GRAPHICAL CALCULATION FOR THREE-DIMENSIONAL QUANTUM COMPUTATION

by

Kentaro Honda

A Master Thesis

Submitted to
the Graduate School of the University of Tokyo
on Feburary 6, 2013
in Partial Fulfillment of the Requirements
for the Degree of Master of Information Science and Technology
in Computer Science

Thesis Supervisor: Masami Hagiya
Professor of Computer Science

ABSTRACT

In these decades, quantum computation and quantum information have attracted attention and been studied well. In many studies on those fields, the traditional method in quantum mechanics, namely calculation on Hilbert spaces, has been used to express quantum systems. However, it is difficult to express interactions between quantum systems with this style, especially when the systems include quantum entanglement, which have higher correlation than any classical systems can have.

Recently, as more sophisticated styles, graphical calculi for quantum computation have been developed. However, these calculi are limited to qubits, i.e., two-dimensional quantum systems. GHZ/W calculus, one of these calculi, is based on classes of quantum entanglement in tripartite qubits, and does computation by composing two kinds of graphical units that are algebras defined on monoidal categories.

We extended GHZ/W calculus to qutrits, i.e., three-dimensional quantum systems. First, we completed classifying quantum entanglement in tripartite qutrits. Then, based on this classification, we defined three graphical units and seven graphical equations as axioms of a graphical calculus for qutrits, named G/W/I calculus. Finally, we proved properties of G/W/I calculus. In the calculus, we can express every qutrits graphically, and define a embedding of GHZ/W calculus. Moreover, we can simulate the two-dimensional calculus via the embedding. Such properties show that our calculus is sufficient to do three-dimensional quantum computation.

Acknowledgements

I would like to express my gratitude to my supervisor, Prof. Masami Hagiya for his support and advice. I would like to thank Dr. Yoshihiko Kakutani for useful discussion and guidance. I am grateful to Dr. Ichiro Hasuo for giving advice to me. I also appreciate discussion with members of Hagiya laboratory, especially Yoichi Hirai and Takahiro Kubota.

Contents

Chapter 1

Introduction

In these decades, quantum computation and quantum communication, which are based on quantum physics, have been studied as new paradigms of computation and communication. Although a quantum computer hasn't been built yet, various algorithms for quantum computation have been produced. These algorithms such as Shor's algorithm [29] show a quantum computer is more powerful than a classical computer. In the area of quantum communication, quantum cryptography gives us information theoretical secure communication [3, 30]. In these studies of the fields, researchers have used a traditional method in quantum physics, namely calculation on Hilbert spaces. However, this method isn't suitable to express interactions between quantum systems, and particularly quantum entanglement, which produces nonlocality in quantum physics and forms a foundation for quantum computation and communication [4].

One of the solutions is using categorical quantum mechanics [1, 26, 27]. It uses monoidal categories instead of Hilbert spaces, and provides categorical foundation of quantum physics, and then of quantum computation and communication. Since monoidal categories have graphical languages, categorical quantum mechanics gives us graphical calculi for quantum computation and communication, as more sophisticated styles. However, these graphical calculi focus on only qubits, i.e., two-dimensional quantum systems, while higher-dimensional systems have the advantage over qubits [2, 5, 6].

We extended GHZ/W calculus, a graphical calculus in categorical quantum mechanics, to qutrits, i.e., three-dimensional quantum systems. The components of GHZ/W calculus are algebras defined on symmetric monoidal categories, called commutative Frobenius algebras (CFAs). The calculus was built in [9] based on the fact that classes of CFAs on $\mathbb{C}^2$ are isomorphic to classes of states of three qubits categorised depending on how entangled a state is. In this paper, at first, we completed classifying entangled states of three qutrits in terms of CFAs. Next, based on this classification, we introduced a graphical calculus for qutrits named G/W/I calculus. Then, we showed several properties of the calculus. For example, G/W/I calculus on $\mathbb{C}^3$ gives us a basis of $\mathbb{C}^3$ and any state of any number of qutrits with the help of states of single qutrits. Finally, we examined difference between GHZ/W calculus on $\mathbb{C}^2$ and G/W/I calculus on $\mathbb{C}^3$. We found that there is an equation holding in the former but not in the latter. To bridge the difference, we defined an embedding of $\mathbb{C}^2$ into G/W/I calculus, and proved that we can simulate two-dimensional calculus in G/W/I calculus.

This paper is an extension of the bachelor's thesis [16] and a paper of the author [17]. To be clear the contributions of this paper, we summarise them here. The following is a contribution that was written in [17], but not in [16].

- We proved Lemma 4.8 that is used to show classification of entangled states of three qutrits as a conjecture in [16].

The followings are written neither in [16] nor [17].

- We built a graphical calculus for qutrits, and showed several properties of the calculus in Section 5.2.
- We proved that the distributive law of GHZ/W calculus doesn't hold on odd-dimensional spaces in Section 5.3.

Chapter 2

Quantum Entanglement

Unlike the classical world, the quantum world lets quantum systems behave counter-intuitively. Especially, it allows systems to have non-local correlations. Quantum entanglement, which produces such correlations, gives us the power to calculate stronger than using the classical one. The purpose of this chapter is to explain a classification of quantum entanglement.

For the readers unfamiliar to quantum information theory, we start this chapter with axioms of quantum information theory. After that, we move to introduce stochastic local operations and classical communication (SLOCC) equivalence relation. It plays an important role in our arguments.

2.1 Single Quantum System

We show axioms of a single quantum system. They are about states, time evolution and measurements.

Axiom 1. For any quantum system, there is the associated Hilbert space $\mathcal{H}$, called the **state space**. Moreover, a state of an isolated system is a unit vector of $\mathcal{H}$. The vector is called a **state vector**.

Given a quantum system, the state space is uniquely determined up to isomorphism. In contrast, even given a Hilbert space $\mathcal{H}$, a quantum system whose state space is $\mathcal{H}$ isn't determined. This asymmetric relation shows that state spaces are abstractions of quantum systems. Since we have no interest in concrete quantum systems, we sometimes use a Hilbert space $\mathcal{H}$ to indicate quantum systems with the state space $\mathcal{H}$.

Remark. To express states of an arbitrary system, we have to use not vectors but matrices. A state that can be expressed using a vector is called a **pure** state, and a non-pure state is called a **mixed** state. In this paper, we deal with just pure states. A part of our future work is to extend our results to mixed states.

Notation 2.1 (Bra, Ket)**.** To indicate vectors, there are various notations such as $\mathbf{v}$, $\vec{v}$, etc. In quantum physics and quantum information theory, a vector is written as $|v\rangle$. Exceptionally, a null vector is written as 0. When considering an inner product space, the inner product of $|v\rangle$ and $|u\rangle$ is written as $\langle v|u\rangle$. This notation induces notation of elements of the dual space. When $|v\rangle$ is an element of an inner product space, an element f of the dual space such that $f(|u\rangle) = \langle v|u\rangle$ is expressed as $\langle v|$. Besides, the cross product of $|v\rangle$ and $|u\rangle$ is written as $|v\rangle\langle u|$. $|v\rangle$ and $\langle v|$ are called a **ket** and a **bra**, respectively. In this paper, we use this **Bra-Ket Notation**. We write the tensor product of $|v\rangle$ and $|u\rangle$ as $|v\rangle \otimes |u\rangle$, $|vu\rangle$ or sometimes $|v\rangle|u\rangle$.

Then, we can define analogous to (classical) bits and trits.

Definition 2.2 (Qubit, Qutrit)**.** A quantum system whose state space is $\mathbb{C}^2$ called a **qubit**. Similarly, a quantum system whose state space is $\mathbb{C}^3$ is a **qutrit**.

Notation 2.3. We take a canonical basis of $\mathbb{C}^2$, and fix it. We write an element of it as $|0\rangle$ and the other as $|1\rangle$, and fix them. Similarly, canonical bases of $\mathbb{C}^3$ are $|0\rangle$, $|1\rangle$ and $|2\rangle$. Obviously, $\langle i|j\rangle = \delta_{i,j}$ where $\delta_{i,j}$ is the Kronecker delta.

