Design and Analysis of Quantum Protocols and Algorithms

Krzysztof Bar
University College

MMathCompSci

May 20, 2012

Acknowledgements

I would like to thank my supervisor prof. Bob Coecke for all the help given during the course of the past year, without his assistance this dissertation never would have been written. I also wanted to thank graduate students Aleks Kissinger and Alex Merry for their patience in answering all my questions. Special thanks to my friends Dan and Michael, who read the drafts and provided many helpful remarks.

Contents

Introduction

The idea of using quantum mechanical phenomena to devise a new computational paradigm first came to prominence in 1982, when physicist Richard Feynman observed that simulation of quantum systems on a classical computer seems to require an exponential amount of resources. He also noticed that a computer based on quantum mechanical features, being a quantum system itself, could perform the same task with only a polynomial amount of resources. The idea was further explored by David Deutsch and led to defining an abstract notion of Quantum Turing Machine in 1985[9]. A major breakthrough came in 1994, when Peter Shor published his famous factoring algorithm[21]. Nowdays research in Quantum Computing concentrates, apart from efforts to physically realise a quantum computer, on quantum cryptography, quantum complexity theory and on the origins of quantum speed-up.

A major difficulty encountered in reasoning about quantum computation is the formalism that is being used. The so-called *Hilbert Spaces* formalism devised by John von Neumann in 1931 as a mathematical foundation for quantum mechanics is still in use today. To perform operations it requires multiplication of matrices, whose size rises exponentially with the increase of quantum system's size. That is why computation in this formalism is cumbersome and far from intuitive.

Because of this reason, many researchers concentrate on finding an alternative formalism that would capture the compositional nature of quantum systems in a more natural way. A promising attempt to achieve that is Categorical Quantum Mechanics, first described by Bob Coecke and Samson Abramsky in 2004[1]. Afterwards, this stream of research has been continued throughout the years in multiple papers written by members of the Quantum Group at the Oxford University Computing Department.

Categorical axiomatisation of Quantum Theory leads to an intuitive language for describing quantum computation - graphical calculi. The subject of this dissertation is to explore its capabilities within different branches of the field of Quantum Computing. Knowledge of Oxford Part C courses on Category Theory and Quantum Computing is assumed throughout. Chapter 1 gives a summary of abstract notions necessary in the categorical axiomatisation. Chapter 2 describes two graphical calculi: Red-green calculus (otherwise known as Z/X-calculus) and Red-green-blue calculus (RGB-calculus). Chapters 3, 4 and 5, discuss three different applications of both calculi. In chapter 3, two quantum theories are compared and the interpretation of Red-green-blue calculus in Spekkens Toy Theory is the author's individual contribution. Chapter 4 analyses three quantum protocols that have never been interpreted in RGB-calculus. In Chapter 5 a new alternative diagrammatical proof of a standard result on classical simulability is presented. These three different applications present the versatility of graphical calculi in reasoning about quantum computation.

Chapter 1

Categorical Quantum Mechanics

The first chapter establishes some preliminary notions used in the categorical approach to Quantum Mechanics and presents the diagrammatical formalism based on it. Section 1 follows the description of monoidal categories given in the Oxford graduate course on Categorical Quantum Mechanics. Section 2 follows Bob Coecke's presentation from [3].

1.1 Symmetric Monoidal Categories

A monoidal category is a category endowed with additional structure that allows us to define composite objects and morphisms. This additional structure is expressed by a binary operator - monoidal tensor product $\otimes$. Along with morphism composition $\circ$, they constitute two methods for producing and acting upon composite systems.

Tensor product $\otimes$ acts on objects in the following way: given A, B in a monoidal category $\mathcal{C}$, $A \otimes B$ is a composite object in $\mathcal{C}$. It also induces an operation on morphisms: given A, B, C, D in $\mathcal{C}$ and for $f : A \to C$, $g : B \to D$, we have $(f \otimes g) : (A \otimes B) \to (C \otimes D)$.

Morphism composition $\circ$ can be thought of as composition in time. When acting with $f \circ g$ on an object, we first act with the morphism g and *after* that with f. Monoidal tensor composition in turn, can be thought of as parallel composition. When acting with $f \otimes g$ on a composite object $A \otimes B$, we act on A with f, *while* acting on B with g.

Any algebraic structure that admits a morphism that preserves the structure's properties may be used to define a category:

- **Set** - sets are objects and functions between sets are arrows
- **FHilb** - finite dimensional Hilbert Spaces are objects and linear maps are arrows
- **Rel** - sets are objects and relations are arrows

All three of these categories can be made into monoidal categories by defining the monoidal tensor product operator $\otimes$:

- **Set** - $\otimes$ is the cartesian product of sets
- **FHilb** - $\otimes$ is the oridinary tensor product of Hilbert Spaces
- **Rel** - as in **Set** $\otimes$ is the cartesian product of sets

Now, we proceed to formally define monoidal categories and attributes that they admit: symmetry, strictness and the dagger functor.

Definition 1.1. A monoidal category consists of a category $\mathcal{C}$, a bifunctorial tensor

$$\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$$

a unit object I and families of natural isomorphisms such that:

- for all objects A, there exist natural isomorphisms called respectively the left and right unitors:
$$\lambda_A : A \simeq \mathrm{I} \otimes A \qquad\qquad \rho_A : A \simeq A \otimes \mathrm{I}$$
- for all objects A, B, C, there exist natural isomorphisms called the associators:
$$\alpha_{A,B,C} : A \otimes (B \otimes C) \simeq (A \otimes B) \otimes C$$

which are subject to certain coherence conditions. MacLane proved that commutativity of the following two diagrams is a sufficient condition to ensure coherence[18].

$$\begin{tikzcd}
A \otimes (I \otimes B) \arrow[r, "\alpha_{A,I,B}"] \arrow[d, "I_A \otimes \lambda_B"'] & (A \otimes I) \otimes B \arrow[dl, "\rho_A \otimes I_B"] \\
A \otimes B &
\end{tikzcd}$$

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

Definition 1.2. A monoidal category is symmetric if there exists a familiy of natural isomorphisms such that for every pair of objects A, B there is a morphism:

$$\sigma_{A,B} : A \otimes B \simeq B \otimes A$$

Definition 1.3. A monoidal category is strict if the natural isomorphisms α, λ and ρ are identities. Every monoidal category is monoidally equivalent to a strict monoidal category.[18]

Due to this fact, from now on we assume that all categories that we consider are strict.

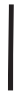
Definition 1.4. A strict dagger monoidal category is a strict monoidal category equipped with an involutive identity-on objects functor $\dagger : \mathcal{C}^{op} \to \mathcal{C}$, such that :

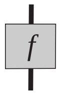
- $\forall A \in \mathcal{C}, \mathcal{A}^{\dagger} = \mathcal{A}$
- $\forall f, g \in \mathcal{C}, f^{\dagger\dagger} = f$ and $(f \otimes g)^{\dagger} = f^{\dagger} \otimes g^{\dagger}$

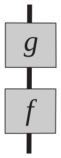
Definition 1.5. A strict dagger symmetric monoidal category **C** is both a strict dagger monoidal category and a strict symmetric monoidal category, such that $\sigma^{\dagger}_{A,B} = \sigma^{-1}_{A,B}$, where $f^{\dagger} : B \to A$ is the adjoint of $f : A \to B$.

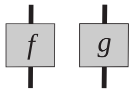
1.2 Graphical Calculi for Quantum Computation

Details of how monoidal categories are used to describe quantum systems in the categorical axiomatisation of Quantum Theory are available in [1]. In the diagrammaric formalism based upon this axiomatisation linear operators are represented as pictures:

$I_A : A \to A \;\equiv$ 

$f : A \to A \;\equiv$ 

$g \circ f : A \to A \;\equiv$ 

$f \otimes g : (A \otimes B) \to (A \otimes B) \;\equiv$ 

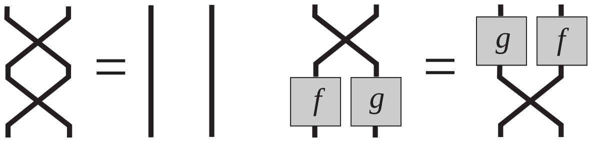
Functional composition is realised by joining inputs and outputs of boxes representing the operators and the tensor product by putting the boxes next to each other. Identity is depicted as a straight wire.

This method also allows to express states $I \xrightarrow{\psi} A$, effects $A \xrightarrow{\pi} I$, constants $I \xrightarrow{\pi} I$ and adjoint mappings by means of pictures. A detailed account of those is available in [3].

Now we quote the most important result of this chapter. A theorem, due to Joyal and Street[13], that establishes the connection between the diagrammatic language and symmetric monoidal categories.

Theorem 1.1. The graphical calculi for monoidal categories and 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 is derivable in the graphical calculus.

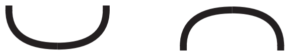
The concept of symmetry allows us to swap components of compound systems and is captured by the following laws:



In equations, they are expressed as (with $\sigma_{A,B}$ as defined in Definition 1.2)

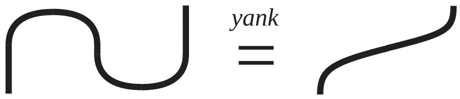
$$\sigma_{B,A} \circ \sigma_{A,B} = 1_{A,B} \qquad \text{and} \qquad \sigma_{A,B} \circ (f \otimes g) = (g \otimes f) \circ \sigma_{A,B}\,.$$

Bell states and Bell effects are expressed by turning the wire:



which are expressed in categorical terms as $I \xrightarrow{\eta_A} A \otimes A$ and $A \otimes A \xrightarrow{\epsilon_A} I$, with η to be rigorously defined later in the chapter.

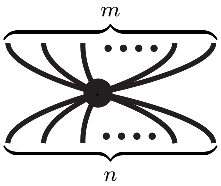
They are subject to the identity $(\epsilon_A \otimes 1_A) \circ (1_A \otimes \eta_A) = 1_A$, which allows us to cancel two consecutive opposite turns by yanking the wire.



Definition 1.6. A symmetric monoidal dagger category in which morphisms η_A, ϵ_A exist for each object A and satisfy certain coherence conditions is called compact. Theorem 1 is extended to dagger compact categories.

To give a more complete description of quantum theory, we include an interpretation of non-degenerate observables.

Definition 1.7. A non-degenerate observable (or basis) for an object A in a dagger symmetric monoidal category is a family of spiders with n front and m back legs, for $n, m \in \mathbb{N}$ denoted $A^{\otimes n} \xrightarrow{\delta_n^m} A^{\otimes m}$ and depicted as:



It is worth noting that δ_0^2 and δ_2^0 correspond to Bell states and Bell effects and because of this, the spider structure captures all features gained by introduction of wire turns.

The following theorem proved in [7] explains why in **FHilb** these spiders represent observables.

Theorem 1.2. In **FHilb**, non-degenerate observables $\{\mathcal{H}^{\otimes n} \xrightarrow{\delta_n^m} \mathcal{H}^{\otimes m}\}_{n,m}$ exactly correspond with orthonormal bases on the underlying Hilbert space $\mathcal{H}$, which in turn correspond to non-degenerate observables on $\mathcal{H}$

The second correspondence is due to the fact that an observable M on an n-dimensional Hilbert Space $\mathcal{H}$ is represented by a linear combination of projections $P_i = |\mathrm{i}\rangle\langle i|$ for some orthonormal basis $\{|i\rangle\}_i$.

The exact nature of the first correspondence is best explained using the copying-deleting pair presentation of non-degenerate observables using Frobenius algebras, for a reference see [3]. There a non-degenerate observable in a dagger symmetric monoidal category is a triple (A, δ, ϵ) where A is an object, $A \xrightarrow{\delta} A \otimes A$ a copying morphism and $A \xrightarrow{\epsilon} I$ a deleting morphism.

An orthonormal basis $\{|i\rangle\}_i$ of a Hilbert Space $\mathcal{H}$ induces two linear maps: the operation that copies the basis vectors and the operation that deletes the basis vectors.

$$\delta : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}; |\mathrm{i}\rangle \to |\mathrm{ii}\rangle \qquad \epsilon : \mathcal{H} \to \mathbb{C}; |\mathrm{i}\rangle \to 1$$

No-cloning theorem implies that the only vectors copied by δ and deleted by ϵ are the basis vectors, so $\{|i\rangle\}_i$ is the only basis corresponding to δ and ϵ.

It is shown in [3] that δ can be thought of as a spider δ_2^1 and ϵ as a spider δ_0^1. The morphisms generated from δ_2^1 and δ_0^1 using composition, tensor products and adjoints, such that their graphical representation is connected are exactly the family of spiders. This is due to the fact that such morphisms only depend on the number of inputs and outputs.

In the subsequent results we assume familiarity with the Dirac bra-ket notation for Quantum Computation. In this notation eigenvectors of Pauli matrices Z, X, Y are denoted by:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |+\rangle = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad |i\rangle = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad |-\rangle = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad |-i\rangle = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}$$

Definition 1.8. Let $\{\psi_1, \dots, \psi_n\}$ be the set of normalized eigenvectors of an observable A, a normalized vector $|\psi'\rangle$ is unbiased for A if for all i we have that $|\langle\psi_i|\psi'\rangle|^2 = \frac{1}{n}$.

Unbiasedness can be understood in terms of all outcomes of a measurement on A being equally likely.

Definition 1.9. Two non-degenerate observables A and B in an n-dimensional Hilbert Space are complementary if their mutually orthogonal normalised eigenvectors $|\psi_1^A\rangle, \dots, |\psi_n^A\rangle$ and $|\psi_1^B\rangle, \dots, |\psi_n^B\rangle$ are unbiased with respect to the other observable. i.e for all i, j it holds that $|\langle\psi_i^A|\psi_j^B\rangle|^2 = \frac{1}{n}$.

This definition extends in a straightforward manner to a finite set of non-degenerate observables:

Definition 1.10. A finite set of non-degenerate observables $A_1, \dots, A_n$ in an n-dimensional Hilbert Space is a set of complementary observables if each pair A_i, A_j is complementary in the sense of the above definition.

Examples of pairs of complementary observables include position and momentum as well as each pair of the set of Z-, X- and Y-observables for a qubit. Let $\alpha \in [0, 2\pi)$:

Observable	Eigenvectors	Unbiased vectors	Examples of unbiased states
Z	$\|0\rangle, \|1\rangle$	$\|0\rangle + e^{i\alpha}\|1\rangle$	$\|+\rangle + \|-\rangle, \|i\rangle + \|-i\rangle$
X	$\|+\rangle, \|-\rangle$	$\|+\rangle + e^{i\alpha}\|-\rangle$	$\|0\rangle + \|1\rangle, \|i\rangle + \|-i\rangle$
Y	$\|i\rangle, \|-i\rangle$	$\|i\rangle + e^{i\alpha}\|-i\rangle$	$\|0\rangle + \|1\rangle, \|+\rangle + \|-\rangle$

Example: $|i\rangle$ is unbiased with respect to the observable X. For a qubit, $n = 2$.

$$|\langle+|i\rangle|^2 = |\langle\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}|\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}\rangle|^2 = |\frac{1}{2}(1+i)|^2 = \frac{1}{2}$$

Notions of unbiasedness and eigenvectors for non-degenerate observables can also be defined for observables in dagger compact categories, but first we have to define an auxiliary notion of the abstract conjugate morphism f_*.

Each observable (A, δ, ϵ) in a dagger compact category is associated with a compact structure $(A, \eta = \delta \circ \epsilon^\dagger, I \to A \otimes A)$. Here, compactness is to be understood in the sense of Definition 1.6. Notice that η can be expressed by a spider δ_2^0 from the family corresponding to the observable.

Definition 1.11. For a morphism $f : A \to B$ and a pair of observables and induced compact structures (A, η_A), (B, η_B) the conjugate morphism $f_* : B \to A$ is defined as

$$f_* = (\eta_A^\dagger \otimes 1_B) \circ (1_A \otimes f^\dagger \ \otimes 1_B) \circ (1_A \otimes \eta_B)$$

For clarity of presentation, we define an operation $\odot$. For two states $I \xrightarrow{\psi} A$ and $I \xrightarrow{\phi} A$ let $\psi \odot \phi := \delta^\dagger \circ (\psi \otimes \phi)$.

Definition 1.12. A state ψ is unbiased with respect to an observable (A, δ, ϵ) in a dagger compact category if the following equality is satisfied:

$$\psi_* \odot \psi = \delta^\dagger \circ (\psi_* \otimes \psi) = \epsilon^\dagger$$

where ψ_* is the abstact conjugate of the state ψ.

Definition 1.13. Eigenstates (equivalently eigenvectors) for an observable $(A, \delta, A \to A \otimes A, \epsilon : A \to I)$ in a dagger symmetric monoidal category are defined to be the states ψ that are copied by δ, i.e. states ψ for which: $\delta \circ \psi = \psi \otimes \psi$.

In the graphical interpretation this equality results in the diagram becoming disconnected. Note that, for this notion, compactness is not required.

Definition 1.14. Two observables $(A, \delta_X, \epsilon_X)$ and $(A, \delta_Y, \epsilon_Y)$ in a dagger compact category are complementary if the eigenvectors of one are unbiased for the other.

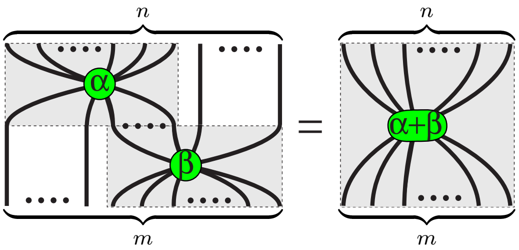
The definition extends to any finite set of observables $\{(A_i, \delta_i, \epsilon_i)\}_i$ in the same way as for observables in a Hilbert Space in Definition 1.10. In graphical calculi we denote observables that are complementary with different colours.

