b_2, c_1, c_2, \ldots, z_1, z_2 \in \{0, \pi\}$, $b_1 = b_2$, $c_1 = c_2$, $\ldots$ and $z_1 = z_2$.

Lemma 34. *Fig. 6.2 is the graphical representation of the set of instructions of the N-party Quantum Secure Direct Communication with GHZ.*

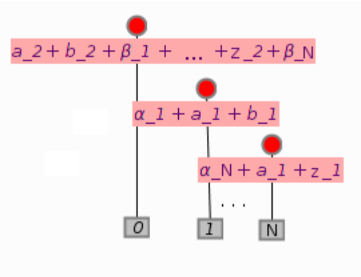
Proof. Box 1 is an N-GHZ state. Box 2 is the encoding of the N-GHZ state into one of the N-GHZ states. Box 3 is Alice's unitary. Box 4 is measurement into the GHZ basis by [13]. Box 5 to $N + 4$ are Bob, Charlie's, $\ldots$ and Zach's unitaries. Because $b_1 = b_2$, $c_1 = c_2$, $\ldots$ and $z_1 = z_2$ and $b_1, b_2, c_1, c_2, \ldots, z_1, z_2 \in \{0, \pi\}$, this is either I or $i\sigma_y$. □

Lemma 35. *The N-party Quantum Secure Direct Communication using N-GHZ states protocol is correct.*

Proof. By Lemma 34 Fig. 6.2 is the graphical representation of the set of instructions. Simplifying this representation in a similar manner as Eq. 6.4 gives



$=$



. (6.8)

Now it is possible for all of them to solve for the phases of the other two. Let the measurement outcome be $\gamma_A, \gamma_B, \dots, \gamma_Z$ for the values of qubit $A, B, \dots Z$ respectively. Then

$$\gamma_A = a_2 + \beta_1 + b_1 + \beta_2 + c_1 \tag{6.9}$$

$$\gamma_B = a_1 + \alpha_1 + b_2 \tag{6.10}$$

$$\dots$$

$$\gamma_Z = a_1 + \alpha_N + z_2. \tag{6.11}$$

Then Alice, Bob, Charlie, . . . and Zach can solve for the unitaries of the others in a similar manner as for the 3-party protocol. □

6.2.3 Security of Quantum Secure Direct Communication with GHZ

There are three different attacks eavesdropper Eve can do; intercept and resend attack, a disturbance attack and a entanglement attack. It will be shown that the 3-party protocol is safe for these attacks. This automatically generalises to the N-party protocol. Note that these percentages are mostly obtained from Dirac notation.

6.2.3.1 Intercept and Resend Attack

In the intercept and resend attack, Eve intercepts the qubits on the quantum channel and replaces them by qubits in $|0\rangle$, $|1\rangle$, $|+\rangle$ or $|-\rangle$. When Bob and Charlie send their qubits back, she would be able to find their unitary operations by measuring the qubits in the correct bases. However, Eve needs to intercept the qubits when Alice sends the qubits to Bob and Charlie respectively. After this the check for eavesdropping takes place. If Eve sends $|01\rangle$ or $|10\rangle$ and Alice, Bob and Charlie select the z- (x-) measuring basis, Eve introduces an error with probability 1 ($\frac{1}{2}$) by Lemma 29 - 31. If Eve sends $|00\rangle$ or $|11\rangle$ and Alice, Bob and Charlie select the z- (x-) measuring basis, Eve introduces an error with probability $\frac{1}{2}$ ($\frac{1}{2}$) by Lemma 29 - 31. If Eve sends $|+-\rangle$ or $|-+\rangle$ and Alice, Bob and Charlie select the z- (x-) measuring basis, Eve introduces an error with probability $\frac{1}{2}^2$ ($\frac{1}{2}$) by Lemma 29 - 31. If Eve sends $|++\rangle$ or $|--\rangle$ and Alice, Bob and Charlie select the z- (x-) measuring basis, Eve introduces an error with probability $\frac{1}{2}^2$ ($\frac{1}{2}$) by Lemma 29 - 31.

6.2.3.2 Disturbance Attack

For this attack, Eve intercepts the qubits when Bob and Charlie send their qubits back to Alice. By measuring these two qubits she will not get any useful information about the entangled state. Alternatively she could apply I or $i\sigma_y$ on the qubits. This would only change the phase of the entanglement. To overcome this, Bob and Charlie can announce random parts of their secret message and their place in the sequence to Alice. If Alice does not find the corresponding bits in her measurement, Eve has disturbed the quantum channel and they can restart the protocol. An alternative way to overcome this would be by encoding the secret with a classical error correction code first.

6.2.3.3 Entanglement Attack

If Eve would intercept the qubits when Alice sends the qubits to Bob and Charlie and entangles her qubit with theirs to create a 4-GHZ state, she might be able to get some information on the secret after Bob and Charlie have applied their unitaries. Although by **F** this does not introduce an error if Alice, Bob and Charlie measure in the z-basis during the eavesdropping test, measuring in to the x-basis introduces an error with $\frac{1}{2}$ probability by Lemma 30 and 31.

6.2.3.4 Impersonation Attack

It seems that Eve could intercept the qubits and pretend to be Bob for example. This could easily be overcome, by not proceeding the protocol until everyone one confirmed receiving the qubits.

6.3 Quantum Secure Communication by Rearranging Particle Orders

In this section the Quantum Secure Communication by Rearranging Particle Orders as described in [39] is presented. It is based on superdense coding with GHZ states. To achieve safe communication between Alice and Bob, the following steps need to be taken:

1. Alice and Bob agree on a superdense coding scheme, like the one in Sec. 5.4. Alice encodes the secret message on a series of $|GHZ\rangle_{ABC}$-states as in the superdense coding scheme.
2. Alice rearranges the A, B and C sequence of qubits. Additionally she randomly inserts some decoy photons in one of $\{|z^+\rangle, |z^-\rangle, |x^+\rangle, |x^-\rangle\}$. Decoy photons are weaker than the rest of the photons. If an eavesdropper tries to intercept the extra photons that sometimes come free at the creation of photons, there is a high probability the decoy photons will be disturbed [43].
3. Alice sends all sequences of qubits to Bob.
4. After Bob confirms that he received all the qubits, Alice announces the places of the decoy photons.
5. Bob measures the decoy photons and announces the outcomes.
6. After Alice's confirmation of the outcomes of the decoy photons, she tells him the correct order for all three sequences.
7. Bob rearranges the particles and measures them in the GHZ basis to retrieve Alice's secret.

Lemma 36. *The Quantum Secure Communication by Rearranging Particle Orders protocol is correct.*

Proof. By Lemma 28. □

6.3.1 Security of Quantum Secure Communication by Rearranging Particle Orders

In this subsection the Security of the of Quantum Secure Communication by Rearranging Particle Orders protocol will be demonstrated. The intercept and resend attack, disturbance attack, entanglement attack and the impersonation attack are discussed. Note that again, it is much more straightforward to get the mentioned percentages from the Dirac presentation than it is from the the graphical presentation.

6.3.1.1 Intercept and Resend Attack

Alice sends all the qubits at once. However, by measuring them Eve cannot get any information about the secret, because the orders are rearranged and decoy photons are added. If Eve decides to keep the qubits and send Bob $\{|z^+\rangle, |z^-\rangle, |x^+\rangle, |x^-\rangle\}$, she has only a $\frac{1}{2}$ probability of not corrupting the measurement outcomes of the decoy photons.

6.3.1.2 Disturbance Attack

If Eve intercepts the qubits and sends random qubits to Bob instead, she has probability $\frac{1}{2}$ of being detected for every decoy qubit.

6.3.1.3 Entanglement Attack

If Eve entangles a qubit with an intercepted qubit and measures it into the z- or x-basis, she has a $\frac{1}{2}$ probability of disturbing the measurement outcome of the decoy photons. Furthermore, even if she remains undetected, measuring just one qubit of an entangled state will not give her any useful information.

6.3.1.4 Impersonation Attack

Eve could intercept the qubits and pretend to be Bob, but the protocol would be interrupted, because Bob did not confirm receiving the qubits.

6.4 Multi-step Quantum Secure Direct Communication with GHZ

In this section the Multi-step Quantum Secure Direct Communication with GHZ protocol as described in [83] is presented. First it will be presented for 3-GHZ and then for M-GHZ.

6.4.1 Multi-step Quantum Secure Direct Communication with 3-GHZ

The Multi-step Quantum Secure Direct Communication with 3-GHZ protocol is based on superdense coding with GHZ as in Sec. 5.4. If Alice and Bob want to communicate safely, this can be managed with the following steps [83]:

1. Alice produces N $|GHZ\rangle_{ABC}$-states.
2. Alice sends the sequence of C-qubits to Bob.
3. There are two different ways to check for eavesdropping now:
   (a) Bob measures an arbitrary subset in the z- or x-basis randomly. He announces the place and basis to Alice, who measures both her qubits in the same basis. They then announce their results to see if eavesdropping has taken place.

(b) Bob measures an arbitrary subset in the z- or x-basis randomly. He announces the place and basis to Alice, who measures both her qubits in the z- basis, if Bob measured in the z-basis and in the Bell basis otherwise. They then announce their results to see if eavesdropping has taken place.

4. Alice now takes an arbitrary subset R of the AB-sequence and randomly applies one of eight different operations on them.
5. Alice encodes her secret message on the remaining particles, with the Superdense coding scheme from Sec. 5.4.
6. Alice sends Bob the B-sequence of qubits.
7. Alice chooses an arbitrary subset of R. They check for eavesdropping in a similar way as in step 3, but with the Alice's and Bob's roles reversed.
8. If no eavesdropping is detected, Alice sends Bob the A-sequence.
9. Alice announces the remaining GHZ states in R and their states. Bob measures these states in the GHZ basis and compares his results. If they are the same, he knows that message is not distorted.
10. Bob now measures the remaining GHZ states into the GHZ basis to retrieve Alice's secret message.

Lemma 37. *The Multi-step Quantum Secure Direct communication with 3-GHZ is correct.*

Proof. By Lemma 28. □

6.4.2 Multi-step Quantum Secure Direct communication with M-GHZ

To achieve secure communication between Alice and Bob, the following steps need to be taken

1. Alice produces N $|GHZ\rangle_{12\ldots M}$-states.
2. Alice sends the sequence of M-qubits to Bob.
3. They pick on of two ways to check for eavesdropping from step 3 of the 3-GHZ protocol.
4. Alice now takes an arbitrary subset R of the $1\ldots(M-1)$-sequences and randomly applies one of 2^M different unitary operations on them.
5. Alice encodes her secret message on the remaining particles, with a Superdense coding scheme for M-GHZ as in Sec. 5.4.6.
6. Alice sends Bob the $(M-1)$-sequence of qubits.
7. Alice chooses an arbitrary subset of R. They check for eavesdropping in a similar way as in step 3, but with the Alice's and Bob's roles reversed.

8. They repeat step 6 and 7 until all the qubits are sent, but for the last sequence of qubits step 7 is skipped. If eavesdropping is detected at any point, the protocol is aborted,
9. Alice announces the remaining random GHZ states and their states. Bob measures these states in the M-GHZ basis and compares his results. If they are the same, he knows that message is not distorted.
10. Bob now measures the remaining GHZ states into the GHZ basis to retrieve Alice's secret message.

Lemma 38. *The Multi-step Quantum Secure Direct communication with M-GHZ protocol is correct.*

Proof. By Sec. 5.4.6. □

6.4.3 Security of Multi-step Quantum Secure Direct communication with GHZ states

In this subsection the security of the Multi-step Quantum Secure Direct communication with GHZ protocol will be demonstrated. First it will be shown that during the test for eavesdropping, there are determined combinations of measurement outcomes they should get. Furthermore, the intercept and resend attack, disturbance attack, entanglement attack and the impersonation attack are discussed. The security will be shown for the protocol with 3-GHZ. This generalises to M-GHZ easily. Note that the percentages mentioned in this subsection are based on both Dirac notation and the ZX-calculus.

6.4.3.1 Test for Eavesdropping

At three stages in this protocol, Alice and Bob test GHZ for eavesdropping, by measuring in the z-, x- or Bell Basis. In Table 6.1 it is shown that for all eight GHZ states measuring in the z-, x- and Bell basis has determined combinations of outcomes.

6.4.3.2 Intercept and Resend Attack

All qubits are sent as singletons. By measuring just one qubit of an entangled state, Eve cannot get any information on the entangled state. If Eve decides to keep the qubits and send Bob $\{|z^+\rangle, |z^-\rangle, |x^+\rangle, |x^-\rangle\}$, she has a $\frac{1}{2}$ probability of corrupting the measurement outcomes.

6.4.3.3 Disturbance Attack

If Eve intercepts the qubits and sends random qubits to Bob instead, she has a $\frac{1}{2}$ probability of being detected for every checked qubit.

6.4.3.4 Entanglement Attack

If Eve entangles a qubit with an intercepted qubit, and measures her qubit in the x-basis she will distort the measurement outcomes with $\frac{1}{2}$ probability if they measure in the x-basis as well. This is, because, she will transform the GHZ state if she gets measurement outcome $|x^{-}\rangle$. The measurement outcomes will not be disturbed if they decide to measure in the z-basis. If Eve measures into the z-basis she will not distort the measurement outcomes if Alice and Bob also measure in the z-basis, but with $\left(\frac{1}{2}\right)^2$ probability if they measure in the x-basis. If Eve postpones the measurement until the bases are announced, she will not disturb the measurement outcomes. However, measuring her single qubit will not give her any information on the total entangled state, which is necessary to retrieve the secret message.

6.4.3.5 Impersonation Attack

Eve can intercept the qubits and pretend to be Bob. This could be easily remedied by inserting a confirmation of reception from Bob after each sequence of qubits is sent.

6.5 Multi-party Quantum Direct Communication with GHZ states

In this section the Multi-party Quantum Direct Communication with GHZ states protocol as described in [46]. First it will be presented for three people and then it will be expanded to an N-party protocol.

6.5.1 Multi-party Quantum Direct Communication with GHZ states for three people

Assuming that Alice wants to share a common secret with Bob and Charlie, the following steps need to be taken[46]:

1. Alice generates N $|GHZ\rangle_{ABC}$-states. She keeps the B and C-sequence and sends Bob the A-sequence.
2. Bob checks whether the received photons are single photons by means of a photon number splitter and single-photon detectors. After Bob confirms that the received photons are single photons, he performs one of $\{I, i\sigma_y, \sigma_x, \sigma_z\}$. Then he randomly inserts decoy photons in one of $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and sends the whole sequence to Charlie.
3. After Charlie confirms receiving the qubits, Bob and Charlie use the decoy photons to check for eavesdropping.

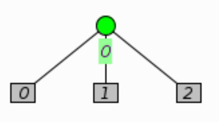
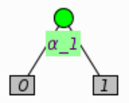
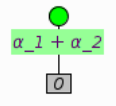
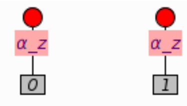
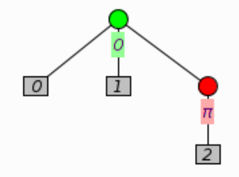
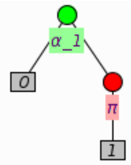
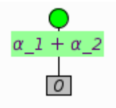
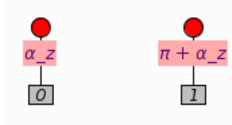
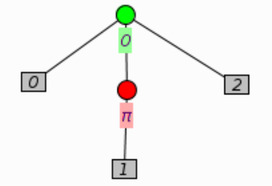
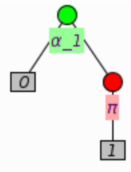
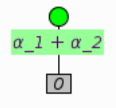
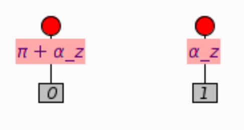
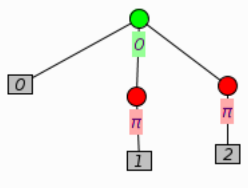
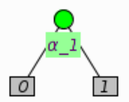
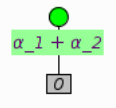
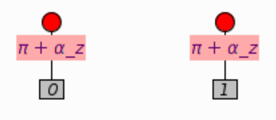
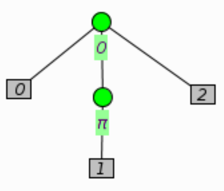
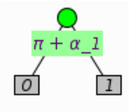
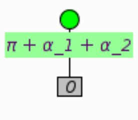
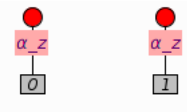
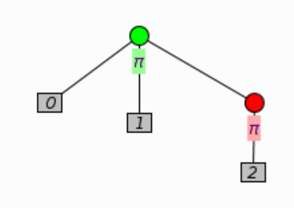
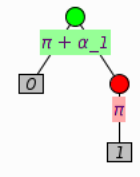
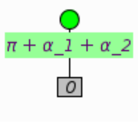
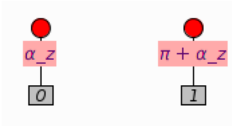
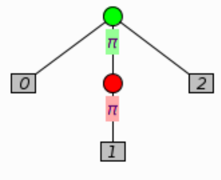
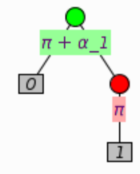
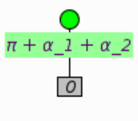
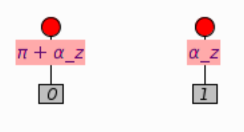
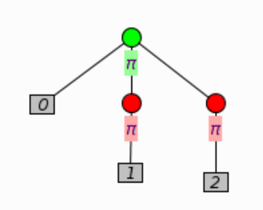
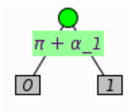
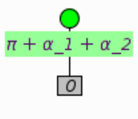
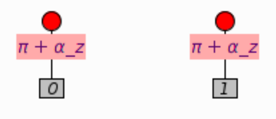
#	State	Bell basis	x-basis	z-basis
0				
1				
2				
3				
4				
5				
6				
7				

Table 6.1: This table shows for each different state in the GHZ class, the Bell basis it is in after one x-basis measurement, the state after two x-basis measurements and the state after one z-basis measurement.

4. After confirming that the channel is safe, Alice encodes her secret with the superdense coding scheme for GHZ from Sec. 5.4. Then she randomly inserts decoy photons in one of $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and sends both sequences to Charlie.
5. After Charlie confirms receiving both sequences, Alice announces the location and state of the decoy photons. Charlie measures the decoy photons to check for eavesdropping.
6. After concluding that the channel was safe, Charlie measures into the GHZ basis. With their measurement outcome and Bob's unitary operations, they can deduce Alice's secret message.

Lemma 39. *The Multi-party Quantum Secure Direct communication with GHZ for three people is correct.*

Proof. By Lemma 28. □

6.5.2 Multi-party Quantum Direct Communication with GHZ states with N people

To expand this protocol to N people, Bob1, Bob2, ..., Bob($N-3$) are added. Step 2 is repeated for all Bobs and the processed qubits are transmitted from Bob to Bob1 to Bob2 to ...Bob($N-3$) sequentially until they are finally passed on to Charlie. Note that they still use a 3-GHZ state. After the last step is finished, Charlie needs the help of all Bobs together to deduce the secret message.

Lemma 40. *The Multi-party Quantum Secure Direct communication with GHZ for N people is correct.*

Proof. By Lemma 28. □

6.5.3 Security of Multi-party Quantum Direct Communication with GHZ states

Since this security depends on decoy photons too, it is similar to the security of the Quantum Secure Communication by Rearranging Particle Orders protocol in Sec. 6.3.1.

6.6 Quantum Direct Communication with GHZ and Entanglement Swapping

The Quantum Direct Communication with GHZ and Entanglement Swapping protocol as described in [40] is presented in this section.

6.6.1 Quantum Direct Communication with GHZ and Entanglement Swapping

Suppose Alice, Bob and Charlie initially share N times two GHZ states: $|GHZ\rangle_{A_1B_1C_1} \otimes |GHZ\rangle_{A_2B_2C_2}$, where $A_i, B_i, C_i, i \in \{1, 2\}$, stand for Alice, Bob and Charlie respectively, to establish secure communication the following steps need to be undertaken:

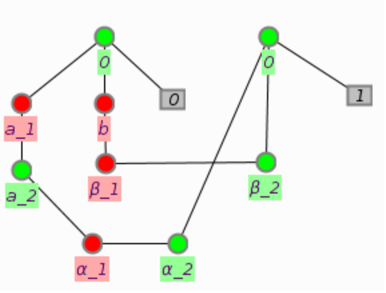
1. Alice encodes 00 as I, 01 as σ_x, 10 as σ_y and 11 as σ_z on the A_1-sequence.
2. Bob encodes 0 as I and 1 as σ_x on the B_1-sequence.
3. Alice and Bob make a Bell state measurement on the qubit sequences A_1A_2 and B_1B_2 respectively.
4. After confirming Alice and Bob did the measurements, Charlie makes a Bell state measurement on the qubit sequence C_1C_2.
5. Alice and Bob publicly announce their measurement outcomes.
6. With this information and her own measurement outcome, Charlie can deduce what unitary Alice and Bob have applied. See Table 6.2 for details. This table can easily be expanded by manipulation of the first eight entries. Go to the measurement outcome Charlie got. Alice and Bob applied the unitary needed to transform measurement outcome they would have gotten without applying unitary to the measurement outcome they actually obtained. An example is shown for Alice and Bob both applying σ_x.

Lemma 41. *Fig. 6.3 is the graphical representation of the set of instructions of the Quantum Direct Communication with GHZ and Entanglement Swapping protocol.*

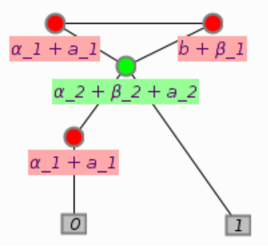
Proof. Box 1 and 2 are two GHZ states, shared by Alice, Bob and Charlie. Box 3 and 4 are Alice's and Bob's unitary operations respectively. Box 5 and 6 are Bell state measurements on qubits A_1A_2 and B_1B_2. □

Lemma 42. *The Quantum Direct Communication with GHZ and Entanglement Swapping protocol is correct.*

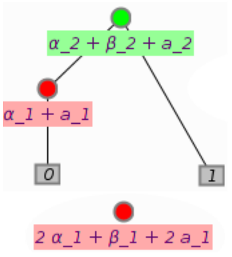
Proof. By Lemma 41 Fig. 6.3 is the graphical representation. Rewriting gives



$\overset{(\mathbf{K1}),(\mathbf{K2})}{=}$



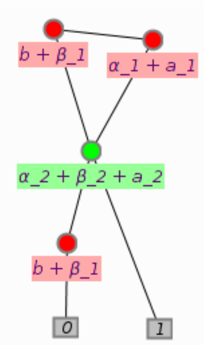
$\overset{(\mathbf{B'}),(\mathbf{S})}{=}$



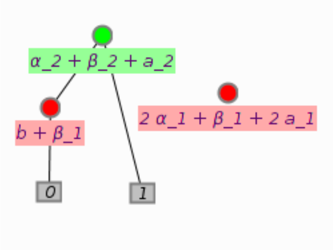
Alice	Bob	Charlie	U Alice	U Bob	a_1	a_2	b	α_1	α_2	β_1	β_2
$\|\phi^+\rangle$	$\|\phi^+\rangle$	$\|\phi^+\rangle$	I	I	0	0	0	0	0	0	0
$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\phi^-\rangle$	I	I	0	0	0	0	0	0	π
$\|\phi^-\rangle$	$\|\phi^+\rangle$	$\|\phi^-\rangle$	I	I	0	0	0	0	π	0	0
$\|\phi^-\rangle$	$\|\phi^-\rangle$	$\|\phi^+\rangle$	I	I	0	0	0	0	π	0	π
$\|\psi^+\rangle$	$\|\psi^+\rangle$	$\|\psi^+\rangle$	I	I	0	0	0	π	0	π	0
$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|\psi^-\rangle$	I	I	0	0	0	π	0	π	π
$\|\psi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$	I	I	0	0	0	π	π	π	0
$\|\psi^-\rangle$	$\|\psi^-\rangle$	$\|\psi^+\rangle$	I	I	0	0	0	π	π	π	π
$\|\phi^+\rangle$	$\|\phi^+\rangle$	$\|\psi^+\rangle$	σ_x	σ_x	π	0	π	0	0	0	0
$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\psi^-\rangle$	σ_x	σ_x	π	0	π	0	0	0	π
$\|\phi^-\rangle$	$\|\phi^+\rangle$	$\|\psi^-\rangle$	σ_x	σ_x	π	0	π	0	π	0	0
$\|\phi^-\rangle$	$\|\phi^-\rangle$	$\|\psi^+\rangle$	σ_x	σ_x	π	0	π	0	π	0	π
$\|\psi^+\rangle$	$\|\psi^+\rangle$	$\|\phi^+\rangle$	σ_x	σ_x	π	0	π	π	0	π	0
$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|\phi^-\rangle$	σ_x	σ_x	π	0	π	π	0	π	π
$\|\psi^-\rangle$	$\|\psi^+\rangle$	$\|\phi^-\rangle$	σ_x	σ_x	π	0	π	π	π	π	0
$\|\psi^-\rangle$	$\|\psi^-\rangle$	$\|\phi^+\rangle$	σ_x	σ_x	π	0	π	π	π	π	π
...	...	...	...	...	...	...	...	...	...	...	...

Table 6.2: Charlie's measurement outcome with Alice's and Bob's measurement outcomes and unitary operations next to the phases of fig. 6.3.

$\overset{(\mathbf{K1}),(\mathbf{K2})}{=}$



$\overset{(\mathbf{B'}),(\mathbf{S})}{=}$



. (6.12)

In Table 6.2 the phases are displayed next to the corresponding measurement outcomes and unitaries. □

6.6.2 Security of Quantum Direct Communication with GHZ and Entanglement Swapping

Since the qubit distribution is not part of this protocol it is safe from an intercept and resend attack, disturbance attack, entanglement attack and impersonation attack, simply because Eve does not have access to the qubits. Note also that Eve cannot deduce Alice's and Bob's unitary operations without Charlie's measurement outcome. This means that the public information is not enough to deduce the secret.