Example 2.4. The following vectors are states of a qubit.

$$|+\rangle := \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \quad |-\rangle := \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

They form an orthonormal basis of $\mathbb{C}^2$. Indeed, orthogonality holds as follows.

$$\langle +|-\rangle = \frac{1}{2}(\langle 0| + \langle 1|)(|0\rangle - |1\rangle) = \frac{1}{2}(\langle 0|0\rangle + \langle 1|0\rangle - \langle 0|1\rangle - \langle 1|1\rangle) = 0.$$

Axiom 2. A discrete time evolution of an isolated quantum system is a unitary operator on its state space.

This axiom defines what we can do for quantum systems without measurements. The unitarity condition forbids us from doing non-invertible or cloning operations [32].

Example 2.5. The following operators on $\mathbb{C}^2$ are unitary.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

They are called the **Pauli matrices**. Another important operator is the following **Hadamard gate** H.

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

This operator maps $|0\rangle$ to $|+\rangle$ and $|1\rangle$ to $|-\rangle$.

Axiom 3. The **observables** of a quantum system are the Hermitian operators on the state space. The eigenvalues of a Hermitian operator are the possible results of the measurement of the observable. After the measurement, the state will be changed depending on the result. If the result of the measurement of an observable A on a state $|\psi\rangle$ is a, the post-measurement state is $\frac{1}{\langle\psi|P_a|\psi\rangle} P_a|\psi\rangle$ where P_a is the projection operator onto the eigenspace with a.

When a Hermitian operator is non-degenerate, the post-measurement state is uniquely determined by the result. In this case, P_a can be written as $|\psi_a\rangle\langle\psi_a|$ where $|\psi_a\rangle$ is the associated eigenvector. The post-measurement state is $\frac{1}{\| |\psi_a\rangle \|}|\psi_a\rangle$.

Example 2.6. Consider measurement of $A := 0|0\rangle\langle 0| + 1|1\rangle\langle 1|$ of a qubit. The reader can check A is a Hermitian without difficulty. A state of a qubit is generally written as

$$|\psi\rangle := \alpha|0\rangle + \beta|1\rangle$$

where α, β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. Then, the result 0 is obtained with probability $|\alpha|^2$. The other result occurs with probability $|\beta|^2$. The post-measurement states are $|0\rangle$ and $|1\rangle$. This example can be easily extended to a state of any quantum system with a finite-dimensional state space. In the following, we often use A to measure states. We refer to measurement of A or its extension as measurement in the canonical basis.

Now, let us take a quantum system $\mathcal{H}$ and a state $|\psi\rangle$ of it. Consider another state $|\phi\rangle := e^{i\theta}|\psi\rangle$. For any observable $A := \sum_a aP_a$, the probabilities of obtaining the result a of the measurement of A on $|\psi\rangle$ and $|\phi\rangle$ are the same. Indeed,

$$\langle\phi|P_a|\phi\rangle = \langle\psi|e^{-i\theta}P_a e^{i\theta}|\psi\rangle = \langle\psi|P_a|\psi\rangle.$$

Even if we do after a unitary operator is applied, they are the same.

$$\langle\phi|U^\dagger P_a U|\phi\rangle = \langle\psi|e^{-i\theta}U^\dagger P_a U e^{i\theta}|\psi\rangle = \langle\psi|U^\dagger P_a U|\psi\rangle$$

Noting the composition of unitary operators is unitary, it means we have no way to distinguish $|\psi\rangle$ and $|\phi\rangle$. Therefore, we regard these states as the same. That is, we can think of a ray $[|\psi\rangle]$ as a state of an isolated quantum system where $[|\psi\rangle]$ is an equivalence class of $|\psi\rangle$ by $\sim$ and $\sim$ is an equivalence relation such that $|\psi\rangle \sim |\phi\rangle$, if and only if, there is a nonzero complex number c such that $|\psi\rangle = c|\phi\rangle$. For this reason, we often omit normalising factors of states.

2.2 Composite Quantum System

Axiom 4. Let J be a finite set and $\{\mathcal{H}_j\}_{j\in J}$ be a set of state spaces of quantum systems. The state space of the composite system of them is $\bigotimes_{j\in J}\mathcal{H}_j$. An observable A'_i of the ith system is equivalent to the observable $\bigotimes_{j\in J}A_j$ of the composite system where A_j are identity operators except $A_i := A'_i$. Moreover, when states of systems are $\{|\psi_j\rangle\}_{j\in J}$, the state of the composite system is $\bigotimes_{j\in J}|\psi_j\rangle$.

Example 2.7. The state space of two qubits is $\mathbb{C}^2\otimes\mathbb{C}^2 \cong \mathbb{C}^4$. The following ket vectors are states of two qubits.

$$|\psi_0\rangle := \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$$

$$|\psi_1\rangle := \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|11\rangle \tag{2.1}$$

$$|EPR\rangle := \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle \tag{2.2}$$

When a state of the zeroth system is $|-\rangle$ and one of the first system is $|1\rangle$, the state of the composite system is $|\psi_1\rangle$ above.

Now, we consider measurement of an observable of a subsystem. Let $|\psi\rangle$ be a state of the composite system of two quantum systems $\mathcal{H}_1, \mathcal{H}_2$. Suppose $|\psi\rangle$ is the tensor product of a state of each system, that is, $|\psi\rangle = |\phi\rangle\otimes|\chi\rangle$. Then, we measure an observable A of $\mathcal{H}_2$ on it. Axiom 4 states the observable of the composite system is $I\otimes A$. After the measurement, $|\psi\rangle$ will be changed to $(I\otimes P_a)|\psi\rangle = |\phi\rangle\otimes P_a|\chi\rangle$ when the result is a. It is noteworthy that a state of $\mathcal{H}_1$ is stable during the measurement. In contrast, if a state is not a tensor product, other systems are affected by a measurement.

Definition 2.8 (Separable, Entangled)**.** A state of a composite system is **separable** when it is the tensor product of a state of each system. A non-separable state is **entangled**.

(2.2) in Example 2.7 is a well-known entangled state. Let consider measurement in the canonical basis of the left side qubit. The associated projection operators of $A \otimes I$ are $P_0 := |0\rangle\langle 0| \otimes I$ and $P_1 := |1\rangle\langle 1| \otimes I$. Suppose the result is 0. It happens with probability $\frac{1}{2}$. Then, the post-measurement state of $|EPR\rangle$ is

$$\begin{aligned}\frac{1}{\|P_0|EPR\rangle\|}P_0|EPR\rangle &= \frac{1}{\sqrt{2}\|P_0|EPR\rangle\|}(|0\rangle\langle 0| \otimes I)(|01\rangle - |10\rangle) \\ &= |01\rangle.\end{aligned}$$

Now, the state of right side qubit is $|1\rangle$. Recall it is not so, before the measurement. It means that measurement affects not just a state of a target system but the whole entangled state.

2.3 Stochastic Local Operations and Classical Communication

The following operator $CNOT$ is a unitary one on $\mathbb{C}^2 \otimes \mathbb{C}^2$.

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

This operator, called the **controlled Not gate**, cannot be written as the tensor product of any operators on $\mathbb{C}^2$. This operator can produce an entangled state from a separable state. For example, see $|\psi_1\rangle$ in (2.1), which is the tensor product of $|-\rangle$ and $|1\rangle$. Then, apply the controlled Not gate to it.

$$\begin{aligned}CNOT|\psi_1\rangle &= \frac{1}{\sqrt{2}}CNOT(|01\rangle - |11\rangle) \\ &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |EPR\rangle\end{aligned}$$

By contrast, an operator that is the tensor product of an operator on each state space cannot generate any entangled state. The property of entanglement gives us a way to capture it.

Definition 2.9 (SLOCC Equivalence)**.** Let $|\psi\rangle$, $|\phi\rangle$ be states of a quantum system. We write $|\psi\rangle \geq_{SLOCC} |\phi\rangle$ when we can convert $|\psi\rangle$ to $|\phi\rangle$ via some local operations and classical communication (LOCC) with nonzero probability. We also say $|\phi\rangle$ can be produced from $|\psi\rangle$ by stochastic LOCC (SLOCC) when $|\psi\rangle \geq_{SLOCC} |\phi\rangle$. **SLOCC equivalence** is the equivalence relation induced by preorder $\geq_{SLOCC}$. That is, $|\psi\rangle$ and $|\phi\rangle$ are SLOCC equivalent, if and only if $|\psi\rangle \geq_{SLOCC} |\phi\rangle$ and $|\phi\rangle \geq_{SLOCC} |\psi\rangle$.