In categorical interpretations of different quantum theories a pivotal role is played by the *phase group* that we associate with the theory. In Chapter 3, we look more closely at Qubit Stabilizer Theory and Spekkens Toy Theory and their categorical interpretetions. But firstly, let us consider the notion of *phase group* in an abstract setting.

Definition 1.15. Let $\mathcal{S}(A, \delta, \epsilon)$ be the set of all states $I \xrightarrow{\psi} A$ that are unbiased for (A, δ, ϵ). Let $\mathcal{U}(A, \delta, \epsilon)$ be the set of all unitary morphisms of the form $U_\psi = \psi \odot 1_A = \delta^\dagger \circ (\psi \otimes 1_A)$. The morphism U_ψ is unitary if and only if it is unbiased for (A, δ, ϵ).

Theorem 1.3. For any observable (A, δ, ε), $(\mathcal{S}(A, \delta, \epsilon), \odot, \epsilon^\dagger)$ and $(\mathcal{U}(A, \delta, \varepsilon), \circ, 1_A)$ are isomorphic Abelian groups. For $\mathcal{S}(A, \delta, \varepsilon)$ the inverse is provided by the conjugate and the adjoint respectively. The group is called the *phase group.*

Since phases originated from the copying-deleting formalism for observables, they have a natural graphical depiction and it is possible to augment spiders to support phases. In the graphical calculi considered here, the following law presents how spiders interact with other spiders of the same colour.



The phases are added, since multiplication in the phase group corresponds to addition of angles. As demonstrated by the example of the X-observable for a qubit in **FHilb** recall that: $\mathcal{S}(A, \delta, \epsilon^\dagger) = \{|+\rangle + e^{i\alpha}|-\rangle \mid \alpha \in [0, 2\pi)\}$. Then for two elements of the group:

$$(|0\rangle + e^{i\alpha}|1\rangle) \odot (|+\rangle + e^{i\alpha'}|-\rangle) = |0\rangle + e^{i(\alpha+\alpha')}|1\rangle$$

Now we discuss the connection between phase groups and non-locality in a particular class of theories – so called Mutually Unbiased Theories. Non-locality in this context means that correlations between the results of measurements violate Bell inequalities. Firstly, we need to introduce the notion of a GHZ-state.

Definition 1.16. A GHZ-state is an entangled quantum state $|GHZ\rangle = \frac{|000\rangle+|111\rangle}{\sqrt{2}}$

Together with the W-state, $|W\rangle = \frac{|100\rangle+|010\rangle+|001\rangle}{\sqrt{3}}$, they represent two different and LOCC-inequivalnet classes of tripartite entanglement. Any tripartite entangled state can be transformed to either GHZ or W using only local operations and classical communication (LOCC). GHZ can be thought of as a maximally entangled tripartite state. The nature of entanglement in the W state can be understood as pairwise entanglement between its qubits. This difference is exhibited by their graphical representations.[3]

GHZ state is important when considering non-locality, because the results of measuring its different subsystems exhibit non-local correlations. GHZ is expressed in categorical terms for an observable (A, δ, ϵ) as the the structure (A, $\Psi : I \to A \otimes A \otimes A, \epsilon : A \to I$), and graphically with a spider δ_3^0.

Definition 1.17. A Mutually Unbiased Theory is a theory where for each state ψ of an elementary system A, and each observable (A, δ, ε), ψ is either an eigenvector or unbiased for (A, δ, ε).

Theorem 1.4. In any mutually unbiased theory all non-local correlations are completely determined by the phase group, and hence classified by finite abelian groups.

Both theories considered in chapter 3: Qubit Stabilizer Theory and Spekkens' Toy Theory are mutually unbiased. Their phase groups are respectively the cyclic group Z_4 and the Klein group $Z_2 \times Z_2$. All differences between their categorical interpretations **Stab** and **Spek** can be traced back to this fact.[6]

If a theory has Z_4 as a subgroup of its phase group, then it is non-local. Theories that have $Z_2 \times Z_2$ as their phase group are local. Z_4 and $Z_2 \times Z_2$ are the only 4-element abelian groups, so for theories with 4-element phase groups these two are the only possibilities.

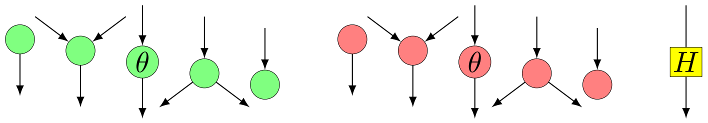
Chapter 2

Dichromatic and Trichromatic Graphical Calculi

In this chapter we introduce two graphical calculi. Red-green calculus presentation follows the approach taken in [4] by Coecke and Duncan. Red-green-blue calculus presentation follows a paper by Lang and Coecke[17].

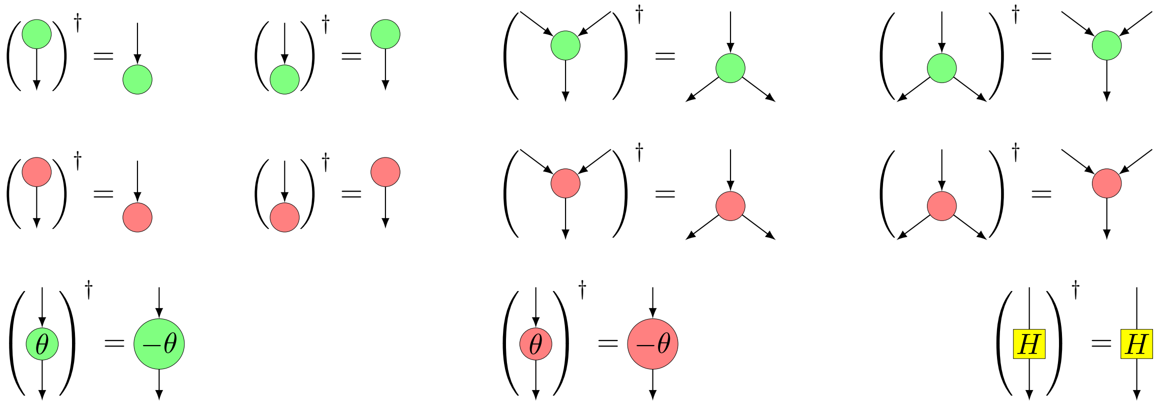
2.1 Red-Green Calculus

Red-green calculus, also known as $Z/X-$ calculus is a calculus of complementary observables for Pauli Z- and X-observables for a qubit. Its main components are two copying-deleting pairs, one for each observable. As indicated before we will use two different colours to distinguish between both complementary observables. Due to the results established in Chapter 1, it is possible to introduce phase angles, we also introduce the Hadamard gate that will act as a colour changer. Numbering will be used to facilitate referring to these equations in later chapters.



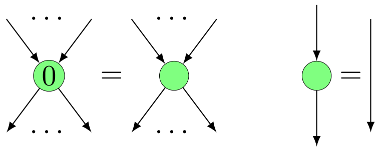
(2.1)

Since it is our aim to present $Z/X-$calculus as a dagger symmetric monoidal category **RG**, here we expose how these generating elements behave under the dagger operation.

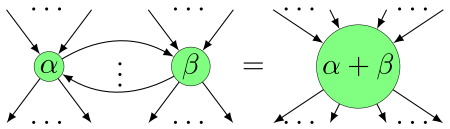


Axioms governing these graphs and rationale behind them are explained carefully in [4], here we give a short summary:

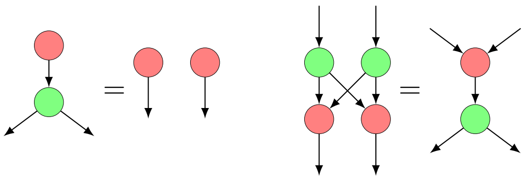
- Only the topology matters
- All equations are valid under flip of colours
- All equations are valid under flip of arrows and †-negation of angles



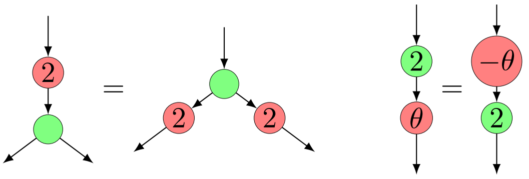
(2.2)



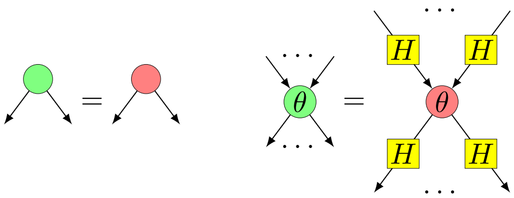
(2.3)



(2.4)

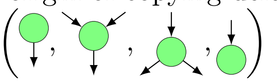
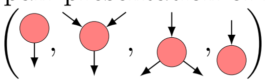


(2.5)



(2.6)

General phases $\alpha \in [0, 2\pi)$ allow for expression of any single-qubit unitary gate and hence together with existence of CNOT gate imply universality of the calculus – any n-qubit unitary map can be depicted in Z/X-calculus. This full version of Z/X-calculus is used to define the notion of classical simulability in Chapter 5. Here, we restrict ourselves to $\alpha \in \{0, \frac{\pi}{2}, \pi, \frac{3}{2}\pi\} \cong \{0, 1, 2, 3\}$ in order to be able to compare categorical representations of Red-green and Red-green-blue calculi. In pictures, phases are denoted using elements of $\{0, 1, 2, 3\}$ to increase clarity of presentation.

Naturally because of the origin of copying-deleting pair presentation of non-degenerate observables, the two tuples  and  form †-special commutative Frobenius Algebras, whose significance is explored in [3].

On the basis of work done by Kissinger in [15], Lang and Coecke suggested a name 'open digraphs' for graphs that are obtained from these generators. Composition is realised by connecting the open ended wires and the tensor product by putting two digraphs side-by-side. The direction of arrows suggests the direction of the flow of information, so incoming wires could be thought of as inputs and outcoming wires as outputs. Structures with neither correspond to constants, here we will omit them for the sake of simplicity.

By the above remarks we have a well-defined symmetric monoidal dagger category **RG**. Using the approach taken by Lang and Coecke in [17], we make the following definition.

Definition 2.1. A category **RG** is a dagger symmetric monoidal category in which the objects are n-fold monoidal products of an object $\star$, denoted $\star^n$ and a morphism from $\star^m$ to $\star^n$ is a dichromatic open digraph from m wires to n wires, built from the sets of green and red generators mentioned above and the Hadamard gate. The identity morphism on each object is depicted as a straight wire. Phases are limited to values from $\{0, \frac{\pi}{2}, \pi, \frac{3}{2}\pi\}$.

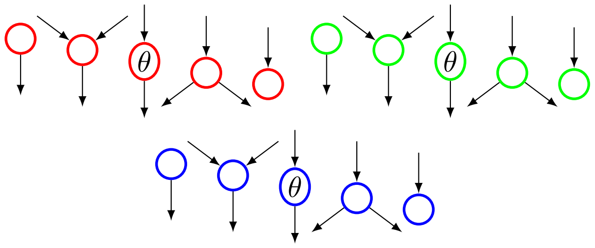
2.2 Red-Green-Blue Calculus

It has been proved that in a Hilbert Space of dimension n at most $n+1$ observables can form a set in which each pair of observables is mutually complementary.[24] If n is a power of a prime, then this number is exactly equal to $n+1$. Since a single qubit is mathematically modelled by a Hilbert Space $\mathcal{H}$ such that $\dim(\mathcal{H}) = 2$ and 2 is a power of a prime, there can be at most three complementary observables within a qubit.

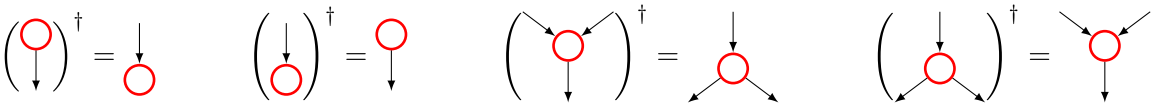
This fact together with incompleteness of Z/X-calculus with respect to Qubit Theory, which will be discussed later in this chapter, lead to the introduction of Red-green-blue calculus. Similarly as for **RG**:

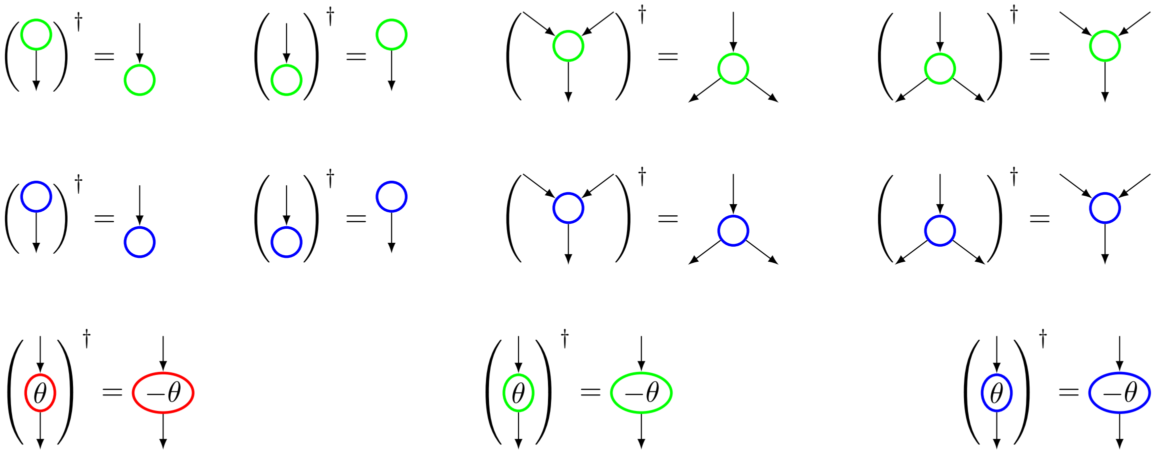
Definition 2.2. A category **RGB** is a dagger symmetric monoidal category with tensor products of $\star$ as objects, and morphisms represented as open digraphs with red, green and blue nodes. The identity morphism on each object is depicted as a straight wire. Composition and monoidal products are as defined for open digraphs.

RGB-calculus is a graphical calculus for three complementary observables. Each colour corresponds to a different observable and we have three sets of generators, instead of two like in Z/X-calculus.



Dagger operation is defined as for **RG**, arrow directions are flipped, copying and deleting morphisms are flipped upside-down and phases negated:

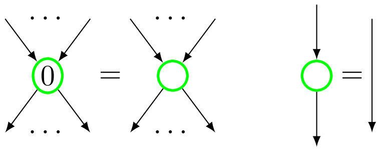




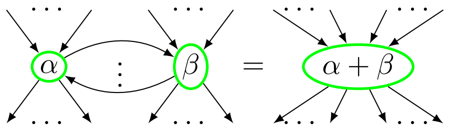
Phases are limited to values from $\{0, \frac{\pi}{2}, \pi, \frac{3}{2}\pi\} \cong \{0, 1, 2, 3\}$. Again, for convenience and clarity of presentation, we utilise the fact that this set forms a group isomorphic to Z_4 and denote phases using elements of this group. Again for clarity, phases '0' are omitted and expressed as a coloured dot without a phase.

Red-green-blue axioms are similar to those of Red-green calculus but there are some subtle differences necessary to accommodate the addition of a third colour. A thorough account of all rules is available at [17].

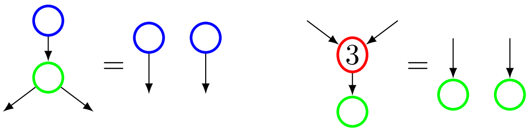
- Only the topology matters
- All equations are valid under even permutation of colours
- All equations are valid under flip of arrows and †-negation of angles



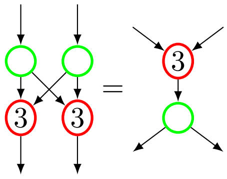
(2.7)



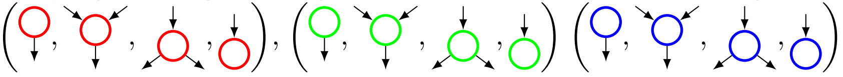
(2.8)



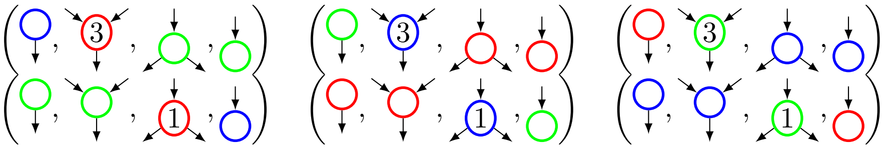
(2.9)



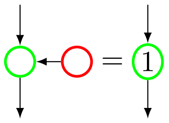
(2.10)

Again, because of the copying-deleting pair origins of the formalism, the tuples of generators of different colours:  form Frobenius Algebras.

It is a consequence of **RGB**-axioms and even coulour permutations and the dagger structure that the following tuples form bialgebras in the sense of the definition stated in [14]. Their copying capabilities will be used in later chapters.