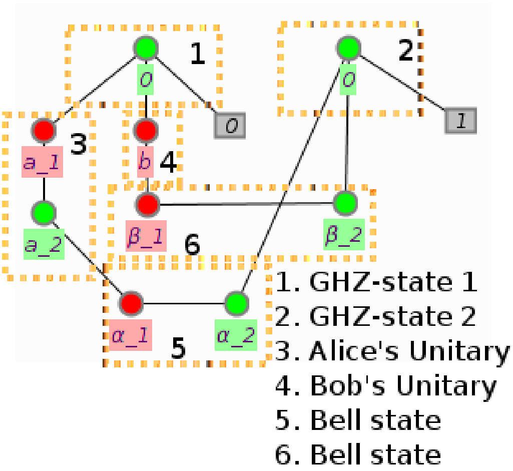


Figure 6.3: Graphical representation of the set of instructions of the Quantum Direct Communication with GHZ and Entanglement Swapping protocol. α_1, α_2, β_1, β_2, $a_1, a_2, b \in \{0, \pi\}$.

6.7 Quantum Direct Communication with Authentication

In this section the Quantum Direct Communication with Authentication protocol as described in [60, 59] will be explained. Moreover, its validity is shown with the ZX-calculus.

6.7.1 Quantum Direct Communication with Authentication

If Alice wants to safely communicate with Bob and there is a trusted, more powerful party Trent, who is not involved in the communication directly, Quantum Authentication can be achieved as follows [60, 59]:

1. Every user (Alice and Bob) has a secret identity (ID_A, ID_B) and a one-way hash function (h_A, h_B) registered with Trent. This identity and hash function are known only to the user and Trent. The hash function h is of the form $h : \{0,1\}^* \times \{0,1\}^c \rightarrow \{0,1\}^l$, where $*$ is an arbitrary length, c the value of a counter and l is a fixed number. Trent calculates Alice's (Bob's) key as $h_A(ID_A, c_A)$ ($h_B(ID_B, c_B)$), where c_A (c_B) is the number of calls on Alice's (Bob's) hash function.
2. Trent generates N $|GHZ\rangle_{ATB}$ - states, where the subscript A, T and B correspond to Alice, Trent and Bob.
3. Trent encodes Alice's and Bob's qubits with their authentication keys. For every bit i he applies the Hadamard operator H to qubit i if the bit is 1, and nothing otherwise.
4. Trent sends Alice's and Bob's qubits to them and keeps his own qubits.
5. Alice and Bob decode their qubits with their authentication keys.

6. They select some random qubits to check for eavesdropping. If the error rate is not higher than the threshold they proceed with the protocol. Otherwise the authentication fails and they start over.

When the authentication is successful, Quantum Direct Communication can be achieved as follows [60, 59]:

1. Alice chooses a random subset R of the her qubits to encode her secret message. Alice encodes the secret message s with a classical error correction code to obtain s'. For every bit j in s' she applies H to qubit j in R if the bit is 0 and $H\sigma_x$ if the bit is 1.
2. She generates a random bit string r and does the same thing for r and the remaining qubits.
3. Alice transfers all her qubits to either Bob or Trent, depending on whether there is a quantum channel between Alice and Bob or not.
4. Bob (Trent) measures qubits AB (AT) in the Bell basis and Trent (Bob) measures his qubits in the x-basic. Trent publicly announces his measurement outcomes. With this information and his own measurement outcomes Bob can deduce Alice's unitary operations as in Table 6.3 [1]. For the values in the table Trent does the x-basis measurement and Bob does the Bell state measurement.

Note that after Alice applies H, the total state looks like

$$\begin{aligned}
(H \otimes I \otimes I) |GHZ\rangle_{ATB} &= \frac{1}{2}((|0\rangle + |1\rangle) |00\rangle + (|0\rangle - |1\rangle) |11\rangle) \\
&= \frac{1}{2}(|000\rangle + |001\rangle + |011\rangle - |111\rangle) \\
&= \frac{1}{4}(|000\rangle - |001\rangle + |110\rangle - |111\rangle - |010\rangle + |011\rangle \\
&\quad + |100\rangle - |101\rangle + |000\rangle + |001\rangle - |110\rangle - |111\rangle \\
&\quad + |010\rangle + |011\rangle + |100\rangle + |101\rangle) \\
&= \frac{1}{4}((|00\rangle + |11\rangle - |01\rangle + |10\rangle)(|0\rangle - |1\rangle) \\
&\quad + (|00\rangle - |11\rangle + |01\rangle + |10\rangle)(|0\rangle + |1\rangle)) \\
&= \frac{1}{2}((|\phi^+\rangle_{AB} - |\psi^-\rangle_{AB}) |-\rangle_T + (|\phi^-\rangle_{AB} + |\psi^+\rangle_{AB}) |+\rangle_T).
\end{aligned} \tag{6.13}$$

[1] Note that table 1 and 2 in [60], which should contain the same information as Table 6.3, actually contain faulty information.

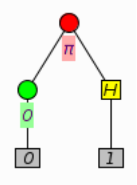
And after she applies $H\sigma_x$, the state looks like

$$\begin{aligned}(H\sigma_x \otimes I \otimes I)\left|GHZ\right\rangle_{ATB} &= \frac{1}{2}((\left|0\right\rangle - \left|1\right\rangle)\left|00\right\rangle + (\left|0\right\rangle + \left|1\right\rangle)\left|11\right\rangle) \\ &= \frac{1}{2}(\left|000\right\rangle - \left|100\right\rangle + \left|011\right\rangle + \left|111\right\rangle) \\ &= \frac{1}{4}(\left|000\right\rangle + \left|001\right\rangle + \left|110\right\rangle + \left|111\right\rangle + \left|010\right\rangle + \left|011\right\rangle \\ &\quad - \left|100\right\rangle - \left|101\right\rangle + \left|000\right\rangle - \left|001\right\rangle - \left|110\right\rangle + \left|111\right\rangle \\ &\quad - \left|010\right\rangle + \left|011\right\rangle - \left|100\right\rangle + \left|101\right\rangle) \\ &= \frac{1}{4}((\left|00\right\rangle + \left|11\right\rangle + \left|01\right\rangle - \left|10\right\rangle)(\left|0\right\rangle + \left|1\right\rangle) \\ &\quad + (\left|00\right\rangle - \left|11\right\rangle - \left|01\right\rangle - \left|10\right\rangle)(\left|0\right\rangle - \left|1\right\rangle)) \\ &= \frac{1}{2}((\left|\phi^+\right\rangle_{AB} + \left|\psi^-\right\rangle_{AB})\left|+\right\rangle_T + (\left|\phi^-\right\rangle_{AB} - \left|\psi^+\right\rangle_{AB})\left|-\right\rangle_T).\end{aligned} \tag{6.14}$$

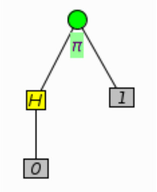
Trent	Bob	Alice	α	β	γ	δ	Trent	Bob	Alice
$\left|-\right\rangle$	$\left|\phi^+\right\rangle$ or $\left|\psi^-\right\rangle$	H	0	π	0	π	$\left|-\right\rangle$	$\frac{1}{\sqrt{2}}(\left|\phi^+\right\rangle - \left|\psi^-\right\rangle)$	H
$\left|+\right\rangle$	$\left|\phi^-\right\rangle$ or $\left|\psi^+\right\rangle$	H	0	0	0	0	$\left|+\right\rangle$	$\frac{1}{\sqrt{2}}(\left|\phi^-\right\rangle + \left|\psi^+\right\rangle)$	H
$\left|+\right\rangle$	$\left|\phi^+\right\rangle$ or $\left|\psi^-\right\rangle$	$H\sigma_x$	π	0	π	0	$\left|+\right\rangle$	$\frac{1}{\sqrt{2}}(\left|\phi^+\right\rangle + \left|\psi^-\right\rangle)$	$H\sigma_x$
$\left|-\right\rangle$	$\left|\phi^-\right\rangle$ or $\left|\psi^+\right\rangle$	$H\sigma_x$	π	π	π	π	$\left|-\right\rangle$	$\frac{1}{\sqrt{2}}(\left|\phi^-\right\rangle - \left|\psi^+\right\rangle)$	$H\sigma_x$

Table 6.3: Alice's unitary operation, given Trent's and Bob's measurement outcomes next to the corresponding phases of Fig. 6.4 and 6.5. Trent measures in the x-basis and Bob measures in the Bell basis.

Lemma 43.

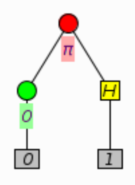


$=$



$$= \frac{1}{\sqrt{2}}(\left|\phi^+\right\rangle - \left|\psi^-\right\rangle)$$

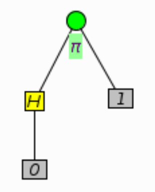
Proof.



$$= (I \otimes H) \left|\psi^+\right\rangle = \frac{1}{2}(|0\rangle\,(|0\rangle - |1\rangle) + |1\rangle\,(|0\rangle + |1\rangle))$$

$$= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\left|\phi^+\right\rangle - \left|\psi^-\right\rangle) \tag{6.15}$$

$$\overset{(\mathbf{C}),(\mathbf{H})}{=}$$

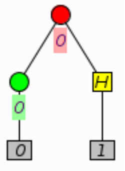


$$= (H \otimes I) \left|\phi^-\right\rangle = \frac{1}{2}((|0\rangle + |1\rangle)\,|0\rangle - (|0\rangle - |1\rangle)\,|1\rangle)$$

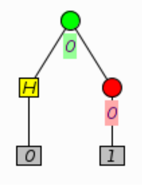
$$= \frac{1}{2}(|00\rangle + |10\rangle - |01\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\left|\phi^+\right\rangle - \left|\psi^-\right\rangle). \tag{6.16}$$

□

Lemma 44.

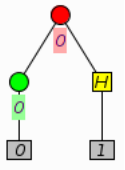


$=$



$$= \frac{1}{\sqrt{2}}(\left|\phi^-\right\rangle + \left|\psi^+\right\rangle)$$

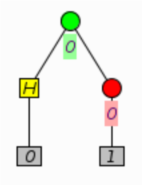
Proof.



$$= (I \otimes H) \left|\phi^+\right\rangle = \frac{1}{2}(|0\rangle\,(|0\rangle + |1\rangle) + |1\rangle\,(|0\rangle - |1\rangle))$$

$$= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(\left|\phi^-\right\rangle + \left|\psi^+\right\rangle) \tag{6.17}$$

$$\overset{(\mathbf{S})}{=}$$

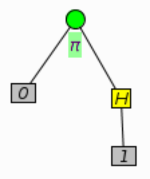


$$= (H \otimes I) \left|\phi^+\right\rangle = \frac{1}{2}((|0\rangle + |1\rangle)\,|0\rangle + (|0\rangle - |1\rangle)\,|1\rangle)$$

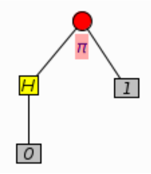
$$= \frac{1}{2}(|00\rangle + |10\rangle + |01\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(\left|\phi^-\right\rangle + \left|\psi^+\right\rangle). \tag{6.18}$$

□

Lemma 45.

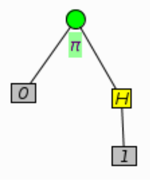


$$=$$



$$= \frac{1}{\sqrt{2}}(\left|\phi^+\right\rangle + \left|\psi^-\right\rangle)$$

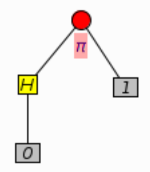
Proof.



$$= (I \otimes H)\left|\phi^-\right\rangle = \frac{1}{2}(|0\rangle(|0\rangle + |1\rangle) - |1\rangle(|0\rangle - |1\rangle))$$

$$= \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\left|\phi^+\right\rangle + \left|\psi^-\right\rangle) \tag{6.19}$$

$$\overset{(\mathbf{C}),(\mathbf{H})}{=}$$

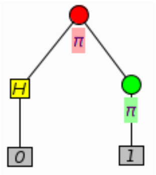


$$= (H \otimes I)\left|\psi^+\right\rangle = \frac{1}{2}((|0\rangle + |1\rangle)|1\rangle + (|0\rangle - |1\rangle)|0\rangle)$$

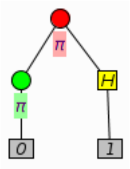
$$= \frac{1}{2}(|01\rangle + |11\rangle + |00\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(\left|\phi^+\right\rangle + \left|\psi^-\right\rangle). \tag{6.20}$$

□

Lemma 46.

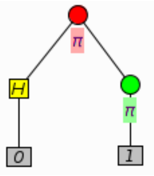


$$=$$

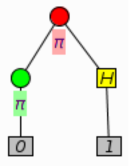


$$= \frac{1}{\sqrt{2}}(\left|\phi^-\right\rangle - \left|\psi^+\right\rangle)$$

Proof.



$$\overset{(\mathbf{C}),(\mathbf{H})}{=}$$



$$= (I \otimes H)\left|\psi^-\right\rangle = \frac{1}{2}(|0\rangle(|0\rangle - |1\rangle) - |1\rangle(|0\rangle + |1\rangle))$$

$$= \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(\left|\phi^-\right\rangle - \left|\psi^+\right\rangle). \tag{6.21}$$

□

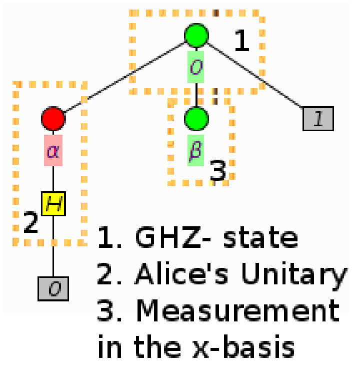


Figure 6.4: Graphical representation of Alice's unitary operation and the x-basis measurement in the set of instructions of the Quantum Direct Communication protocol. $\alpha, \beta \in \{0, \pi\}$

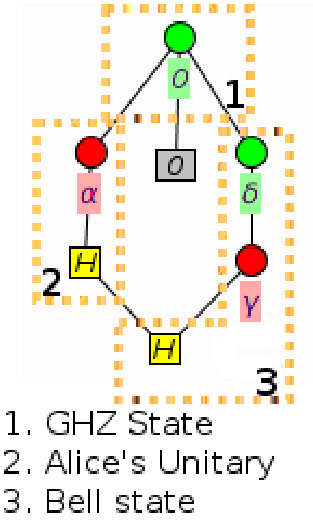


Figure 6.5: Graphical representation of Alice's unitary operation and the Bell basis measurement in the set of instructions of the Quantum Direct Communication protocol. $\alpha, \gamma, \delta \in \{0, \pi\}$

Lemma 47. *Fig. 6.4 is the graphical representation of Alice's unitary operation and the x-basis measurement, as part of the set of instructions of the Quantum Direct Communication protocol.*

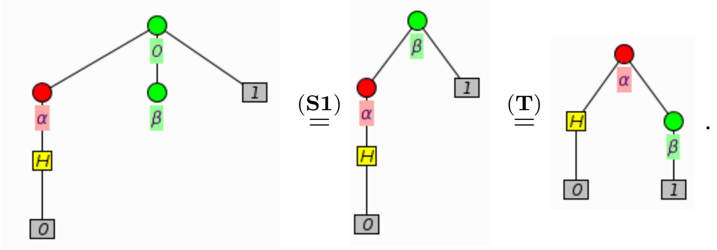
Proof. Box 1 is a GHZ state. Box 2 is $H\sigma_x$ or H, depending on the value of α. Box 3 is a measurement in the x-basis. □

Lemma 48. *Fig. 6.5 is the graphical representation of Alice's unitary operation and the Bell state measurement, as part of the set of instructions of the Quantum Direct Communication protocol.*

Proof. Box 1 is a GHZ state. Box 2 is $H\sigma_x$ or H, depending on the value of α. Box 2 is $\frac{1}{\sqrt{2}}(\langle\phi^+| \pm \langle\psi^-|)$ or $\frac{1}{\sqrt{2}}(\langle\phi^-| \pm \langle\psi^+|)$, depending on the values of γ and δ by Lemma 43 - 46. These are the values it should take by Eq. 6.13 and 6.14. □

Lemma 49. *The measurement outcome in the x-basis and Alice's unitary imply the measurement outcome in the Bell basis.*

Proof. The graphical representation is given in Fig. 6.4 by Lemma 47.

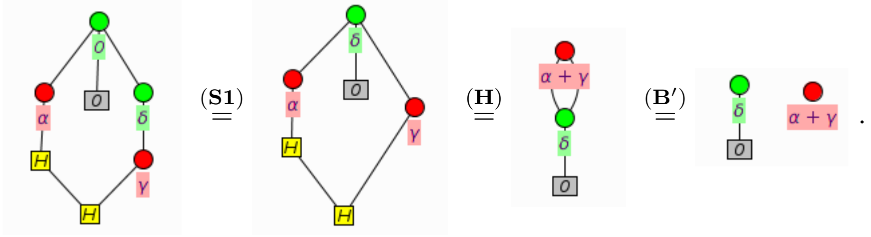


(6.22)

The possible values for α and β are given in Table 6.3; they imply the correct Bell basis states as expected. □

Lemma 50. *The measurement outcome in the Bell basis and Alice's unitary imply the measurement outcome in the x-basis.*

Proof. The graphical representation is given in Fig. 6.5 by Lemma 48.



(6.23)

The possible values for α, γ and δ are given in Table 6.3; they imply the correct x-basis states as expected. □

Corollary 51. *The Quantum Direct Communication Protocol is correct.*

6.7.2 Security of Quantum Direct Communication with Authentication

There are four different attacks eavesdropper Eve can do; intercept and resend attack, disturbance attack, entanglement attack and the impersonation attack. It will be shown that the 3-party protocol is safe for these attacks. This automatically generalises to the N-party protocol. Note that finding the probabilities presented in this subsection is much more straightforward in Dirac notation, than in the ZX-calculus.

6.7.2.1 Intercept and Resend Attack

In the intercept and resend Attack Eve intercepts the qubits on the quantum channel when Trent sends the qubits to Alice and instead sends Bob and Alice qubits in one of $\{|0\rangle, |1\rangle, |+\rangle, |1\rangle\}$. However, during the authentication process, Eve introduces an error with $\frac{1}{2}$ probability, because there is a $\frac{1}{2}$ probability she guessed correctly, whether they will apply a Hadamard gate or not. Then there is $\frac{1}{2}$ probability she guessed the right state. If she guessed wrong, there is still $\frac{1}{2}$ probability that they get the correct measurement outcome.

6.7.2.2 Disturbance Attack

For this attack, Eve intercepts the qubits when Alice sends her qubits to Bob (Trent). She starts by applying a Hadamard gate. However, by measuring this qubit she is not able to find out whether Alice applied σ_x or not. Alternatively she could apply H or $H\sigma_x$ on the qubits. This would only change the phase of the entanglement. To overcome this, Alice can announce random parts of their secret message and their place in the sequence to Bob. If Bob does not find the corresponding bits in his measurement, Eve has disturbed the quantum channel. If she did not disturb too many qubits, he could still retrieve the secret with the error correction code Otherwise they restart the protocol.

6.7.2.3 Entanglement Attack

If Eve would intercept the qubits when Trent sends the qubits to Alice and Bob and entangles her qubit with Alice's to create a 4-GHZ state, she can intercept Alice's qubit again when she sends it to Bob (Trent) and try to get some information. Although this introduces no error when Alice, Trent and Bob measure into the z-basis during the check for eavesdropping, it introduces an error with probability $\frac{1}{2}$ by Lemma 30 and 31, when they measure into x-basis. So Eve introduces an error with probability $\frac{1}{4}$ overall.

6.7.2.4 Impersonation Attack

In the Impersonation Attack Eve intercepts the qubits on the quantum channel when Trent sends the qubits to Alice and Bob and impersonates herself as being Alice and Bob. Like Alice and Bob would have done, she measures the selected qubits into the z- or x-basis, during the check for eavesdropping. If the bit was 0, she introduces no error. However, if the bit was 1 and a Hadamard gate is applied, she introduces an error with probability $\frac{1}{2}$, per check bit by Lemma 29 - 31. Thus she introduces an error with probability $\frac{1}{4}$.

6.8 Improved Quantum Direct Communication with Authentication

This section reviews the Improved Quantum Direct Communication with Authentication protocol as proposed by Zhang et al. in [90]. First it will be shown that the previous protocol is prone to an attack by Trent, after which the improved version will be presented. Finally it will be shown that this improved version is not prone to a Trent-attack.

6.8.1 Trent-Attack of the Quantum Direct Communication protocol

After the authentication is completed, Alice sends her qubits to either Bob or Trent. If Trent obtains Alice's qubits, either by a man in the middle attack, or because this is part of the protocol, he can obtain the secret. This is done as follows [60]

1. Trent applies a Hadamard gate on Alice's qubits.
2. He measures both qubits in the z-basis. From the outcomes he can deduce Alice's unitary operation. If they are the same she applied H, if they are different she applied $H\sigma_x$, which can be inferred from Table 6.4.

Lemma 52. *Fig. 6.6 is the graphical representation of the set of instructions of the Trent-Attack of the Quantum Direct Communication Protocol.*

Proof. Box 1 is a GHZ state, Box 2 is Alice's unitary. Box 3 is a Hadamard gate and finally box 4 is a measurement into the z-basis. □

Lemma 53. *The Trent-Attack of the Quantum Direct Communication protocol is correct.*

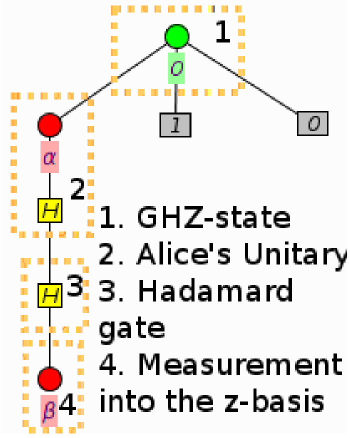
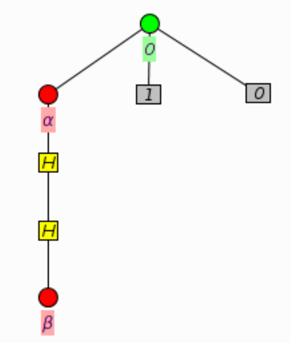
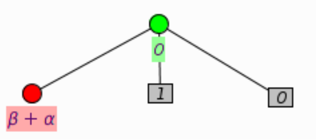


Figure 6.6: Graphical representation of the set of instructions of the Trent-Attack of the Quantum Direct Communication protocol. $\alpha, \beta \in \{0, \pi\}$

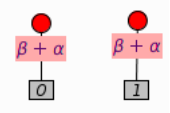
Proof. Fig 6.6 is the graphical representation by Lemma 52. Simplifying it yields



$$\overset{(\mathbf{H})}{=}$$



$$\overset{(\mathbf{B1})/(\mathbf{M})}{=}$$



$$. \qquad (6.24)$$

In table 6.4 it is shown that the corresponding phases yield the correct results. □

Alice's qubit	Trent's qubit	Alice's unitary	α	β	$\alpha+\beta$	Trent's qubit
$\|0\rangle$	$\|0\rangle$	H	0	0	0	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$	H	0	π	π	$\|1\rangle$
$\|0\rangle$	$\|1\rangle$	$H\sigma_x$	π	0	π	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$H\sigma_x$	π	π	0	$\|0\rangle$

Table 6.4: Alice's unitary operation, given Trent's measurement outcomes next to the corresponding phases of Fig. 6.6.

6.8.2 Improved Quantum Direct Communication with Authentication protocol

To prevent a Trent-attack, Zhang et al. propose to alter the Quantum Direct Communication with Authentication protocol from [60, 59]. Their improved protocol is exactly the same,

Trent	Bob	Alice	α	β	γ	Trent	Bob	Alice
$\|-\rangle$	$\|\phi^+\rangle$ or $\|\psi^-\rangle$	H	0	π	π	$\|-\rangle$	$\frac{1}{\sqrt{2}}(\|\phi^+\rangle - \|\psi^-\rangle)$	H
$\|+\rangle$	$\|\phi^-\rangle$ or $\|\psi^+\rangle$	H	0	0	0	$\|+\rangle$	$\frac{1}{\sqrt{2}}(\|\phi^-\rangle + \|\psi^+\rangle)$	H
$\|+\rangle$	$\|\phi^+\rangle$ or $\|\psi^-\rangle$	$H\sigma_z$	π	0	π	$\|+\rangle$	$\frac{1}{\sqrt{2}}(\|\phi^+\rangle - \|\psi^-\rangle)$	$H\sigma_x$
$\|-\rangle$	$\|\phi^-\rangle$ or $\|\psi^+\rangle$	$H\sigma_z$	π	π	0	$\|-\rangle$	$\frac{1}{\sqrt{2}}(\|\phi^-\rangle + \|\psi^+\rangle)$	$H\sigma_x$

Table 6.5: Alice's unitary operation, given Trent's and Bob's measurement outcomes next to the corresponding phases of Fig. 6.7 and 6.8. Trent measures in the x-basis and Bob measures in the Bell basis.

except that instead of applying $H\sigma_x$, they proposes to apply $H\sigma_z$. Trent's and Bob's measurement outcomes together with Alice's unitary operation are displayed in Table 6.5.