Theorem 2.10 ([13])**.** *Let $|\psi\rangle$, $|\phi\rangle$ be states of the composite system consisting of $\{\mathcal{H}_j\}_{j\in J}$. $|\psi\rangle$ is SLOCC equivalent to $|\phi\rangle$, if and only if, there are invertible matrices $\{L_j\}_{j\in J}$ such that $|\psi\rangle = \left(\bigotimes_{j\in J} L_j\right)|\phi\rangle$.*

SLOCC equivalence expresses how entangled states are. We will explain this point using an example.

Example 2.11. The followings are states of three qubits, called **GHZ state** and **W state**.

$$\begin{aligned}|GHZ\rangle &:= \frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle \\ |W\rangle &:= \frac{1}{\sqrt{3}}|001\rangle + \frac{1}{\sqrt{3}}|010\rangle + \frac{1}{\sqrt{3}}|100\rangle\end{aligned}$$

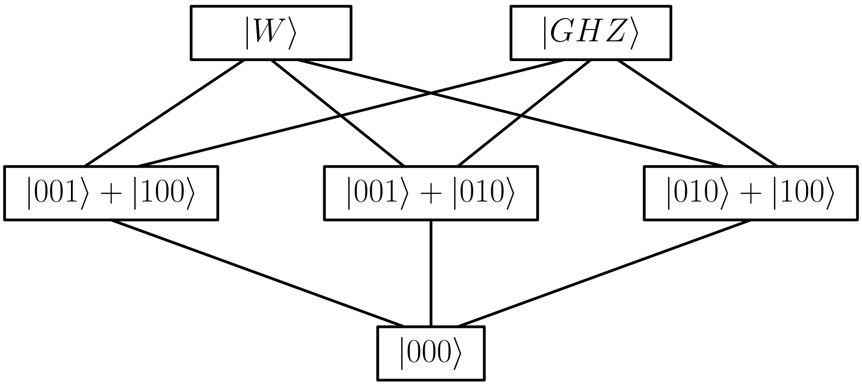


Figure 2.1: The SLOCC equivalence classes of three qubits

Let measure the leftmost qubit in the canonical basis. The possible post-measurement states of GHZ state are $|000\rangle$ and $|111\rangle$. They are both separable states. However, it is possible to get $|001\rangle + |010\rangle$ as the post-measurement state of W state with probability $\frac{2}{3}$. This state is entangled about the centre and rightmost qubits. It implies these states have different kind of entanglement. By contrast, the all post-measurement states of $|\psi_2\rangle := \frac{1}{2}|000\rangle + \frac{\sqrt{3}}{2}|111\rangle$ is separable like GHZ state, while it is impossible to convert $|\psi_2\rangle$ to $|GHZ\rangle$ deterministically. It means entanglement of $|\psi_2\rangle$ is weaker than of $|GHZ\rangle$, but they are states entangled in the same manner. SLOCC equivalence captures this property. Indeed, $|GHZ\rangle$ and $|\psi_2\rangle$ are SLOCC equivalent, although $|W\rangle$ is inequivalent to them.

An SLOCC equivalence class is an equivalence class by SLOCC equivalence. For reasons mentioned above, these equivalence classes are classes of states divided by the manner how to be entangled. At the last of this chapter, we show examples of SLOCC equivalence classes.

Example 2.12. In one qubits, there is only one SLOCC equivalence class. All states of two qubits are divided to two groups, namely separable states and entangled states. These groups are the SLOCC equivalence classes of two qubits.

Example 2.13 ([13])**.** In three qubits, there are six SLOCC equivalence classes. Representatives of them are $|GHZ\rangle$, $|W\rangle$, $|001\rangle+|010\rangle$, $|001\rangle+|100\rangle$, $|010\rangle+|100\rangle$ and $|000\rangle$. The lattice structure they form is given as the Hasse diagram in Figure 2.1.

Example 2.14 ([20, 21, 31, 33])**.** The numbers of SLOCC equivalence classes in qubits more than four are uncountably infinite. Similarly, the numbers of classes in three quantum systems whose dimensions are larger than two are also uncountably infinite.

Chapter 3

Commutative Frobenius Algebra

In this chapter, we show a short introduction for a monoidal category and its graphical language. After that, we give an explanation of a commutative Frobenius algebra in such a category. A monoidal category and this algebra in the category are abstraction of a vector space and a commutative Frobenius algebra in the space.

3.1 Monoidal Category

Definition 3.1 (Categry)**.** A **category** C is a sextuple $\langle Obj(C), Arr(C), dom, cod, id, \circ\rangle$ consisting of :

$Obj(C)$	:	a collection
$Arr(C)$	:	a collection
dom	:	assignment each element f in $Arr(C)$ an element $\mathrm{dom}f$ in $Obj(C)$
cod	:	assignment each element f in $Arr(C)$ an element $\mathrm{cod}f$ in $Obj(C)$
id	:	assignment each element a in $Obj(C)$ an element 1_a in $Arr(C)$ such that $\mathrm{dom}1_a = \mathrm{cod}1_a = a$
$\circ$	:	assignment a pair $\langle g, f\rangle$ of elements in $Arr(C)$ such that $\mathrm{dom}g = \mathrm{cod}f$ an element $g \circ f$ in $Arr(C)$ such that $\mathrm{dom}g \circ f = \mathrm{dom}f$ and $\mathrm{cod}g \circ f = \mathrm{cod}g$

satisfying the following axioms.

1. (Composition Law) For any trio $\langle h, g, f\rangle$ of elements in $Arr(C)$ such that $\mathrm{dom}h = \mathrm{cod}g$ and $\mathrm{dom}g = \mathrm{cod}f$,

$$h \circ (g \circ f) = (h \circ g) \circ f$$

2. (Unit Law) For any element f in $Arr(C)$,

$$f \circ 1_{\mathrm{dom}f} = f \text{ and } 1_{\mathrm{cod}f} \circ f = f$$

Elements of $Obj(C)$ and $Arr(C)$ are called **objects** and **arrows** of C. $\mathrm{dom}f$ and $\mathrm{cod}f$ are the **domain** and the **codomain** of f. 1_a is the **identity arrow** of a. $g \circ f$ is called the **composite** of g and f.

Notation 3.2. Let C be a category. In this paper, we use "$a \in C$" and "f in C" to show "a is an object of C" and "f is an arrow of C", respectively. Moreover, "$f : a \to b$" or "$a \xrightarrow{f} b$" means "a is the domain of f and b is the codomain of f". Using this notation, the composite of $g : b \to c$ and $f : a \to b$ can be written as $a \xrightarrow{f} b \xrightarrow{g} c$.

Example 3.3. A category whose objects are all sets and arrows are all functions is called **Set**.

Example 3.4. Set theory induces another example of category. A set can be regarded as a category whose objects are the elements of the set and functions are just identity arrows.

Example 3.5. A set equipped with multiplication and the unit, namely a monoid, can be regarded as a category in another way. Elements of a monoid are arrows between the object of the category, and composition is multiplication of them. The identity arrow is obviously the unit.

Example 3.6. $\mathbf{Vect}_K$ is a category whose objects are all vector spaces over K, arrows are all linear functions between them.

Definition 3.7 (Subcategory)**.** Let C be a category. A **subcategory** of C is a category whose objects are a subcollection of the objects of C, arrows are a subcollection of the arrows of C, identities and composites are inherited from C. A subcategory D of C is **full** when for any objects $a, b \in D$ and an arrow $f : a \to b$ in C, f is an arrow of D.

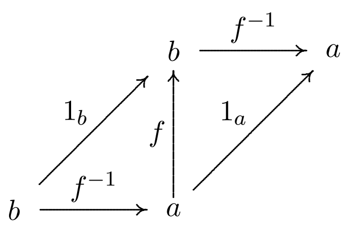
Example 3.8. $\mathbf{FdHilb}_K$ is a full subcategory of $\mathbf{Vect}_K$ whose objects are the finite dimensional Hilbert spaces over K.