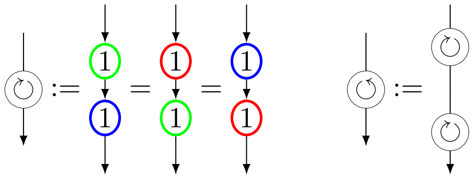


Phases can be expressed using the copying and deleting operation, by the following equation:

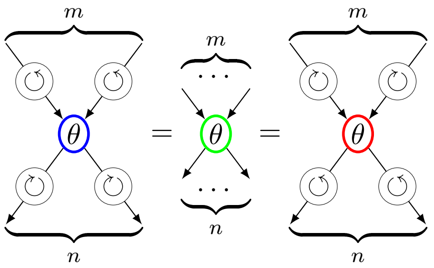


(2.11)

One of the significant advantages of introducing the third colour is that we are now able to realise the change of colour operation without introducing an additional primitive structure, like the Hadamard gate used in Z/X. In RGB colour rotation gates are expressed using known generators and their effect on different colours is as follows:

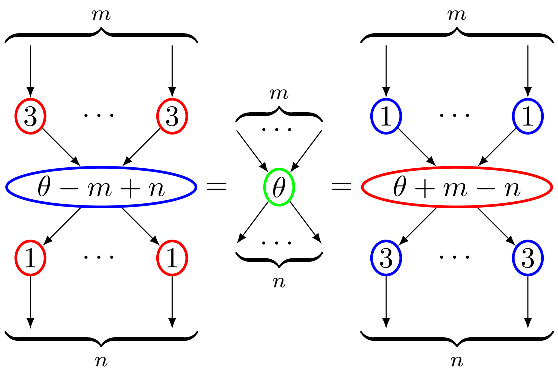


(2.12)



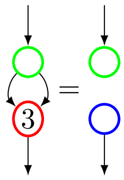
(2.13)

Each colour may be expressed using two remaining colours as a consequence of the following derivable equation:



(2.14)

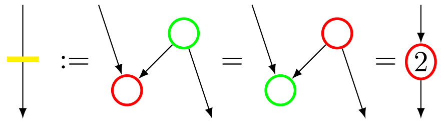
Another useful derivable result that we state is:



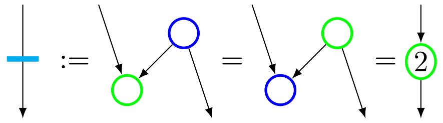
(2.15)

It is a version of the Hopf law[14], that holds under appropriate modifications for all six bialgebra tuples defined above. It shows that each of them is also a Hopf Algebra. It is worth noting that this law results in a radical change of the diagram topology.

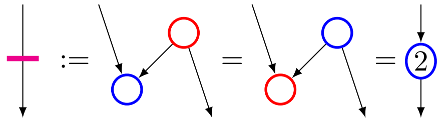
In Red-green calculus the compact structure of the pair of complement of complementary observables is compatible. However that is not the case for complementary observables in Red-green-blue calculus. In order to be able to define an operation flipping the direction of arrows and leaving the rest of the digraph unmodified, we need dualizers[4]. There are three, one per each pair of colours:



(2.16)

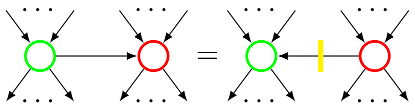


(2.17)

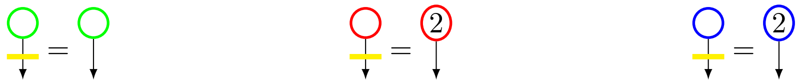


(2.18)

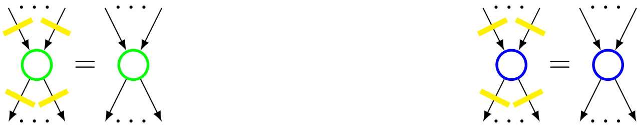
And their arrow flipping capabilities are exhibited by the following law (that also works under even colour permutations).



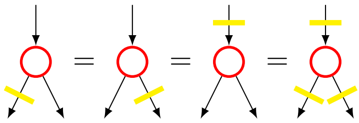
(2.19)



(2.20)



(2.21)

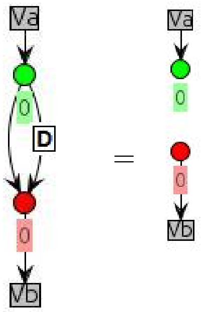


(2.22)

In Red-Green calculus the dualizer reduces to identity, hence edges can be thought of as undirected.

Now we will provide a result that relates dualizers to the concept of complementarity and gives a diagrammatical characterisation of complementary observables.

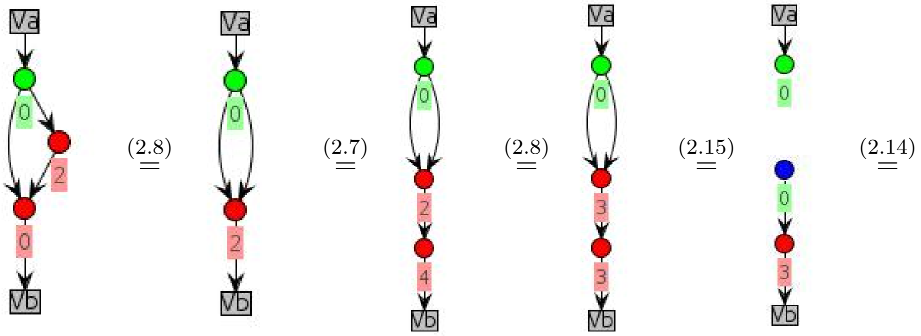
Theorem 2.1. A pair of observables $(A, \delta_X, \epsilon_X)$, $(A, \delta_Y, \epsilon_Y)$ is complementary if and only if the following equation is satisfied:

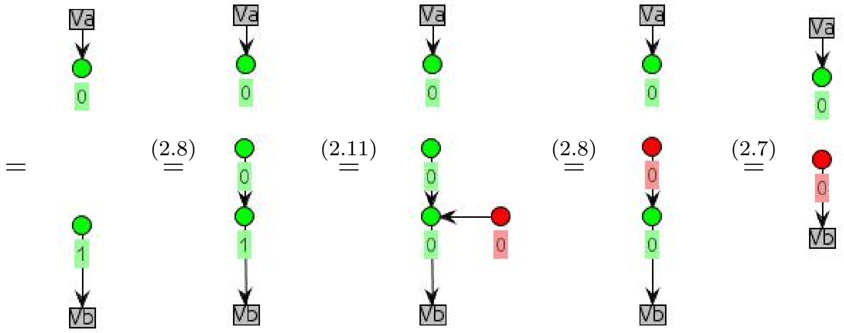


where D is a dualiser.

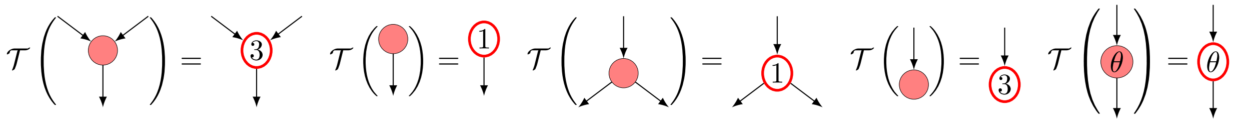
Grey boundary boxes, used here and in the remaining chapters, denote inputs and outputs and are used to capture wires incoming and outcoming from the digraph.

In Red-green calculus this is equivalent to the familiar version of the Hopf Law, and in Red-green-blue it can be ilustrated by an example:



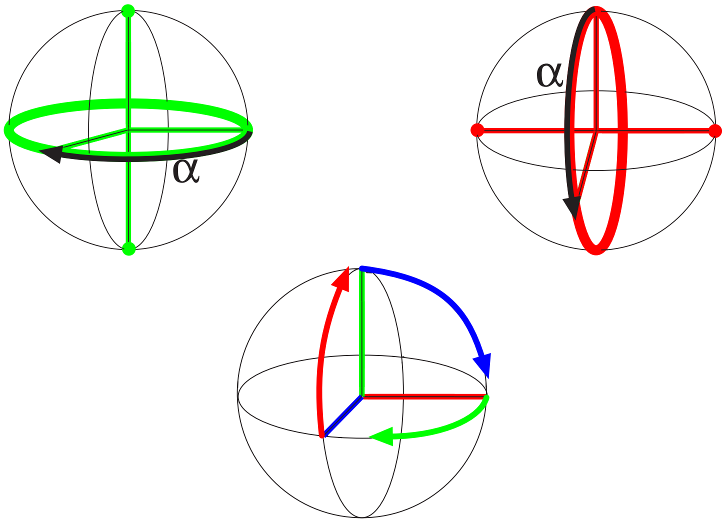


In [17] Coecke and Lang provide a translation from **RG** to **RGB** by defining a functor $\mathcal{T}$: **RG** $\to$ **RGB** on generators of **RG**. $\mathcal{T}$ maps green generators to green generators and acts on red generators as follows:



The fact that $\mathcal{T}$ is a functor allows us to conclude that all protocols expressible in **RG** are also expressible in **RGB**. It is used as a starting point for results obtained in Chaper 4, since it guarantees that any quantum protocol expressible in Red-green calculus is expressible in Red-green-blue calculus.

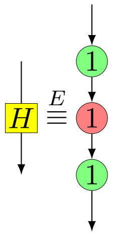
The action on red generators can be justified by Bloch Sphere representations of observables that are taken as primitives for both calculi.



From these pictures we can conclude that this is due to the different position of the red deleting point on the Bloch Sphere.

Two alternate routes of extending **RG** have been considered. The first is to add the observable Y to Z/X-calculus. It is true that we showed in Chapter 1 that observables X, Z and Y for a qubit are complementary. It is however the case that the compact structures of pairs of observables Z, Y and X, Y are not complementary. This together with the fact that Z, X observables share a compact structure would lead to an asymmetry.[8]

The second is to add an important equation, which is true in Qubit Stabilizer Theory but not provable in **RG**[20], the so called Euler decomposition of the Hadamard gate:



(2.23)

Definition 2.3. A category $\mathbf{RG}^+$ is a dagger symmetric monoidal category obtained by quotienting the category **RG** by the Euler Decomposition relation on morphisms of **RG**.

Coecke and Lang in [17] define a functor $\mathcal{S}$: **RGB**→ $\mathbf{RG}^+$ and lift the functor $\mathcal{T}$ that we defined earlier to $\mathcal{S}$: $\mathbf{RG}^+$ →**RGB**. They proved that $\mathcal{T}$ and $\mathcal{S}$ are inverse functors, hence showing that **RGB** and $\mathbf{RG}^+$ are isomorphic categories.

Chapter 3

Graphical Calculi and Quantum Theories

In this chapter we present two different quantum theories, Qubit Stabilizer Theory (QST) and Spekkens Toy Theory (STT) and apply the categorical approach and graphical calculi to analyse the differences between them. For QST, both categorical description as well as interpretation of **RG** and **RGB** in the theory follow the presentation in [17]. For STT, categorical description is given as in [5]. Examples and the rest of the chapter are the author's original contribution.

3.1 Qubit Stabilizer Theory

Qubit Stabilizer Theory is an important subset of Quantum Theory. We investigate it because it exhibits many standard quantum features despite its limited nature. Among others, it has non-locality, incompatible observables and allows us to prove the no-cloning theorem. The practical aspect also has its significance. QST is much more likely to be physically realised than full Quantum Theory.

Stabilizer Qubit Theory is a restriction of the standard Quantum Theory in which only a limited set of systems, states and operators is allowed. In this theory:

- Only measurements in X- Z- and Y-eigenbases are allowed
- Quantum systems consist of qubits that, when subject to measurement, admit eigenstates of Pauli operators.
- States are eigenstates of n-fold tensor products of Pauli operators
- One qubit operators preserve stabilizer states, they coincide with so-called Clifford unitaries

Clifford unitaries include the Hadamard gate, CNOT gate and Pauli operators. All n-qubit Clifford unitaries can be simulated using just these gates. States that can be realised in this theory include: $|0\rangle, |1\rangle, |+\rangle, |-\rangle, |i\rangle, |-i\rangle$ for a single qubit, their tensor products and the Bell state for a pair of qubits. By this we can see that quantum protocols, like the Quantum Teleportation protocol are obtainable in QST, which is another reason why we investigate it.

To establish interpretation of both calculi in Qubit Stabilizer Theory, we first have to provide a categorical axiomatisation of this theory.

Definition 3.1. The category **Stab** is the subcategory of $\mathbf{FdHilb}_Q$ (category of qubits, as defined in [17]) generated by the following linear maps:

- single-qubit Clifford unitaries: $Q \to Q$
- $\delta_{Stab} : Q \to Q \otimes Q \begin{cases} |0\rangle & \mapsto |00\rangle \\ |1\rangle & \mapsto |11\rangle \end{cases}$
- $\epsilon_{Stab} : Q \to 1 \begin{cases} |+\rangle & \mapsto 1 \\ |-\rangle & \mapsto 0 \end{cases}$

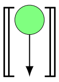
We want to demonstrate that **Stab** is a correct categorical representation of QST. Clearly all morphisms obtained by composing generators of **Stab** correspond to elements of QST. For completeness, we need to show that all elements of QST are obtainable in **Stab**.

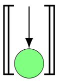
Six stabilizer states are obtained by taking the transpose of the deleting morphism: $\epsilon^\dagger$ and acting on it with single-qubit Clifford unitaries, tensor products of these six states are all states allowed in QST. All single-qubit Clifford unitaries are already expressible in **Stab**, being its generators. What remains is to show that the Controlled-Not gate is realised by:

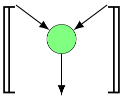
$$CNOT = (I_Q \otimes H) \circ (I_Q \otimes \delta^\dagger_{Stab}) \circ (I_Q \otimes H \otimes I_Q) \circ (\delta_{Stab} \otimes I_Q) \circ (I_Q \otimes H)$$

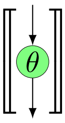
Where, I_Q is the identity morphism on the object Q, and H is the Hadamard gate. Both are Clifford unitaries, so CNOT is expressible in **Stab**. All multiple qubit operators that are allowed in QST can now be generated in **Stab** from single qubit Clifford unitaries and CNOT. Therefore, **Stab** does indeed capture all the operations definable in Qubit Stabilizer Theory.

Now, using the approach taken by [17] we define two functors $\llbracket\cdot\rrbracket_{\mathbf{RG}}$:**RG** → **Stab** and $\llbracket\cdot\rrbracket_{\mathbf{RGB}}$:**RGB**→**Stab** that have the following effect on the generators:

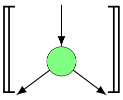

$_{\mathbf{RG}} = |+\rangle$

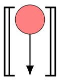

$_{\mathbf{RG}} = \langle +|$

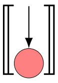

$_{\mathbf{RG}} = |0\rangle\langle 00| + |1\rangle\langle 11|$

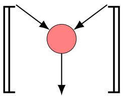


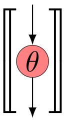
$_{\mathbf{RG}} = |0\rangle\langle 0| + e^{i\frac{\pi}{2}\theta}|1\rangle\langle 1|$


$_{\mathbf{RG}} = |00\rangle\langle 0| + |11\rangle\langle 1|$

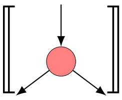

$_{\mathbf{RG}} = |0\rangle$

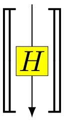

$_{\mathbf{RG}} = \langle 0|$


$_{\mathbf{RG}} = |+\rangle\langle ++| + |-\rangle\langle --|$

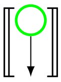


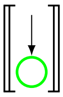
$_{\mathbf{RG}} = |+\rangle\langle +| + e^{i\frac{\pi}{2}\theta}|-\rangle\langle -|$

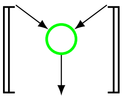

$_{\mathbf{RG}} = |++\rangle\langle +| + |--\rangle\langle -|$

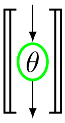


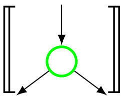
$_{\mathbf{RG}} = |+\rangle\langle 0| + |-\rangle\langle 1|$

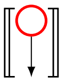

$_{\mathbf{RGB}} = |+\rangle$

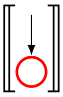

$_{\mathbf{RGB}} = \langle +|$

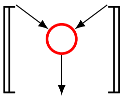

$_{\mathbf{RGB}} = |0\rangle \langle 00| + |1\rangle \langle 11|$

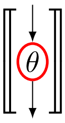

$_{\mathbf{RGB}} = |0\rangle \langle 0| + e^{i\theta\frac{\pi}{2}} |1\rangle \langle 1|$

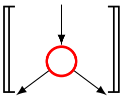

$_{\mathbf{RGB}} = |00\rangle \langle 0| + |11\rangle \langle 1|$

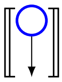

$_{\mathbf{RGB}} = |i\rangle$

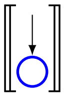

$_{\mathbf{RGB}} = \langle i|$

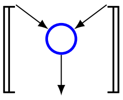

$_{\mathbf{RGB}} = |+\rangle \langle ++| + i\, |-\rangle \langle --|$

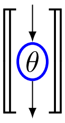

$_{\mathbf{RGB}} = |+\rangle \langle +| + e^{i\theta\frac{\pi}{2}} |-\rangle \langle -|$

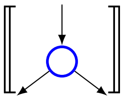

$_{\mathbf{RGB}} = |++\rangle \langle +| - i\, |--\rangle \langle -|$


$_{\mathbf{RGB}} = |0\rangle$


$_{\mathbf{RGB}} = \langle 0|$


$_{\mathbf{RGB}} = |i\rangle \langle ii| + |-i\rangle \langle -i - i|$


$_{\mathbf{RGB}} = |i\rangle \langle i| + e^{i\theta\frac{\pi}{2}} |-i\rangle \langle -i|$


$_{\mathbf{RGB}} = |ii\rangle \langle i| + |-i - i\rangle \langle -i|$

Both are symmetric monoidal †-functors. A diagram made of these two functors and previously defined $\mathcal{T}$ commutes.[17] This shows that all quantum computation expressible in either **RG** or **RGB** is expressible using Qubit Stabilizer Theory.

3.2 Spekkens Toy Theory

There are two main ways of explaining the physical meaning of quantum states. In the ontic approach, quantum states are states of physical reality. In the epistemic approach they represent our incomplete knowledge about the system. Spekkens Toy theory takes the epistemic view of quantum mechanics and uses the so called 'knowledge balance principle' to be able to express some quantum features.