Note that after applying $H\sigma_z$, the system is in the state

$$\begin{aligned}
(H\sigma_z \otimes I \otimes I)\,|GHZ\rangle_{ATB} &= (H \otimes I \otimes I)\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle) \\
&= \frac{1}{2}((|0\rangle + |1\rangle)\,|00\rangle - (|0\rangle - |1\rangle)\,|11\rangle) \\
&= \frac{1}{2}(|000\rangle + |100\rangle - |011\rangle + |111\rangle) \\
&= \frac{1}{4}(|000\rangle - |001\rangle - |110\rangle + |111\rangle + |010\rangle - |011\rangle \\
&\quad + |100\rangle - |101\rangle + |000\rangle + |001\rangle + |110\rangle \\
&\quad + |111\rangle - |010\rangle - |011\rangle + |100\rangle + |101\rangle) \\
&= \frac{1}{4}((|00\rangle - |11\rangle + |01\rangle + |10\rangle)(|0\rangle - |1\rangle) \\
&\quad + (|00\rangle + |11\rangle - |01\rangle + |10\rangle)(|0\rangle + |1\rangle)) \\
&= \frac{1}{2}((|\phi^-\rangle_{AB} + |\psi^+\rangle_{AB})\,|-\rangle_T + (|\phi^+\rangle_{AB} - |\psi^-\rangle_{AB})\,|+\rangle_T)
\end{aligned} \tag{6.25}$$

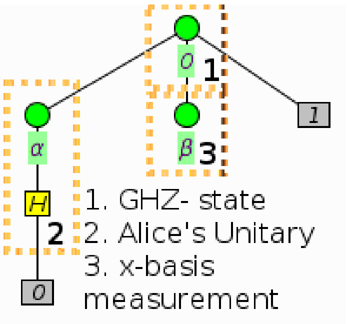


Figure 6.7: Graphical representation of Alice's unitary operation and the x-basis measurement in the set of instructions of the Improved Quantum Direct Communication protocol. $\alpha, \beta \in \{0, \pi\}$

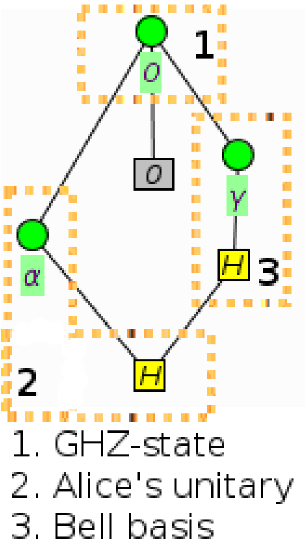


Figure 6.8: Graphical representation of Alice's unitary operation and the Bell basis measurement in the set of instructions of the Improved Quantum Direct Communication protocol. $\alpha, \gamma \in \{0, \pi\}$

Lemma 54. *Fig. 6.7 is the graphical representation of Alice's unitary operation and the x-basis measurement in the set of instructions of the Improved Quantum Direct Communication protocol.*

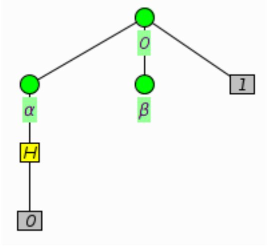
Proof. Box 1 is a GHZ state, box 2 is H or $H\sigma_z$, depending on the value of α and box 3 is a measurement into the x-basis. □

Lemma 55. *Fig. 6.8 is the graphical representation of Alice's unitary operation and the Bell basis measurement in the set of instructions of the Improved Quantum Direct Communication protocol.*

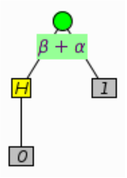
Proof. Box 1 is a GHZ state and box 2 is H or $H\sigma_z$, depending on the value of α. Finally, box 3 is $\frac{1}{\sqrt{2}}(\langle\phi^-| + \langle\psi^+|)$ or $\frac{1}{\sqrt{2}}(\langle\phi^+| - \langle\psi^-|)$ by Lemma 43 and 44. This is the outcome of the Bell state measurement by Eq. 6.13 and 6.25. □

Lemma 56. *The measurement outcome in the x-basis and Alice's unitary imply the measurement outcome in the Bell basis.*

Proof. The graphical representation is given in Fig. 6.7 by Lemma 54.



$\overset{\text{(S1)}}{=}$

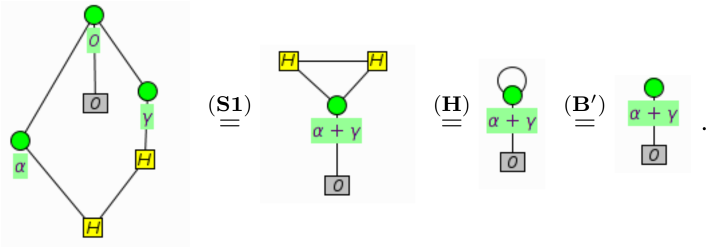


. (6.26)

The possible values for α and β are given in Table 6.5; they imply the correct Bell basis states as expected. □

Lemma 57. *The measurement outcome in the Bell basis and Alice's unitary imply the measurement outcome in the x-basis.*

Proof. The graphical representation is given in Fig. 6.8 by Lemma 55.



(6.27)

The possible values for α and γ are given in Table 6.5; they imply the correct x-basis states as expected. □

Corollary 58. *The Improved Quantum Direct Communication Protocol is correct.*

6.8.3 Security of Improved Quantum Direct Communication with Authentication Protocol

This protocol is safe for different kinds of attacks from Eve, in the same manner as the original Quantum Direct Communication with Authentication Protocol. What is left to show is that the Improved Quantum Direct Communication with Authentication Protocol is actually an improvement of the Quantum Direct Communication Protocol, i.e. that this protocol is not prone to a Trent-attack as described in subsection 6.8.1. It will be shown that no matter what unitary Alice applies, Trent will always get two measurement outcomes that are the same, as can be seen in Table 6.6. He can therefore not deduce Alice unitary operation and thus not deduce any information about the secret.

Lemma 59. *Fig. 6.9 is the graphical representation of the set of instructions of the Trent-Attack of the Improved Quantum Direct Communication Protocol.*

Proof. Box 1 is a GHZ state, box 2 is Alice's unitary, box 3 is a Hadamard operation and finally box 4 is a measurement into the z-basis. □

Lemma 60. *The Improved Quantum Direct Communication with Authentication protocol is not prone to a Trent-attack.*

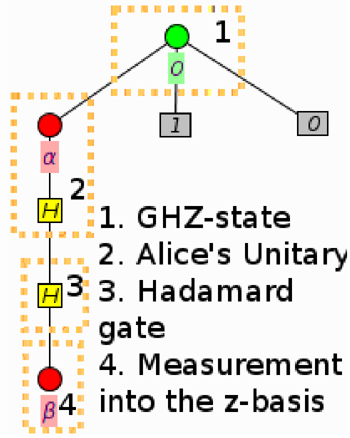
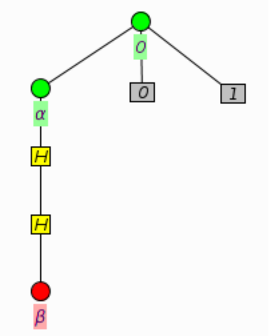
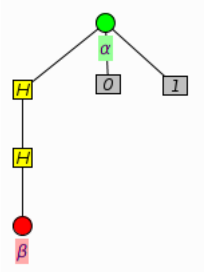


Figure 6.9: Graphical representation of the set of instructions of the Trent-Attack of the Improved Quantum Direct Communication protocol. $\alpha, \beta \in \{0, \pi\}$

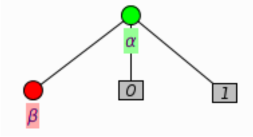
Proof. By Lemma 59 Fig. 6.9 is the graphical representation. Simplifying it gives



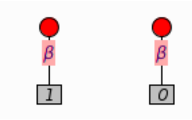
$\overset{(\mathbf{S1})}{=}$



$\overset{(\mathbf{H})}{=}$



$\overset{(\mathbf{B1})/(\mathbf{M})/(\mathbf{Z})/(\mathbf{Z'})}{=}$



. (6.28)

In table 6.6 it is shown that the corresponding phases yield the correct results, i.e. for both possible unitary operations that Alice could apply, Trent will get two measurement outcomes that are the same. With his measurement outcomes he can therefore not deduce what unitary Alice applied and thus not get any information about the secret. □

Alice's qubit	Trent's qubit	Alice's unitary	α	β	Trent's qubit
$\|0\rangle$	$\|0\rangle$	H	0	0	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$	H	0	π	$\|1\rangle$
$\|0\rangle$	$\|0\rangle$	$H\sigma_x$	π	0	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$	$H\sigma_x$	π	π	$\|1\rangle$

Table 6.6: Alice's unitary operation, given Trent's measurement outcomes next to the corresponding phases of Fig. 6.9.

6.9 Efficient Quantum Direct Communication with Authentication

This section discusses the Efficient Quantum Secure Direct Communication with authentication protocol as presented in [65]. This protocol is yet another improvement on the Quantum Direct Communication Protocol from [60, 59], because it is more efficient. First the protocol will be presented and its correctness will be shown by means of the ZX-calculus, then it will be shown that this protocol is safe for the Trent-attack from [90] as well.

6.9.1 Efficient Quantum Direct Communication with Authentication Protocol

The only difference between this protocol and the protocol in [60, 59] is Alice's encoding of the qubits. She applies I for 00, σ_x for 01, $i\sigma_y$ for 10 an σ_z for 11. With this protocol Alice can thus send 2 bits for every GHZ state. Alice's unitaries with the corresponding measurements outcomes are displayed in Table 6.7. Trent measures into the x-basis and Bob makes a Bell basis measurement.

Trent	Bob	Alice	α	β	γ	ϵ	$\alpha+\epsilon$	$\alpha+\gamma$	Trent	Bob	Alice
$\|+\rangle$	$\|\phi^+\rangle$	I	0	0	0	0	0	0	$\|+\rangle$	$\|\phi^+\rangle$	I
$\|+\rangle$	$\|\psi^+\rangle$	σ_x	0	π	0	0	0	0	$\|+\rangle$	$\|\psi^+\rangle$	σ_x
$\|+\rangle$	$\|\psi^-\rangle$	$i\sigma_y$	π	π	π	0	π	0	$\|+\rangle$	$\|\psi^-\rangle$	$i\sigma_y$
$\|+\rangle$	$\|\phi^-\rangle$	σ_z	π	0	π	0	π	0	$\|+\rangle$	$\|\phi^-\rangle$	σ_z
$\|-\rangle$	$\|\phi^-\rangle$	I	0	0	π	π	π	π	$\|-\rangle$	$\|\phi^-\rangle$	I
$\|-\rangle$	$\|\psi^-\rangle$	σ_x	0	π	π	π	π	π	$\|-\rangle$	$\|\psi^-\rangle$	σ_x
$\|-\rangle$	$\|\psi^+\rangle$	$i\sigma_y$	π	π	0	π	0	π	$\|-\rangle$	$\|\psi^+\rangle$	$i\sigma_y$
$\|-\rangle$	$\|\phi^+\rangle$	σ_z	π	0	0	π	0	π	$\|-\rangle$	$\|\phi^+\rangle$	σ_z

Table 6.7: Alice's unitary operation, given Trent's and Bob's measurement outcomes next to the corresponding phases of Fig. 6.10 and 6.11. Trent measures in the x-basis and Bob measures in the Bell basis.

Lemma 61. *Fig. 6.10 is the graphical representation of Alice's unitary and the measurement into the x-basis, as described in the set of instructions of the Efficient Quantum Direct Communication Protocol.*

Proof. Box 1 is a GHZ state, box 2 is Alice's unitary operation and finally box 3 is an x-basis measurement. □

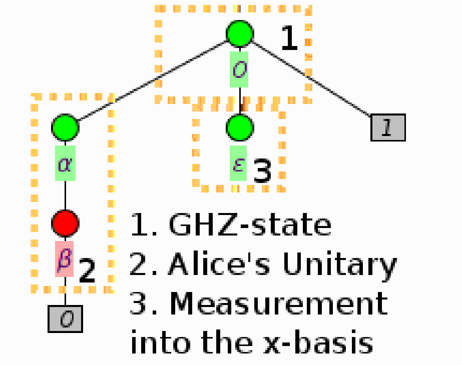


Figure 6.10: Graphical representation of Alice's unitary and the measurement into the x-basis, as described in the set of instructions of the Efficient Quantum Direct Communication Protocol. $\alpha, \epsilon \in \{0, \pi\}$

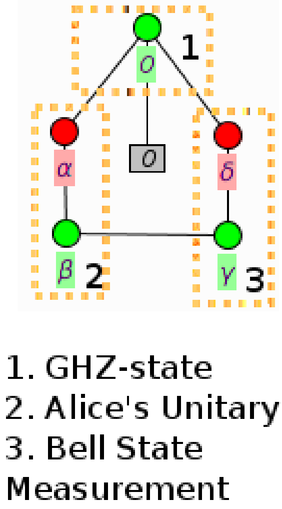


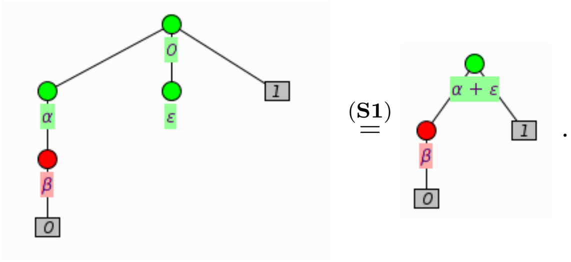
Figure 6.11: Graphical representation of Alice's unitary and the measurement into the Bell basis, as described in the set of instructions of the Efficient Quantum Direct Communication Protocol. $\alpha, \beta, \gamma, \delta \in \{0, \pi\}$

Lemma 62. *Fig. 6.11 is the graphical representation of Alice's unitary and the measurement into the Bell basis, as described in the set of instructions of the Efficient Quantum Direct Communication Protocol.*

Proof. Box 1 is a GHZ state, box 2 is Alice's unitary operation and finally box 3 is a Bell state measurement. □

Lemma 63. *The measurement outcome in the x-basis and Alice's unitary imply the measurement outcome in the Bell basis.*

Proof. The graphical representation is given in Fig. 6.10 by Lemma 61.

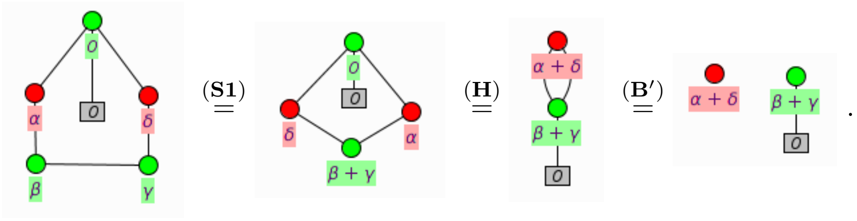


(6.29)

The possible values for α and β are given in Table 6.7; they imply the correct Bell basis states as expected. □

Lemma 64. *The measurement outcome in the Bell basis and Alice's unitary imply the measurement outcome in the x-basis.*

Proof. The graphical representation is given in Fig. 6.11 by Lemma 62.



(6.30)

The possible values for α and γ are given in Table 6.7; they imply the correct x-basis states as expected. □

Corollary 65. *The Efficient Quantum Direct Communication Protocol is correct.*

6.9.2 Security of Efficient Quantum Direct Communication with Authentication Protocol

This protocol is safe for different kinds of attack from Eve, in the same manner as the original Quantum Direct Communication with Authentication Protocol. What is left to show is that the Efficient Quantum Direct Communication with Authentication Protocol is not prone to a Trent-attack as described in subsection 6.8.1. It will be shown that no matter what unitary Alice applies, Trent will always get arbitrary measurement outcomes, as can be seen in Table 6.8. He can therefore not deduce Alice unitary operation and thus not deduce any information about the secret.

Lemma 66. *Fig. 6.12 is the graphical representation of the set of instructions of the Trent-Attack of the Improved Quantum Direct Communication Protocol.*

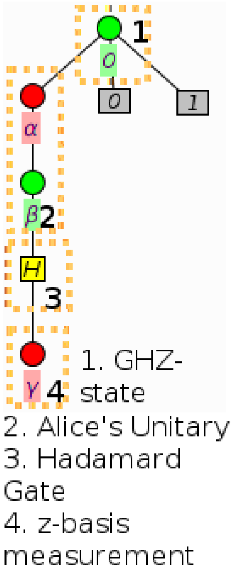
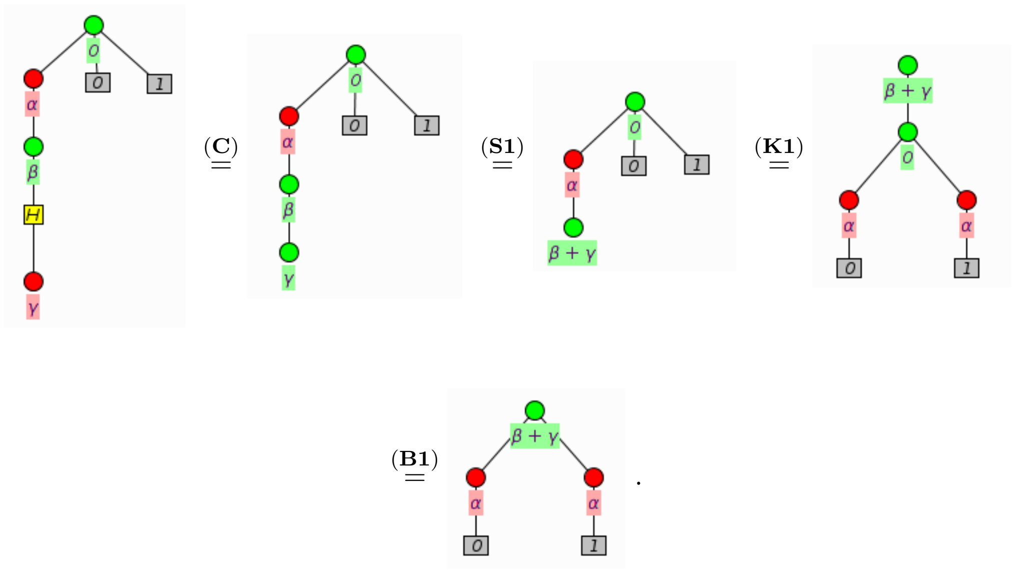


Figure 6.12: Graphical representation of the set of instructions of the Trent-Attack of the Efficient Quantum Direct Communication protocol. $\alpha, \beta \in \{0, \pi\}$

Proof. Box 1 is a GHZ state, box 2 is Alice's unitary, box 3 is a Hadamard gate and finally box 4 is a measurement into the z-basis. □

Lemma 67. *The Efficient Quantum Direct Communication with Authentication protocol is not prone to a Trent-attack as described in subsection 6.8.1.*

Proof. By Lemma 66 Fig. 6.12 is the graphical representation. Simplifying it gives



(6.31)

In Table 6.8 it is shown that the corresponding phases yield the correct results, i.e. for both possible unitary operations that Alice could apply. Trent will get arbitrary outcomes. This is because after applying a Hadamard qubit on Alice's qubit and measuring it into the

z-basis, the remaining two qubits are still entangled. Trent can get no useful information about this entangled state by just measuring one qubit. Moreover, even if he could, that would not reveal Alice's unitary operation either. He can therefore not get any information about Alice's unitary, nor about the secret that she encoded. □

Alice's qubit	State of TB	Alice's unitary	α	β	γ	State of TB
$\|0\rangle$	$\|\phi^+\rangle$	I	0	0	0	$\|\phi^+\rangle$
$\|1\rangle$	$\|\phi^-\rangle$	I	0	0	π	$\|\phi^-\rangle$
$\|0\rangle$	$\|\phi^+\rangle$	σ_x	π	0	0	$\|\phi^+\rangle$
$\|1\rangle$	$\|\phi^-\rangle$	σ_x	π	0	π	$\|\phi^-\rangle$
$\|0\rangle$	$-\|\phi^-\rangle$	$i\sigma_y$	π	π	0	$-\|\phi^-\rangle$
$\|1\rangle$	$\|\phi^+\rangle$	$i\sigma_y$	π	π	π	$\|\phi^+\rangle$
$\|0\rangle$	$-\|\phi^-\rangle$	σ_z	0	π	0	$-\|\phi^-\rangle$
$\|1\rangle$	$\|\phi^+\rangle$	σ_z	0	π	π	$\|\phi^+\rangle$

Table 6.8: Alice's unitary operation, given Trent's measurement outcomes next to the corresponding phases of Fig. 6.12.

I would not call [entanglement] one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought.

Erwin Schrödinger
(1887-1961)

7 Quantum Protocols with W_3

The W_3-state is SLOCC inequivalent to the GHZ state [35]. Though W_3 has a more complex structure, Teleportation and Key Distribution can be achieved with this state as well. Because this state is inherently different from GHZ, naturally it provides different possibilities too, such as Leader Election and Pairwise Key Distribution. Though these protocols are not new, they have never been presented in the ZX-calculus before now.

First leader election will be presented. Then pairwise and partial key sharing will be explained. Finally teleportation will be described.

7.1 Leader Election with W

In this section the Leader Election protocol as described in [36, 32] will be presented. Leader election is the problem of choosing one leader among a group of people, such that each person in the group has an equal chance of becoming the leader, if they all play fair. The protocol will be shown to work for $|W_3\rangle$. This automatically generalises to $|W_N\rangle$. Assuming each of the three people has one qubit of $|W_3\rangle$, leader election is done as follows:

1. Each measures his or her qubit in the z-basis.
2. The one who obtains $|z^-\rangle$ is the leader. The other ones are followers.

Lemma 68. *There is always exactly one person with the outcome $|z^-\rangle$.*

Proof. By Eq. 4.20. This shows that if someone has the outcome $|z^-\rangle$, the other two automatically have the outcome $|z^+\rangle$. □

7.2 Pairwise Quantum Key Distribution with W_3

In this section the Quantum Key Distribution protocol with W_3 from [50] will be explained. It will moreover be shown by means of the ZX-calculus that this protocol works.

7.2.1 Pairwise Quantum Key Distribution with W_3 protocol

Alice, Bob and Charlie share a series of W_3-states in the Pairwise Quantum Key Distribution with W_3 protocol and perform measurements on their qubits in such way that two of them will share a common (classical) key. Assuming they share a series of W_3-states, the protocol can be established as follows:

1. All choose at random the x- or the z-basis to measure their qubit in.
2. Each announces publicly his or her measurement direction.
3. For security reasons, they randomly choose to announce their measurement outcomes, to check for eavesdropping. If they do, the protocol is restarted.
4. If the overall measurement basis is $z-x-x$, $x-z-x$ or $x-x-z$, they continue with the protocol. Otherwise they start over and discard these measurement outcomes.
5. The one who measured along the z-axis is the decider. S/he tells the others whether the outcome is $\langle z^+|$. Otherwise they restart the protocol.
6. The other two now know that they have the same outcome, i.e. they share a bit now.
7. Repeat the protocol until the desired amount of key bits are obtained.
8. Use the information from step 3 to check for eavesdropping. If eavesdropping is detected, discard the obtained key bits and start a new quantum channel to repeat the protocol.

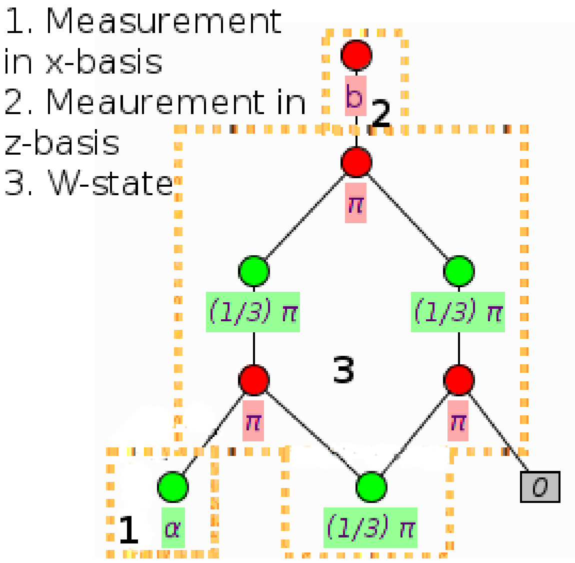


Figure 7.1: Graphical representation of the set of instructions of the Pairwise Quantum Key Distribution with W_3 protocol. $\alpha, b \in 0, \pi$

Lemma 69. *Fig. 7.1 is the graphical representation of the set of the instructions of the Pairwise Quantum Key Distribution with W_3 protocol, when the first two measurements are in the z- and x-basis.*

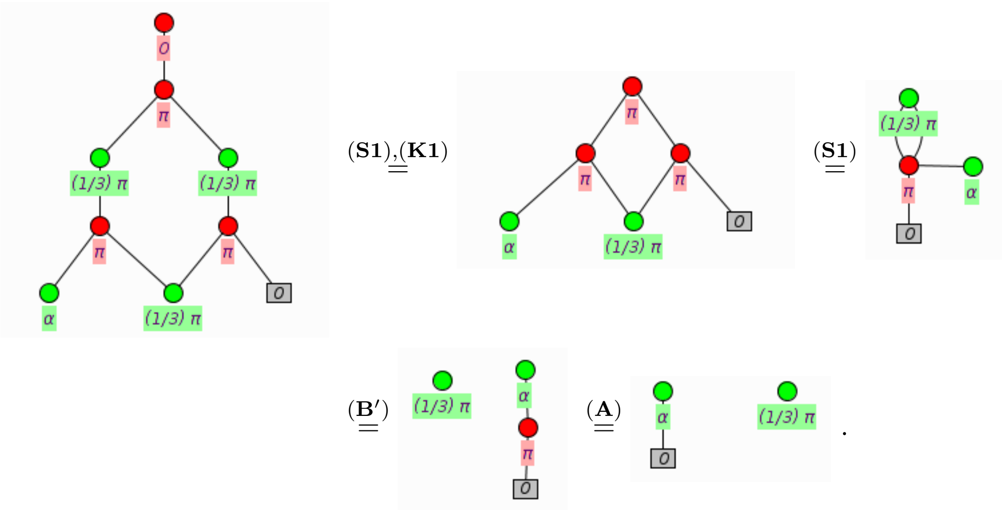
Proof. Box 1 is a measurement in the x-basis, box 2 is a measurement into the z-basis. Box 3 is the W_3-state. □

Lemma 70. *If any one of them gets the outcome $\langle z^-|$ the entanglement will be broken and the outcomes for the other two will be $|z^+\rangle$.*

Proof. Setting $b = \pi$, then by Eq 4.18. □

Lemma 71. *When there is a proper overall measuring basis and the decider has the outcome $\langle z^+|$, the other two always have the same result.*

Proof. Let $\alpha \in \{0, \pi\}$ and set $b = 0$, then



. (7.1)

□

Corollary 72. *The Pairwise Quantum Key Distribution with W_3 protocol is correct.*

7.3 Partial Quantum Key Sharing with W_3

In this section the Partial Quantum Key Sharing protocol with W_3 from [50] will be explained. It will moreover be shown by means of the ZX-calculus that this protocol is correct.

7.3.1 Partial Quantum Key Sharing with W_3 protocol

Assuming Alice, Bob and Charlie share a series of W_3-states the Partial Quantum Key with W_3 protocol by replacing 4-6 of the previous protocol by

4. If the overall measurement basis is $z{-}z{-}z$, they continue with the protocol. Otherwise they start over and discard these measurement outcomes.
5. When Bob and Charlie cooperate, they can deduce Alice's measurement outcome, because there are always two $\langle z^+|$-outcomes and one $\langle z^-|$-outcome. Note that if either Bob or Charlie measures $\langle z^-|$, s/he can deduce Alice's measurement outcome without help of the other. This is why it is called a *partial* quantum key sharing protocol, because Bob and Charlie may have partial knowledge about Alice's key without help of the other.

Note that the Pairwise and Partial Key Sharing protocols can easily be combined, because their overall valid bases do not overlap.

Lemma 73. *If all three measure in the z-basis, the outcome is always $\langle z^-z^+z^+|$, $\langle z^+z^-z^+|$ or $\langle z^+z^+z^-|$.*

Proof. By Lemma 68. □

Corollary 74. *Partial Quantum Key Sharing with W_3 protocol is correct.*

7.4 Teleportation via a W_3-state

This section describes the Teleportation via a W_3-state as described in [51].