Notations such as $a \xrightarrow{f} b$ give another notation, that is, a diagram. Being a diagram constructed by arrows commutative, the arrows composed of the paths in a diagram are the same. Precisely, a commutative diagram is defined in the following.

Definition 3.9 (Commutative Diagram)**.** Let C be a category, and G be a directed graph, whose vertices and edges are labelled by objects and arrows of C such that the source and the target of an edge are labelled by the domain and the codomain of the label of the edge, respectively. G **commutes** when for any pair $\langle v, v' \rangle$ of vertices, any arrow composed of all labels of a path from v to v' in order is the same arrow.

Example 3.3 shows an arrow is an abstraction of a function. Some properties of functions, such as isomorphisms, can be written in terms of categories.

Definition 3.10 (isomorphism)**.** An arrow $f : a \to b$ is an **isomorphism** when there is an arrow $f^{-1} : b \to a$ such that the following diagram commutes.



a and b are **isomorphic**, when there is an isomorphism $f : a \to b$.

An arrow plays a central role in category theory. For example, a category can be redefined without saying objects. We can define not only arrows in a category, but also arrows between categories, which are called functors.

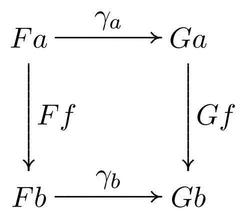
Definition 3.11 (Functor)**.** Let C, D be categories. A **functor** F from C to D consists of an assignment each object $a \in C$ an object $Fa \in D$ and an assignment each arrow $f : a \to b$ in C an arrow $Ff : Fa \to Fb$ in D preserving identity arrows and compositions. A functor F from C to D is written as $F : C \to D$.

Example 3.12. Let **Mon** be the category of monoids. The monoid homomorphisms are the arrows of **Mon**. Then, there is a functor $U : \mathbf{Mon} \to \mathbf{Set}$ that leads a monoid to its underlying set. U is called a **forgetful functor**.

Example 3.13. Categories and functors form a category. **Cat** is a category whose objects are all (small) categories and arrows are all functors between them.

Additionally, we can define arrows between functors.

Definition 3.14 (Natural Transformation)**.** Let $F, G : C \to D$ be functors. A **natural transformation** γ from F to G, written as $\gamma : F \dot{\to} G$, is an assignment each object $a \in C$ an arrow $\gamma_a : Fa \to Ga$ in D making the following diagram commutative for any arrow $f : a \to b$ in C.



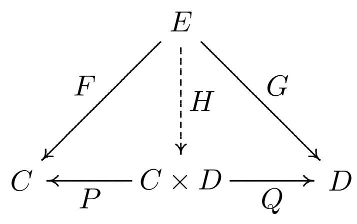
γ_a is called a **component** of γ. We sometimes identify a natural transformation with its components. When any component of γ is an isomorphism, γ is called a **natural isomorphism**. We write it as $\gamma : F \cong G$.

Example 3.15. Let $I : \mathbf{Vect}_K \to \mathbf{Vect}_K$ be the identity functor and $(-)^{**} : \mathbf{Vect}_K \to \mathbf{Vect}_K$ be a functor that maps a vector space to its double dual space. A canonical linear mapping $e_V : V \to V^{**}$ defined as $e_V(v)(f) = f(v)$ induces a natural transformation $e : I \dot{\to} (-)^{**}$.

Example 3.16. Let C, D be categories. D^C is a category whose objects are all functors from C to D and arrows are all natural transformations between them. Such categories are called **functor categories**.

Given categories, we can construct a new category using functors. We give a definition of such a category here.

Definition 3.17 (Product Category)**.** Let C, D be categories. There is a category $C \times D$ and functors $P : C \times D \to C$, $Q : C \times D \to D$ such that for any category E and functors $F : E \to C$, $G : E \to D$, there is a unique functor $H : E \to C \times D$ subject to the following commutative diagram.



$C \times D$ is called a **product category**.

Example 3.18. Let C, D be categories. A category whose objects are the pairs $\langle c, d \rangle$ where $c \in C$ and $d \in D$, and arrows are the pairs $\langle f, g \rangle : \langle a, b \rangle \to \langle c, d \rangle$ where $f : a \to c$ in C and $g : b \to d$ in D is a product category of C and D. Moreover, any product category of C and D is isomorphic to this category in **Cat**.

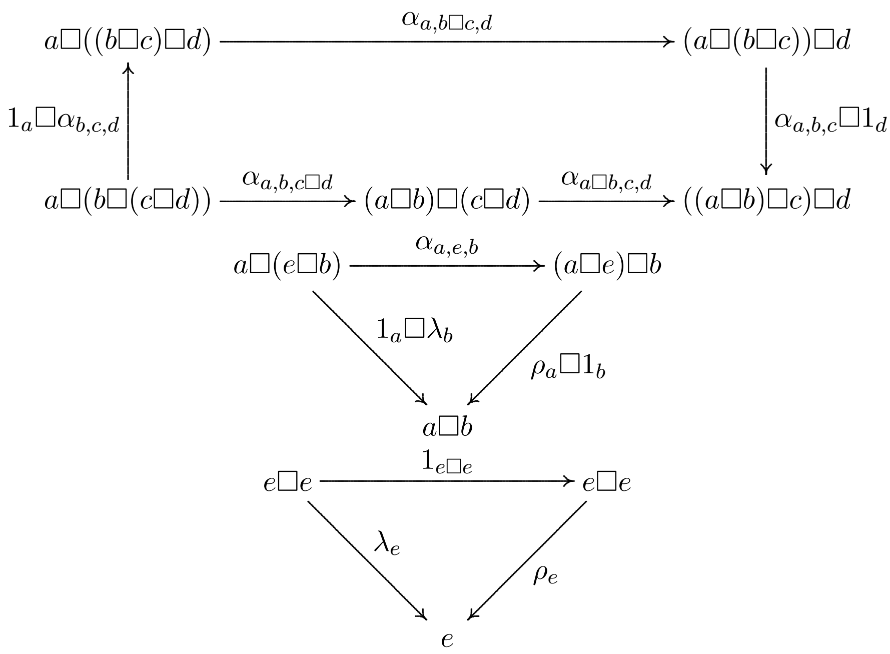
Definition 3.19 (Bifunctor)**.** A functor from a product category is called a **bifunctor**.

Since the structure of a category is too simple, it is difficult to use a category as it is. There are many extensions of a category, such as having limits, CCC, etc. In the rest of this section, we give a monoidal category, which is a category with "tensor".

Definition 3.20 (Monoidal Category)**.** A **monoidal category** M is a sextuple $\langle M, -\Box-, e, \alpha, \lambda, \rho\rangle$ consisting of :

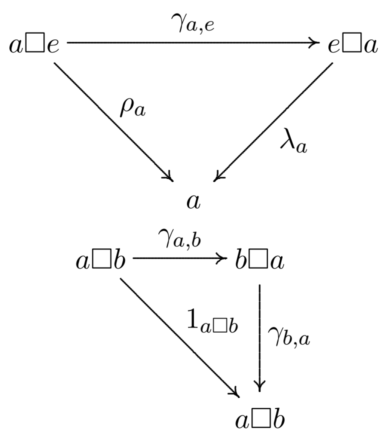
M	:	a category
$-\Box-$	:	a bifunctor $M \times M \to M$
e	:	an object of M
α	:	a natural isomorphism $\alpha_{a,b,c} : a\Box(b\Box c) \cong (a\Box b)\Box c$
λ	:	a natural isomorphism $\lambda_a : e\Box a \cong a$
ρ	:	a natural isomorphism $\rho_a : a\Box e \cong a$.

making the following diagrams commutative:



$-\Box-$ and e are called the **multiplication** and the **unit** of M. M is **strict** when $\alpha_{a,b,c}$, λ_a and ρ_a are identity arrows for any $a, b, c \in M$.