The most simple system in this theory is described by a state space with just four states denoted $\mathrm{IV} = \{1, 2, 3, 4\}$. More complex systems are produced by composing state spaces of multiple primitive systems by taking Cartesian products IV^n. We call the system's real physical state – the ontic state, our state of knowledge about the system is called the epistemic state. An epistemic state is always a subset of the state space of the system. The knowledge balance principle puts a restriction on which epistemic states can be admitted by the system. It is stated in full generality and explained in [22].

It can be thought of as a rule enforcing that the amount of knowlege about the system we have is equal to the amount we do not have. For the elementary system $\{1, 2, 3, 4\}$ only six epistemic states of maximal knowledge are allowed. These are: $1 \vee 2$, $3 \vee 4$, $1 \vee 3$, $2 \vee 4$, $1 \vee 4$, $2 \vee 3$

It is not a coincidence that the number of epistemic states is equal to the number of Pauli eigenstates in Qubit Stabilizer Theory. There is the following correspondence:

$$\begin{array}{ll} 1 \vee 2 \Leftrightarrow |0\rangle & 3 \vee 4 \Leftrightarrow |1\rangle \\ 1 \vee 3 \Leftrightarrow |+\rangle & 2 \vee 4 \Leftrightarrow |-\rangle \\ 1 \vee 4 \Leftrightarrow |i\rangle & 2 \vee 3 \Leftrightarrow |-i\rangle \end{array}$$

Notice that each pair of epistemic states that shares no ontic states is mapped to a pair of orthogonal stabilizer states.

Transformations are limited to those that preserve the knowledge balance principle. These turn out to be the permutations of the four ontic states. Measurements are limited to those that distinguish between the epistemic states of the system.

Let us consider the example of performing a measurement of the primitive system with state space IV. We could for instance ask whether the system is in the epistemic state $1 \vee 3$. The result of this measurement will be either 'yes' (if the physical state of the system is either 1 or 3) or 'no' otherwise.

There is however one subtlety, it occurs if we want to distinguish between two epistemic states, for example $1 \vee 3$ and $2 \vee 4$, and the system is in $2 \vee 3$. In such a case, if we were to obtain an answer, we would be able to uniquely determine the physical state of the system, thus contradicting the knowledge balance principle. Answer '$1 \vee 3$' indicates ontic state 3 and '$2 \vee 4$' indicates ontic state 2. This is not permitted. To prevent this from happening, we assume that the physical state is subject to a probabilistic disturbance. It either undergoes a transition or stays the same and both events happen with equal probability. In this example, if we obtain $1 \vee 3$ as a result of the measurement, then the physical state either remains 1 or randomly changes to 3, resulting in the epistemic state of the system: $1 \vee 3$.

This concept is captured in the best way by a relation on the ontic state space and leads us to a categorical interpretation **Spek** as a subcategory of the category of finite relations. **FRel** is a dagger symmetric monoidal category and so is **Spek** as its subcategory.

Definition 3.2. The category **Spek** is a subcategory of **FRel** defined inductively as follows:

- Objects are the single element set I=$\{*\}$, the four element set IV=$\{1, 2, 3, 4\}$ and its n-fold Cartesian products IV^n.
- Morphisms are relations generated by composition, Cartesian product and relational converse from the following generating relations:
  - All permutations $\{\sigma_i :$IV$\to$IV$\}$ of the four element set, there are 24 of them and they form a group isomorphic to S$_4$.
  - A relation δ_Z : IV$\to$IV$\times$IV:

$$\delta_Z = \begin{cases} 1 \sim \{(1,1),(2,2)\} \\ 2 \sim \{(1,2),(2,1)\} \\ 3 \sim \{(3,3),(4,4)\} \\ 4 \sim \{(3,4),(4,3)\} \end{cases}$$

  - A relation ϵ_Z: IV$\to$I defined by $\{1,3\} \sim *$.
  - The relevant unit, associativity and symmetry natural isomorphisms.

It is worth mentioning that there is a bijection between states and operations of both theories. Isomorphism is however not achieved, due to the way operations compose. The reason for using Z in the subscript of δ_Z and ϵ_Z will soon become clear.

We use the grid notation to denote the copying relations δ : IV$\to$IV$\otimes$IV, in a 4 by 4 grid, we say that $x \sim (y, z)$ if there is an x at the position (y, z) in the grid. In this notation δ_Z has the form:

1	2		
2	1		
		3	4
		4	3

We set $x_0 := \epsilon_Z^{\dagger}$ and apply permutations to it to obtain 6 states. Each of them is a relation of the type I$\to$IV:

$$\begin{array}{lll} z_0 := * \sim \{1,2\} & x_0 := * \sim \{1,3\} & y_0 := * \sim \{1,4\} \\ z_1 := * \sim \{3,4\} & x_1 := * \sim \{2,4\} & y_1 := * \sim \{2,3\} \end{array}$$

These turn out to be the eigenvectors (which in this context we call classical points) of three observables that are definable in **Spek**.

Let us consider how the tuple (IV, δ_Z, ϵ_Z) interacts with the states z_0, z_1.

$$\delta_Z \circ z_0 = * \sim \{(1,1),(1,2),(2,1),(2,2)\} = (* \sim \{1,2\}) \otimes (* \sim \{1,2\}) = z_0 \otimes z_0$$
$$\delta_Z \circ z_1 = * \sim \{(3,3),(3,4),(4,3),(4,4)\} = (* \sim \{3,4\}) \otimes (* \sim \{3,4\}) = z_1 \otimes z_1$$

By this computation we can see that both z_0 and z_1 are copied by δ_Z, hence, by the definition 1.8, they are the classical points of (IV, δ_Z, ϵ_Z). The subscript in δ_Z was chosen to indicate the basis that this operator copies. The remaining four points are unbiased for δ_Z and form a phase group:

Lemma 3.1. $(\{x_0, x_1, y_0, y_1\}, \odot)$ is an abelian group isomorphic to $Z_2 \times Z_2$, where $\odot$ is the abstract operation defined in chapter 1.

Proof. The fact that $(\{x_0, x_1, y_0, y_1\}, \odot)$ is an abelian group follows by Theorem 1.3. We show that the group is isomorphic to $Z_2 \times Z_2$. Since the only other 4 element abelian group is Z_4, it is sufficient to show that our group is not isomorphic to Z_4. To ensure that, we show that each element squares to the identity element, i.e. the group is not cyclic.

$$x_0 \odot x_0 = \delta_Z^{\dagger} \circ (x_0 \otimes x_0) = \delta_Z^{\dagger} \circ (* \sim \{(1,1),(1,3),(3,1),(3,3)\}) = (* \sim \{1,3\})$$
$$x_1 \odot 1_0 = \delta_Z^{\dagger} \circ (x_1 \otimes x_1) = \delta_Z^{\dagger} \circ (* \sim \{(2,2),(2,4),(4,2),(4,4)\}) = (* \sim \{1,3\})$$
$$y_0 \odot y_0 = \delta_Z^{\dagger} \circ (y_0 \otimes y_0) = \delta_Z^{\dagger} \circ (* \sim \{(1,1),(1,4),(4,1),(4,4)\}) = (* \sim \{1,3\})$$
$$y_1 \odot y_1 = \delta_Z^{\dagger} \circ (y_0 \otimes y_0) = \delta_Z^{\dagger} \circ (* \sim \{(2,2),(2,3),(3,2),(3,3)\}) = (* \sim \{1,3\})$$

Hence all elements square to one element, now sufficient to show that x_0 is the identity:

$$x_0 \odot y_0 = \delta_Z^{\dagger} \circ (y_0 \otimes y_0) = \delta_Z^{\dagger} \circ (* \sim \{(1,1),(3,1),(1,4),(3,4)\}) = (* \sim \{1,4\}) = y_0$$
$$y_0 \odot x_0 = \delta_Z^{\dagger} \circ (y_0 \otimes y_0) = \delta_Z^{\dagger} \circ (* \sim \{(1,1),(4,1),(1,3),(4,3)\}) = (* \sim \{1,4\}) = y_0$$

similarly for x_1 and y_1. Therefore, $(\{x_0, x_1, y_0, y_1\}, \odot)$ is isomorphic to $Z_2 \times Z_2$. □

Each element of the set $\{x_0, x_1, y_0, y_1\}$ induces a relation $(x_i \odot_Z 1_{IV})$: IV$\to$ IV. Given by: $(x_i \odot_Z 1_{IV}) = \delta_Z^{\dagger} \circ (x_1 \otimes 1_{IV})$, for example:

$$(x_1 \odot_Z 1_{IV}) = \delta_Z^{\dagger} \circ (x_1 \otimes 1_{IV}) = \delta_Z^{\dagger} \circ \begin{cases} 1 \sim \{(2,1),(4,1)\} \\ 2 \sim \{(2,2),(4,2)\} \\ 3 \sim \{(2,3),(4,3)\} \\ 4 \sim \{(2,4),(4,4)\} \end{cases} = \begin{cases} 1 \sim 2 \\ 2 \sim 1 \\ 3 \sim 4 \\ 4 \sim 3 \end{cases}$$

Other induced relations are as follows:

$$\delta_Z^{\dagger} \circ (x_0 \otimes 1_{IV}) = \begin{cases} 1 \sim 1 \\ 2 \sim 2 \\ 3 \sim 3 \\ 4 \sim 4 \end{cases} \qquad \delta_Z^{\dagger} \circ (y_0 \otimes 1_{IV}) = \begin{cases} 1 \sim 1 \\ 2 \sim 2 \\ 3 \sim 4 \\ 4 \sim 3 \end{cases} \qquad \delta_Z^{\dagger} \circ (y_1 \otimes 1_{IV}) = \begin{cases} 1 \sim 2 \\ 2 \sim 1 \\ 3 \sim 3 \\ 4 \sim 4 \end{cases}$$

By the results from chapter 1, $(\{(x_0 \odot_Z 1_{IV}), (x_1 \odot_Z 1_{IV}), (y_0 \odot_Z 1_{IV}), (y_1 \odot_Z 1_{IV})\}, \circ)$ is a group isomorphic to $(\{x_0, x_1, y_0, y_1\}, \odot)$, where $\circ$ is the usual relational composition. The significance of this result will become apparent in the later part of this chapter.

One may be tempted to define (IV, δ_Z, ϵ_Z) to be an observable in **Spek**. However composing δ_Z with different permutations results in obtaining three tuples (IV, $\delta_Z^{'}$, $x_1^{\dagger}$), (IV, $\delta_Z^{''}$, $y_0^{\dagger}$), (IV, $\delta_Z^{'''}$, $y_1^{\dagger}$), that have the same classical and unbiased points. Hence, we label $Z := \{(IV, \delta_Z, \epsilon_Z), (IV, \delta_Z^{'}, x_1^{\dagger}), (IV, \delta_Z^{''}, y_0^{\dagger}), (IV, \delta_Z^{'''}, y_1^{\dagger})\}$ and define it to be the first observable. Its classical points are z_0, z_1 and unbiased points are x_0, x_1, y_0, y_1.

By applying further permutations we obtain two more observables: X and Y which are generated by δ_X and δ_Y which are represented by the two grid diagrams:

$$\delta_X : \begin{array}{|c|c|c|c|} \hline 1 & & 3 & \\ \hline & 2 & & 4 \\ \hline 3 & & 1 & \\ \hline & 4 & & 2 \\ \hline \end{array} \qquad \delta_Y : \begin{array}{|c|c|c|c|} \hline 1 & & & 4 \\ \hline & 3 & 2 & \\ \hline & 2 & 3 & \\ \hline 4 & & & 1 \\ \hline \end{array}$$

Labels chosen for the 6 states enumerated above, indicate which of them are classical and unbiased points of observables X and Y.

Since each observable consists of 4 tuples, we augment the notion of complementarity.

Definition 3.3. [5] Two observables O_1, O_2 in **Spek** are complementary if there exists a pair of tuples (IV, δ_1, ϵ_1)$\in O_1$ and (IV, δ_2, ϵ_2)$\in O_2$, complementary in the usual sense.

Lemma 3.2. *Each pair of the set of observables $\{Z, X, Y\}$ in* **Spek** *is complementary.*

Again, like for **Stab** we want to argue that **Spek** is a categorical Model of Spekkens' Toy Theory. There is a straightforward bijective correspondence between six epistemic states of the primitive system IV and six classical points in **Spek**. Now, following the presentation due to [5], any two-system state is obtainable by applying permutations of IV to one of these states. Both are expressible in **Spek** :

$$\delta_Z \circ \epsilon_Z : \mathrm{I} \to \mathrm{IV} \times \mathrm{IV} :: * \sim \{(1,1),(2,2),(3,3),(4,4)\}$$
$$\delta_Z \circ z_0 = z_0 \otimes z_0 : \mathrm{I} \to \mathrm{IV} \times \mathrm{IV} :: * \sim \{(1,1),(1,2),(2,1),(2,2)\}$$

The composition $\delta_Z \circ \epsilon_Z$ is sometimes referred to as a 'Bell state' – a counterpart of maximally entangled state of two qubits.

For three systems, all states can be generated using permutations from the GHZ state, expressed in **Spek** as $(\delta_Z \otimes I_{IV}) \circ (\delta_Z \circ \epsilon_Z)$, where the second component is a Bell state.

Probabilistic perturbations discussed earlier in this chapter, that are caused by measurement, are expressed by permutations composed with relations of the form:

$$(x_0 \circ z_0^\dagger) \text{ :IV}\to\text{IV:: } \{1,2\} \sim \{1,3\}$$

Hence, all the components of Spekkens' Toy Theory are expressible in **Spek**, which is its categorical counterpart. Now we may proceed to apply graphical calculi to analyse **Spek**.

As showed earlier for observable Z, each observable is associated with a phase group. In **Spek** each phase group is isomorphic to $Z_2 \times Z_2$. We state thee complementary obervables in **Spek** explicitly:

$$G_Z = (\{(x_0 \odot_Z 1_{IV}), (x_1 \odot_Z 1_{IV}), (y_0 \odot_Z 1_{IV}), (y_1 \odot_Z 1_{IV})\}, \circ) =$$

$$= (\{1_{IV}, \begin{cases} 1 \sim 2 \\ 2 \sim 1 \end{cases}, \begin{cases} 3 \sim 4 \\ 4 \sim 3 \end{cases}, \begin{cases} 1 \sim 2 \\ 2 \sim 1 \\ 3 \sim 4 \\ 4 \sim 3 \end{cases} \}, \circ)$$

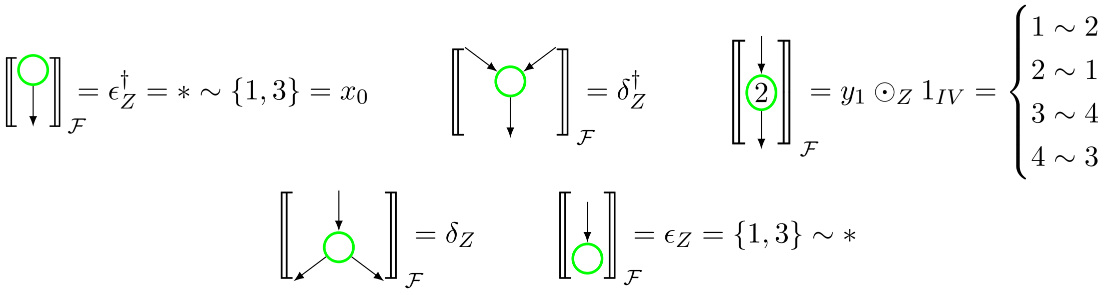
$$G_Y = (\{(x_0 \odot_Y 1_{IV}), (x_1 \odot_Y 1_{IV}), (z_0 \odot_Y 1_{IV}), (z_1 \odot_Y 1_{IV})\}, \circ)$$

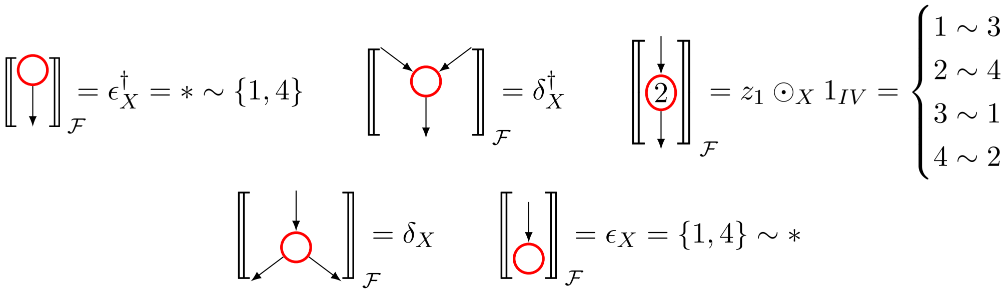
$$= (\{1_{IV}, \begin{cases} 1 \sim 4 \\ 4 \sim 1 \end{cases}, \begin{cases} 2 \sim 3 \\ 3 \sim 2 \end{cases}, \begin{cases} 1 \sim 4 \\ 2 \sim 3 \\ 3 \sim 2 \\ 4 \sim 1 \end{cases} \}, \circ)$$

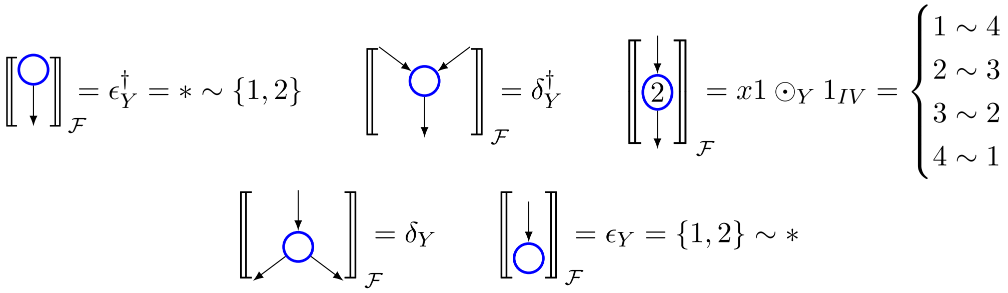
$$G_X = (\{(z_0 \odot_X 1_{IV}), (z_1 \odot_X 1_{IV}), (y_0 \odot_X 1_{IV}), (y_1 \odot_X 1_{IV})\}, \circ)$$

$$= (\{1_{IV}, \begin{cases} 1 \sim 3 \\ 3 \sim 1 \end{cases}, \begin{cases} 2 \sim 4 \\ 4 \sim 2 \end{cases}, \begin{cases} 1 \sim 3 \\ 2 \sim 4 \\ 3 \sim 1 \\ 4 \sim 2 \end{cases} \}, \circ)$$

Now let **RGB-Even** be a subcategory of **RGB** generated by generators of **RGB** with phase angles limited to the set $\{0, 2\}$, i.e. with odd angles excluded. Then let $[\![\cdot]\!]_{\mathcal{F}}$:**RGB-Even**→**Spek** be a functor that acts on the generators as follows:


$= \epsilon_Z^\dagger = * \sim \{1,3\} = x_0$
$= \delta_Z^\dagger$
2
$= y_1 \odot_Z 1_{IV} = \begin{cases} 1 \sim 2 \\ 2 \sim 1 \\ 3 \sim 4 \\ 4 \sim 3 \end{cases}$
$= \delta_Z$
$= \epsilon_Z = \{1,3\} \sim *$
$\mathcal{F}$


$= \epsilon_X^\dagger = * \sim \{1,4\}$
$= \delta_X^\dagger$
2
$= z_1 \odot_X 1_{IV} = \begin{cases} 1 \sim 3 \\ 2 \sim 4 \\ 3 \sim 1 \\ 4 \sim 2 \end{cases}$
$= \delta_X$
$= \epsilon_X = \{1,4\} \sim *$
$\mathcal{F}$


$= \epsilon_Y^\dagger = * \sim \{1,2\}$
$= \delta_Y^\dagger$
2
$= x1 \odot_Y 1_{IV} = \begin{cases} 1 \sim 4 \\ 2 \sim 3 \\ 3 \sim 2 \\ 4 \sim 1 \end{cases}$
$= \delta_Y$
$= \epsilon_Y = \{1,2\} \sim *$
$\mathcal{F}$

Theorem 3.3. $\mathcal{F}$ is a symmetric monoidal †-functor.