7.4.1 Teleportation via a W_3-state protocol

Assuming Alice, Bob and Charlie share a W_3-state, teleportation of an arbitrary single qubit state to Charlie can be achieved as follows [51]:

1. Alice performs a Bell measurement on her qubits and classically communicates her outcome to Charlie.
2. Bob measures his qubit in the z-basis. If his outcome is $|1\rangle$, the teleportation fails. Otherwise they can continue the protocol. He communicates this information to Charlie over a classical channel,
3. Charlie applies the unitary corresponding to Alice's measurement outcome as in Table 7.1.

Lemma 75. *Fig. 7.2 is the graphical representation of the Teleportation via a W_3-state protocol.*

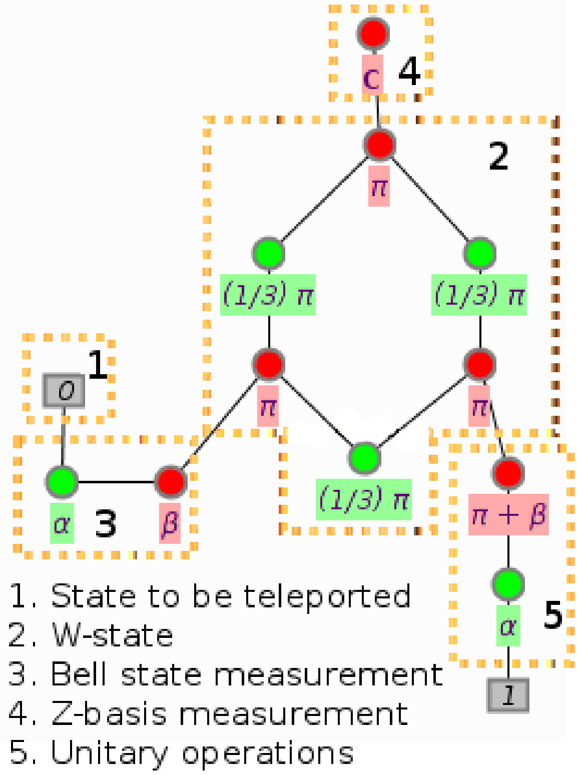


Figure 7.2: Graphical representation of the set of instructions of the Teleportation via a W_3-state protocol. $\alpha, \beta, c \in \{0, \pi\}$

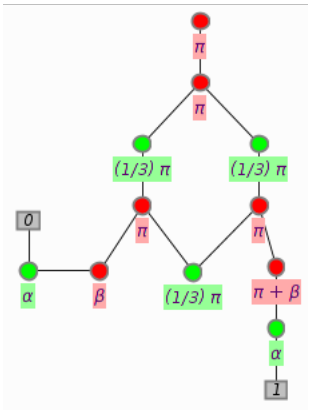
Alice	Unitary	α	β	Unitary
$\|\phi^+\rangle$	σ_x	0	0	σ_x
$\|\phi^-\rangle$	$\sigma_x\sigma_z$	π	0	$\sigma_x\sigma_z$
$\|\psi^+\rangle$	I	0	π	I
$\|\psi^-\rangle$	σ_z	π	π	σ_z

Table 7.1: Measurement outcomes and Charlie's unitary operations. Additionally the corresponding phases of Fig. 7.2 are displayed.

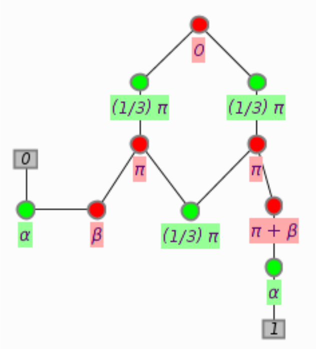
Proof. Box 1 is an arbitrary quantum state to be teleported. Box 2 is the W_3-state. Box 3 is Alice's Bell state measurement and Box 4 is Bob's z-basis measurement. Finally, box 5 is the unitary Charlie applies to her qubit. In Table 7.1 it can be seen that the measurement outcomes correspond to the correct unitary operations. □

Lemma 76. *If Bob gets measurement outcome $|1\rangle$, the teleportation fails.*

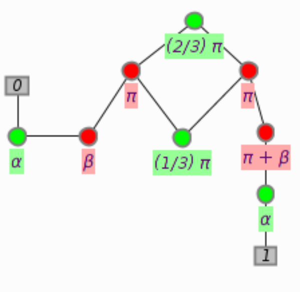
Proof. By Lemma 75 Fig. 7.2 is the graphical representation. Setting $c = \pi$, will make the entanglement break up.



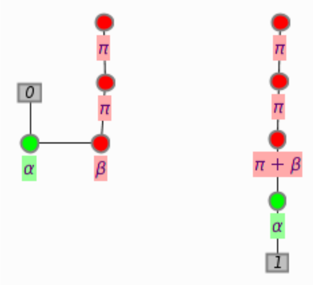
$\overset{(\mathbf{S1})}{=}$



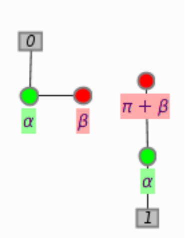
$\overset{(\mathbf{S1})}{=}$



$\overset{(\mathbf{E})}{=}$



$\overset{(\mathbf{S1})}{=}$

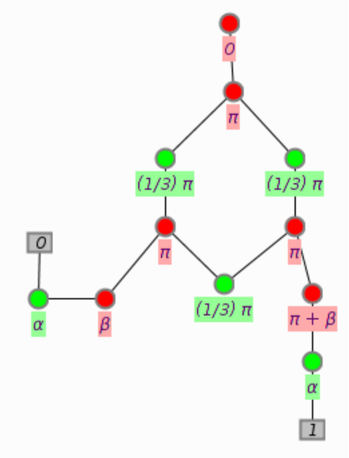


. (7.2)

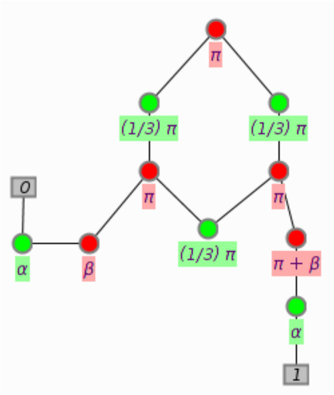
□

Lemma 77. *The Teleportation via a W_3-state protocol is correct.*

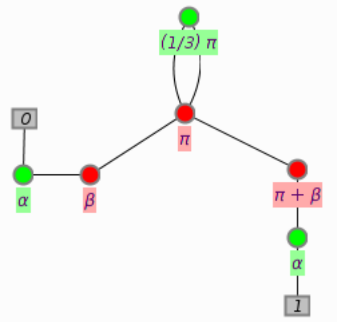
Proof.



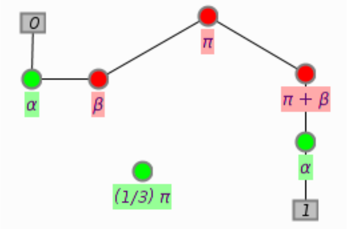
$\overset{(\mathbf{S1})}{=}$



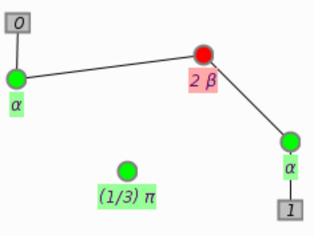
$\overset{(\mathbf{S1})/(\mathbf{K2})}{=}$



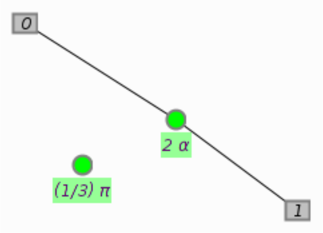
$\overset{(\mathbf{B'})}{=}$



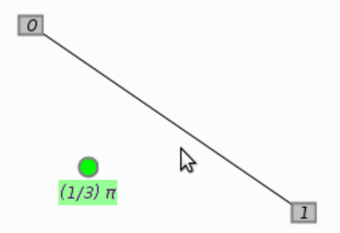
$\overset{(\mathbf{S1})}{=}$



$\overset{(\mathbf{S})}{=}$



$\overset{(\mathbf{S2})}{=}$



. (7.3)

□

You have zero privacy anyway.
Get over it.

Scott McNealy (1954-)

8 Quantum Direct Communication Protocols with W

Different quantum direct communication protocols with W_4 and W_3 are presented in this chapter. The ZX-calculus has never been applied on so many protocols involving the W-state before.

First the W_4-state will be introduced and its security explored. Then QDC, Improved QDC and Efficient QDC with W_4 will be described. Finally QDC with W_3 will be presented.

8.1 The W_4-state

In this section the representation of W_4 is explored. First this is done in Dirac notation. Then, from there, its graphical interpretation is deduced. The W_4-state looks like

$$|W_4\rangle = \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle) \tag{8.1}$$

and is represented by the mapping

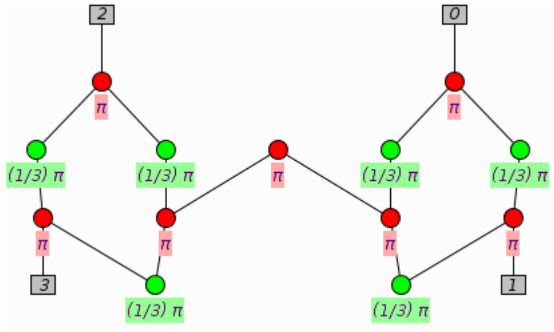
$$W :: \begin{cases} |0\rangle \mapsto |W_3\rangle \\ |1\rangle \mapsto |000\rangle . \end{cases}$$

Its Dirac representation can be rewritten as [25]

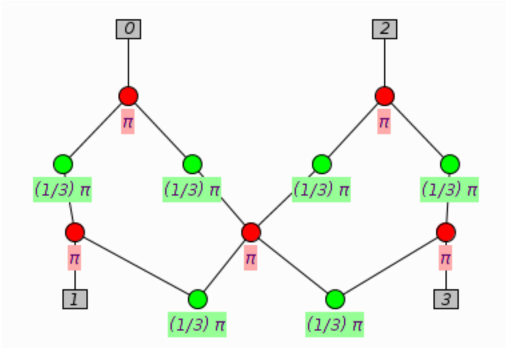
$$\begin{aligned} |W_4\rangle &= \frac{3\sqrt{2}}{2}(I \otimes I \otimes \langle\psi^+| \otimes I \otimes I)(|W_3\rangle \otimes |W_3\rangle) \\ &= \frac{\sqrt{2}}{2}(I \otimes \langle\psi^+| \otimes I)(|001001\rangle + |001010\rangle + |001100\rangle + |010001\rangle \\ &\quad + |010010\rangle + |010100\rangle + |100001\rangle + |100010\rangle + |100100\rangle) \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{2}\left(\left(\langle 01 \mid 10\rangle + \langle 10 \mid 10\rangle\right)|0001\rangle + \left(\langle 01 \mid 10\rangle + \langle 10 \mid 10\rangle\right)|0010\rangle\right.\\
&\quad + \left(\langle 01 \mid 11\rangle + \langle 10 \mid 11\rangle\right)|0000\rangle \left(\langle 01 \mid 00\rangle + \langle 10 \mid 00\rangle\right)|0101\rangle\\
&\quad + \left(\langle 01 \mid 00\rangle + \langle 10 \mid 00\rangle\right)|0110\rangle + \left(\langle 01 \mid 01\rangle + \langle 10 \mid 01\rangle\right)|0100\rangle\\
&\quad + \left(\langle 01 \mid 00\rangle + \langle 10 \mid 00\rangle\right)|1001\rangle + \left(\langle 01 \mid 00\rangle + \langle 10 \mid 00\rangle\right)|1010\rangle\\
&\quad \left. + \left(\langle 01 \mid 01\rangle + \langle 10 \mid 01\rangle\right)|1000\rangle\right.\\
&= \frac{1}{2}\left(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle\right).
\end{aligned}$$

In the graphical calculus this looks like

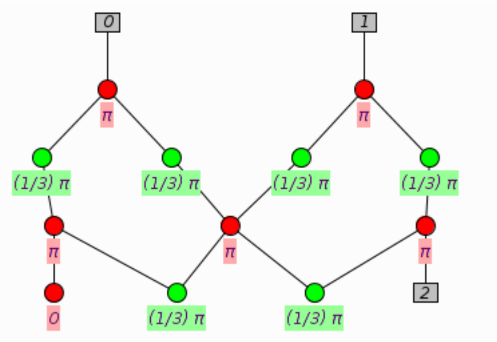


$\overset{(\mathbf{S})}{=}$

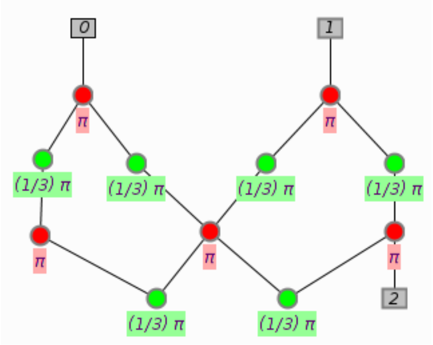


. (8.2)

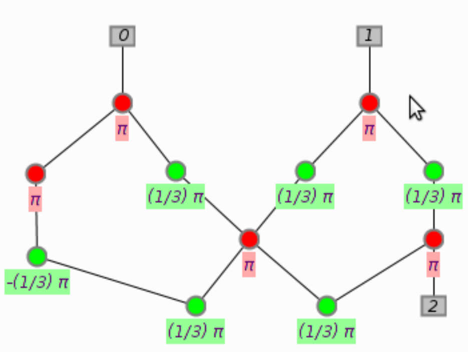
It can be checked that this indeed corresponds to the correct mapping. Plugging $|0\rangle$ gives



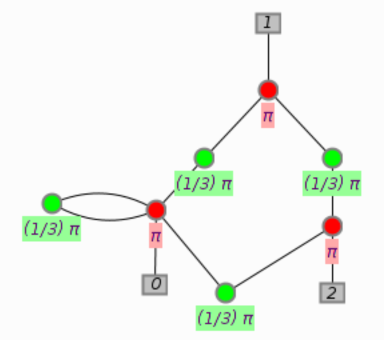
$\overset{(\mathbf{S})}{=}$



$\overset{(\mathbf{K2})}{=}$

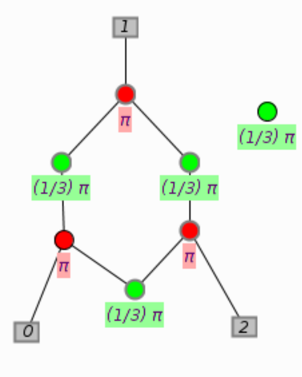


$\overset{(\mathbf{S})}{=}$



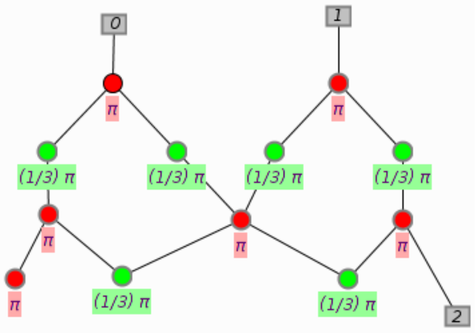
(8.3)

$\overset{(\mathbf{B}')}{=}$

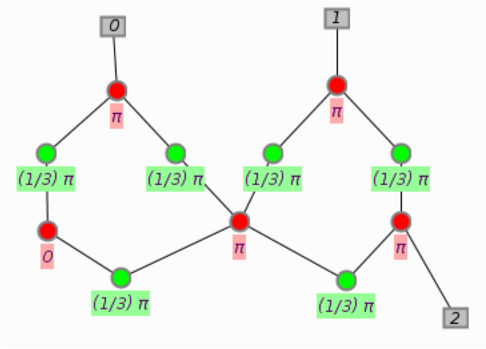


$= |W_3\rangle\,.$ (8.4)

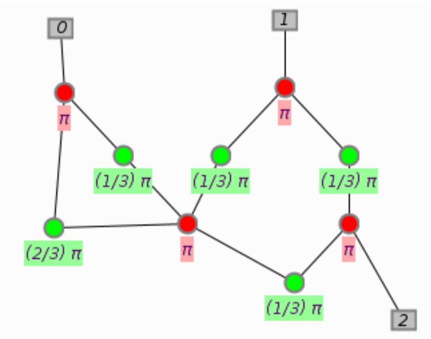
And plugging $|1\rangle$ gives



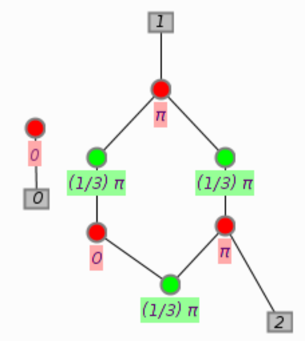
$\overset{(\mathbf{S})}{=}$



$\overset{(\mathbf{S})}{=}$

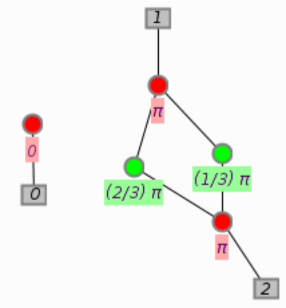


$\overset{(\mathbf{E})}{=}$

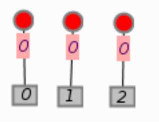


(8.5)

$\overset{(\mathbf{S})}{=}$



$\overset{(\mathbf{E})}{=}$



$= |000\rangle\,.$ (8.6)

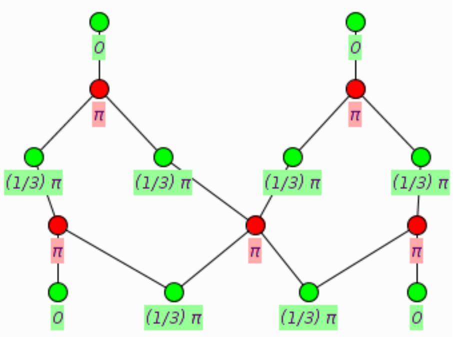
8.2 Security of W_4

The W_4-state can be rewritten as

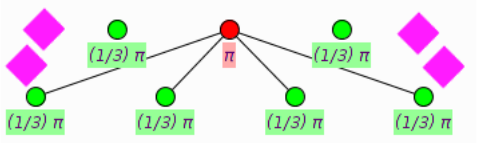
$$|W_4\rangle = \frac{1}{2}(|\psi^+\rangle(|\phi^+\rangle + |\phi^-\rangle) + (|\phi^+\rangle + |\phi^-\rangle)|\psi^+\rangle) \tag{8.7}$$

$$\begin{aligned} &= \frac{1}{4}(|{+}{+}\rangle(2|{+}{+}\rangle + |{+}{-}\rangle + |{-}{+}\rangle) + |{-}{-}\rangle(2|{-}{-}\rangle + |{+}{-}\rangle + |{-}{+}\rangle) \\ &\quad + |{+}{-}\rangle(|{+}{+}\rangle + |{-}{-}\rangle) + |{-}{+}\rangle(|{+}{+}\rangle + |{-}{-}\rangle)). \end{aligned} \tag{8.8}$$

The latter representation can be checked with scalars. The probability to get all $|+\rangle$ / $|-\rangle$ is $\frac{1}{4} \times \frac{1}{4} \times 2 = \frac{1}{8}$. The probability to get a combination of 1 $|-\rangle$ and three $|+\rangle$/ 1 $|+\rangle$ and 3 $|-\rangle$ is $(\frac{1}{8} \times \frac{1}{4} \times 2) + (\frac{1}{2} \times \frac{1}{4}) + (\frac{1}{2} \times \frac{1}{4}) = \frac{3}{8}$. So plugging these different combinations should give two groups of scalars that are distinct. Because scalars are considered now, scalars will be included again. See Chapter 4 for more details. Note that $s =$ ◆ and $\frac{1}{s} =$ ◆ . Plugging $|{+}{+}{+}{+}\rangle$ then gives

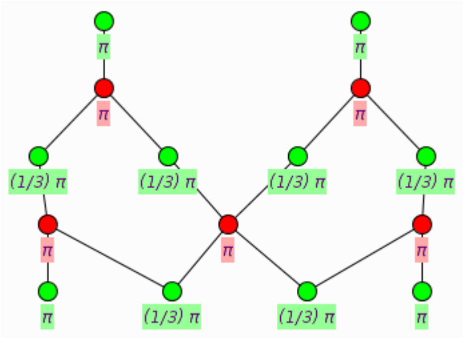


$\overset{\mathbf{(B1)}/\mathbf{(Z')}}{=}$

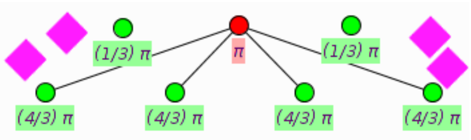


, (8.9)

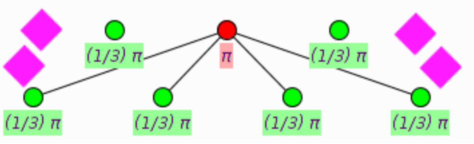
and $|{-}{-}{-}{-}\rangle$



$\overset{\mathbf{(B1)}/\mathbf{(Z')}}{=}$

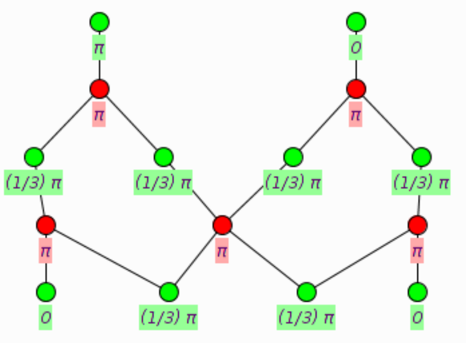


$\overset{\mathbf{(K1)}}{=}$

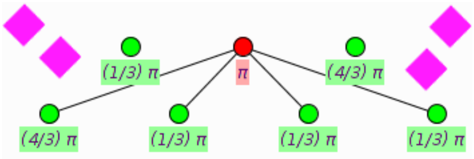


. (8.10)

Plugging 1 $|-\rangle$ and 3 $|+\rangle$ gives

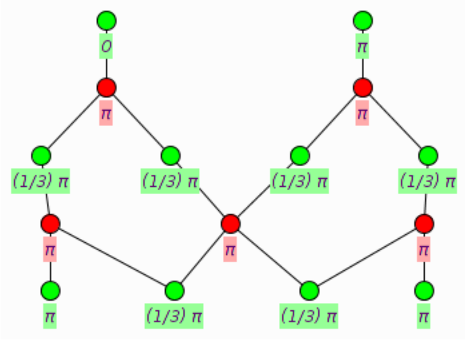


$\overset{(\mathbf{B1})/(\mathbf{Z}')}{=}$

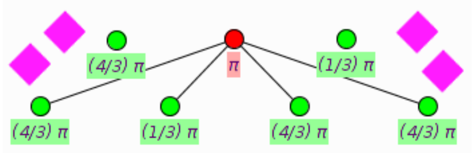


, (8.11)

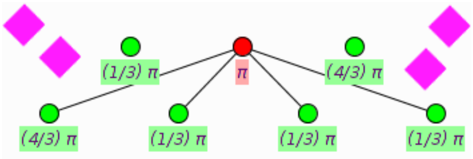
and plugging 1 $|+\rangle$ and 3 $|-\rangle$



$\overset{(\mathbf{B1})/(\mathbf{Z}')}{=}$

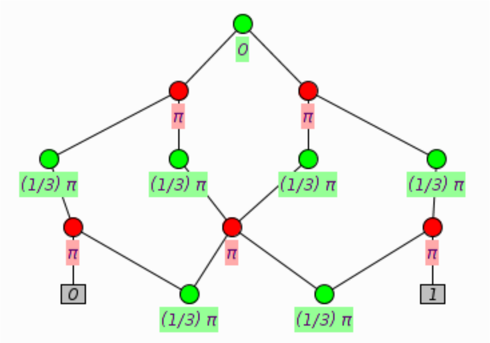


$\overset{(\mathbf{K1})}{=}$

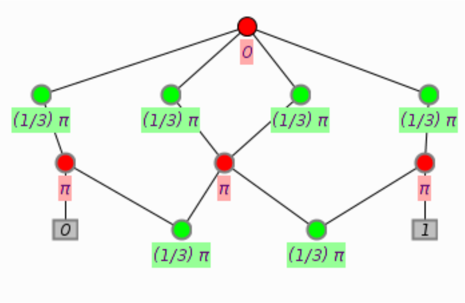


. (8.12)

The W_4-state is symmetric under exchange of any two qubits. This is not the case for the graphical representation presented above; exchanging an output from the left and the right does not work when plugging Bell states. It works when both inputs are taken from the same side (See Eq. 8.14), but plugging $|\phi^-\rangle$ for example with an input from the left and right, gives



$\overset{(\mathbf{S})}{=}$



, (8.13)

which does not seem to be rewritable to Eq. 8.14 with the current rules.

8.3 Quantum Secure Direct Communication with W_4

This section describes the Quantum Secure Direct Communication with $|W_4\rangle$ as described in [16].

8.3.1 Quantum Secure Direct Communication with W_4

When Alice wants to transmit a secret message to Bob, this can be achieved with the following steps:

1. Alice produces N $|W_4\rangle_{A_1A_2B_1B_2}$-states, where A_1, A_2, B_1, B_2 stand for Alice 1, Alice 2, Bob 1 and Bob 2.
2. Alice keeps the particle sequence A_1A_2 and sends Bob B_1B_2.
3. Alice chooses a sufficiently large subset and randomly measures her qubits in the z-, x- or Bell basis. Bob measures in the same basis and they publish their results to check for eavesdropping.
4. After concluding that the quantum channel is safe Alice measures her qubits in the Bell basis.
5. Beforehand Alice and Bob have agreed on the following encoding: $|\psi^+\rangle \rightarrow 0$ and $|\phi^\pm\rangle \rightarrow 1$. If the bit that Alice wants to encode is the same as her measurement outcome she sends Bob the classical bit 0, otherwise she sends him 1.
6. Bob also measures his qubits into the Bell basis. With this information and the information Alice sent him, he can deduce her secret message. The correct combinations are shown in Table 8.1

Secret Message	Alice	Bob	Classical Information
0	$\|\psi^+\rangle$	$\|\phi^\pm\rangle$	0
0	$\|\phi^\pm\rangle$	$\|\psi^+\rangle$	1
1	$\|\phi^\pm\rangle$	$\|\psi^+\rangle$	0
1	$\|\psi^+\rangle$	$\|\phi^\pm\rangle$	1

Table 8.1: This table shows Alice's secret message, together with her and Bob's measurement outcomes and the classical information that she sends to Bob.