Definition 3.21 (Symmetric Monoidal Category)**.** A monoidal category is **symmetric** when it is equipped with a natural isomorphism $\gamma_{a,b} : a\Box b \cong b\Box a$ and the following diagrams commute.



$$\begin{array}{ccc} (a\Box b)\Box c & \xrightarrow{\gamma_{a\Box b,c}} & c\Box(a\Box b) \\ \downarrow{\scriptstyle \alpha^{-1}_{a,b,c}} & & \downarrow{\scriptstyle \alpha_{c,a,b}} \\ a\Box(b\Box c) & & (c\Box a)\Box b \\ \downarrow{\scriptstyle 1_a\Box\gamma_{b,c}} & & \downarrow{\scriptstyle \gamma_{c,a}\Box 1_b} \\ a\Box(c\Box b) & \xrightarrow{\alpha_{a,c,b}} & (a\Box c)\Box b \end{array}$$

We say "a monoidal category is **planar**" to emphasise that we don't care about whether or not a monoidal category has an additional structure.

A symmetric monoidal category has four structural arrows. Considering their composites and products, there are so many arrows between similar objects. However, the following theorem shows we don't have to pay attention to them.

Theorem 3.22 (Coherence Theorem [22]). *For any symmetric monoidal category, any diagram whose edges are labelled by α, λ, ρ, γ, identities, their composite and their products commutes.*

Example 3.23. **Set** is an example of symmetric monoidal categories. The multiplication is $\times$ and the unit is the unit set $\{*\}$.

Example 3.24. $\mathbf{Vect}_K$ is a symmetric monoidal category whose multiplication is $\otimes$ and unit is K.

Example 3.25. $\mathbf{FdHilb}_K$ is also a symmetric monoidal category whose monoidal structure is inherited from $\mathbf{Vect}_K$.

In the previous chapter, we showed Hilbert spaces over $\mathbb{C}$ play important roles in quantum information theory. As our main interest is about $\mathbb{C}^3$, the last example gives justification to study symmetric monoidal categories. In the paper, we especially focus on $\mathbf{FdHilb}_{\mathbb{C}}$. For simplicity, we abbreviate $\mathbf{FdHilb}_{\mathbb{C}}$ as **FdHilb**.

3.2 Graphical Language

As shown above, category theory has a commutative diagram to express equations between arrows. However, these diagrams are often complex and difficult to trace paths. Categories have another way to express these equations. Fortunately, the method, using graphical languages is especially effective for monoidal categories that we are interested in.

For a category, a graphical language interprets arrows as boxes and wires. We summarise the interpretation in Table 3.1. Objects and arrows are written as wires and boxes. Exceptionally, identity arrows are expressed as wires. Wires expressing the domain and the codomain of an arrow are connected to the upper and the lower side of the box, respectively. We sometimes refer to these wires as inputs and outputs. Composition of arrows is connection of boxes via a wire. Using this graphical language, we can state equations of arrows in terms of graphs.

Theorem 3.26 (Coherence Theorem of Graphical Language for Category [28]). *A well-formed equation between arrows follows from the axioms of category, if and only if, their diagrams are the same up to graph isomorphism, where a well-formed equation is an equation that the domain and the codomain of both sides of it are the same.*

Table 3.1: Graphical language for category

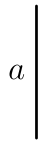
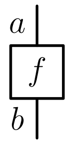
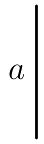
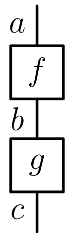
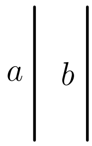
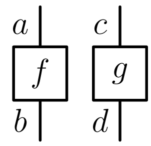
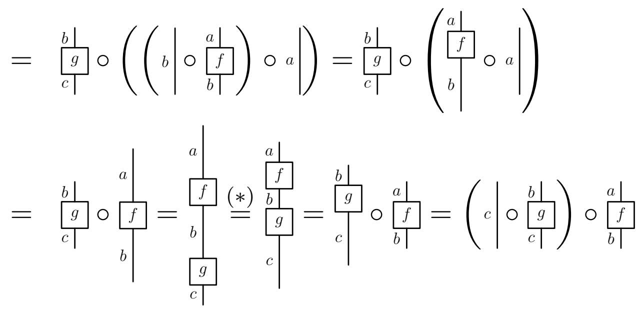
object a		arrow $a \xrightarrow{f} b$	
identity $1_a : a \to a$		composite $a \xrightarrow{f} b \xrightarrow{g} c$	

Table 3.2: Graphical language for monoidal category

object $a \Box b$ 	unit e	arrow $(f : a \to b) \Box (g : c \to d)$	

Example 3.27. $g \circ ((1_b \circ f) \circ 1_a) = (1_c \circ g) \circ f$ holds in any category. Indeed,

$g \circ ((1_b \circ f) \circ 1_a)$



$$= (1_c \circ g) \circ f$$

The equation $(*)$ follows from the coherence theorem.

Now, we move to a graphical language for a planar monoidal category. Recall a monoidal category is a category with multiplication $\Box$. Like for a category, we summarise a graphical language for a monoidal category in Table 3.2. A product of objects or arrows is a graph obtained by writing their components in parallel. When the domain or the codomain of arrow is a product, of course, a wire connected to the box is replaced with parallel lines. The unit object is exceptionally interpreted as an empty line. We think that it is a bit hard to understand this language, so we will give an example using the language. Before that, we check coherence theorem for a monoidal category. Note the difference from coherence theorem for a category.

Table 3.3: Triangle Expression of Arrows

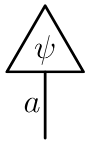
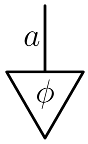
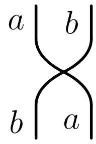
arrow $\psi : e \to a$ 	arrow $\phi : a \to e$ 

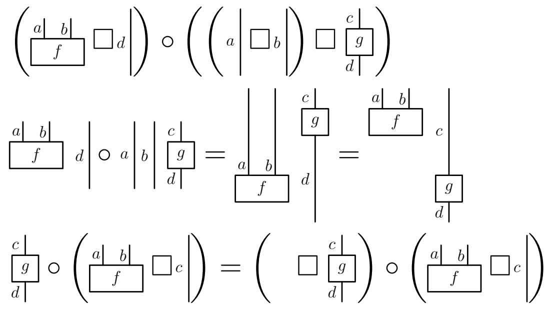
Table 3.4: Graphical language for symmetric monoidal category

$\gamma_{a,b} : a\Box b \to b\Box a$ 

Theorem 3.28 (Coherence Theorem of Graphical Language for Monoidal Category [28]). *A well-formed equation between arrows follows from the axioms of a monoidal category, if and only if, their diagrams are the same up to planar isotopy.*

Example 3.29. Let M be a monoidal category, and $f : a\Box b \to e$, $g : c \to d$ be arrows of M. Then, $(f\Box 1_d) \circ ((1_a\Box 1_b)\Box g) = (1_e\Box g) \circ (f\Box 1_c)$.

$$(f\Box 1_d) \circ ((1_a\Box 1_b)\Box g) =$$



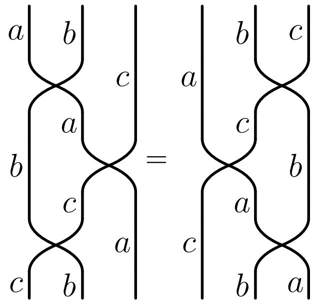
$$= (1_e\Box g) \circ (f\Box 1_c)$$

To emphasise that the domain or the codomain is the unit, we often use triangles referring to arrows from or to the unit (Table 3.3).

Then, we add a symmetric natural isomorphism γ. In a graphical language for a symmetric monoidal category, γ is interpreted as a crossing of wires (Table 3.4). The other components are the same with the components for a planar monoidal category. Of course, coherence theorem also holds in this language.

Theorem 3.30 (Coherence Theorem of Graphical Language for Symmetric Monoidal Category [28]). *A well-formed equation between arrows follows from the axioms of a symmetric monoidal category, if and only if, their diagrams are the same up to graph isomorphism.*

Example 3.31. The Yang-Baxter equation $(\gamma_{b,c}\Box 1_a) \circ (1_b\Box\gamma_{a,c}) \circ (\gamma_{a,b}\Box 1_c) = (1_c\Box\gamma_{a,b}) \circ (\gamma_{a,c}\Box 1_b) \circ (1_a\Box\gamma_{b,c})$ holds in any symmetric monoidal category. Comparing both sides of the following graphical equation, the readers can easily check its correctness.



3.3 Commutative Frobenius Algebra

Now, we are away from categories for a while, and recall vector spaces. Vector spaces have addition and scalar multiplication. However, vector spaces aren't equipped with "multiplication". Vector spaces with monoid structures are called algebras.