Proof. We check that $[\![f]\!]_\mathcal{F}$=$[\![g]\!]_\mathcal{F}$ holds for each rule $f = g$ in **RGB**. Also, for all generators g, we check that $[\![\cdot]\!]_\mathcal{F}$ preserved the †-structure: $[\![g]\!]_\mathcal{F}{}^\dagger$=$[\![g^\dagger]\!]_\mathcal{F}$ and that $[\![\cdot]\!]_\mathcal{F}$ respects the symmetric monoidal structure on generators. □

The idea to interpret even phases as these relations originated from the fact that both $(\{1_{IV}, \begin{cases} 1 \sim 2 \\ 2 \sim 1 \\ 3 \sim 4 \\ 4 \sim 3 \end{cases} \begin{cases} 1 \sim 3 \\ 2 \sim 4 \\ 3 \sim 1 \\ 4 \sim 2 \end{cases}, \begin{cases} 1 \sim 4 \\ 2 \sim 3 \\ 3 \sim 2 \\ 4 \sim 1 \end{cases} \}, \circ)$ and the group of dualizers (three even phases and the identity) are groups isomorphic to $Z_2 \times Z_2$.

The only elements of **RGB** that we are unable to interpret in **Spek** are odd phases. This comes as no surprise, as an opposite result would imply that we could recreate in **Spek** all quantum mechanical behaviours that it is known not to support (for example phase gates).

As clearly visible from the presentation of phase groups for different observables, each of these relations decomposes into two smaller factors. The question remains whether there is any piece of structure in **RGB**, that we could associate with these factors. Since even phases in **RGB** decompose to two odd phases of the same colour that cannot be translated into **Spek**, we conjecture that there is no such structure in **RGB**.

The consequence the fact that we are able to interpret generators of **RGB-Even** is that all quantum computational operations expressible using these generators are expressible in Spekkens Toy Theory. In particular this applies to some of the protocols considered in the next chapter.

Chapter 4

Quantum Protocols

In this chapter we consider the application of graphical calculi to expressing and proving correctness of quantum protocols. The concept was briefly explored in a paper by Coecke and Duncan[4], but the most extensive and thorough analysis of the topic appeared in Anne Hillebrand's MFoCS dissertation[11]. She formally defines notions used in description of quantum protocols within Red-green calculus and presents a variety of protocols in this way. Here, we use her ideas to interpret and prove correctness of several protocols in Red-green-blue calculus. Further, we proceed to compare the complexity of Red-green and Red-green-blue interpretations. Throughout the chapter we will refer to different parties involved in quantum protocols as Alice, Bob and Charlie and to the evesdropper as Eve, these names are a long standing convention in cryptography.

4.1 Quantum Protocols in Graphical Calculi

One of the most serious physical difficulties encountered in the process of building a quantum computer is the phenomenon of decoherence of the quantum state. Once qubits come in contact with the surrounding environment an inadvertent measurement is conducted and the quantum state collapses. Unfortunately, it is extremely difficult to keep qubits separated from the outside environment. This effectively limits the size of today's quantum computers to at most a couple of qubits. In the current state of technology, it is unlikely that quantum computers consisting of many more will be physically realisable in the near future. Many quantum algorithms require at least a few thousand qubits to be able to solve problems of size sufficient for the quantum speed-up advantage to manifest. So, it is reasonable to turn our attention to applications that are perhaps less spectacular, but nonetheless offer improvement over classical methods.

Quantum protocols, especially security protocols offer exactly this. Their most important feature is that due to quantum mechanical effects, they provide protection from malicious evesdroppers. This is achieved because of the influence that measurement has on the quantum state. If Eve attempts to tamper with the message, she unintentionally performs a measurement and her interference can be detected by Alice and Bob. We mentioned earlier that inadvertent measurements constitute a great obstacle on the path to constructing a quantum computer. Here their effect is beneficial and they allow us to devise completely secure quantum protocols.

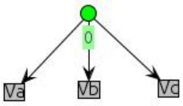
Before we proceed to presentation of specific protocols, we need to establish several preliminary facts. In this chapter we will be using the following definitions[11]:

Definition 4.1. A quantum protocol consists of two parts, the set of instructions and the desired behaviour. The set of instructions is an ordered list of operations to perform in order to achieve the desired behaviour, otherwise referred to as the goal of the protocol.

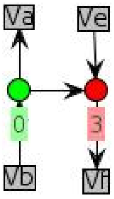
Definition 4.2. A quantum protocol is considered to be correct or valid if the set of instructions implies the desired behaviour.

Since Red-green-blue calculus is the language in which we will express the protocols, we first need to show a couple of technical results, whose relevance will become clear in the later part of this chapter. Grey boundary boxes denote inputs and outputs and are used to capture incoming and outcoming wires.

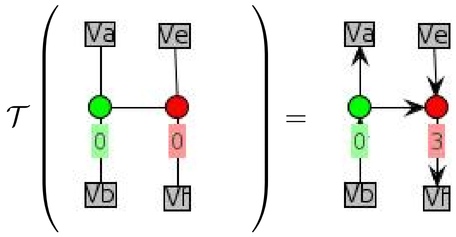
Lemma 4.1. The GHZ state, represented in the Dirac's notation by $|GHZ\rangle = \frac{|000\rangle+|111\rangle}{\sqrt{2}}$ and defined in chapter 1 is represented in RGB-calculus by:



Lemma 4.2. The Controlled-Not gate is graphically represented in RGB-calculus by:

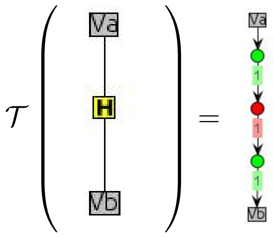


Proof. Using the results from Chapter 2 and the functor $\mathcal{T}$: **RG**$\rightarrow$**RGB**:



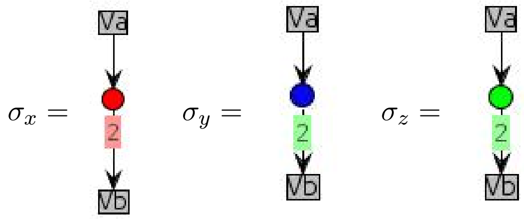
□

Lemma 4.3. The Hadamard gate is represented in RGB-calculus by:



Proof. It has been showed in Chapter 2 that categories **RG**$^+$ and **RGB** are isomorphic, hence we could apply the functor $\mathcal{T}$: **RG**$\rightarrow$**RGB** to the Euler's decomposition of the Hadamard gate, to obtain the required result. □

Lemma 4.4. Let $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ denote three Pauli matrices, they are represented in RGB-calculus by phase angles 2:



Proof. This follows by interpretation of these digraphs in **Stab**. □

As stated before, when considering *RGB*-calculus representations of quantum operations, we omit constants. This leads to another result that will be used while proving correctness of quantum protocols.

Lemma 4.5. The set $\{I, \sigma_x, \sigma_z, \sigma_y\}$ forms a group under composition in **RGB** isomorphic to $Z_2 \times Z_2$. In particular, the product of all three non-identity elements is equal to the identity. Hence any Pauli gate may be replaced by a combination of two others.

Note, that three Pauli operators in *RGB*-calculus are exactly the three dualizers (as defined in 2.16-2.18), used to flip the direction of arrows. We will use this fact in section 4.3.

4.2 Quantum Secret Key Sharing with GHZ

The first protocol we discuss is a basic case of secure communication. Alice wants to send a message to Bob and Charlie, but she wants them to be able to read the message only if they cooperate. If one of them attempts to recover the message on their own, they should be unsuccessful. Such a situation could occur, for instance, if Alice had a set of instructions to be performed and she knew that exactly one of Bob and Charlie is not trustworthy and will not fulfill the tasks if working on their own. Then the requirement above guarantees that her instructions will be followed.

An easy classical solution is to encode the message in binary and then split it into two parts A and B, such that when a bitwise or operation is performed on A and B, the original message is retrieved. This idea however, does not deal with the problem of presence of potential evesdroppers. As mentioned at the beginning of this chapter, quantum cryptography provides a solution, as interference of Eve can always be detected. The obvious approach would be to send classically obtained messages A and B using quantum cryptography and then, as previously, combine them using bitwise or operation. However, a more elegant solution using multipartite entanglement as a resource was devised and first presented in [12]. This is the protocol that we will consider.

Let Alice, Bob and Charlie share a GHZ state, so that each of them holds one qubit. The instructions for Secret Key Sharing are as follows:

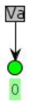
- Alice, Bob and Charlie each decide whether to measure their qubit in the x- or y-direction and they inform others about their choice.

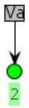
- If the combination of their choices is valid, cooperation between Bob and Charlie is possible to recover Alice's result of measurement, this result is then used as a joint key between Alice and both parties.

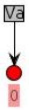
The table below summarises Charlie's qubit state depending on Alice's and Bob's state. If Charlie decides to measure the qubit along axis that corresponds to this state, a valid combination of measurement directions is obtained and Charlie together with Bob may deduce Alice's result. If he chooses a wrong axis, then no informaiton about Alice's state can be recovered. Thus, exactly half of all the combinations are valid.

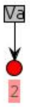
	$\langle +\vert$	$\langle -\vert$	$\langle i\vert$	$\langle -i\vert$
$\langle +\vert$	$\langle +\vert$	$\langle -\vert$	$\langle -i\vert$	$\langle i\vert$
$\langle -\vert$	$\langle -\vert$	$\langle +\vert$	$\langle i\vert$	$\langle -i\vert$
$\langle i\vert$	$\langle -i\vert$	$\langle i\vert$	$\langle -\vert$	$\langle +\vert$
$\langle -i\vert$	$\langle i\vert$	$\langle -i\vert$	$\langle +\vert$	$\langle -\vert$

Note, that results of measurements in the x- and y- direction are represented graphically as:

$\langle +| =$ 

$\langle -| =$ 

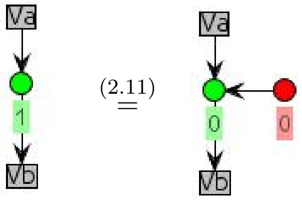
$\langle i| =$ 

$\langle -i| =$ 

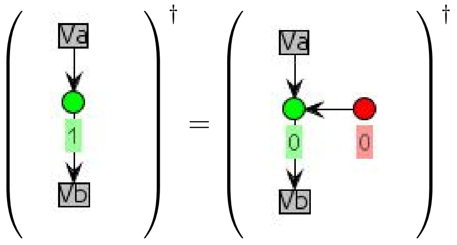
With the representation of GHZ justified in Lemma 4.1. correctness of the protocol will be proven if we manage to replicate the results from the table above in RGB calculus.

Theorem 4.6. Quantum secret key sharing with GHZ is a valid protocol.

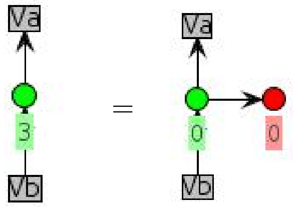
Proof. We need to consider cases, let A denote Alice's measurement result and B Bob's. First let's derive an auxilliary result using †-properties of **RGB**:



implies that:

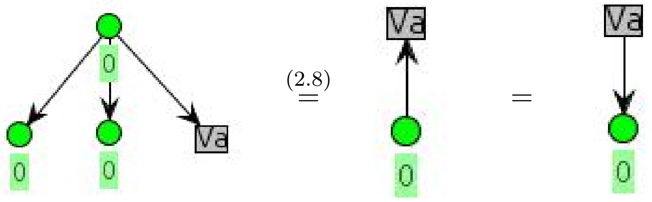


hence:



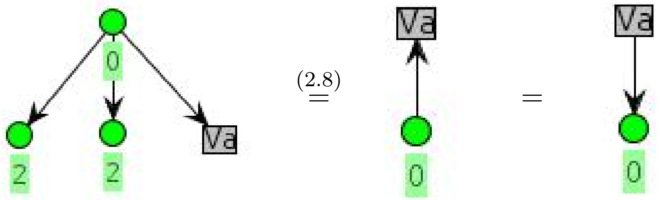
(∗)

- A=B=⟨+|



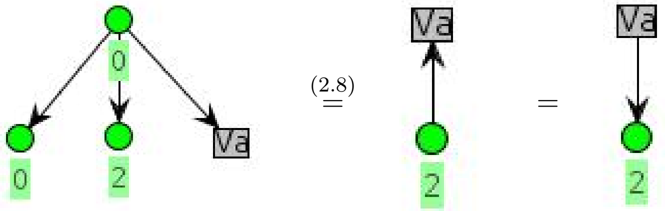
$= \langle + |$

- A=B=⟨−|



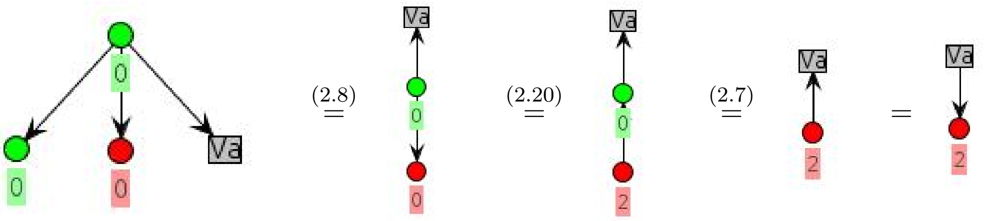
$= \langle + |$

- A=⟨+|, B=⟨−|, symmetrically for A=⟨−|, B=⟨+|



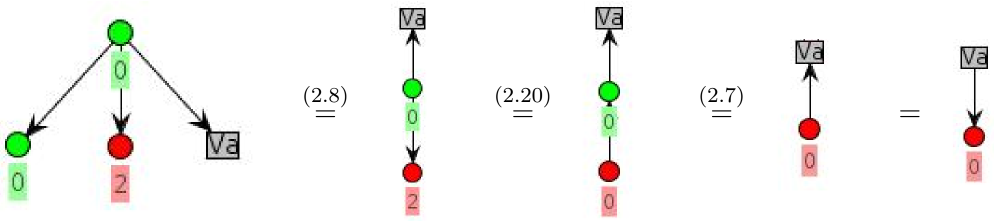
$= \langle - |$

- A=⟨+|, B=⟨i|, symmetrically for A=⟨i|, B=⟨+|



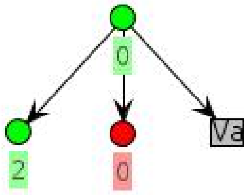
$= \langle -i |$

- A=⟨+|, B=⟨$-i$|, symmetrically for A=⟨$-i$|, B=⟨+|

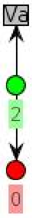


$= \langle i |$

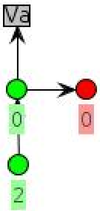
- A=⟨−|, B=⟨i|, symmetrically for A=⟨i|, B=⟨−|



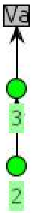
$\overset{(2.8)}{=}$



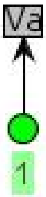
$\overset{(2.8)}{=}$



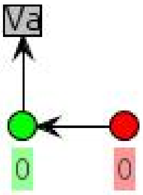
$\overset{(*)}{=}$



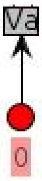
$=$ $\overset{(2.8)}{=}$



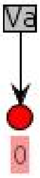
$\overset{(2.11)}{=}$



$\overset{(2.7)}{=}$

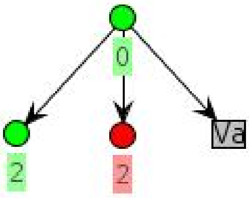


$=$

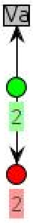


$= \langle i|$

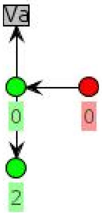
- A=⟨−|, B=⟨$-i$|, symmetrically for A=⟨$-i$|, B=⟨−|