Lemma 78. *A $|\phi^\pm\rangle$-outcome in one of the Bell basis measurements in the set of instructions of the Quantum Secure Direct Communication with $|W_4\rangle$ protocol implies the outcome $|\psi^+\rangle$ for the other Bell basis measurement.*

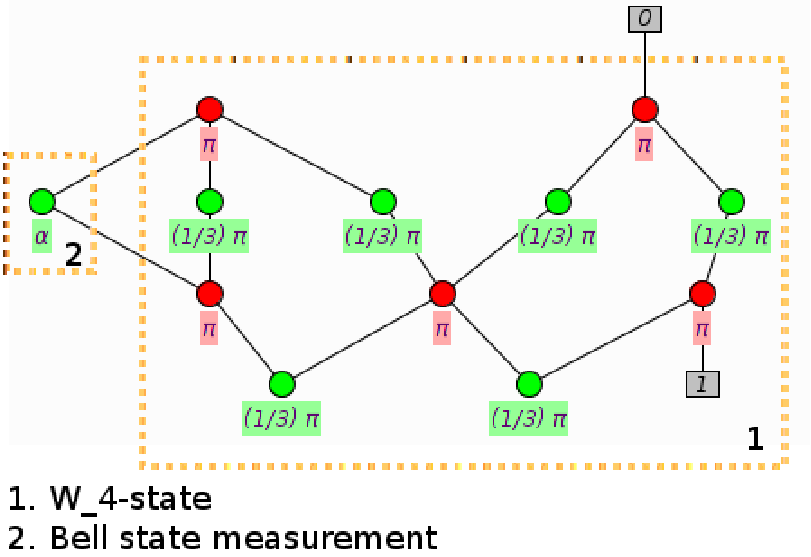
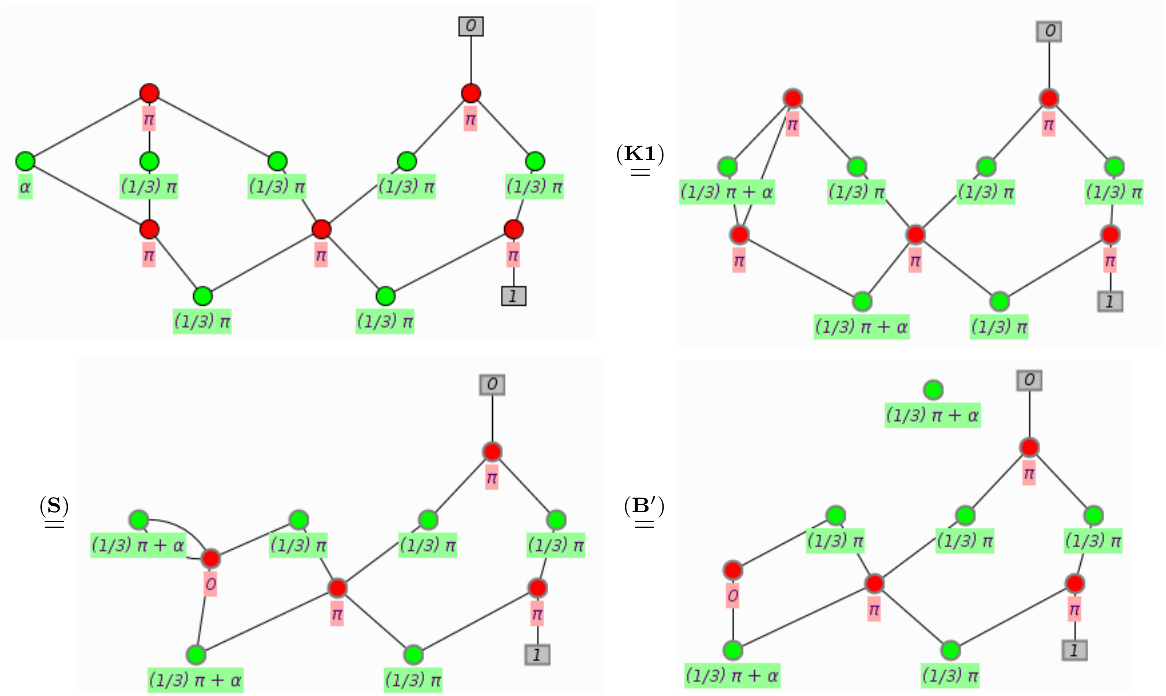
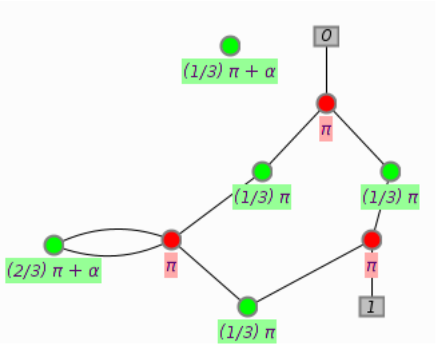


Figure 8.1: Graphical representation of a $|\phi^{\pm}\rangle$-outcome for Alice's Bell basis measurements in the set of instructions of the Quantum Secure Direct Communication with $|W_4\rangle$ protocol. $\alpha \in \{0, \pi\}$

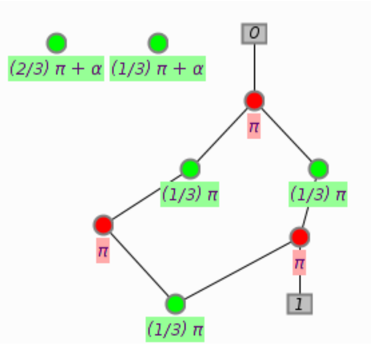
Proof. Because $|W_4\rangle$ is a symmetric state, it only needs to be checked for Alice measurement outcome and then it holds for Bob's measurement outcome as well by symmetry. Fig. 8.1 is the graphical representation of a $|\phi^{\pm}\rangle$-outcome for Alice's Bell basis measurement. Rewriting gives


$\overset{(\mathbf{K1})}{=}$
$\overset{(\mathbf{S})}{=}$
$\overset{(\mathbf{B'})}{=}$
0
π
α
(1/3) π
(1/3) π + α
1

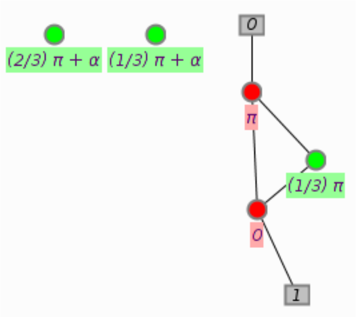
$\overset{(\mathbf{S})}{=}$



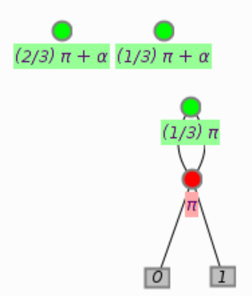
$\overset{(\mathbf{B}')}{=}$



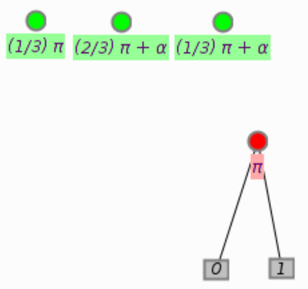
$\overset{(\mathbf{K2})}{=}$



$\overset{(\mathbf{S})}{=}$



$\overset{(\mathbf{B}')}{=}$



. (8.14)

In Table 8.1 the correct combinations are shown and indeed a $|\phi^{\pm}\rangle$ implies a $|\psi^{+}\rangle$-outcome. □

Corollary 79. *The Quantum Secure Direct Communication with W_4 protocol is correct.*

8.3.2 Security Of Quantum Secure Direct Communication with W_4

In this subsection the security of the Quantum Secure Direct Communication with W_4 protocol is discussed. Possible attacks are intercept and resend attack, disturbance attack, entanglement attack and impersonation attack.

8.3.2.1 Intercept and Resend Attack

In this section the intercept and resend Attack of Quantum Secure Direct Communication with W_4 is presented as described in [84, 62]. Eve can eavesdrop the message unnoticed, through the following steps [62]:

1. Eve intercepts the qubits Alice sends to Bob.
2. Eve waits for Alice's announcement of the control qubits. Eve leaves these qubits alone and measures the rest of the qubits in the Bell basis.
3. Eve can now do two things, send the original qubits, so that Bob can retrieve the secret message too, or send him $|\phi^{\pm}\rangle, |\psi^{+}\rangle$ randomly and disturb the secret message Bob retrieves.
4. Eve waits for Alice's classical message. With that she can retrieve the secret message.

Since Eve does not touch the control qubits, there is no way for Alice and Bob to find out that Eve has intercepted the qubits.

Another way for Eve to eavesdrop the message with only a $\frac{1}{12}$ chance of being noticed is the following[84]:

1. Eve intercepts the qubits Alice sends to Bob.
2. She measures them in the Z-basis.
3. If her measurement outcome is $|00\rangle$ ($|01\rangle$ or $|10\rangle$) she resends particles to Bob in $|00\rangle$ ($|\psi^{+}\rangle$)
4. Eve can deduce the state of Alice's qubit with her measurement outcomes. Therefore she can retrieve the secret in the same way as Bob with Alice's classical information.

If Alice and Bob measure the control qubits in the Z- or Bell basis, Eve's interference will not be detected by Eq. 8.4, 8.6, 4.17 and 4.18 If they measure into the X-basis, they will get an illegal combination of measurement outcomes with $\frac{1}{4}$ probability. So the overall chance of being detected is $\frac{1}{3} \times \frac{1}{4} = \frac{1}{12}$. This is quite easily deduced when working with Dirac notation, but not possible in the ZX-calculus. For more details the reader is referred to [84].

8.3.2.2 Disturbance Attack

When Eve chooses to intercept the qubits and then resends random entangled states to Bob as described in the first eavesdropping scheme above, she has disturbed the quantum channel. Because she does not touch the control qubits, she will not be noticed by Alice and Bob [62].

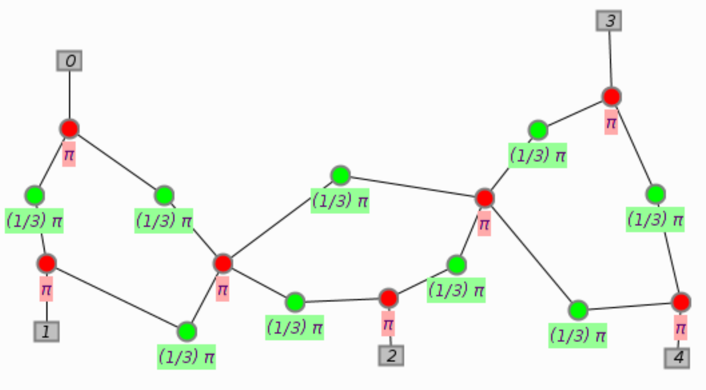
8.3.2.3 Entanglement Attack

Suppose Eve originally shares $|W_5\rangle$ or $|W_6\rangle$ with Alice and Bob. They can be rewritten in similar ways as the W_4-state [25]

$$|W_N\rangle = (I \otimes I \otimes \cdots \otimes \langle\psi^+| \otimes I \otimes I)(|W_{N-1}\rangle \otimes |W_3\rangle). \tag{8.15}$$

Then W_5 graphically looks like

$$|W_5\rangle = \tag{8.16}$$



.

Like the W_4 state, this graphical representation has some symmetry issues. W_6's graphical representation is constructed by "sticking on" another W_3 state by Eq. 8.15 and seems to suffer from even more symmetry problems. It seems therefore not possible to use this representation to prove that Eve would be detected during the security check by means of the ZX-calculus. For a presentation in Dirac notation the reader is referred to [16].

8.3.2.4 Impersonation Attack

If Eve intercepts the qubits when Alice sends them to Bob and then acts like Bob, she will not be detected. This can easily be remedied by introducing a confirmation of receiving the qubits, before continuing the protocol.

8.4 Improved Quantum Secure Direct Communication with W_4

In this section the Improved Quantum Secure Direct Communication with $|W_4\rangle$ as described in [62] is presented. This protocol is exactly the same, except for a few modifications to prevent a disturbance attack, impersonation attack and a intercept and resend attack in Step 3 and 5:

4. After confirming that Bob has received the qubits, Alice chooses a sufficiently large subset and randomly measures her qubits in the z-, x- or Bell basis. Bob measures in the same basis and they publish their results to check for eavesdropping.

...

8. Beforehand Alice and Bob have agreed on the following encoding: $|\psi^+\rangle \rightarrow 0$ and $|\phi^\pm\rangle \rightarrow 1$. If the bit that Alice wants to encode is the same as her measurement outcome she sends Bob the classical bit 0, otherwise she sends him 1. She inserts some random qubits in the sequence. She announces the random qubits and their places to Bob, to check whether the message is disturbed.

8.4.1 Security of Improved Quantum Secure Direct Communication with W_4

In this subsection the security of the Improved Quantum Secure Direct Communication with W_4 protocol are discussed. Possible attacks are intercept and resend attack, disturbance attack, entanglement attack and impersonation attack.

8.4.1.1 Intercept and Resend Attack

If Eve intercepts the qubits when Alice sends them to Bob, Alice will not proceed with the protocol until Bob has confirmed that he has received the qubits. It is therefore not possible for Eve to wait for Alice to announce the places of the checking qubits. If she does not know the place of these, there are three things she can do. She can measure all the qubits in the z-basis and then send them Bob. As before Eve can use her measurement outcomes to deduce Alice's measurement outcomes. If this is the case, she will be detected during the check with $\frac{1}{12}$ probability [84]. Another option is to measure all the qubits and send Bob $\{|\phi^\pm\rangle, |\psi+\rangle\}$. She will be detected during the check for eavesdropping with $\frac{1}{2}$ probability. Finally she can choose not to do anything with the qubits. Now she will not be detected, but she will also not get any information about the secret message.

8.4.1.2 Disturbance Attack

A disturbance attack will either be noticed during the eavesdropping check or it will be detected during the check for disturbance, when Alice publishes the random bits she inserted into the sequence.

8.4.1.3 Entanglement Attack

This protocol is safe from an entanglement attack in the same manner as the Quantum Secure Direct Communication with W_4 protocol.

8.4.1.4 Impersonation Attack

If Eve intercepts the qubits when Alice sends them to Bob and then acts like Bob, the protocol is aborted, because Bob did not confirm with Alice that the qubits arrived.

Alice	Bob	Unitary	α	β	γ	b_1	b_2	c_1	c_2
$\|\phi^+\rangle\,/\,\|\phi^-\rangle$	$\|\psi^+\rangle$	$I\otimes I$	0	0	0	$0/\pi$	0	0	π
$\|\phi^+\rangle\,/\,\|\phi^-\rangle$	$\|\phi^+\rangle$	$I\otimes\sigma_x$	0	π	0	$0/\pi$	0	0	0
$\|\phi^+\rangle\,/\,\|\phi^-\rangle$	$\|\phi^-\rangle$	$\sigma_z\otimes i\sigma_y$	π	π	π	$0/\pi$	0	π	0
$\|\phi^+\rangle\,/\,\|\phi^-\rangle$	$\|\psi^-\rangle$	$\sigma_z\otimes\sigma_x$	π	0	π	$0/\pi$	0	π	π
$\|\psi^+\rangle$	$\|\psi^+\rangle\,/\,\|\psi^-\rangle$	$I\otimes\sigma_x$	0	π	0	0	π	$0/\pi$	π
$\|\psi^+\rangle$	$\|\phi^+\rangle\,/\,\|\phi^-\rangle$	$I\otimes I$	0	0	0	0	π	$0/\pi$	0
$\|\psi^-\rangle$	$\|\psi^+\rangle\,/\,\|\psi^-\rangle$	$\sigma_z\otimes i\sigma_y$	π	π	π	π	π	o/π	π
$\|\psi^-\rangle$	$\|\phi^+\rangle\,/\,\|\phi^-\rangle$	$\sigma_z\otimes\sigma_x$	π	0	π	π	π	o/π	0

Table 8.2: Alice's and Bob's measurement, together with Alice's unitary operation, next to the corresponding phases of Fig. 8.2 and 8.3.

8.5 Efficient Quantum Secure Direct Communication with W_4

In this section the Efficient Quantum Secure Direct Communication with W_4 protocol as described in [64] is presented.

8.5.1 Efficient Quantum Secure Direct Communication with W_4

Suppose Alice and Bob want to communicate safely, secure communication with W_4 can be achieved as follows:

1. Alice prepares N $|W_4\rangle_{ABCD}$- states.
2. Alice performs one of $\{(I\otimes I),(I\otimes\sigma_x),(\sigma_z\otimes i\sigma_y),(\sigma_z\otimes\sigma_z)\}$ on qubit A and D of each W_4-state, for 00, 01, 10 and 11 respectively.
3. Alice prepares l single photons in $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ randomly. She inserts these into the sequence of C- and D-particles and sends these (updated) sequences to Bob.
4. After confirming that Bob received the qubits, Alice publicly announces the place and states of the single-photons. Bob now makes a suitable measurement on these qubits and compares the results with Alice's publication. If they do not correspond, the scheme is aborted and restarted.
5. Otherwise Alice performs a Bell-basis measurement on particle sequence AB and Bob performs a Bell-basis measurement on the CD-sequence.
6. Alice publishes her measurement result. With this information and his own measurement outcome, Bob can deduce what unitaries Alice applied by Table 8.2.

Lemma 80. *Fig. 8.2 is the graphical representation of Alice's measurement and her unitary in the set of instructions of the Efficient Quantum Secure Direct Communication with* W_4 *protocol.*

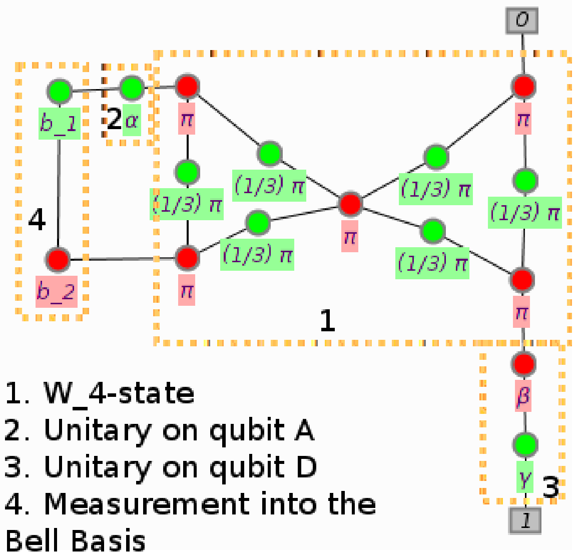


Figure 8.2: Graphical representation of Alice's measurement and her unitary in the set of instructions of the Efficient Quantum Secure Direct Communication with W_4 protocol. $\alpha, \beta, \gamma, b_1, b_2 \in \{0, \pi\}$.

Proof. Box 1 is a W_4-state by Eq. 8.2, box 2 is the unitary on qubit A, i.e. I or σ_z. Box 3 is the unitary on qubit B, and finally box 4 is a Bell basis measurement on qubit A and B. □

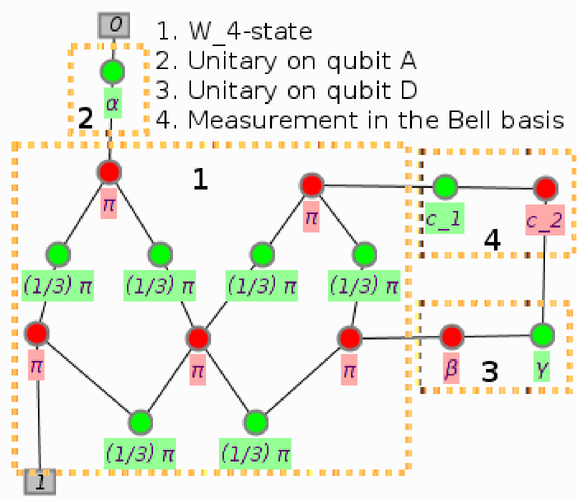


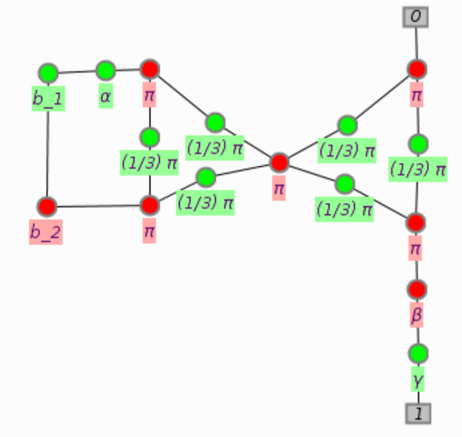
Figure 8.3: Graphical representation of Bob's measurement and Alice's unitary in the set of instructions of the Efficient Quantum Secure Direct Communication with W_4 protocol. $\alpha, \beta, \gamma, c_1, c_2 \in \{0, \pi\}$.

Lemma 81. *Fig. 8.3 is the graphical representation of Bob's measurement and Alice's unitary in the set of instructions of the Efficient Quantum Secure Direct Communication with W_4 protocol.*

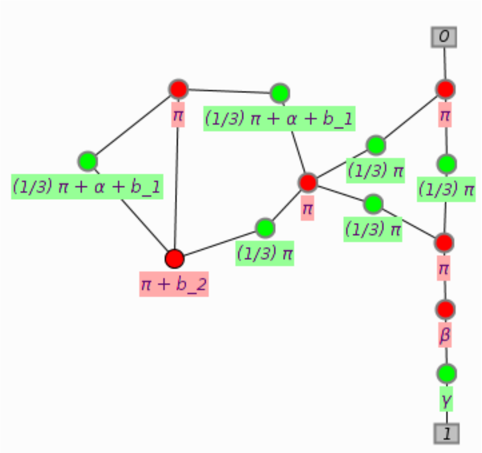
Proof. As Lemma 80. □

Lemma 82. *Alice's measurement outcomes together with her unitary operations imply Bob's measurement outcomes for the first four entries of Table. 8.2.*

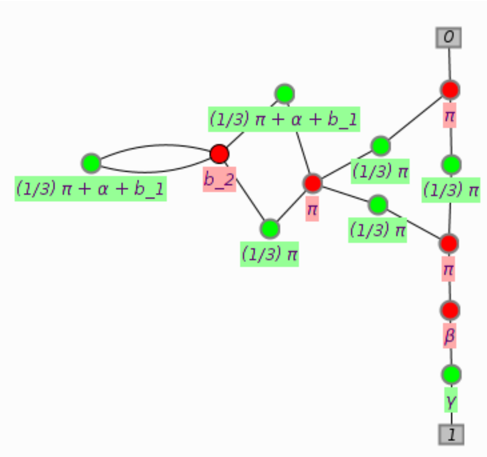
Proof. Fig. 8.2 is the graphical representation by Lemma 80. Rewriting this gives



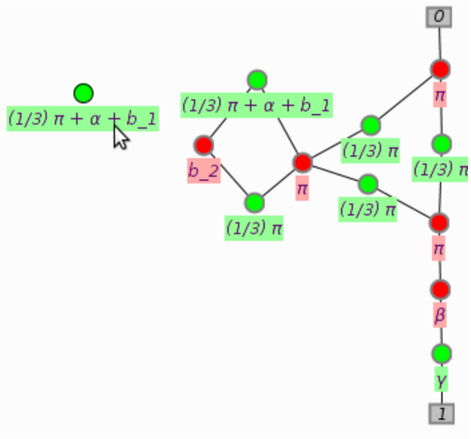
$\overset{(\mathbf{S})}{=}$



$\overset{(\mathbf{S})}{=}$

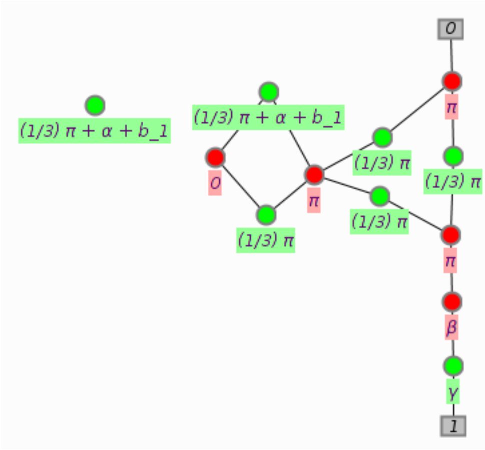


$\overset{(\mathbf{B}')}{=}$

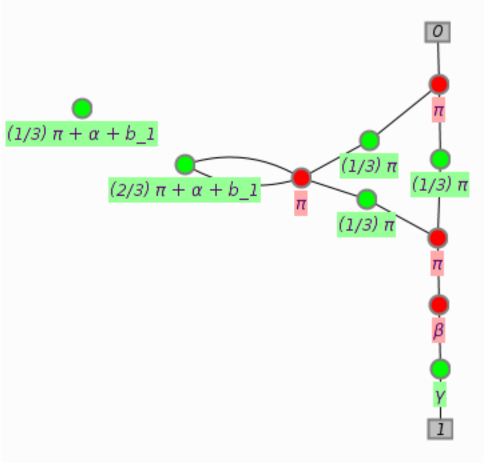


. (8.17)

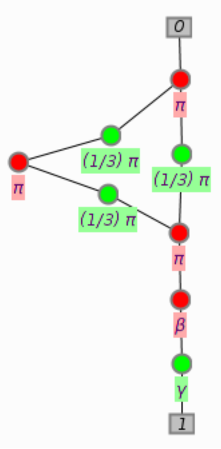
For the first four entries $b_2 = 0$. Substitution gives



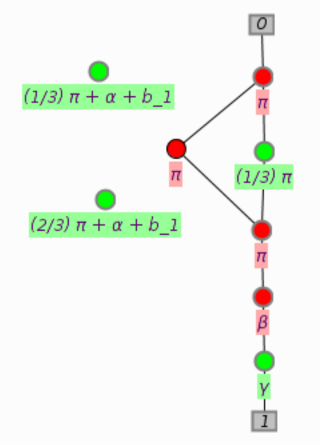
$\overset{(\mathbf{S})}{=}$



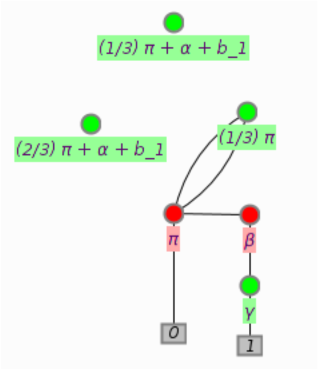
$\overset{(\mathbf{B}')}{=}$



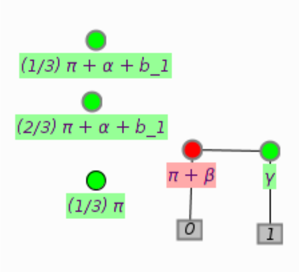
$\overset{(\mathbf{S})/(\mathbf{K2})}{=}$