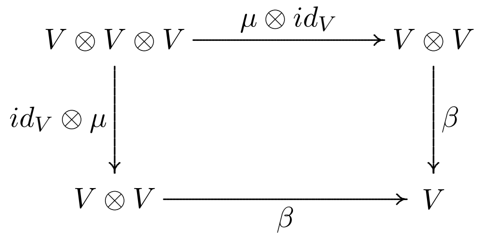
Definition 3.32 (Algebra)**.** A vector space V over a field K is called an **algebra** when it has a bilinear multiplication $\cdot$ and the unit $1 \in V$ of the multiplication. Explicitly, $\cdot$ and 1 satisfy the following axioms.

(Left Distributivity)	$(v + u) \cdot w = v \cdot w + u \cdot w$
(Right Distributivity)	$v \cdot (u + w) = v \cdot u + v \cdot w$
(Compatibility of Scalar Multiplication)	$(\alpha v) \cdot (\beta u) = \alpha\beta(v \cdot u)$
(Unit Law)	$1 \cdot v = v = v \cdot 1$

An algebra is **associative** and **commutative** when the multiplication is associative and commutative, respectively. These properties are given as the following equations.

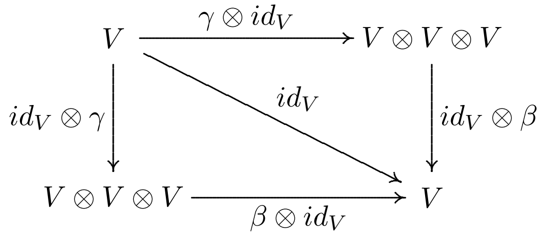
(Associative Law)	$(v \cdot u) \cdot w = v \cdot (u \cdot w)$
(Commutative Law)	$v \cdot u = u \cdot v$

Definition 3.33 (Frobenius Algebra)**.** Let V be an algebra over K with a multiplication μ. A bilinear functional is called a **pairing**. A pairing $\beta : V \otimes V \to K$ is **associative** when the following diagram commutes.



(3.1)

An associative pairing $\beta : V \otimes V \to K$ is a **Frobenius pairing** when there is a linear function $\gamma : K \to V \otimes V$ such that the following diagram commutes.



(3.2)

A **Frobenius algebra** is an associative algebra V over a field K with a Frobenius paring.

Notation 3.34. We often abbreviate a Frobenius algebra as an FA, and a commutative Frobenius algebra as a CFA.

Example 3.35. The field of complex numbers $\mathbb{C}$ is an example of Frobenius algebra. $\mathbb{C}$ is a two-dimensional vector space over $\mathbb{R}$ with usual addition $+$ and real multiplication. The usual multiplication $\cdot$ and 1 make $\mathbb{C}$ an algebra. The real part of multiplication, namely $\beta((a,b,c,d)^t) = a - d$ is a Frobenius paring. The coparing of β is $\gamma(1) = (1,0,0,-1)^t$. Indeed, the left triangle of (3.2) commutes.

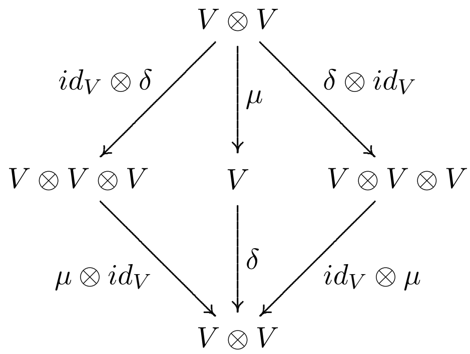
$$\begin{aligned}(\beta \otimes id_{\mathbb{C}}) \circ (id_{\mathbb{C}} \otimes \gamma)(a+bi) &= (\beta \otimes id_{\mathbb{C}})((a+bi) \otimes (1,0,0,-1)^t) \\ &= (\beta \otimes id_{\mathbb{C}})((a,0,0,-a,b,0,0,-b)^t) \\ &= (a,0) - (0,-b) = (a,b) = a+bi\end{aligned}$$

The right side also commutes.

A Frobenius pairing induces the dual of algebraic structure, and the relationship between them gives another definition of Frobenius algebras.

Definition 3.36 (Coalgebra)**.** A **coalgebra** is a vector space with a linear comultiplication δ and the counit ϵ of the comultiplication. A coalgebra is **coassociative** and **cocommutative** when the comultiplication is coassociative and cocommutative, respectively.

Definition 3.37 (Frobenius Algebra)**.** A Frobenius algebra is a quintuple $\langle V, \mu, \eta, \delta, \epsilon\rangle$ where $\langle V, \mu, \eta\rangle$ is an algebra and $\langle V, \delta, \epsilon\rangle$ is a coalgebra subject to the commutative diagram.

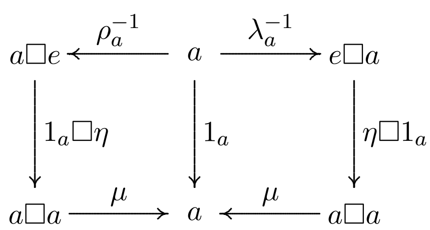


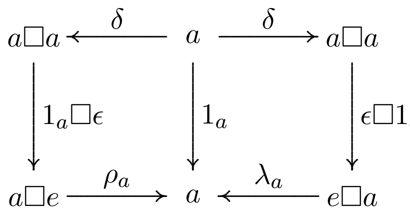
A Frobenius algebra is commutative when it is commutative as an algebra.

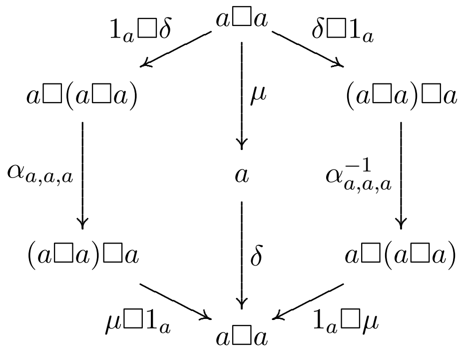
Proposition 3.38 ([19])**.** *These two definitions of Frobenius algebra are equivalent.*

Now, let back to monoidal categories from vector spaces. Note the above functions such as μ, δ are linear, and so arrows of $\mathbf{Vect}_K$. Therefore, we can generalise a Frobenius algebra to the categorical one.

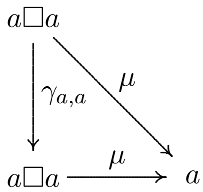
Definition 3.39 (Internal Frobenius Algebra)**.** Let M be a monoidal category. A **Frobenius algebra** in M is a quintuple $\langle a, \mu : a\Box a \to a, \eta : e \to a, \delta : a \to a\Box a, \epsilon : a \to e\rangle$ where a is an object and $\mu, \eta, \delta, \epsilon$ are arrows of M making the following diagrams commutative.







a is called a **Frobenius object**. A Frobenius algebra in a symmetric monoidal category is **commutative** when the following diagram commutes.



Example 3.40. A Frobenius algebra in $\mathbf{Vect}_K$ is a Frobenius algebra defined at the beginning of this section.

Example 3.41. An algebra $\mathcal{G}_2 \coloneqq \langle \mathbb{C}^2, \mu, \eta, \delta, \epsilon \rangle$ defined as follows is a Frobenius algebra in **FdHilb**, and then in $\mathbf{Vect}_{\mathbb{C}}$.

$$\mu \coloneqq |0\rangle\langle 00| + |1\rangle\langle 11| \quad \eta \coloneqq |0\rangle + |1\rangle$$

$$\delta \coloneqq |00\rangle\langle 0| + |11\rangle\langle 1| \quad \epsilon \coloneqq \langle 0| + \langle 1|$$

Proposition 3.42 ([19])**.** *Let $\langle a, \mu, \eta, \delta, \epsilon \rangle$ be a Frobenius algebra in a monoidal category M.*

1. *μ is associative and δ is coassociative.*
2. *Suppose M is symmetric. Then, μ is commutative, if and only if, δ is cocommutative.*

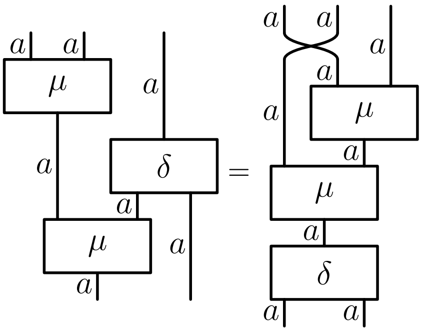
In the previous section, we showed an arrow in a symmetric monoidal category can be written using its graphical language. We use this language to express commutative Frobenius algebras.