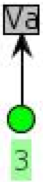
$\overset{(2.8)}{=}$



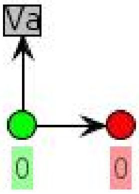
$\overset{(2.8,2.20)}{=}$



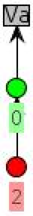
$\overset{(2.11)}{=}$



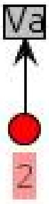
$=$ $\overset{(*)}{=}$



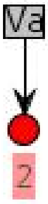
$\overset{(2.20)}{=}$



$\overset{(2.7)}{=}$

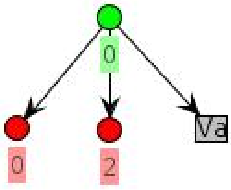


$=$

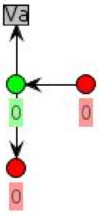


$= \langle -i|$

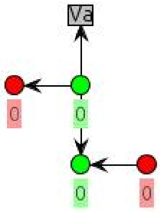
- A=⟨i|, B=⟨$-i$|, symmetrically for A=⟨$-i$|, B=⟨i|



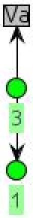
$\overset{(2.8)}{=}$



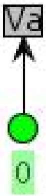
$\overset{(2.8)}{=}$



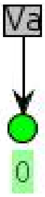
$\overset{(*)}{=}$



$=$ $\overset{(2.8)}{=}$

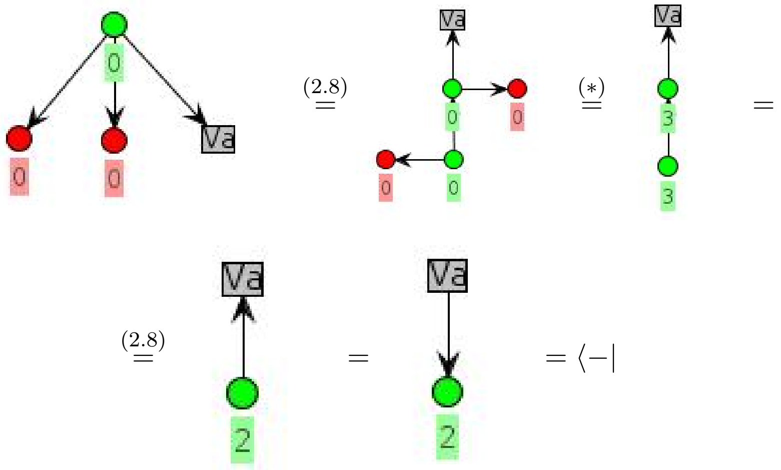


$=$

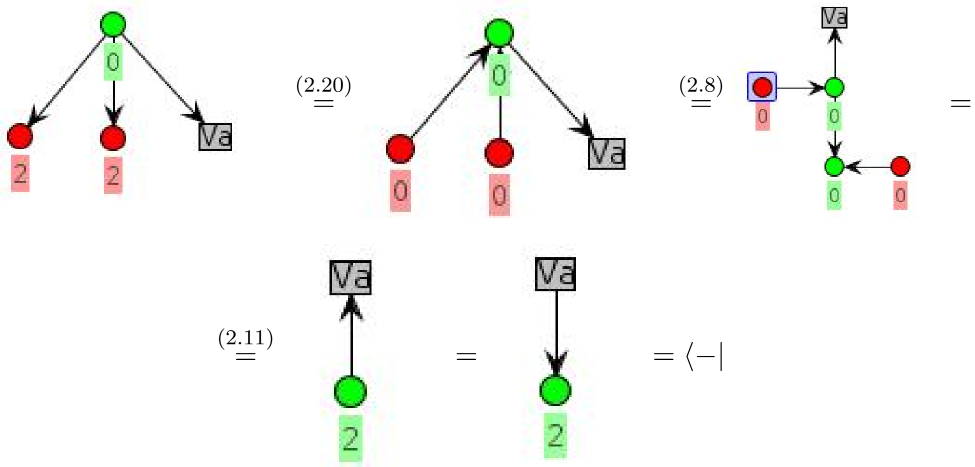


$= \langle +|$

- A=B=$\langle i|$



- A=B=$\langle -i|$



The results from the table are thus replicated, hence the set of instructions realises the goal of the protocol, so by Definition 4.1, the protocol is valid. □

As an aside, we add that the protocol can be extended to four and more parties in a straightforward manner. All that is necessary for the case with n participants is an n-GHZ multipartite state.[11]

The proof of this protocol's correctness in Red-green calculus as shown by Hillebrand is less complex than the proof above. This is due to the fact that in Z/X-calculus both $\langle i|$ and $\langle -i|$ are represented using the same colour as $\langle +|$ and $\langle -|$ and only have different phases. In that proof, in all cases the graphs collapse to the required result in one step, using the green-spider rule. This shows a very important fact: representing a protocol in RGB-calculus does not always offer better results than the Z/X-calculus representation.

4.3 Quantum Secret State Sharing with GHZ

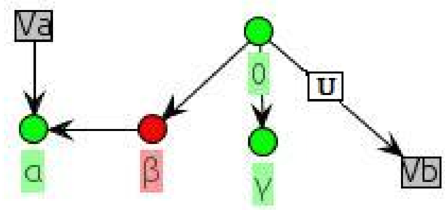
In this protocol, the problem is the same as in the previous section, but this time Alice wants to send a stream of qubits. At her disposal she has an unlimited number of GHZ triplets. Qubits of each GHZ state are divided between her, Bob and Charlie in the same way as in the Secret Key Sharing protocol. Instructions for transfering each qubit are as outlined in [12]:

- Alice measures both her qubits in the Bell basis. One qubit is a member of the GHZ triplet, the other is the one being transferred.
- Bob measures his qubit along the x-axis.
- Alice announces her result publicly, as does Bob. On that basis Charlie determines what unitaries to apply to his qubit to recover Alice's state.

The following table lists the corrections that Charlie needs to make depending on Alice's and Bob's measurement result.

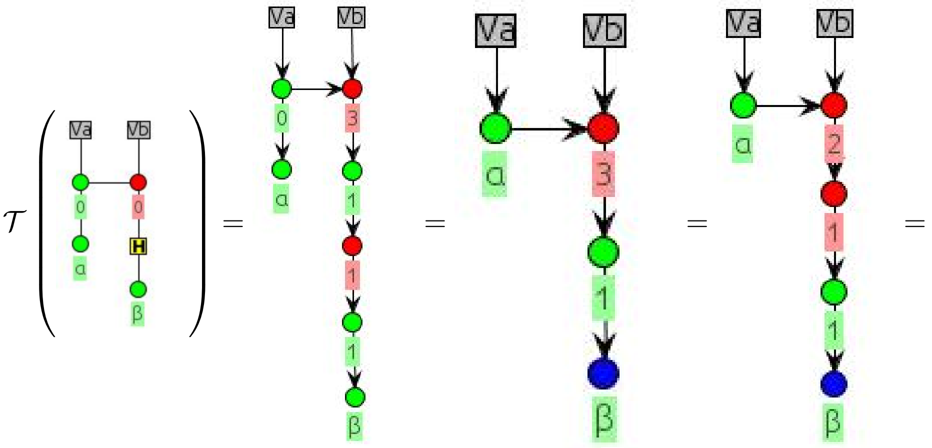
	$\langle\Phi^+\|$	$\langle\Phi^-\|$	$\langle\Psi^+\|$	$\langle\Psi^-\|$
$\langle+\|$	I	σ_z	σ_x	$\sigma_x\sigma_z$
$\langle-\|$	σ_z	I	$\sigma_x\sigma_z$	σ_x

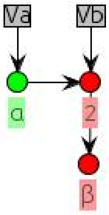
The following is a diagrammatical RGB representation of the initial setup and the set of instructions in the Quantum Secret State Sharing with GHZ protocol.

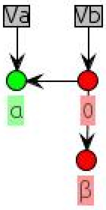


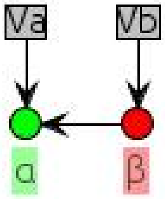
Alice's qubit and the GHZ qubit that she holds are measured in the Bell basis, the result of this measurement is denoted using α and β. Measurement in the x-basis is performed on the second qubit of the GHZ triplet, we will denote its result by γ. Finally, a unitary local operation U is performed on Charlie's qubit, which is the third qubit of the GHZ state.

The following computation justifies the representation of Bell basis measurement, using functor $\mathcal{T}$: **RG**→**RGB** defined in chapter 2:



$\overset{(2.13)}{=}$ 

$\overset{(2.16)}{=}$ 

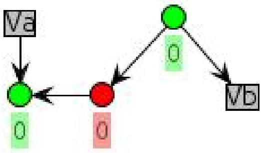
$\overset{(2.8)}{=}$ 

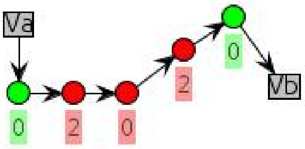
The table below contains eight different possible combinations of measurements outcomes, four for Bell basis measurement of two qubits multiplied by two for the x-basis.

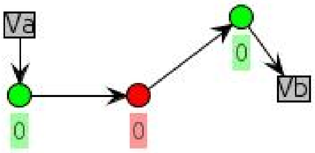
α	β	γ	Bell state	x-state	unitary
0	0	0	$\langle\Phi^+\vert$	$\langle+\vert$	I
0	0	2	$\langle\Phi^+\vert$	$\langle-\vert$	σ_z
0	2	0	$\langle\Psi^+\vert$	$\langle+\vert$	σ_x
0	2	2	$\langle\Psi^+\vert$	$\langle-\vert$	$\sigma_x\sigma_z$
2	0	0	$\langle\Phi^-\vert$	$\langle+\vert$	σ_z
2	0	2	$\langle\Phi^-\vert$	$\langle-\vert$	I
2	2	0	$\langle\Psi^-\vert$	$\langle+\vert$	$\sigma_x\sigma_z$
2	2	2	$\langle\Psi^-\vert$	$\langle-\vert$	σ_x

Lemma 4.7. Quantum Secret State sharing with GHZ is a correct protocol.

Proof. In order to prove this statement, we need to show that in all eight cases outlined above the graphical representation of the protocol's instructions simplifies to a straight wire, which signifies transfer of Alice's qubit. But first we provide a justification for arrow direction flipping using dualizers:



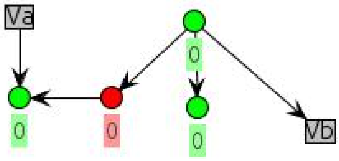
$\overset{(2.8)}{=}$ 

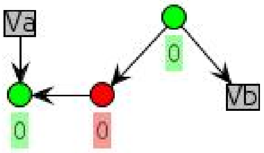
$\overset{(2.19)}{=}$ 

$(*)$

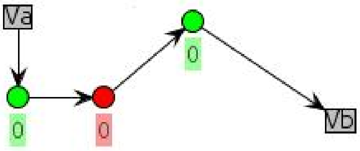
Now, we consider cases:

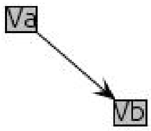
- $\alpha = \beta = \gamma = 0$



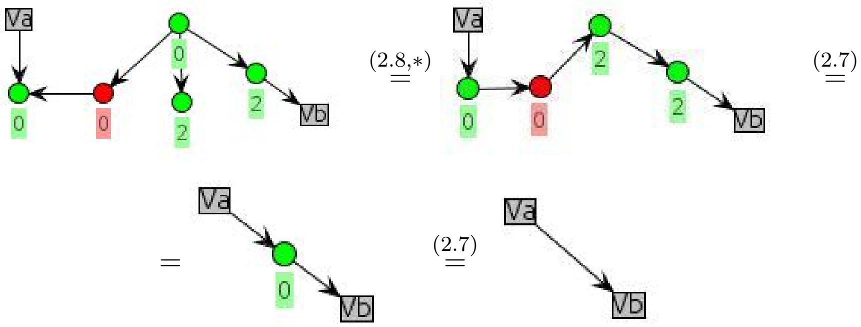
$\overset{(2.8,*)}{=}$ 

$\overset{(*)}{=}$

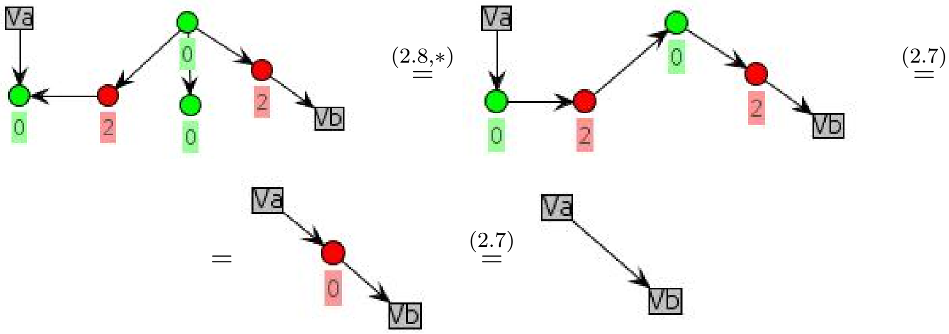
$=$ 

$\overset{(2.7)}{=}$ 

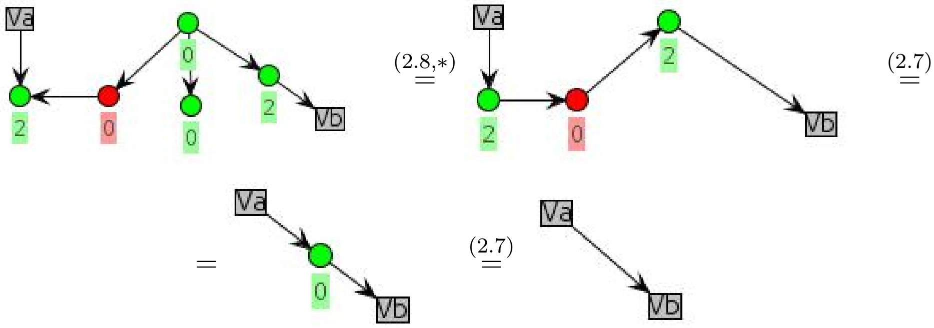
- $\alpha = \beta = 0, \gamma = 2$



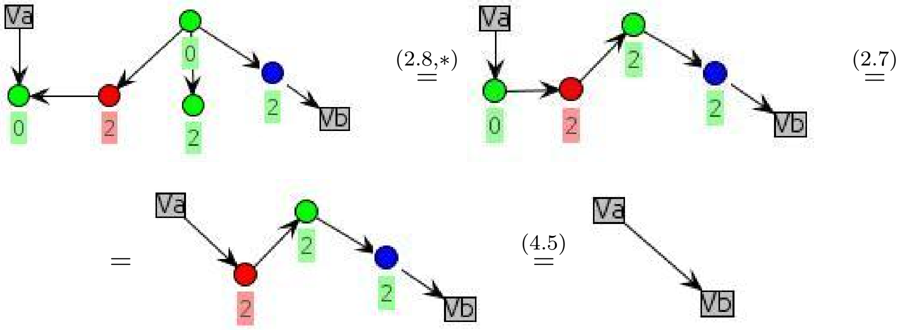
- $\alpha = 0, \beta = 2, \gamma = 0$



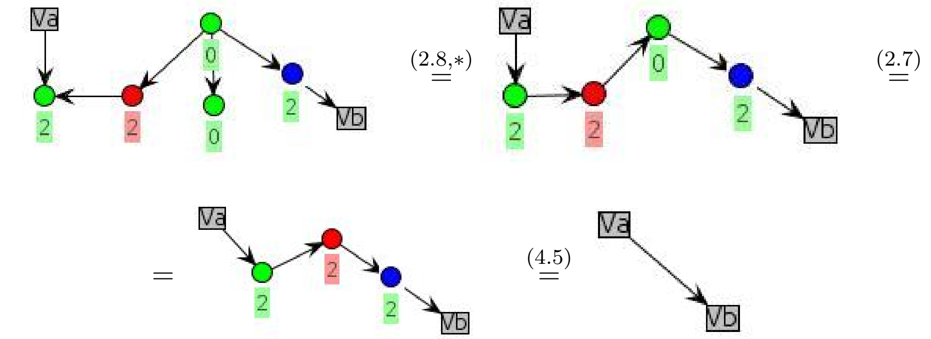
- $\alpha = 2, \beta = \gamma = 0$



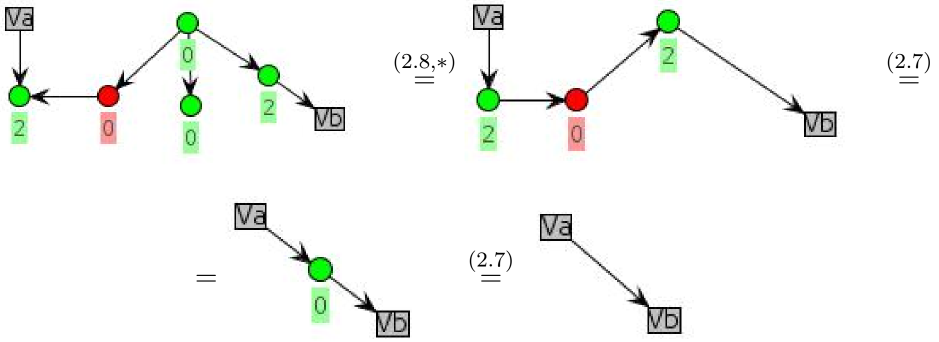
- $\alpha = 0, \beta = \gamma = 2$, before this case is considered, let us note that due to the result from Lemma 4.5, $\sigma_x \sigma_z$ may be graphically represented by the graphical representation of σ_y.