$\overset{(\mathbf{S})}{=}$



$\overset{(\mathbf{B}')}{=}$

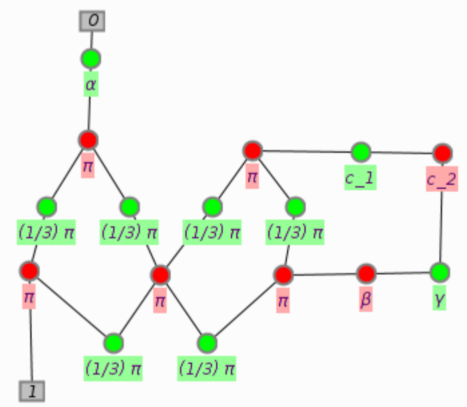


. (8.18)

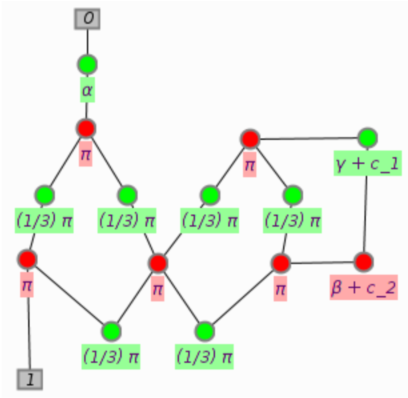
□

Lemma 83. *Bob's measurement outcomes together with Alice's unitary operations imply Alice's measurement outcomes for the last four entries of Table. 8.2.*

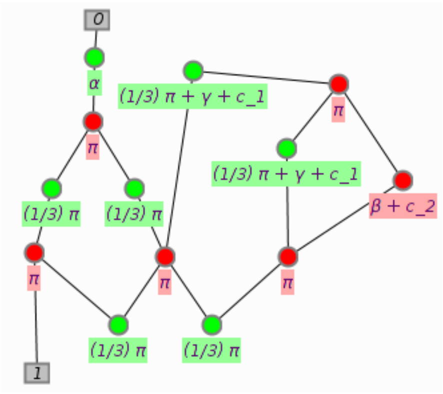
Proof. Fig. 8.2 is the graphical representation by Lemma 80. Rewriting this gives



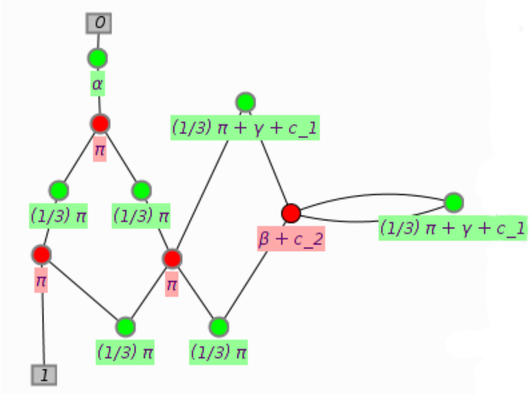
$\overset{(\mathbf{S}),(\mathbf{K2})}{=}$



$\overset{(\mathbf{K2})}{=}$

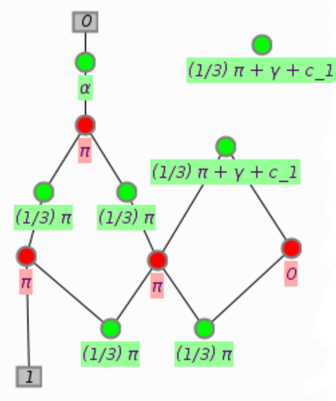


$\overset{(\mathbf{S})}{=}$

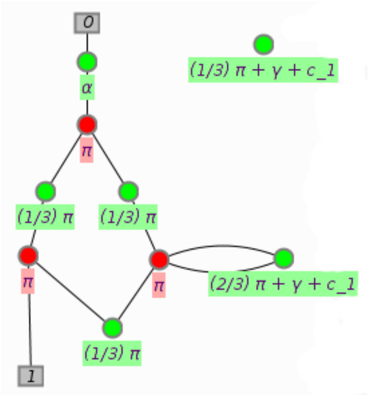


. (8.19)

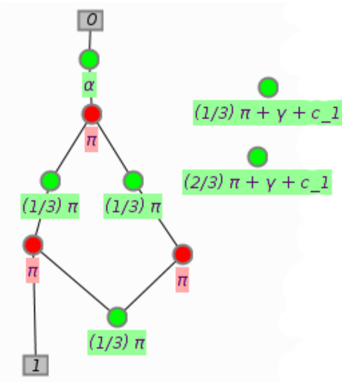
For the first four entries $\beta + c_2 = 0$. Substitution gives



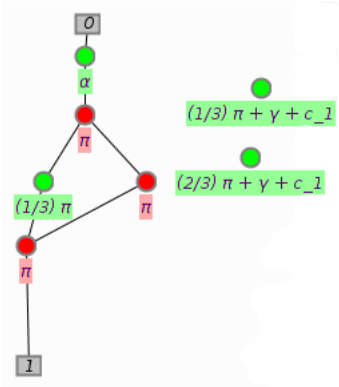
$\overset{(\mathbf{S})}{=}$



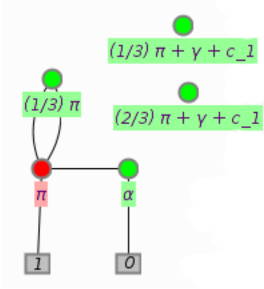
$\overset{(\mathbf{B'})}{=}$



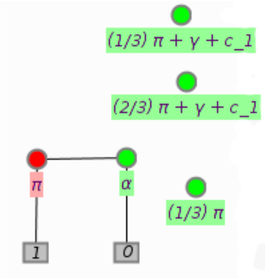
$\overset{(\mathbf{S}),(\mathbf{K2})}{=}$



$\overset{(\mathbf{S})}{=}$



$\overset{(\mathbf{B'})}{=}$



. (8.20)

□

Corollary 84. *The Efficient Quantum Secure Direct Communication with W_4 protocol is correct.*

8.5.2 Security of Efficient Quantum Secure Direct Communication with W_4 protocol

There are four different attacks Eve can do; intercept and resend attack, a disturbance attack, a entanglement attack and a impersonation attack.

8.5.2.1 Intercept and Resend Attack

In the intercept and resend attack, Eve intercepts the qubits on the quantum channel when Alice sends the qubits to Bob and replaces them by qubits in $|0\rangle$, $|1\rangle$, $|+\rangle$ or $|-\rangle$. When Eve measures the qubits in the Bell basis, she can deduce the secret message when Alice publishes her measurement outcomes. However, during the check with single photons, Eve disturbs the outcome with $\frac{1}{2}$ probability. If Eve measures the qubits in the Bell basis and then sends them on, she introduces an error with the single photons with $\frac{5}{8}$ probability. When the pair of single photons is in just the z- or just the x-basis, Eve's measurement introduces an error with probability $\frac{1}{2}$. When one is in the z-basis and the other in the x-basis, Eve's measurement introduces an error with probability $\frac{3}{4}$. The overall error probability is thus $\left(\frac{1}{2} \times \frac{1}{2}\right) + \left(\frac{1}{2} \times \frac{3}{4}\right) = \frac{5}{8}$.

8.5.2.2 Disturbance Attack

For this attack, Eve intercepts the qubits on the quantum channel when Alice sends the qubits to Bob. She could apply on of the four unitary operations on the qubits. This would only change the phase of the entanglement. To overcome this, Alice can announce random parts of their secret message to Bob and their place in the sequence. If Bob does not find the corresponding bits in her measurement, Eve has disturbed the quantum channel and they can restart the protocol. An alternative way to overcome this would be by encoding the secret with a classical error correction code first.

8.5.2.3 Entanglement Attack

If Eve would intercept the qubits when Alice sends the qubits to Bob and entangles a qubit with every qubit in the C and D sequence, she might be able to get some information on the secret later. However during the eavesdropping test with single photons, this introduces an error with $\frac{1}{2}$ probability.

8.5.2.4 Impersonation Attack

If Eve intercepts the qubits and pretends to be Bob, she will not be detected. This can easily be overcome by introducing a confirmation of Bob before proceeding with the protocol.

8.6 Quantum Secure Direct Communication with W_3

In this section the Quantum Secure Direct Communication with W_3 protocol as described in [84] is presented.

8.6.1 Quantum Secure Direct Communication with W_3

When Alice wants to transmit a secret message to Bob, this can be achieved with the following steps (slightly altered from [84]):

1. Alice prepares N $|W_3\rangle_{A_1A_2B}$-states, where A_1A_2B stands for Alice 1, Alice 2 and Bob respectively. To an arbitrary subset of these states she applies a Hadamard gate to the B qubit.
2. Alice picks a sufficiently large subset of N, called the checking sequence.
3. Alice encodes her secret message on the remaining qubits. She applies I for bit 0 and $i\sigma_y$ for 1.
4. Alice sends the B-sequence to Bob.
5. Alice publicly announces on which qubits she applied a Hadamard gate. Bob applies a Hadamard gate on the corresponding qubits.
6. Alice publishes the position of the checking sequence. Both Alice and Bob measure their qubits in the z-basis and publish their results.
7. After concluding that the quantum channel is safe, Alice and Bob both perform a z-basis measurement on the remaining qubits.
8. Alice publicly announces her measurement results. With this information and his own measurement outcome, Bob can deduce Alice's secret message from Table 8.3.

Lemma 85. *After step 5 of the set of instructions of the Quantum Secure Direct Communication with W_3 protocol, the state of each W-state is as in Fig. 8.4.*

Proof. Obviously this is what the W-state looks like if no Hadamard gate was applied and consequently Bob does not apply a Hadamard gate either. What is left to show is that it is in this state when both Alice and Bob apply a Hadamard gate.

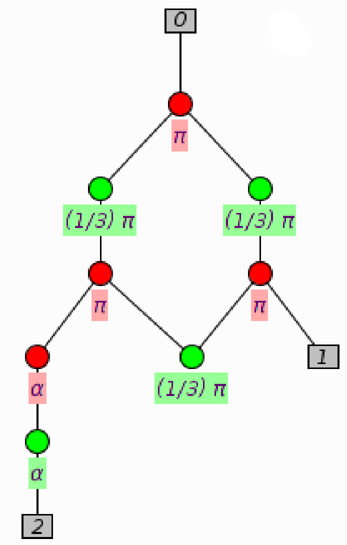
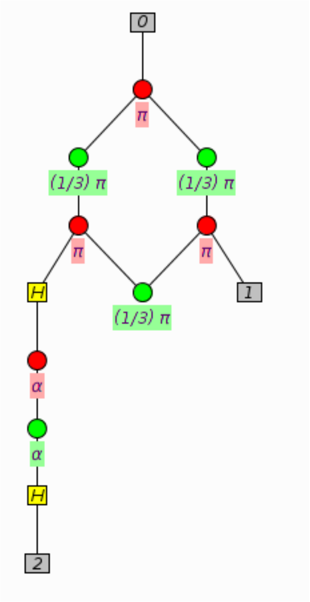
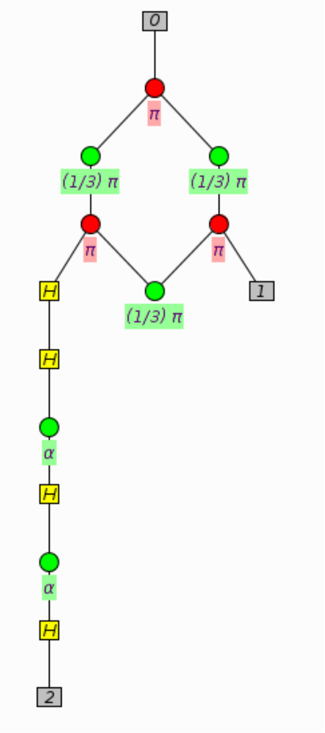


Figure 8.4: The state of each W-state after step 5 of the set of instructions of the Quantum Secure Direct Communication with W_3 protocol. $\alpha \in \{0, \pi\}$

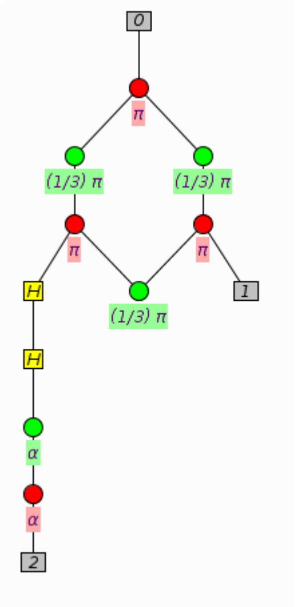
Graphically this is



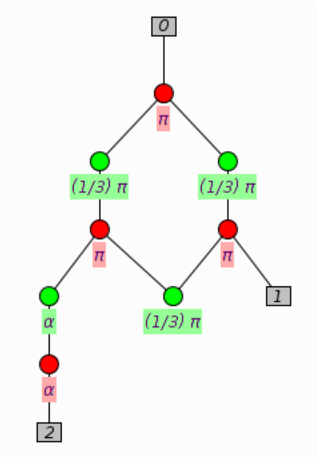
$\overset{(\mathbf{C})}{=}$



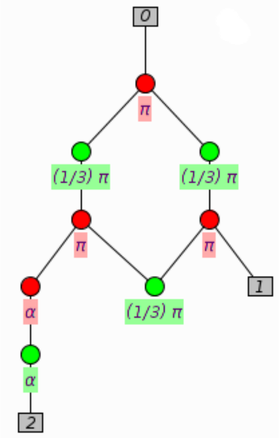
$\overset{(\mathbf{C})}{=}$



$\overset{(\mathbf{H})}{=}$



$\overset{(\mathbf{K2})}{=}$



. (8.21)

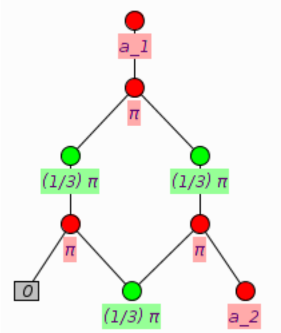
□

Secret	Alice 1	Alice 2	Bob	a_1	a_2	α	Secret
0	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	π	0	0	0
0	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	0	π	0	0
1	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	π	0	π	1
1	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	0	π	π	1
1	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	0	0	π	1
0	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	0	0	0	0

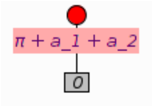
Table 8.3: This table shows Alice's secret message, together with the correct combinations of measurement outcomes. Additionally the corresponding phases of Eq. 8.23 are displayed.

Lemma 86. *The Quantum Secure Direct Communication with W_3 protocol is correct.*

Proof. Lemma 85 gives the graphical representation after step 5. From Lemma 68 we have

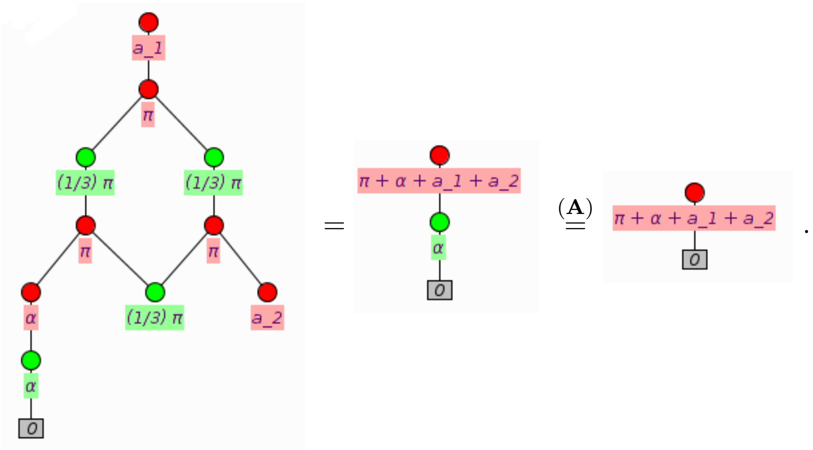


$=$



. (8.22)

Combining Eq. 8.22 and Lemma 85 gives



(8.23)

In Table 8.3 the phases are displayed next to the corresponding states; they imply the correct secret message. □

8.6.2 Security of Quantum Secure Direct Communication with W_3

8.6.2.1 Intercept and Resend Attack

Eve can intercept the qubits when Alice sends the B-sequence to Bob. However, she cannot get any useful information when she measures these qubits, because she doesn't know on which qubits the Hadamard gate is applied. If she keeps the qubits and sends Bob $\{|+\rangle, |-\rangle, |0\rangle, |1\rangle\}$ randomly, she has $\frac{1}{2}$ probability of being detected for every qubit of the checking sequence.

8.6.2.2 Disturbance Attack

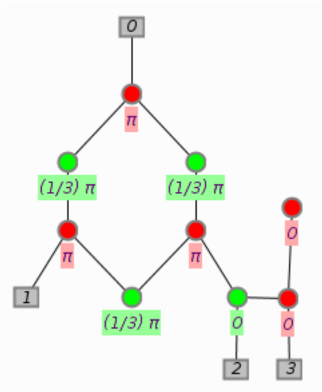
Applying random Hadamard gates to the qubits, will be detected with $\frac{1}{2}$ probability. Other operations such as σ_x will either be detected with 1 probability or not disturb the measurement outcomes.

8.6.2.3 Entanglement Attack

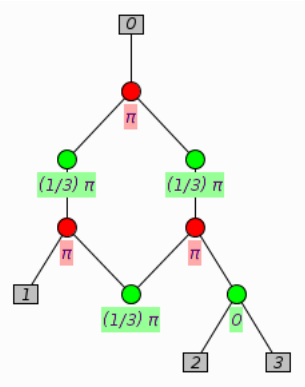
If Eve intercept the B-sequence, she could entangle an ancillary qubit by means of a CNOT gate.

Lemma 87. *If it is a W_3-state, Eve will not disturb he measurement outcomes and be able to retrieve Bob's measurement outcome.*

Proof. Applying a CNOT operation to a W-state gives

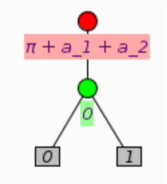


$$\overset{(\mathbf{S})}{=}$$

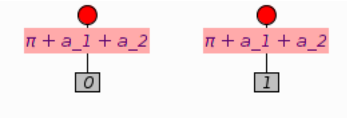


$$. \tag{8.24}$$

Combining this with Eq. 8.22 gives



$$\overset{(\mathbf{B1})/(\mathbf{M})}{=}$$

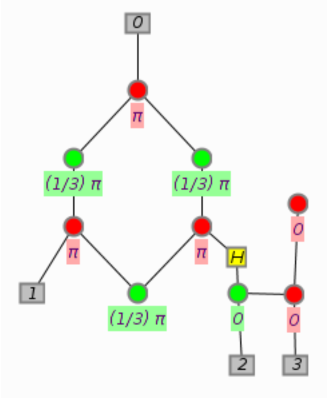


$$. \tag{8.25}$$

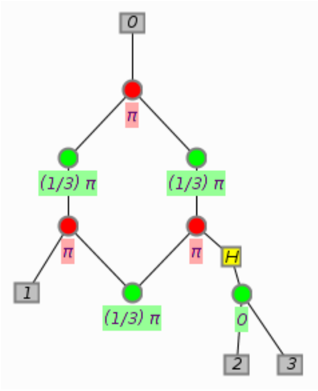
□

Lemma 88. *If it is a W-state with a Hadamard gate applied, Eve will disturb the measurement outcomes with $\frac{1}{2}$ probability. Also, she will not find anything out about the entangled state.*

Proof. Applying a CNOT operation to a W-state with a Hadamard gate applied gives

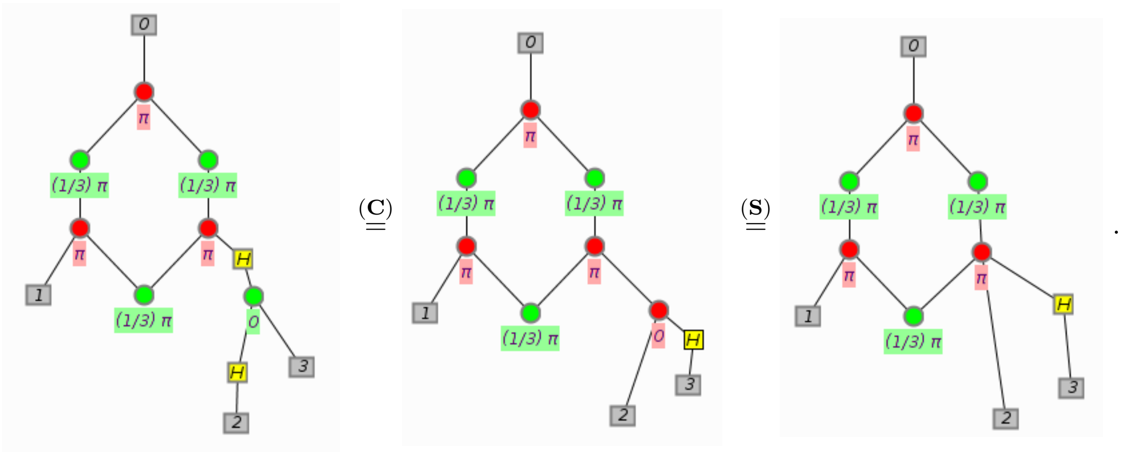


$$\overset{(\mathbf{S})}{=}$$



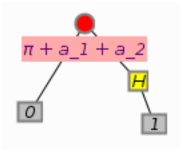
$$. \tag{8.26}$$

Then, after Eve sends the qubits to Bob he applies another Hadamard gate:



(8.27)

Combining this with Eq. 8.22 gives



. (8.28)

□

So overall, Eve has a $\frac{1}{4}$ chance of being detected.

8.6.2.4 Impersonation Attack

Eve could intercept the qubits and pretend to be Bob. This could easily be overcome by introducing a confirmation from Bob that he received the qubits.

Observations not only disturb what is to be measured, they produce it.

Pascual Jordan (1902-1980)

9 Teleportation of Multiparticle States

In this chapter two Teleportation protocols are presented, that teleport two or more particles at once. First the Teleportation of GHZ-like states is presented. Lastly Teleportation of an Arbitrary Two Particle State with EPR-pairs is presented.

9.1 Teleportation of GHZ-like states through one EPR-pair

In this section it will be shown how states of the form $|\phi\rangle_N = a\,|0\cdots 0\rangle + b\,|1\cdots 1\rangle$, where $|a|^2 + |b|^2 = 1$, can be teleported through one EPR-pair. Without loss of generality, this EPR-pair will be assumed to be $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. This protocol is described in [85]. The protocol will first be explained for $|\phi\rangle_2 = a\,|00\rangle_{12} + b\,|11\rangle_{12}$, $|a|^2 + |b|^2 = 1$ and then be expanded to $|\phi\rangle_N$. Finally Controlled Teleportation of $|\phi\rangle_N = a\,|00\cdots 0\rangle_{12\cdots N} + |11\cdots 1\rangle_{12\cdots N}$ will be presented.

9.1.1 Teleportation of $|\phi\rangle_2$ through one EPR-pair

Assuming Alice and Bob share $|\phi^+\rangle_{AB}$, the Teleportation of $|\phi\rangle_2$ through one EPR-pair, can be achieved with the following steps [85]:

1. First Alice makes a Bell-basis measurement on the first qubit to be teleported and A. She sends her outcome to Bob via classical communication.
2. Bob applies a single qubit unitary operation on B, conditioned on Alice's measurement outcome. This unitary is one of $\{I, \sigma_x, i\sigma_y, \sigma_z\}$. The correct unitaries can be found in Table 9.1.
3. Now Alice performs a Hadamard operation on the second qubit to be teleported and does a measurement into the z-basis. She communicates the outcome to Bob via a classical channel.
4. According to Alice's measurement outcome, Bob applies I (for $|0\rangle$) or σ_z (for $|1\rangle$) to B.

5. Bob introduces an auxiliary particle a in the state $|0\rangle$. Then Bob applies a CNOT operation, with B as the control qubit and the auxiliary qubit as the target qubit.

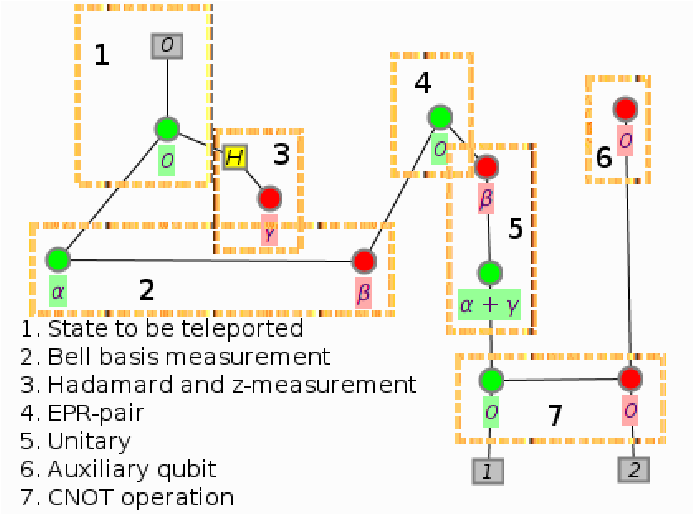
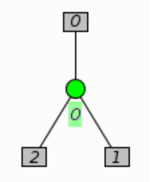


Figure 9.1: Graphical representation of the set of instructions of Teleportation of $|\phi\rangle_2$ through one EPR-pair protocol. $\alpha, \beta, \gamma \in \{0, \pi\}$

Lemma 89. *Fig. 9.1 shows the graphical representation of the set of instructions of the Teleportation of $|\phi\rangle_2$ through one EPR-pair protocol.*

Proof. By Lemma 10 $|\phi\rangle_2 =$ 

as in box 1. Box 4 is ϕ, the quantum channel. The left qubit of ϕ_2 is measured into the Bell basis together with A in box 2. Then Bob performs a unitary operator on B in box 5. Alice applies a Hadamard gate to the right qubit of $|\phi\rangle_2$ and measurements it into the z-basis in box 3. Depending on this outcome, Bob performs σ_z on B (box 5 again). He prepares an auxiliary qubit in the state $|0\rangle$ (box 6) and performs a CNOT operation on it, with B as the control qubit in box 7. In Table 9.1 it is shown that the measurement outcomes correspond to the correct unitary transforms.