Definition 3.43 (graph)**.** Let $\mathcal{F} \coloneqq \langle a, \mu, \eta, \delta, \epsilon \rangle$ be a commutative Frobenius algebra in a symmetric monoidal category. μ, η, δ, ϵ, structural arrows of the symmetric monoidal category, their composite and their product are called **$\mathcal{F}$-graphs**.

The latter definition of a commutative Frobenius algebra immediately induces an important theorem about $\mathcal{F}$-graphs. It states these $\mathcal{F}$-graphs are determined by topological properties of their graphical expression.

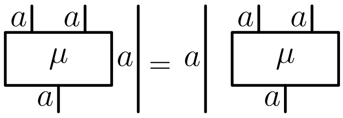
Theorem 3.44 ([19])**.** *Connected $\mathcal{F}$-graphs with the same number of inputs, the same number of outputs and the same number of loops are the same arrows where the number of loops is the maximum number of wires we can remove without destroying their connection.*

Example 3.45. The following equation holds for any Frobenius algebra. The readers can check its correctness by counting the numbers of inputs, outputs and loops.



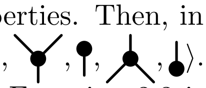
(3.3)

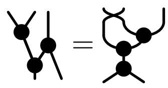
However, the connectedness condition implies the following equation doesn't always true.



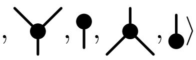
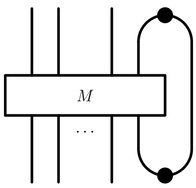
(3.4)

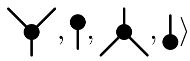
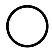
Indeed, Example 3.35 is a counter example.

Since all wires of $\mathcal{F}$-graphs are labelled by the Frobenius object, we can omit these labels. Besides, because of Theorem 3.44, we can also remove labels of boxes without any confusion as long as we keep their topological properties. Then, in the following, we express a Frobenius algebra $\langle a, \mu, \eta, \delta, \epsilon \rangle$ as $\langle a,$  $\rangle$. We sometimes omit a Frobenius object a. Using this notation, Equation 3.3 is rewritten as follows.

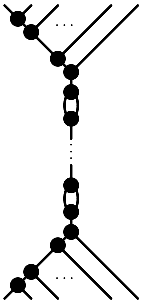


A CFA in **FdHilb** gives operations of a vector space.

Proposition 3.46 ([9])**.** *For any CFA* $\langle \mathcal{H},$  $\rangle$ *and arrow* $M : V \otimes \mathcal{H} \to W \otimes \mathcal{H}$ *in* **FdHilb**,  *is the partial trace of* M*.*

Proposition 3.47 ([9])**.** *For any CFA* $\langle \mathcal{H},$  $\rangle$ *in* **FdHilb**,  $= \mathrm{Tr}\Big(\,\big|\,\Big) = \dim \mathcal{H}$.

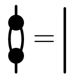
As a straightforward consequence of Theorem 3.44, a connected $\mathcal{F}$-graph has a normal form.

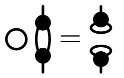


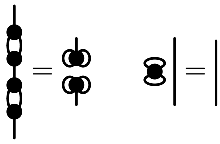
Note that a normal form uses neither nor . It consists of three parts. The uppermost part gathers all inputs into a wire using . The centre part is made up of loops . The numbers of its inputs and outputs are fixed to one. In contrast to the uppermost part, the lowermost part makes all outputs from a wire by .

Since arrows in a well-formed equation have the same domains and the same codomains, any connected $\mathcal{F}$-graph of a CFA has the unique number of inputs and outputs. Then, the uppermost and lowermost parts of the normal form of an $\mathcal{F}$-graph are unique. However, the number of loops of an $\mathcal{F}$-graph is indefinite. The fact allows us to classify CFAs using their loops.

Definition 3.48 (Special, Anti-special, Intermediate Special)**.** A commutative Frobenius algebra $\langle$, , , $\rangle$ is **special**, **anti-special** and **intermediate special** when Equation (3.5), Equation (3.6) and Equations (3.7) hold, respectively.

 (3.5)

 (3.6)

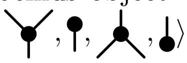
 (3.7)

Notation 3.49. Emphasising difference between classes, we use white dots , black dots and white dots with central black dots to indicate special commutative Frobenius algebras (SCFAs), anti-special commutative Frobenius algebras (ACFAs) and intermediate special commutative Frobenius algebras (IS-CFAs), respectively.

These classes are meaningful. The following examples show the definitions are not empty.

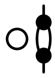
Example 3.50. $\mathcal{G}_2$ in Example 3.41 is an SCFA. Indeed,

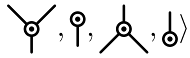
 $= (|0\rangle\langle 00| + |1\rangle\langle 11|)(|00\rangle\langle 0| + |11\rangle\langle 1|) = |0\rangle\langle 0| + |1\rangle\langle 1| =$

Example 3.51. A Frobenius object $\mathbb{C}^2$ has another Frobenius algebra that is anti-special. $\mathcal{W}_2 := \langle \mathbb{C}^2,$  $\rangle$ defined as follows is an ACFA.

 $:= |0\rangle\langle 01| + |0\rangle\langle 10| + |1\rangle\langle 11|$  $:= |1\rangle$

 $:= |00\rangle\langle 0| + |01\rangle\langle 1| + |10\rangle\langle 1|$  $:= \langle 0|$

 $= 2(|0\rangle\langle 01| + |0\rangle\langle 10| + |1\rangle\langle 11|)(|00\rangle\langle 0| + |01\rangle\langle 1| + |10\rangle\langle 1|) = 4|0\rangle\langle 1| =$ 

Example 3.52. Another Frobenius object gives an example of an ISCFA. The following $\mathcal{I} := \langle \mathbb{C}^3,$  $\rangle$ is intermediate special.

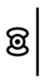
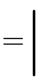
 $:= |0\rangle\langle 01| + |0\rangle\langle 10| + |1\rangle\langle 11| + |2\rangle\langle 22|$  $:= |1\rangle + |2\rangle$

 $:= |00\rangle\langle 0| + |01\rangle\langle 1| + |10\rangle\langle 1| + |22\rangle\langle 2|$  $:= \langle 0| + \langle 2|$

We have to check that ISCFA conditions (3.7) hold.

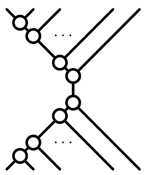

$$\begin{aligned} &= (|0\rangle\langle 01| + |0\rangle\langle 10| + |1\rangle\langle 11| + |2\rangle\langle 22|)(|00\rangle\langle 0| + |01\rangle\langle 1| + |10\rangle\langle 1| + |22\rangle\langle 2|) \\ &= 2|0\rangle\langle 1| + |2\rangle\langle 2| \end{aligned}$$

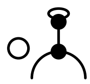
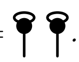
 $= (2|0\rangle\langle 1| + |2\rangle\langle 2|)(2|0\rangle\langle 1| + |2\rangle\langle 2|) = |2\rangle\langle 2| =$ 

 $= ((\langle 0| + \langle 2|)|2\rangle\langle 2|(|1\rangle + |2\rangle)) \otimes 1_{\mathbb{C}^3} = 1_{\mathbb{C}^3} =$ 

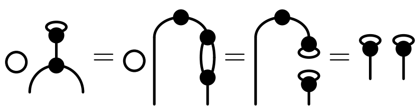
Using the conditions of each class, we can redefine a normal form of an $\mathcal{F}$-graph.

Proposition 3.53 ([9])**.** *Any connected $\mathcal{F}$-graph of an SCFA $\mathcal{F}$ is equal to the following graph.*

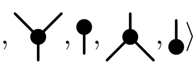


Proposition 3.54 ([9])**.** *For any ACFA,*  $=$ .