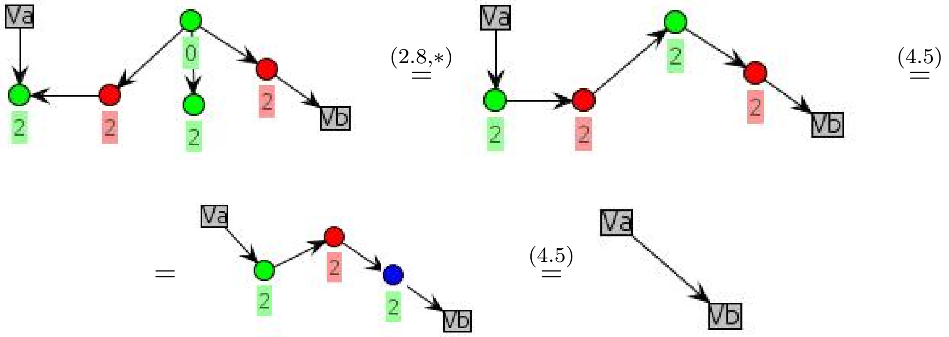
- $\alpha = \beta = 2, \gamma = 0$



- $\alpha = 2, \beta = 0, \gamma = 2$



- $\alpha = \beta = \gamma = 2$



□

An important remark is that a variant of this protocol in which Alice holds one qubit of the GHZ state and Diana holds two that are normally held by Bob and Charlie is nothing but teleportation of a quantum state through GHZ. This is analysed in detail in [11].

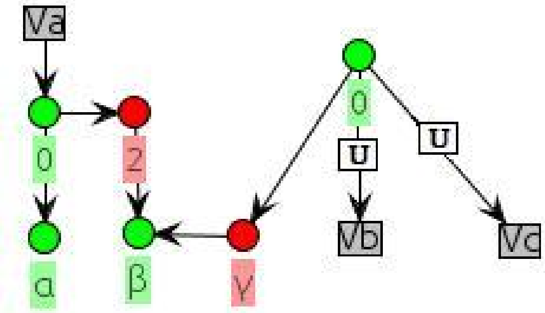
Proof of this result in Red-Green calculus, due to Hillebrand, has a comparable level of simplicity. The part of the digraph denoting Bell's measurement is rewritten more efficiently, but Charlie's unitary corrections are expressed in a less elegant way. This is due to the fact that all three observables are explicitly used in the protocol and RGB-calculus has primitive structures to support all three, whereas Z/X-calculus does not.

4.4 EPR Teleportation through GHZ

In this next protocol Alice wants to teleport an entangled state $|\psi\rangle = \alpha|01\rangle + \beta|10\rangle(\alpha^2+\beta^2 = 1)$ to Bob and Charlie. The three parties share a GHZ state and as in other protocols, each holds one qubit of the triplet. The instructions of the protocol, as they appear in [10] are as follows:

- Alice measures the first qubit of the EPR pair in the x-basis, simultaneously she measures the second qubit of the pair and her GHZ qubit in the Bell basis. She announces the results of both measurements to Bob and Charlie.
- Depending on the information provided by Alice, Bob and Charlie deduce what unitaries to apply to their individual qubits. The appropriate combinations are displayed in the table below.

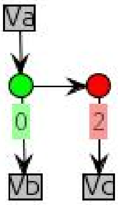
The following digraph presents the initial setup and the set of instructions in the EPR teleportation through GHZ protocol.



The first qubit of the EPR pair is measured in the x-basis, the result is denoted by α. The Bell basis measurement on two remaining Alice's qubits is denoted by β and γ. Two other members of the GHZ triplet are subject to unitary corrections U performed by Bob and Charlie. Note, that again there are 8 possible measurement outcomes, similarly as for Quantum Secret Sharing, we present them in the table, along with unitary corrections to be applied (constants are omitted for simplicity):

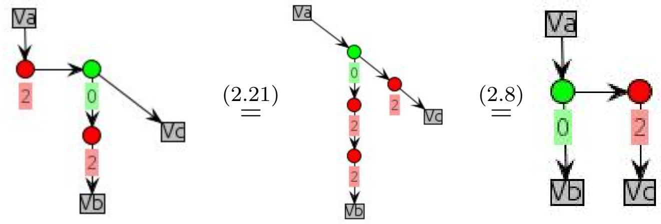
Bell basis outcome	x-basis outcome	Bob's unitary	Charlie's unitary	α	β	γ
$\langle\Phi^+|$	$\langle+|$	σ_x	I	0	0	0
$\langle\Phi^-|$	$\langle+|$	σ_y	I	0	2	0
$\langle\Phi^+|$	$\langle-|$	σ_y	I	2	0	0
$\langle\Phi^-|$	$\langle-|$	σ_x	I	2	2	0
$\langle\Psi^+|$	$\langle+|$	I	σ_x	0	0	2
$\langle\Psi^-|$	$\langle+|$	I	σ_y	0	2	2
$\langle\Psi^+|$	$\langle-|$	I	σ_y	2	0	2
$\langle\Psi^-|$	$\langle-|$	I	σ_x	2	2	2

The state $|\psi\rangle$ that Alice wants to teleport is realised graphically as:



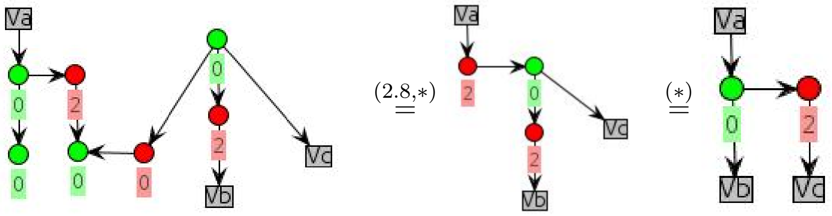
Lemma 4.8. EPR teleportation through GHZ is a valid protocol.

Proof. It is necessary to show for all 8 cases enumerated in the table above that the diagrammatic RGB representation of the protocol's initial setup and instructions can be rewritten using rules of RGB-calculus into the representation of the EPR pair that Alice wants to teleport. First let's show a result that is a consequence of the way dualizers interact with colours in **RGB**:

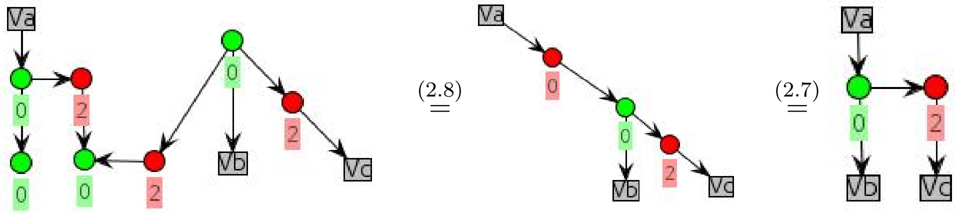


(∗)

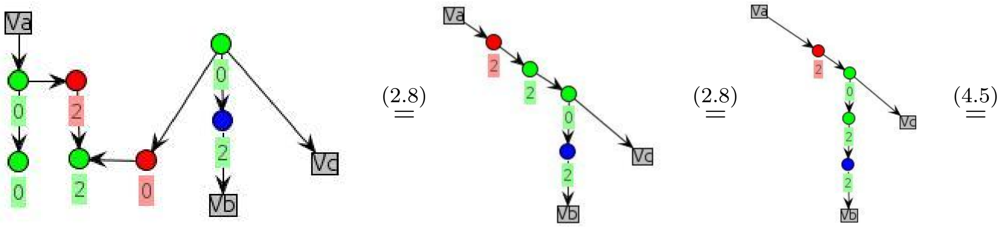
- $\alpha = \beta = \gamma = 0$

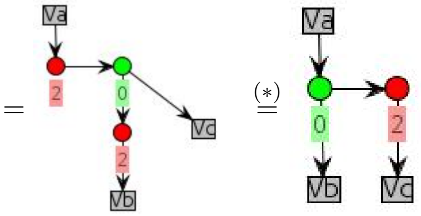


- $\alpha = \beta = 0, \gamma = 2$

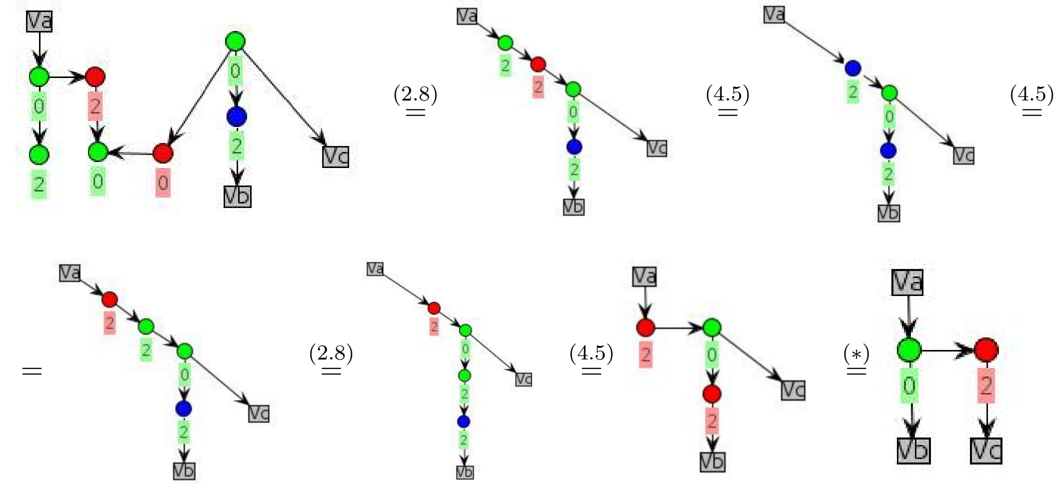


- $\alpha = 0, \beta = 2, \gamma = 0$

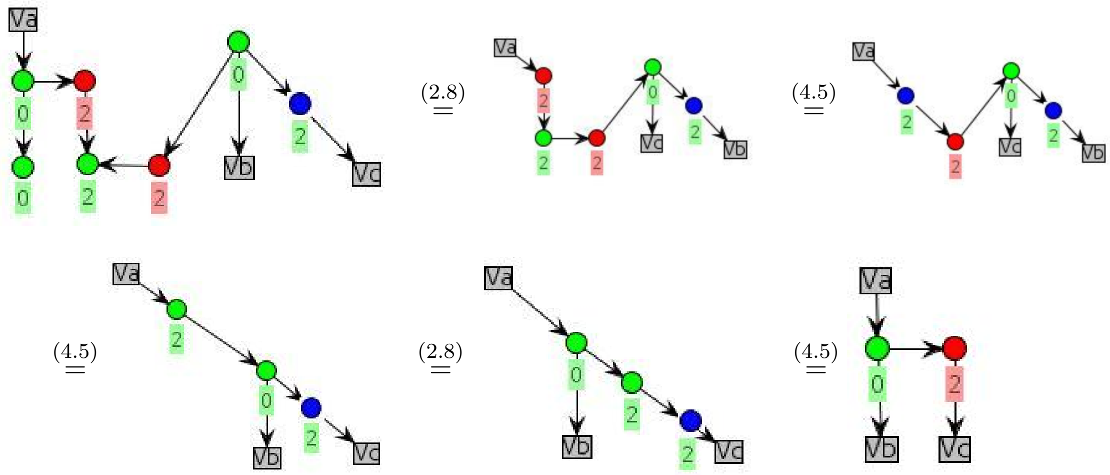




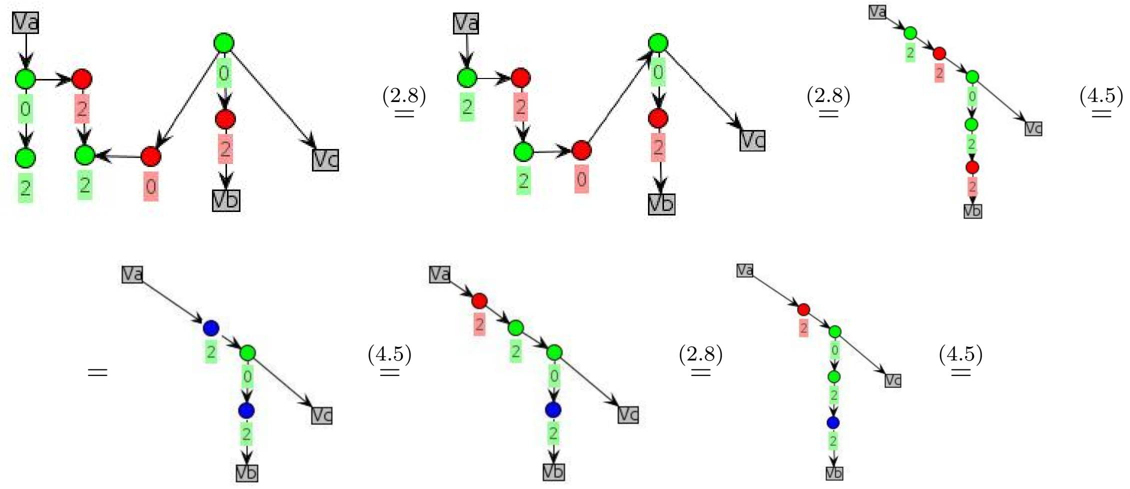
- $\alpha = 2, \beta = \gamma = 0$



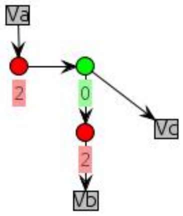
- $\alpha = 0, \beta = \gamma = 2$



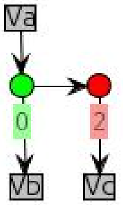
- $\alpha = \beta = 2, \gamma = 0$



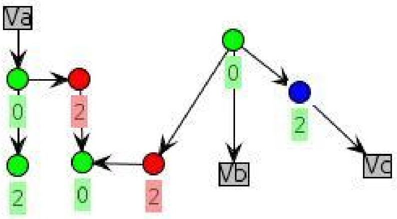
$=$



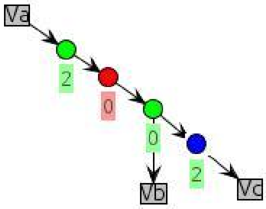
$\overset{(*)}{=}$



- $\alpha = 2, \beta = 0, \gamma = 2$

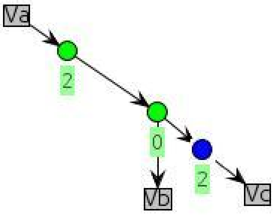


$\overset{(2.8)}{=}$

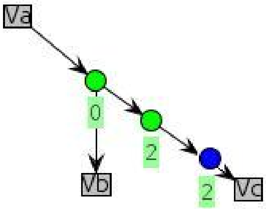


$\overset{(2.7)}{=}$

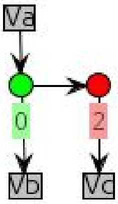
$=$



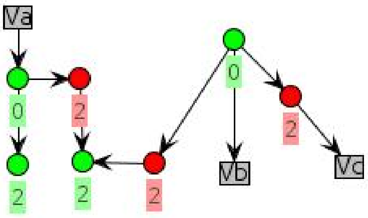
$\overset{(2.8)}{=}$



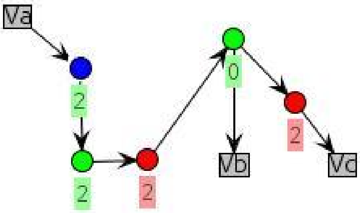
$\overset{(4.5)}{=}$



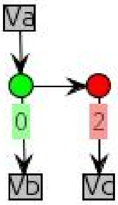
- $\alpha = \beta = \gamma = 2$



$\overset{(2.8,4.5)}{=}$



$\overset{(4.5)}{=}$



□

As in the case of protocols from sections 4.2 and 4.3 Hillebrand proves the correctness of EPR teleportation through GHZ in Z/X-calculus.[11] Due to the elegant representation of unitary corrections, the proof in RGB is significantly simpler.

As an aside, let's consider the presentations of Quantum Secret State Sharing and EPR teleportation in the context of results from Chapter 3. Graphical representations of both protocols only use generators from the subcategory **RGB-Even** and hence by the above, we showed that both protocols are realisable in **Spek** and therefore in Spekkens Toy Theory.

Analysis performed in this chapter illustrates that it is possible to apply Red-green-blue calculus to express and prove correctness of quantum protocols. Three considered examples show that RGB-calculus in some cases offers an advantage over Red-green calculus, especially when three complementary observables of a qubit are explicitly mentioned. However, when the observable Y is absent, description with Z/X-calculus is superior.

Chapter 5

Classical Simulability of Quantum Algorithms

So far in chapters 3 and 4 we showed that graphical calculi and categorical approach to quantum mechanics can be applied to analyse differences between quantum theories and to describe and prove correctness of quantum protocols. In this chapter we show how to capture the notion of classical simulability of quantum computation within Z/X-calculus. We use this concept to provide an alternative, diagrammatical proof of a standard result in Quantum Computing due to Browne [2], that the Quantum Fourier Transform is classically simulable on eigenstate inputs.

5.1 Classical Simulability in Z/X-Calculus

The idea of simulating quantum computation on a classical computer might seem a bit counterintuitive, why would one want to deprive oneself of the benefits of quantum speed-up? Of course, given appropriate time and memory resources any quantum computation can be simulated by a classical computer, but here we are interested in simulation that is efficient. If a quantum algorithm can be efficiently classically simulated then it means that an efficient classical algorithm solving the given problem is thus constructed. Therefore classical simulation of quantum computation can be seen as a mean of devising efficient classical algorithms. Analysis of classical simulation also gives us an additional insight into the origins of quantum speed-up. It allows us to pinpoint precisely which components of the quantum algorithm are responsible for the advantage over classical computation and which are merely classical procedures disguised as quantum operations.