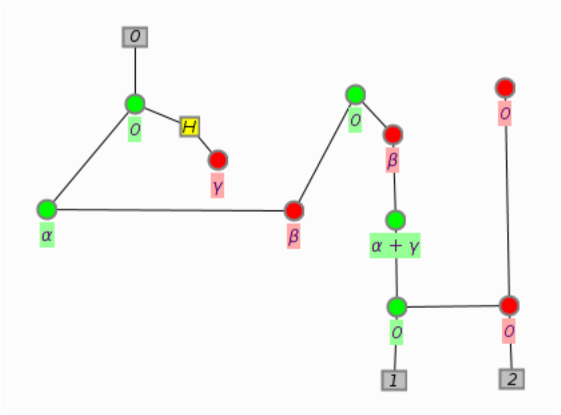
□

Lemma 90. *The Teleportation of $|\phi\rangle_2$ through one EPR-pair protocol is correct.*

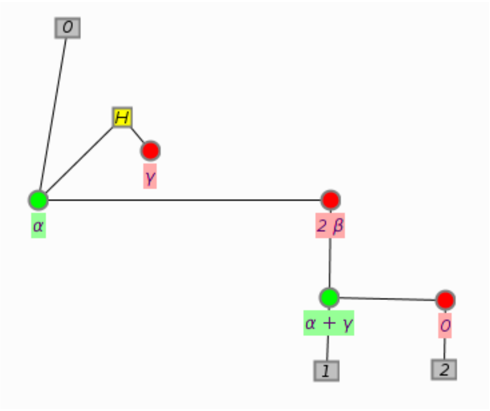
Alice's Result 1	Alice's result 2	Bob's Unitary	α	β	γ	Resulting Unitary
$\lvert\phi^+\rangle$	$\lvert 0\rangle$	I	0	0	0	I
$\lvert\phi^+\rangle$	$\lvert 1\rangle$	$I\sigma_z = \sigma_z$	0	0	π	σ_z
$\lvert\psi^+\rangle$	$\lvert 0\rangle$	σ_x	0	π	0	σ_x
$\lvert\psi^+\rangle$	$\lvert 1\rangle$	$\sigma_x\sigma_z = i\sigma_y$	0	π	π	$i\sigma_y$
$\lvert\phi^-\rangle$	$\lvert 0\rangle$	σ_z	π	0	0	σ_z
$\lvert\phi^-\rangle$	$\lvert 1\rangle$	$\sigma_z\sigma_z = I$	π	0	π	I
$\lvert\psi^-\rangle$	$\lvert 0\rangle$	$i\sigma_y$	π	π	0	$i\sigma_y$
$\lvert\psi^-\rangle$	$\lvert 1\rangle$	$i\sigma_y\sigma_z = \sigma_x$	π	π	π	σ_x

Table 9.1: This table shows Bob's unitary operation, given Alice's measurement outcomes next to the corresponding phases of Fig. 9.1.

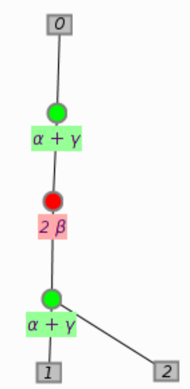
Proof. By Lemma 89 Fig. 9.1 is the graphical representation. Rewriting gives



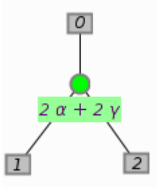
$\overset{(\mathbf{S1})}{=}$



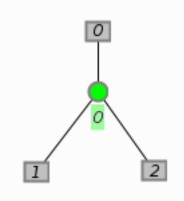
$\overset{(\mathbf{C})}{=}$



$\overset{(\mathbf{S1})}{=}$



$\overset{(\mathbf{S1})}{=}$



. (9.1)

□

9.1.2 Teleportation of $|\phi\rangle_N$ through one EPR-pair

Assuming Alice and Bob share $|\phi^+\rangle_{AB}$, the Teleportation of $|\phi\rangle_N$ through one EPR-pair, can be achieved with the following protocol [85, 92, 87]:

1. First Alice makes a Bell-basis measurement on the first qubit of $|\phi\rangle_N$ and A. She sends her outcome to Bob via classical communication.

2. Bob applies a single qubit unitary operation on B, conditioned on Alice's measurement outcome. This unitary is one of $\{I, \sigma_x, i\sigma_y, \sigma_z\}$. The correct unitaries can be found in Table 9.2.
3. Now Alice performs a Hadamard operation on the other $(N-1)$ qubits of $|\phi\rangle_N$ and does a measurement into the z-basis. She communicates the outcome
$$\gamma_{(N-1)} = \begin{cases} 1, & \text{if the number of } |1\rangle \text{ is odd} \\ 0, & \text{otherwise} \end{cases}$$
to Bob via a classical channel.
4. According to $\gamma_{(N-1)}$, Bob applies I (for 0) or σ_z (for 1) to B.
5. Bob introduces $(N-1)$ auxiliary particle $a_2, \cdots, a_N$ in the state $|0\rangle$. Then Bob applies $(N-1)$ CNOT operations, with B as the control qubit and the auxiliary qubits as the target qubits.

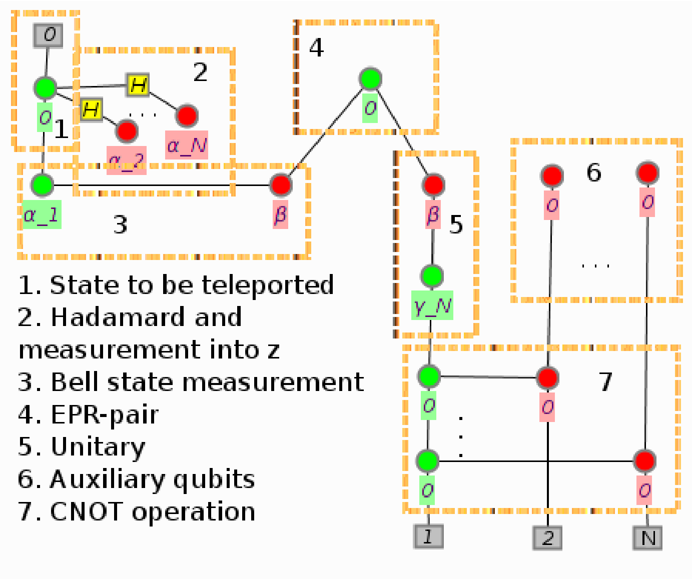
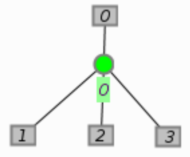
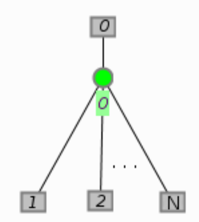


Figure 9.2: Graphical representation of the Teleportation of $|\phi\rangle_N$ through one EPR-pair protocol. $\alpha_i, \beta \in \{0, \pi\}$ and $1 \leq i \leq N$. $\gamma_N = \alpha_1 + \alpha_2 + \cdots + \alpha_N \pmod{2\pi}$.

Lemma 91. *Fig. 9.2 is the graphical representation of the set of instructions of the Teleportation of $|\phi\rangle_N$ through one EPR-pair protocol.*

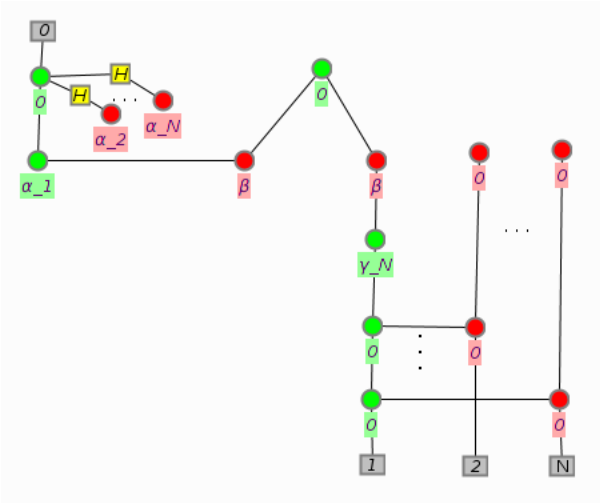
Proof. By Lemma 14 $|\phi\rangle_3 =$ . Likewise $|\phi\rangle_N =$ , which is in box 1. Box 4 is the shared EPR pair AB. Alice does a measurement into the Bell basis with the left qubit of state to be teleported and A, giving α_1 and β in box 3. Then Bob applies some unitary operation on B based on the outcome in box 5. Alice applies a Hadamard operation on the remaining $(N-1)$ qubits of $|\phi\rangle_N$ and measures them into the z-basis (box 2). Bob applies σ_z or I, based on these outcomes on B (box 5 again). Then Bob introduces $(N-1)$ auxiliary qubits in $|0\rangle$ (box 6), with which he performs $(N-1)$ Controlled not operations, with B as the control qubit (box 7). In Table 9.2 it can be seen that the measurement outcomes yield the same unitary transforms. □

Alice's Result 1	$\gamma_{(N-1)}$	Bob's Unitary	α_1	β	γ_N	Resulting Unitary
$\|\phi^+\rangle$	0	I	0	0	0	I
$\|\phi^+\rangle$	1	$I\sigma_z = \sigma_z$	0	0	π	σ_z
$\|\psi^+\rangle$	0	σ_x	0	π	0	σ_x
$\|\psi^+\rangle$	1	$\sigma_x\sigma_z = i\sigma_y$	0	π	π	$i\sigma_y$
$\|\phi^-\rangle$	0	σ_z	π	0	π	σ_z
$\|\phi^-\rangle$	1	$\sigma_z\sigma_z = I$	π	0	0	I
$\|\psi^-\rangle$	0	$i\sigma_y$	π	π	π	$i\sigma_y$
$\|\psi^-\rangle$	1	$i\sigma_y\sigma_z = \sigma_x$	π	π	0	σ_x

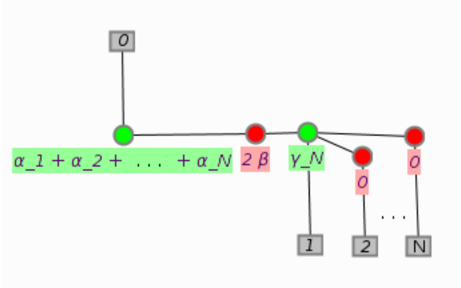
Table 9.2: This table shows Bob's unitary operation, given Alice's measurement outcomes next to the corresponding phases of Fig. 9.2.

Lemma 92. *The Teleportation of $|\phi\rangle_N$ through one EPR-pair protocol is correct.*

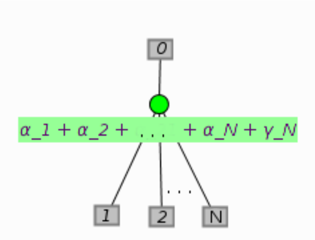
Proof. By Lemma 91 Fig. 9.2 is the graphical representation. Simplification gives



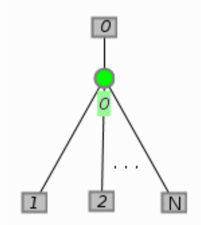
$\overset{(\mathbf{S1})}{=}$



$\overset{(\mathbf{S})}{=}$



$\overset{(\mathbf{S1})}{=}$



. (9.2)

□

9.1.3 Controlled Teleportation of $|\phi\rangle_N$ through a GHZ state

Suppose Alice, Bob and Charlie share a GHZ state $|GHZ\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. To achieve Controlled Teleportation of $|\phi\rangle_N$ to Bob to following steps need to be performed after step 3 of the normal Teleportation of $|\phi\rangle_N$ protocol (slightly altered from [85]):

4. Charlie performs a Hadamard operation on C and measures into the z-basis. She communicates her result
$$\alpha_{C'} = \begin{cases} 1, & \text{if } \alpha_C = |1\rangle \\ 0, & \text{otherwise} \end{cases}$$
to Bob.
5. According to $\gamma_{(N-1)} + \alpha_{C'} \pmod 2$, Bob applies I (for 0) or σ_z (for 1) to his particle.
6. Bob introduces $(N-1)$ auxiliary particle $a_2, \cdots, a_N$ in the state $|0\rangle$. Then Bob applies $(N-1)$ CNOT operations, with his qubit as the control qubit and the auxiliary qubits as the target qubits.

Lemma 93. *Fig. 9.3 is the graphical representation of the set of instructions of the Controlled Teleportation of $|\phi\rangle_N$ through one EPR-pair protocol.*

Proof. Box 1 is the state to be teleported. Box 4 is the GHZ state, which is the state through which it will be teleported. Alice measures into the Bell basis (box 3), and based on these outcomes Bob applies a unitary operation on his qubit (box 6). Alice and Charlie apply a Hadamard operation on their qubits and measure into the z-basis (box 2 and 5). Bob applies σ_z based on their combined outcomes (box 6). He then introduces $(N-1)$ auxiliary qubits (box 7) and performs ((N-1)) CNOT operation with qubit B as the control qubit (box 8). For the corresponding unitary operators see Table 9.3. □

Lemma 94. *The Controlled Teleportation of $|\phi\rangle_N$ through one EPR-pair protocol is correct.*

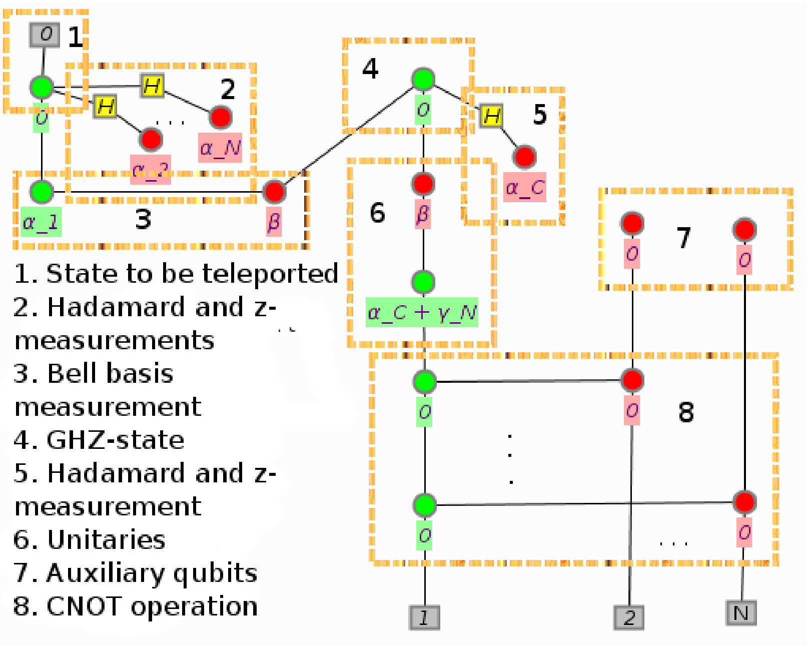
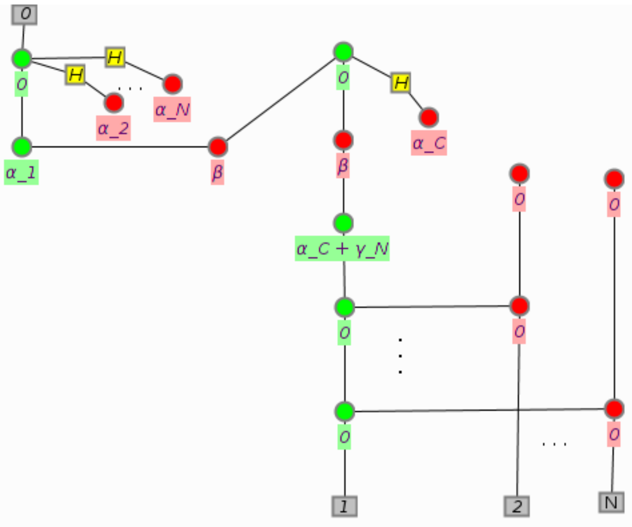
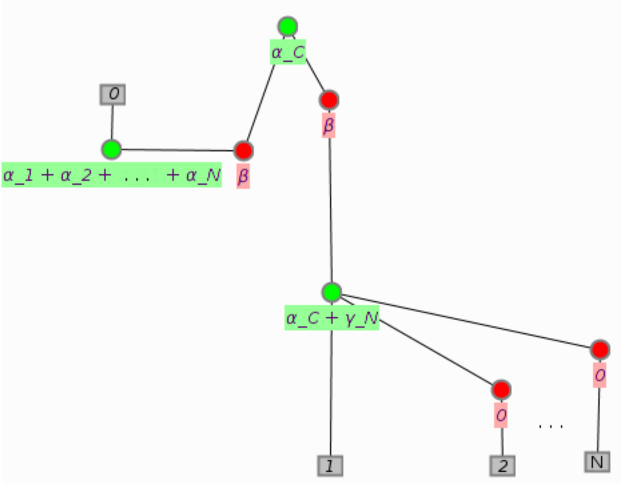


Figure 9.3: Graphical representation of the Controlled Teleportation of $|\phi\rangle_N$ through one EPR-pair protocol. $\alpha_i, \alpha_C\beta, \in \{0, \pi\}$ and $1 \leq i \leq N$. $\gamma_N = \alpha_1 + \alpha_2 + \cdots + \alpha_N \pmod{2\pi}$.

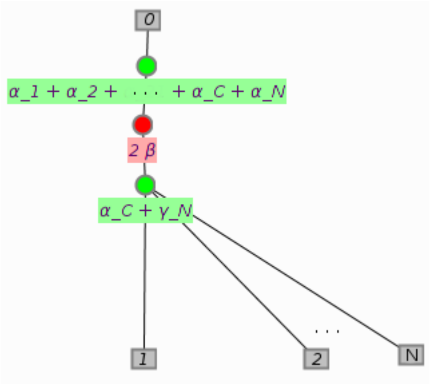
Proof. By Lemma 93 Fig. 9.3 is the graphical representation. Rewriting gives



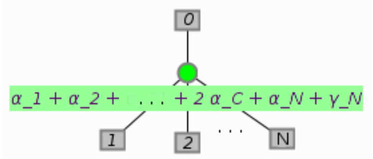
$\overset{(\mathbf{S1}),(\mathbf{C})}{=}$



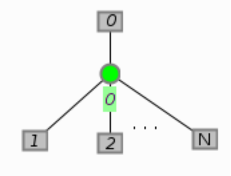
$\overset{(\mathbf{S})/(\mathbf{K2})}{=}$



$\overset{(\mathbf{S})}{=}$



$=$



. (9.3)

□

9.2 Two-party Quantum-state Sharing of an Arbitrary Two Particle State with EPR-pairs

This section describes the Two-party Quantum-state Sharing of an Arbitrary Two Particle State with EPR-pairs protocol as described in [30].

9.2.1 Quantum-state Sharing of an Arbitrary Two Particle State with EPR-pairs for two people

Suppose Alice wants to share an unknown two particle state $|\Phi\rangle_{xy} = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$, where $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$, with Charlie in such a way that she needs Bob help to retrieve the state. This can be established with the following protocol [30]:

Bell State	$\gamma_{(N-1)}$	$\alpha_{C'}$	Bob's Unitary	α_1	β	α_C	γ_N	Unitary
$\|\phi^+\rangle$	0	0	I	0	0	0	0	I
$\|\phi^+\rangle$	0	1	$I\sigma_z = \sigma_z$	0	0	π	π	σ_z
$\|\phi^+\rangle$	1	0	$I\sigma_z = \sigma_z$	0	0	0	π	σ_z
$\|\phi^+\rangle$	1	1	I	0	0	π	0	I
$\|\psi^+\rangle$	0	0	σ_x	0	π	0	0	σ_x
$\|\psi^+\rangle$	0	1	$\sigma_x\sigma_z = i\sigma_y$	0	π	π	π	$i\sigma_y$
$\|\psi^+\rangle$	1	0	$\sigma_x\sigma_z = i\sigma_y$	0	π	0	π	$i\sigma_y$
$\|\psi^+\rangle$	1	1	σ_x	0	π	π	0	σ_x
$\|\phi^-\rangle$	0	0	σ_z	π	0	0	π	σ_z
$\|\phi^-\rangle$	0	1	$\sigma_z\sigma_z = I$	π	0	π	0	I
$\|\phi^-\rangle$	1	0	$\sigma_z\sigma_z = I$	π	0	0	0	I
$\|\phi^-\rangle$	1	1	σ_z	π	0	π	π	σ_z
$\|\psi^-\rangle$	0	0	$i\sigma_y$	π	π	0	π	$i\sigma_y$
$\|\psi^-\rangle$	0	1	$i\sigma_y\sigma_z = \sigma_x$	π	π	π	0	σ_x
$\|\psi^-\rangle$	1	0	$i\sigma_y\sigma_z = \sigma_x$	π	π	0	0	σ_x
$\|\psi^-\rangle$	1	1	$i\sigma_y = i\sigma_y$	π	π	π	π	$i\sigma_y$

Table 9.3: This table shows Bob's unitary operation, given Alice's and Charlie's measurement outcomes, next to the corresponding phases of Fig. 9.3.

1. Alice shares two $|\phi^+\rangle$ pairs with Bob, $|\phi^+\rangle_{a_1b_1}$ and $|\phi^+\rangle_{a_2b_2}$.
2. Alice shares two $|\phi^+\rangle$ pairs with Charlie, $|\phi^+\rangle_{c_1d_1}$ and $|\phi^+\rangle_{c_2d_2}$.
3. Alice measures qubits xa_1a_2 into the GHZ basis and communicates her result classically.
4. Alice measure qubits yc_1c_2 into the GHZ basis and communicates her result classically.
5. Bob measures both his qubits into the x-basis and communicates his results via a classical channel.
6. Charlie applies a unitary operator $U_C = U_i \otimes U_j$ on her qubits, depending on Alice's and Bob's measurement outcomes. The corresponding unitary operations can be found in Table 9.4.

Lemma 95. *Fig. 9.4 is the graphical representation of the set of instruction of the Quantum-state Sharing of an Arbitrary Two Particle State with EPR-pairs for two people protocol.*

Proof. Box 1 is the state to be teleported. Box 2 is $|\phi^+\rangle_{a_1b_1}$, 3 is $|\phi^+\rangle_{a_2b_2}$, 4 is $|\phi^+\rangle_{c_1d_1}$ and 5 is $|\phi^+\rangle_{c_2d_2}$. Box 6 is the GHZ measurement of xa_1a_2 and 7 is the GHZ measurement yc_1c_2 by Eq. 5.29. Box 8 and 9 are Bob's measurement outcomes in the x-basis. Finally, box 10 and 11 are the unitaries that Charlie applies on her qubits. It can be seen in Table 9.4 that the phases of Fig. 9.4 indeed give all possible combinations of measurement outcomes with the proper unitary operations. □

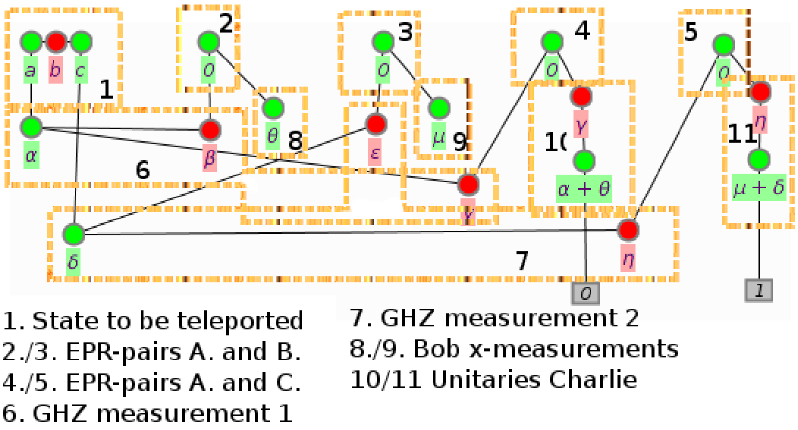
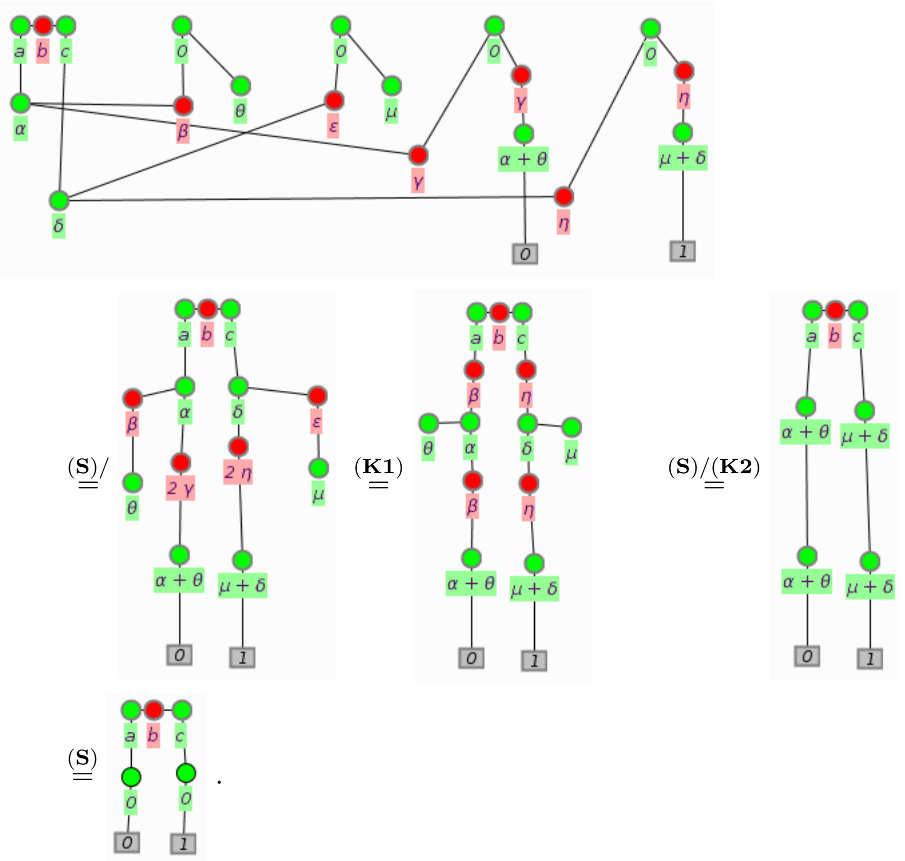


Figure 9.4: Graphical representation of the set of instructions of the Quantum-State Sharing of an Arbitrary Two Particle State with EPR-pairs for two people protocol. $a, b, c \in [0, 2\pi)$ and $\alpha, \beta, \gamma, \delta, \epsilon, \eta, \theta, \mu \in \{0, \pi\}$.

Lemma 96. *The Quantum-state sharing of an Arbitrary Two Particle State with EPR-pairs for two people protocol is correct.*

Proof. By reducing the graphical representation of the set of instructions, it can be shown that the set of instructions implies the desired behaviour, namely teleportation of $|\Phi\rangle_{xy}$ to Charlie.


$\overset{(\mathbf{S})/}{=}$
$\overset{(\mathbf{K1})}{=}$
$\overset{(\mathbf{S})/(\mathbf{K2})}{=}$
$\overset{(\mathbf{S})}{=}$
.

(9.4)

□

A_1	A_2	B_1	B_2	U_C	α	γ	δ	η	θ	μ	Implied U_C
$\|0i0\rangle + \|1\bar{i}1\rangle$	$\|0i0\rangle + \|1\bar{i}1\rangle$	$\|+\rangle$	$\|+\rangle$	$I \otimes I$	0	0	0	0	0	0	$I \otimes I$
$\|0i0\rangle - \|1\bar{i}1\rangle$	$\|0i0\rangle + \|1\bar{i}1\rangle$	$\|-\rangle$	$\|-\rangle$	$I \otimes \sigma_z$	π	0	0	0	π	π	$I \otimes \sigma_z$
$\|0i0\rangle + \|1\bar{i}1\rangle$	$\|0i0\rangle - \|1\bar{i}1\rangle$	$\|-\rangle$	$\|-\rangle$	$\sigma_z \otimes I$	0	0	π	0	π	π	$\sigma_z \otimes I$
$\|0i0\rangle - \|1\bar{i}1\rangle$	$\|0i0\rangle - \|1\bar{i}1\rangle$	$\|+\rangle$	$\|+\rangle$	$\sigma_z \otimes \sigma_z$	π	0	π	0	0	0	$\sigma_z \otimes \sigma_z$
$\|0i0\rangle + \|1\bar{i}1\rangle$	$\|0i1\rangle + \|1\bar{i}0\rangle$	$\|+\rangle$	$\|+\rangle$	$I \otimes \sigma_x$	0	0	0	π	0	0	$I \otimes \sigma_x$
$\|0i0\rangle - \|1\bar{i}1\rangle$	$\|0i1\rangle + \|1\bar{i}0\rangle$	$\|-\rangle$	$\|-\rangle$	$I \otimes i\sigma_y$	π	0	0	π	π	π	$I \otimes i\sigma_y$
$\|0i0\rangle + \|1\bar{i}1\rangle$	$\|0i1\rangle - \|1\bar{i}0\rangle$	$\|-\rangle$	$\|-\rangle$	$\sigma_z \otimes \sigma_x$	0	0	π	π	π	π	$\sigma_z \otimes \sigma_x$
$\|0i0\rangle - \|1\bar{i}1\rangle$	$\|0i1\rangle - \|1\bar{i}0\rangle$	$\|+\rangle$	$\|+\rangle$	$\sigma_z \otimes i\sigma_y$	π	0	π	π	0	0	$\sigma_z \otimes i\sigma_y$
$\|0i0\rangle + \|1\bar{i}1\rangle$	$\|0i0\rangle + \|1\bar{i}1\rangle$	$\|+\rangle$	$\|+\rangle$	$\sigma_x \otimes I$	0	π	0	0	0	0	$\sigma_x \otimes I$
$\|0i0\rangle - \|1\bar{i}1\rangle$	$\|0i0\rangle + \|1\bar{i}1\rangle$	$\|-\rangle$	$\|-\rangle$	$\sigma_x \otimes \sigma_z$	π	π	0	0	π	π	$\sigma_x \otimes \sigma_z$
$\|0i0\rangle + \|1\bar{i}1\rangle$	$\|0i0\rangle - \|1\bar{i}1\rangle$	$\|-\rangle$	$\|-\rangle$	$i\sigma_y \otimes I$	0	π	π	0	π	π	$i\sigma_y \otimes I$
$\|0i0\rangle - \|1\bar{i}1\rangle$	$\|0i0\rangle - \|1\bar{i}1\rangle$	$\|+\rangle$	$\|+\rangle$	$i\sigma_y \otimes \sigma_z$	π	π	π	0	0	0	$i\sigma_y \otimes \sigma_z$
$\|0i0\rangle + \|1\bar{i}1\rangle$	$\|0i1\rangle + \|1\bar{i}0\rangle$	$\|+\rangle$	$\|+\rangle$	$\sigma_x \otimes \sigma_x$	0	π	0	π	0	0	$\sigma_x \otimes \sigma_x$
$\|0i0\rangle - \|1\bar{i}1\rangle$	$\|0i1\rangle + \|1\bar{i}0\rangle$	$\|-\rangle$	$\|-\rangle$	$\sigma_x \otimes i\sigma_y$	π	π	0	π	π	π	$\sigma_x \otimes i\sigma_y$
$\|0i0\rangle - \|1\bar{i}1\rangle$	$\|0i1\rangle + \|1\bar{i}0\rangle$	$\|-\rangle$	$\|-\rangle$	$i\sigma_y \otimes \sigma_x$	0	π	π	π	π	π	$i\sigma_y \otimes \sigma_x$
$\|0i0\rangle + \|1\bar{i}1\rangle$	$\|0i1\rangle + \|1\bar{i}0\rangle$	$\|+\rangle$	$\|+\rangle$	$i\sigma_y \otimes i\sigma_y$	π	π	π	π	0	0	$i\sigma_y \otimes i\sigma_y$

Table 9.4: This table shows Charlie's unitary operation, given Alice's and Bob's measurement outcomes next to the corresponding phases of Fig. 9.4.

I was born not knowing and have had only a little time to change that here and there.

Richard Feynman (1918-1988)

10 Conclusion

10.1 Conclusions

In this dissertation over 25 different quantum protocols have been shown to be correct by means of the ZX-calculus. Although the ZX-calculus has been tested on a few protocols before, it has never been applied on so many protocols involving multipartite entangled states. Additionally, it was never considered in relation to security protocols, such as quantum key distribution and quantum direct communication. Furthermore, some previous research has gone into the representation of the W-state, but until now this representation was never used in relation to quantum protocols, like leader election, key distribution, teleportation and QDC.

In order to achieve this, a graphical representation of several elements has been given in Chapter 4, such as the Pauli-matrices, measurements into different bases, $|\phi_N\rangle$ and much more. These elements have been combined into the graphical representation of teleportation, key distribution, superdense coding, leader election and QDC protocols. Then, by rewriting these graphs with a few intuitive, simple rules, these protocols have all been shown to be correct. All of these protocols are measurement based protocols and involve a 'flow' of information and this is what the ZX-calculus is most useful for. It is clear from the short and simple proofs, that the ZX-calculus provides a simpler and more intuitive notion of the behaviour of quantum systems.

Albeit the diagrammatic language has been described as "Kindergarten Quantum Mechanics" [21], it is not as simple as that. It is true that once the graphical representation is there, the derivations are pretty straightforward. Finding this graphical representation on the other hand, is by no means as clear cut. For example in Chapter 6 quite a lot of arithmetic with Dirac notation had to be done, before appropriate representations in the ZX-calculus could be found. Moreover, in most cases one needs to know in what state the system is, before one can produce its representation in the ZX-calculus. What can be concluded from this, is that presenting a protocol in either Dirac notation or in the ZX-calculus is not optimal. Instead a presentation that combines the two, as done in this dissertation, would be best. Dirac notation is needed to establish the state of the system, after which the graphical representation can be easily found. Once the graphical representation is there, the workings of the protocol can easily be deduced by intuitive manipulations of the diagram.

Although th ZX-calculus is very suitable for measurement based quantum protocols that involve transfer of information, it is not apt to check the security of quantum cryptography and QDC protocols. The reason for this is that the red/green-calculus does not always allow one to calculate all possible combinations of measurement outcomes and it is never possible to calculate their probability. Detection of eavesdropping depends on the probability of getting illegal combinations of measurement outcomes. Although one can easily plug different measurement outcomes, in this representation one cannot check whether these measurement outcomes are even possible, and if so, what their probability is. It is known that scalars have no input and no output in the ZX-calculus [22], but their actual value is mostly unknown. Further research could go into the graphical representation of different scalars.

10.2 Future Outlook

In this section areas for future research are explored.

10.2.1 Classical Information

Many quantum algorithms could be made more efficient and less costly if the use of quantum resources was reduced. This can be done by combining classical algorithms with quantum algorithms. This is done for example in [88, 82, 81] and [69]. At this moment there is no formalism to adequately describe a system that makes use of both quantum and classical resources. The development of such a formalism would make the research into this area easier. Key distribution protocols could for example be enhanced with veto capabilities, as described in [10] and [11] or with classical threshold schemes [74].

10.2.2 Noisy channels, and Arbitrary Unitary operations

The ZX-calculus makes use of perfect quantum channels most of the time, i.e. maximally entangled states. In reality however, this is usually not the case. The way the ZX-calculus is now, makes it difficult to represent an quantum channel, because most of the rules work best for dots with phases 0 or π. Additionally, most of protocols designed for noisy quantum channels make use of other unitaries than just the Hadamard gate and (combinations of) the Pauli-matrices. These unitary operations usually do not have a phase of 0 or π, making it difficult to reason with. Protocols such the Probabilistic Teleportation through non-maximally entangled states in [19] are difficult, if not impossible to represent in the ZX-calculus.

Furthermore, there are a lot of protocols that do make use of pure entangled states, but still make use of arbitrary unitary operations. For example in [91] a teleportation protocol for arbitrary GHZ state through pure entangled states is presented. Other examples include [5, 79, 80, 17, 34, 29, 89, 67, 51, 19].

The Hadamard gate and the Pauli-matrices are defined in the ZX-calculus in such a way that their behaviour is determined easily. Although other unitaries can be formed by means of the Hilbert space representation, it is not straightforward how they will behave. More research could be done into the properties of dots with arbitrary phases. Then algorithms involving imperfect quantum channels, as well as protocols involving other unitaries than Hadamard and the Pauli-matrices can be represented in the red/green-calculus.

10.2.3 Higher dimensions

The ZX-calculus is designed for two dimensional Hilbert spaces. However there are quite a few protocols making use of qutrits, such as [20] for a threshold key distribution scheme, [61] for a teleportation scheme and [86, 63] for QDC protocols. Further research could go into incorporating higher dimensional particles like qutrits in the ZX-calculus.

10.2.4 Graphical Representation of arbitrary entangled states

Although it is known what GHZ-like states, the N-GHZ and W_3-state look like in the ZX-calculus, there are still a lot of entangled states, for which the graphical representation is still unknown. Especially the W_N-states and W-like states cause trouble. As mentioned in Chapter 8 the W_N, $N \geq 4$ seem to have increasingly more symmetry issues as N goes up with the representation as it is now. A different representation needs to be found that is symmetric. Then protocols involving W_N-states can be explored as well.

Furthermore, some specific entangled states can be useful in for example [67], where different bipartite states are teleported through different tripartite states. Unfortunately, there is no graphical representation for most of these states yet. Other protocols involve specific classes of W-states, such as [51, 89, 17, 34, 4]. Further research could investigate the graphical representation of different entangled states. Some research has already been done into this direction in the investigation of the GHZ/W-calculus [25, 26, 75].

10.2.5 Quantomatic

During the the work on this dissertation I have worked extensively with `quantomatic`[57]. It is jointly worked on by researchers from Edinburgh, Cambridge and Oxford. At the moment they are looking to expand it in such a way that any graphical calculus can easily be added, i.e. all the vertex types and corresponding axioms. The GHZ/W-calculus [25] could for example be added, or the Red/Green/Blue-calculus that is under construction right now. Another thing they are looking into is theory derivation; given a calculus with its axioms, what theories can be derived from that. A start on this has been made by Frot; he is developing QuantoCosy. QuantoCosy is a synthesis tool for discovering lemmas built on Isabelle/IsaPlanner.

Bibliography

[1] S. Abramsky and B. Coecke. A categorical semantics of quantum protocols. In Logic in Computer Science, 2004. Proceedings of the 19th Annual IEEE Symposium on, pages 415 – 425, july 2004.

[2] S. Abramsky and N. Tzevelekos. New Structures for Physics, chapter Introduction to categories and categorical logic. Springer, 2010.

[3] P. Agrawal and A. Pati. Perfect teleportation and superdense coding with W states. Physical Review A, 74:062320, 2006.

[4] P. Agrawal and A. Pati. Perfect teleportation and superdense coding with w states. Physical Review A, 74(6):062320, Dec 2006.

[5] S. Bandyopadhyay. Teleportation and secret sharing with pure entangled states. ArXiv Quantum Physics e-prints, Feb 2000.

[6] C. Bennett. Quantum cryptography using any two nonorthogonal states. Physical Review Letters, 68(21):3121–3124, May 1992.

[7] C. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing, volume 175, pages 175–179. Bangalore, India, 1984.

[8] C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosenk channels. Physical Review Letters, 70(13):1895–1899, Mar 1993.

[9] C. Bennett, G. Brassard, and N. Mermin. Quantum cryptography without Bell's theorem. Physical Review Letters, 68(5):557–559, Feb 1992.

[10] A. Beutelspacher. How to say "no". Lecture Notes in Computer Science, 434:491–496, 1990.

[11] C. Blundo, A. De Santis, L. Gargano, and Vaccaro U. Secret sharing schemes with veto capabilities. Lecture Notes in Computer Science, 781:82–89, 1994.

[12] K. Boström and T. Felbinger. Deterministic secure direct communication using entanglement. Physical Review Letters, 89(18):187902, Oct 2002.

[13] D. Bruss, A. Ekert, S. F. Huelga, J.-W. Pan, and A. Zeilinger. Quantum Computing with Controlled-Not and Few Qubits, volume 355. The Royal Society, 1997.

[14] Q-Y. Cai. The "ping-pong" protocol can be attacked without eavesdropping. Physical Review Letters, 91(10):109801, Sep 2003.

[15] Q.-Y. Cai. Eavesdropping on the two-way quantum communication protocols with invisible photons. Physics Letters A, 351(1-2):23 – 25, 2006.

[16] H.-J. Cao and H.-S. Song. Quantum secure direct communication with w state. Chinese Physics Letters, 23:290–292, February 2006.

[17] Z.-L. Cao and W. Song. Teleportation of a two-particle entangled state via W class states. Physica A: Statistical Mechanics and its Applications, 347:177 – 183, 2005.

[18] J. L. Cereceda. Quantum dense coding using three qubits. ArXiv Quantum Physics e-prints, May 2001.

[19] L.-B. Chen. Teleportation of an arbitrary three-particle state. Chinese Physics, 11:999–1003, October 2002.

[20] R. Cleve, D. Gottesman, and H.-K. Lo. How to share a quantum secret. Physical Review Letters, 83:648–651, 1999.

[21] B. Coecke. Kindergarten quantum mechanics: Lecture notes. AIP Conference Proceedings, 810(1):81–98, 2006.

[22] B. Coecke. Quantum picturalism. Contemporary Physics, 51:59–83, 2010.

[23] B. Coecke and R. Duncan. Interacting quantum observables: categorical algebra and diagrammatics. New Journal of Physics, 13(4):043016, 2011.

[24] B. Coecke and B. Edwards. Three qubit entanglement within graphical Z/X-calculus. In HPC, pages 22–33, 2010.

[25] B. Coecke and A. Kissinger. The compositional structure of multipartite quantum entanglement. ArXiv Quantum Physics e-prints, Feb 2010.

[26] B. Coecke, A. Kissinger, A. Merry, and S. Roy. The GHZ/W-calculus contains rational arithmetic. In HPC, pages 34–48, 2010.

[27] B. Coecke and E. O. Paquette. Categories for the practising physicist. ArXiv Quantum Physics e-prints, October 2009.

[28] B. Coecke and S. Perdrix. Environment and classical channels in categorical quantum mechanics. In Proceedings of the 24th international conference/19th annual conference on Computer science logic, CSL'10/EACSL'10, pages 230–240. Springer-Verlag, 2010.

[29] H.-Y. Dai, P.-X. Chen, and C.-Z. Li. Teleportation of an arbitrary two-particle state by two partial entangled three-particle GHZ-states. Communications in Theoretical Physics, 43:799–802, 2005.

[30] F.-G. Deng, X.-H. Li, C.-Y. Li, P. Zhou, and H.-Y. Zhou. Multiparty quantum-state sharing of an arbitrary two-particle state with einstein-podolsky-rosen pairs. Physical Review A, 72(4):044301, Oct 2005.

[31] F.-G. Deng, G. Long, and X.-S. Liu. Two-step quantum direct communication protocol using the einstein-podolsky-rosen pair block. Physical Review A, 68(4):042317, Oct 2003.

[32] E. D'Hondt and P. Panangaden. The computational power of the W and GHZ states. Journal of Quantum Information and Computation, 6(2):173–183, 2005.

[33] A. Doering. Quantum computer science lexture notes. Available from `https://www.cs.ox.ac.uk/teaching/materials10-11/quantum/`, March 2011.

[34] L. Dong, X.-M. Xiu, and Y.-J. Gao. Probabilistic teleportation of a two-particle state by two three-particle general w states. Acta Physica Polonica, 38:1985–1991, 2007.

[35] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. Physical Review A, 62(6):062314, Nov 2000.

[36] E. D'Hondt and P. Panangaden. Leader election and distributed consensus with quantum resources. ArXiv Quantum Physics e-prints, 2005.

[37] A. Ekert. Quantum cryptography based on bell's theorem. Physical Review Letters, 67(6):661–663, Aug 1991.

[38] Richard Feynman and Peter W. Shor. Simulating physics with computers. SIAM Journal on Computing, 26:1484–1509, 1982.

[39] G. Gan. Efficient quantum secure communication protocol by rearranging particle orders. Communications in Theoretical Physics, 52(5):845, 2009.

[40] T. Gao, F. Yan, and Z. Wang. Deterministic secure direct communication using GHZ states and swapping quantum entanglement. Journal of Physics A: Mathematical and General, 38(25):5761, 2005.

[41] V. N. Gorbachev and A. I. Trubilko. Quantum teleportation of an EPR pair by three-particle entanglement. Journal of Experimental and Theoretical Physics Letters, 91(quant-ph/9906110):894–898, 2000.

[42] V. N. Gorbachev, A. I. Trubilko, A. I. Zhiliba, and E. S. Yakovleva. Teleportation of entangled states and dense coding using a multiparticle quantum channel. Technical report, November 2000.

[43] D. Graham-Rowe. Foolproof quantum cryptography. Technology Review, March 2007.

[44] I.N. Herstein. Abstract Algebra. Wiley, 1999.

[45] M. Hillery, V. Buzek, and A. Berthiaume. Quantum secret sharing. Physical Review A, 59:1829–1834, 1999.

[46] T. Hwang, C.-C. Hwang, and C.-M. Li. Multiparty quantum secret sharing based on GHZ states. Physica Scripta, 83(4):45–49, April 2011.

[47] H. Imai, J. Mueller-Quade, A. C. A. Nascimento, P. Tuyls, and A. Winter. A Quantum Information Theoretical Model for Quantum Secret Sharing Schemes. ArXiv Quantum Physics e-prints, November 2003.

[48] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger. Quantum cryptography with entangled photons. Physical Review Letters, 84(20):4729–4732, May 2000.

[49] X.-R. Jin, X. Ji, Y.-Q. Zhang, S. Zhang, S.-K. Hong, K.-H. Yeon, and C.-I. Um. Three-party quantum secure direct communication based on GHZ states. Physics Letters A, 354:67–70, May 2006.

[50] J. Joo, J. Lee, J. Jang, and Y.-J. Park. Quantum secure communication via W states. ArXiv Quantum Physics e-prints, 2002.

[51] J. Joo, Y.-J. Park, S. Oh, and J. Kim. Quantum teleportation via a W state. New Journal of Physics, 5:136. 7 p, Jun 2003.

[52] A. Joyal and R. Street. The geometry of tensor calculus. Advances in Mathematics, 88:55–112, 1991.

[53] André Joyal and Ross Street. The geometry of tensor calculus, i. Advances in Mathematics, 88(1):55 – 112, 1991.

[54] R. Jozsa and N. Linden. On the role of entanglement in quantum-computational speed-up. In Proceedings of the Royal Society London A, volume 459, Aug 2003.

[55] A. Karlsson and M. Bourennane. Quantum teleportation using three-particle entanglement. Physical Review A, 58:4394–4400, 1998.

[56] A. Kissinger. Exploring a quantum theory with graph rewriting and computer algebra. In J. Carette, L. Dixon, C. Coen, and S. Watt, editors, Intelligent Computer Mathematics, volume 5625 of Lecture Notes in Computer Science, pages 90–105. Springer Berlin / Heidelberg, 2009.

[57] A. Kissinger, A. Merry, B. Frot, L. Dixon, M. Soloviev, and R. Duncan. Quantomatic. http://sites.google.com/site/quantomatic/home, 2008-present.

[58] S. Mac Lane. Categories for the Working Mathematician. Springer, 1998.

[59] H. Lee, J. Lim, and H. Yang. Quantum direct communication with authentication. Physical Review A, 73(4):042305, Apr 2006.

[60] H. Lee, J. Lim, and H. J. Yang. Quantum direct communication with authentication. ArXiv Quantum Physics e-prints, (quant-ph/0512051), Dec 2005.

[61] J. Lee, H. Min, and S. Oh. Multipartite entanglement for entanglement teleportation. Physical Review A, 66(5):052318, Nov 2002.

[62] J. Liu, Y.-M. Liu, H.-J. Cao, S.-H. Shi, and Z.-J. Zhang. Revisiting Quantum Secure Direct Communication with W State. Chinese Physics Letters, 23:2652–2655, October 2006.

[63] J. Liu, Y.-M. Liu, Y. Xia, and Z.-J. Zhang. Revisiting controlled quantum secure direct communication using a non-symmetric quantum channel with quantum superdense coding. Communications in Theoretical Physics, 49(4):887, 2008.

[64] W. Liu, H. Chen, T. Ma, and W. Tian. An efficient deterministic secure quantum communication scheme with W state. In Proceedings of the 2008 International Conference on Computational Intelligence and Security - Volume 01, CIS '08, pages 52–55, Washington, DC, USA, 2008. IEEE Computer Society.

[65] W.-J. Liu, H.-W. Chen, Z.-Q. Li, and Z.-H. Liu. Efficient Quantum Secure Direct Communication with Authentication. Chinese Physics Letters, 25:2354–2357, July 2008.

[66] H.-K. Lo, X. Ma, and K. Chen. Decoy state quantum key distribution. Physical Review Letters, 94(23):230504, Jun 2005.

[67] L. Marinatto and T. Weber. Which kind of two-particle states can be teleported through a three-particle quantum channel? Foundations of Physics Letters, 13:119–132, 2000. 10.1023/A:1007875331710.

[68] N. Mermin. Simple unified form for the major no-hidden-variables theorems. Physical Review Letters, 65(27):3373–3376, Dec 1990.

[69] A. Nascimento, J. Mueller-Quade, and H. Ima. Improving quantum secret-sharing schemes. Physical Review A, 64, 2001.

[70] M. Nielsen and I. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, 2000.

[71] C. Pagonis, M. Redhead, and R. Clifton. The breakdown of quantum non-locality in the classical limit. Physics Letters A, 155(8-9):441 – 444, 1991.

[72] R. Penrose. Application of negative dimensional tensors. Combinatorial Mathematics and its Applications, pages 221–244, 1971.

[73] B. Pierce. Basic Category Theory for Computer Scientists. MIT Press, 1991.

[74] K. Rietjens. Quantum secret sharing schemes. Master's thesis, Technische Universiteit Eindhoven, 2004.

[75] S. Roy. A compositional characterization of multipartite quantum states. Master's thesis, University of Oxford, 2010.

[76] B. Schneier. Applied cryptography: protocols, algorithms, and source code in C. John Wiley & Sons, Inc., 1996.

[77] Peter Selinger. Dagger compact closed categories and completely positive maps. Electronic Notes in Theoretical Computer Science (ENTCS), 170:139–163, March 2007.

[78] A. Shamir. How to share a secret. Communications of the ACM,, 22:612–613, 1979.

[79] B.-S. Shi, Y.-K. Jiang, and G.-C. Guo. Probabilistic teleportation of two-particle entangled state. Physics Letters A, 268(3):161 – 164, 2000.

[80] B.-S. Shi and A. Tomita. Teleportation of an unknown state by w state. Physics Letters A, 296(4-5):161 – 164, 2002.

[81] S. Singh and R. Srikanth. Generalized quantum secret sharing. Phys. Rev. A, 71:012328, Jan 2005.

[82] A. Smith. Quantum secret sharing for general access structures, 2000.

[83] C. Wang, F. Deng, and G. Long. Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state. Optics Communications, 253(1-3):15 – 20, 2005.

[84] J. Wang, Q. Zhang, and C.-J. Tang. Quantum secure communication scheme with W state. ArXiv Quantum Physics e-prints, March 2006.

[85] Y.-H. Wang, C.-S. Yu, and H.-S. Song. Teleportation of an arbitrary multipartite GHZ-class state by one EPR pair. Chinese Physics Letters, 23:3142–3144, December 2006.

[86] Y. Xia and H.-S. Song. Controlled quantum secure direct communication using a non-symmetric quantum channel with quantum superdense coding. Physics Letters A, 364(2):117 – 122, 2007.

[87] Y. Xia, J. Song, P.-M. Lu, and H.-S. Song. Teleportation of an N-photon Greenberger-Horne-Zeilinger (GHZ) polarization-entangled state using linear optical elements. Journal of the Optical Society of America B, 27:A1–A6, 2010.

[88] L. Xiao, G. L. Long, F.-G. Deng, and J.-W. Pan. Efficient multi-party quantum secret sharing schemes. ArXiv Quantum Physics e-prints, 2004.

[89] X.-M. Xiu, L. Dong, Y.-J. Gao, and F. Chi. Quantum teleportation schemes of an N-particle state via three-particle general W states. Communications in Theoretical Physics, 49:905–908, April 2008.

[90] Z.-J. Zhang, J. Liu, D. Wang, and S.-H. Shi. Comment on "Quantum direct communication with authentication". Physical Review A, 75(2):026301, Feb 2007.

[91] P. Zhou, X.-H. Li, F.-G. Deng, and Zhou H.-Y. Probabilistic teleportation of an arbitrary GHZ-class state with a pure entangled two-particle quantum channel and its application in quantum state sharing. Chinese Physics, 16(10):2867, 2007.

[92] P. Zhou, X.-H. Li, F.-G. Deng, and H.-Y. Zhou. Probabilistic teleportation of an arbitrary GHZ-class state with a pure entangled two-particle quantum channel and its application in quantum state sharing. Chinese Physics, 16:2867–2874, October 2007.