Definition 5.1. An algorithm is said to be efficient if its running time is a polynomial in the size of the input.

The definition of efficient classical simulation of quantum computation, as given by Van Den Nest[23] is as follows:

Definition 5.2. Consider a uniform family of quantum circuits $\mathcal{U} \equiv \mathcal{U}_N$ acting on the N-qubit input state $|\mathbf{0}\rangle \equiv |0\rangle^{\otimes N}$, and followed by a measurement of the first qubit in the computational basis. Then the outcome is a classical bit $\alpha \in \{0, 1\}$. The probability that the result α occurs is given by $\pi(\alpha) = \langle \mathbf{0}|\mathcal{U}^{\dagger}[|\alpha\rangle\langle\alpha|\otimes I]\mathcal{U}|\mathbf{0}\rangle$. We say that the above quantum computation can be efficiently simulated classically if it is possible to evaluate $\pi(0)$ up to M digits in poly(N, M) time on a classical computer.

In this chapter we consider an full version of Z/X-calculus, as defined in [4]. Phase angles now range over a continuous set $[0, 2\pi)$, as opposed to a discrete set $\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ as in the category **RG** from Chapter 2.

The following theorem gives a sufficient condition for efficient classical simulability within Z/X-calculus, assuming that quantum computation is described in the standard Hilbert Spaces formalism:

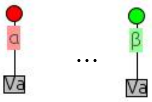
Theorem 5.1. If the graph that represents the initial setup of a quantum computation Q on an input I can be rewritten into a product state

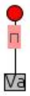
- In a number of steps polynomial in the size of the input
- Using the rules of the red-green calculus

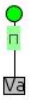
Then the quantum computation Q on input I can be efficiently classically simulated.

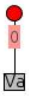
Proof. Let Q be a quantum computation whose diagrammatical representation in Z/X-calculus satisfies all the conditions. Then the corresponding classical procedure is as follows: 1. Translate Q into its representation in Z/X-calculus 2. Rewrite the representation to a product state 3. Translate the obtained product state back to its Hilbert Space formalism equivalent Both translations are performed in a polynomial number of steps, as is the procedure of rewriting, hence the classical algorithm is an efficient simulation of Q. □

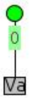
The general form of a product state expressed in Z/X-calculus is:

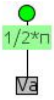


where $\alpha, \beta \in [0, 2\pi)$. Examples of product states include: 





and 



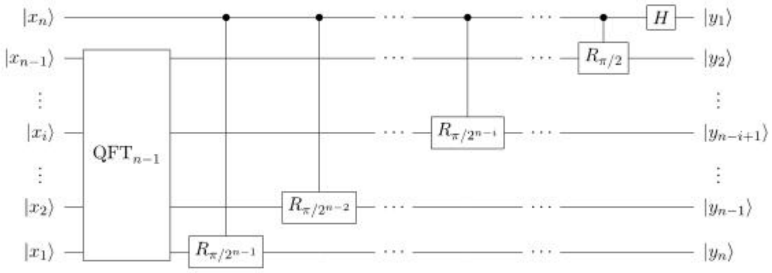
.

We now proceed to illustrate applications of this theorem with an example. The specific algorithm chosen is the Quantum Fourier Transform, a procedure that is in the heart of the most spectacular example of quantum speed-up - Shor's algorithm[21]. Otherwise known as the factoring algorithm, it computes prime factors of a natural number in time polynomial in the number of bits in that number's binary representation. If realised physically it would constitute a breach in security of all security protocols that exploit the difficulty of computing prime factors on a classical computer. This includes the widely popular RSA encryption protocol.

Definition 5.3. Quantum Fourier Transform is a linear transformation on qubits that is the quantum counterpart of the Discrete Fourier Transform. QFT is the classical DFT applied to the vector of amplitudes of a quantum state. It can be interpreted as a unitary matrix acting on a quantum state:

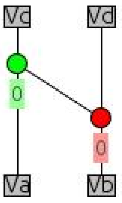
$$F_N = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \dots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \dots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \dots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \dots & \omega^{(N-1)(N-1)} \end{bmatrix}$$

Schematically, QFT can be expressed by a quantum circuit. In the following diagram H denotes the Hadamard gate and R_α represents the Controlled Phase gate with phase α. It is worth noting that the order of qubits is reversed on output.

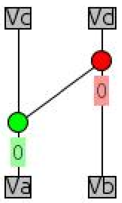


To translate the QFT circuit into Red-green calculus, we need the Hadamard gate, as well as the controlled phase gate (denoted R_α). The former, being one of the primitive elements, is easily realisable, the latter requires composing several basic operators. Firstly, we need to construct the CNOT gate:

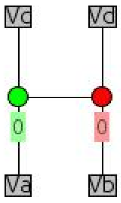
$CNOT = (I\otimes\delta_X)\circ(\delta_Z\otimes I)$



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



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



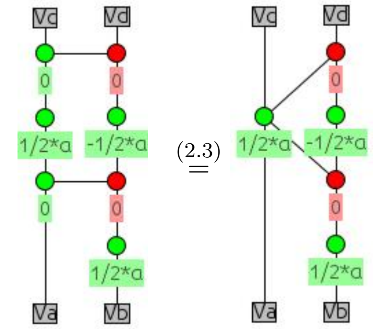
then, following the result presented in [4] we compose CNOTs with green phase gates (denoted Z_α):

Correctness may be verified by multiplying matrices corresponding to these gates:

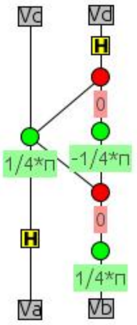
$$(I\otimes Z_\alpha)\circ CNOT\circ(Z_\alpha\otimes Z_\alpha)\circ CNOT = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\alpha}{2}} \end{pmatrix} \right) \circ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \circ$$

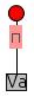
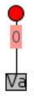
$$\circ \left(\begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\alpha}{2}} \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & e^{-\frac{i\alpha}{2}} \end{pmatrix} \right) \circ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{pmatrix} = R_\alpha$$

In Red-green calculus the above product of matrices is expressed as:

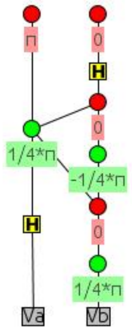


For two qubits the QFT circuit translated into Z/X-calculus is depicted as follows:



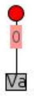
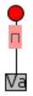
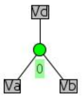
Due to qubit reversal on output, visible on the QFT circuit graph, the qubits are first swapped. The sample input, say $|0\rangle \otimes |1\rangle$ is denoted (after the swap) by  .

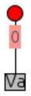
Plugging the input results in yields:

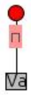


5.2 Classical Simulability of QFT in Z/X-Calculus

Before we proceed to the graphical proof, we prove the following useful lemma:

Lemma 5.2. In red-green calculus, when one of ,  is fed into a green copy , the resulting graph is disconnected.

Proof. This follows by axioms of Z/X-calculus. Note that $|0\rangle$ and $|1\rangle$ represented respectively by 

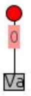
 and 

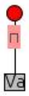
 are eigenstates of the observable $(A, \delta_X, \epsilon_X)$ in the sense of Definition 1.13, and are copied by the δ_X operation. □

Now, we quote the following standard result due to Browne[2] and provide a new diagrammatical proof:

Theorem 5.3. Let I be an input of the form: $\overbrace{|0\dots0\rangle}^{n_1} \otimes \overbrace{|1\dots1\rangle}^{n_2} \otimes \dots \otimes \overbrace{|0\dots0\rangle}^{n_{k-1}} \otimes \overbrace{|1\dots1\rangle}^{n_k}$, and $\{n_1, \dots, n_k\} \subseteq \{0, 1, 2, 3, \dots\}$ i.e. I is a product state of computational basis states. Quantum Fourier transform run on I can be efficiently simulated on a classical computer.

Proof. In red-green calculus inputs of this form are product states consisting of:

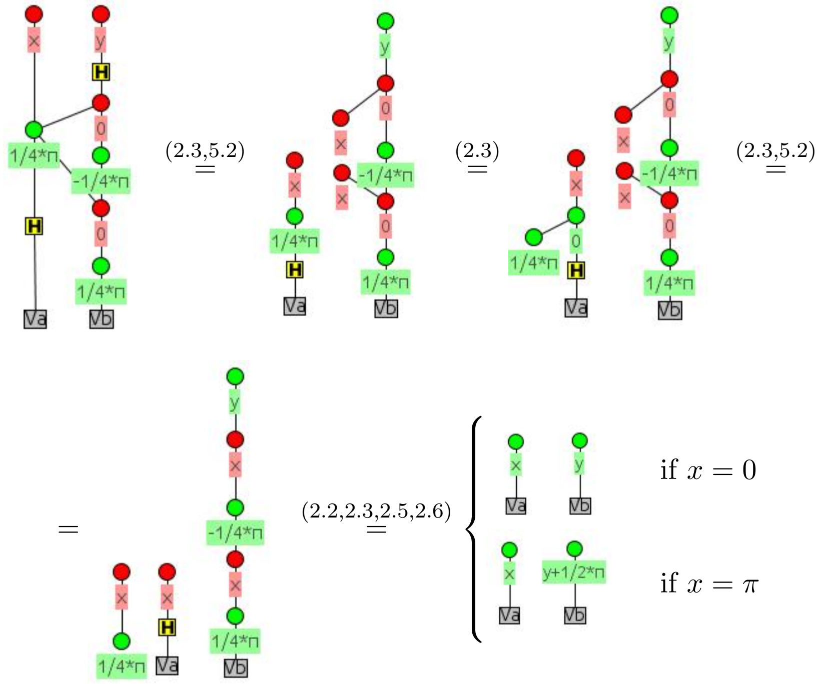
$|0\rangle =$ 

 $|1\rangle =$ 

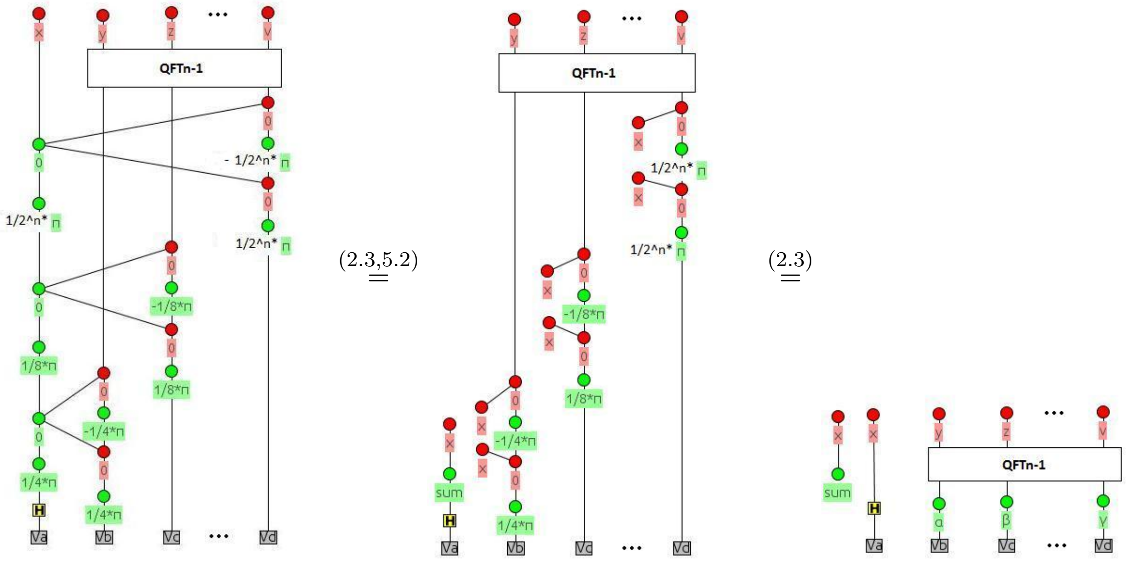
 .

We argue inductively that the result of performing QFT on such an input is a product state, then Theorem 5.1 will give us the required result. Let α, β, γ and *sum* denote phases and $x, y, z, v \in \{0, \pi\}$

- Base case: 2 qubits



- Inductive step: Assuming the result holds for QFT$_{n-1}$, let's chow the result for QFT$_n$.



By the inductive hypothesis, the result of computing QFT_{n-1} is a product state, hence the whole graph is a product state.

The fact, that the number of gates in the quantum circuit realising QFT is polynomial in the number of input qubits is a standard QC result.[19] By the means of translation provided earlier in this chapter, the size of the corresponding graph in red-green calculus has the same order of magnitude as the size of the quantum circuit. Then, it is clearly visible by the above computation that the number of rewrites per gate is constant. Hence, the overall number of rewrites in the process is polynomial in the number of input qubits.

Also, by the above graphical argument that only used red-green calculus rules, the resulting graph is disconnected and has the form of a product state and thus, we may conclude by Theorem 5.1 that QFT is classically simulable on eigenstate inputs. □

This shows that Z/X-calculus may be succesfully applied to reason about efficient classical simulation of quantum algorithms.

The results in Chapters 4 and 5 were achieved with aid of Quantomatic - a semi-automated tool for reasoning about quantum system that is being developed in Oxford by a team of researchers[16]. Quantomatic was also used to generate digraphs included in those two chapters. Pictures in Chapter 1 are taken from [3] and those in Chapter 2 from [17].

Further work based on the results presented here, includes showing completeness of **RGB** with respect to **Stab**. An important stepping stone would be to provide a graphical proof of Gottesmann-Knill theorem[23], a result on classical simulability of stabilizer circuits. Other topics include describing further quantum security protocols, especially those that use all three complementary observables of a qubit and investigating the computational complexity of rewriting digraphs.

The results obtained in this chapter, together with the applications to analysis of quantum theories and quantum protocols considered here are only a fraction of the Quantum Mechanical topics where graphical calculi based on categorical axiomatisation can be used. But even on their own they show that Red-green and Red-green-blue calculi are powerful and versatile tools for analysis of Quantum Computation.

Bibliography

[1] Samson Abramsky and Bob Coecke. A categorical semantics of quantum protocols. Mar 2007. arXiv:quant-ph/0402130v5.

[2] Daniel Browne. Efficient classical simulation of the quantum Fourier transform. May 2007. doi:10.1088/1367-2630/9/5/146.

[3] Bob Coecke. Quantum Picturalism. Aug 2009. arXiv:0908.1787v1 [quant-ph].

[4] Bob Coecke and Ross Duncan. Interacting Quantum Observables: Categorical Algebra and Diagrammatics. *New J. Phys.*, 13(043016), Jun 2011. arXiv:0906.4725v3.

[5] Bob Coecke and Bill Edwards. Toy quantum Categories. arXiv:0808.1037v1.

[6] Bob Coecke, Bill Edwards, and Robert Spekkens. Phase groups and the origin of non-locality for qubits. Mar 2010. arXiv:1003.5005v1 [quant-ph].

[7] Bob Coecke, Dusko Pavlovic, and Jamie Vicary. A new description of orthogonal bases. 2008. arXiv:0810.0812.

[8] Bob Coecke, Simon Pedrix, and Eric Paquette. Bases in diagrammatic quantum protocols. *Electronic Notes in Theoretical Computer Science 218*, 2008.

[9] David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Royal Society (London), Proceedings, Series A - Mathematical and Physical Sciences*, Jul 1985.

[10] Valery Gorbachev and Andrey Trubilko. Quantum teleportation of an EPR pair by three-particle entanglement. *Journal of Experimental and Theoretical Physics Letters*, 2000. arXiv:quant-ph/9906110v1.

[11] Anne Hillebrand. Quantum Protocols involving Multiparticle Entanglement and their Representations in the zx-calculus. 2011. http://www.cs.ox.ac.uk/bob.coecke/Anne.pdf.

[12] Mark Hillery, Buzek Vladimir, and Andre Berthiaume. Quantum secret sharing. *Physical Review*, 1998. arXiv:quant-ph/9806063v2.

[13] Andre Joyal and Ross Street. The Geometry of tensor calculus. *I. Adv. Math. 88, pp. 55-112.*, 1991.

[14] Christian Kassel. Quantum groups. *Springer*, 1995.

[15] Aleks Kissinger and Lucas Dixon. Open graphs and monoidal theories. 2011. arXiv:1011.4114.

[16] Aleks Kissinger, Alexander Merry, Lucas Dixon, and Ross Duncan. Quantomatic. sites.google.com/site/quantomatic.

[17] Alex Lang and Bob Coecke. Trichromatic Open Digraphs for Understanding Qubits. Oct 2011. arXiv:1110.2613v2.

[18] Saunders McLane. Categories for the Working Mathematician. *Springer. ISBN 0-387-98403-8. (Volume 5 in the series Graduate Texts in Mathematics)*, Sep 1998.

[19] David Mermin. Quantum Computer Science. *Cambridge University Press*, 2007.

[20] Simon Pedrix and Ross Duncan. Graph states and the necessity of Euler decomposition. *Mathematical Theory and Computational Practice*, 2010.

[21] Peter Shor. Algorithms for quantum computation: Discrete logarithms and factoring. *Proc. 35nd Annual Symposium on Foundations of Computer Science (Shafi Goldwasser, ed.), IEEE Computer Society Press, 124-134*, 1994.

[22] Rob Spekkens. Evidence for the epistemic view of quantum states: A toy theory. 10.1103/PhysRevA.75.032110.

[23] Maarten Van den Nest. Classical simulation of quantum computation, the Gottesman-Knill theorem, and slightly beyond. Oct 2009. arXiv:0811.0898v2 [quant-ph].

[24] Pawel Wocjan and Thomas Beth. New Construction of Mutually Unbiased Bases in Square Dimensions. Jul 2004. arXiv:quant-ph/0407081v1.