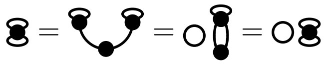
Proof.



□

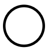
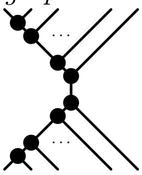
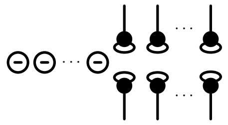
Proposition 3.55 ([9])**.** *Let $\langle \mathcal{H},$*  *$\rangle$ be an ACFA in* **FdHilb**. *If* $\dim \mathcal{H} > 1$, *then*  $= 0$.

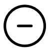
Proof.

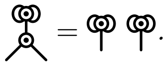


□

Proposition 3.56 ([9])**.** *In* **FdHilb***, any connected $\mathcal{F}$-graph of an ACFA $\mathcal{F}$ is equal to one of the following graphs.*

1. 0 *2.*  *3.*  *4.* 

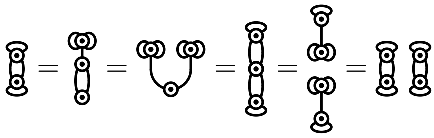
where  *is an arrow such that*  *is equal to* $1_{\mathbb{C}}$*, that is, an empty line.*

Lemma 3.57. *For any ISCFA,* *.*

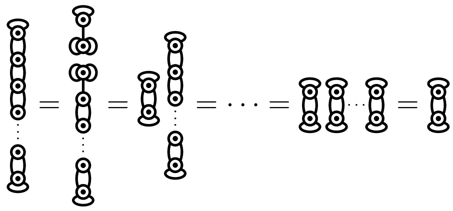
Proof. See Proposition 3.54. □

Lemma 3.58. *Any connected $\mathcal{F}$-graph of an ISCFA $\mathcal{F}$ whose numbers of inputs and outputs are zero, and number of loops is larger than two is equal to* *. Moreover, if $\mathcal{F}$ is in* **FdHilb***,*  *is* 0 *or* 1*.*

Proof.

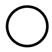


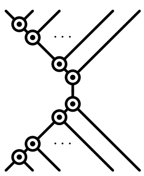
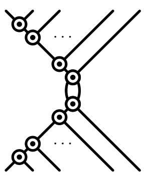
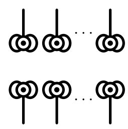
In **FdHilb**, it concludes  is 0 or 1. Besides, $n+4$ loops can be divided to $n+3$ and 3 loops where $0 \leq n \in \mathbb{N}$.



□

Proposition 3.59. *In* **FdHilb***, any connected $\mathcal{F}$-graph of an ISCFA $\mathcal{F}$ is equal to one of the following graphs.*

1. 0 *2.* 1 *3.* 

4.  *5.*  *6.* 

Chapter 4

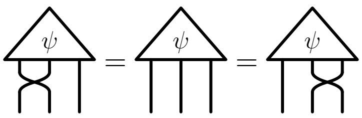
Quantum States and CFAs

In this chapter, we connect the previous two chapters. CFAs in **FdHilb** have strong correspondence to some entangled states of tripartite quantum systems. Moreover, SLOCC equivalence classes of three qubits, described in the last of Chapter 2, can be interpreted as classes of CFAs on $\mathbb{C}^2$ via the correspondence. This interpretation also can be used for three qutrits.

4.1 Quantum States and CFAs

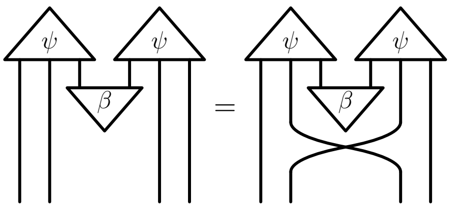
There are many kinds of quantum systems. Here, we focus on tripartite systems consisting of the same kind of systems, e.g. three qubits, three qutrits, etc. Some states of these systems are not influenced by an exchange of a role of each system. These states, called symmetric states, are important, because we can operate them without distinguishing component systems. To connect CFAs, we impose a restriction on symmetric states.

Definition 4.1 (Symmetric)**.** A **symmetric** state is a state $|\psi\rangle$ subject to the following equation.



(4.1)

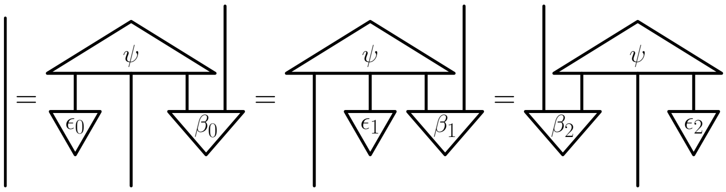
Moreover, a state is **strongly symmetric** if it is symmetric and there is $\langle\beta| : \mathcal{H} \otimes \mathcal{H} \to K$ such that the following equation holds.



(4.2)

Another important property of states is SLOCC maximal. Recall the preorder $\geq_{SLOCC}$. SLOCC maximal states are maximal for this preorder. That is, a state $|\psi\rangle$ is SLOCC maximal when for any state $|\phi\rangle$, if $|\phi\rangle$ can be converted to $|\psi\rangle$ via SLOCC, then the reverse conversion is possible.

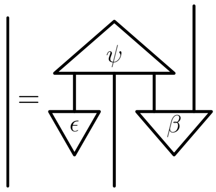
Definition 4.2 (Strongly SLOCC Maximal)**.** A state is **strongly SLOCC maximal** if there are $\langle\beta_0|, \langle\beta_1|, \langle\beta_2| : \mathcal{H}\otimes\mathcal{H} \to \mathbb{C}$ and $\langle\epsilon_0|, \langle\epsilon_1|, \langle\epsilon_2| : \mathcal{H} \to \mathbb{C}$ such that the following equation holds.



(4.3)

The above definition needs many linear functions. However, for symmetric states, the definition can be rewritten more simply.

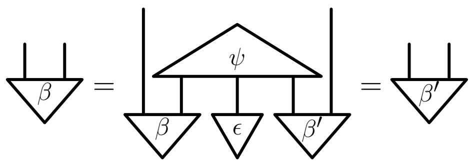
Proposition 4.3 ([9])**.** *A symmetric state is strongly SLOCC maximal, if and only if, there are* $\langle\beta| : \mathcal{H}\otimes\mathcal{H} \to \mathbb{C}$ *and* $\langle\epsilon| : \mathcal{H} \to \mathbb{C}$ *making the following equation true.*



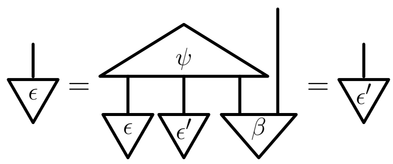
(4.4)

Definition 4.4 (Frobenius state)**.** A state is called a **Frobenius** state when it is strongly symmetric and strongly SLOCC maximal for the same $\langle\beta| : \mathcal{H}\otimes\mathcal{H} \to \mathbb{C}$. That is, a Frobenius state is a state $|\psi\rangle$ with $\langle\beta| : \mathcal{H}\otimes\mathcal{H} \to \mathbb{C}$ and $\langle\epsilon| : \mathcal{H} \to \mathbb{C}$ such that equations (4.2) and (4.4) hold. We call $\langle|\psi\rangle, \langle\beta|, \langle\epsilon|\rangle$ a **Frobenius trio**.

Remark. Even if a Frobenius state is fixed, an associated Frobenius trio is not necessarily unique. However, given a state and another component of a Frobenius trio, the other is uniquely determined. Indeed,



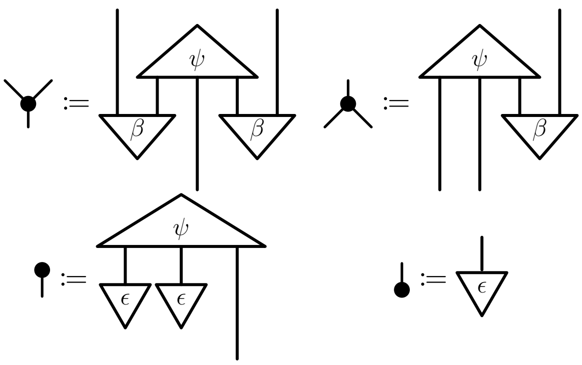
(4.5)



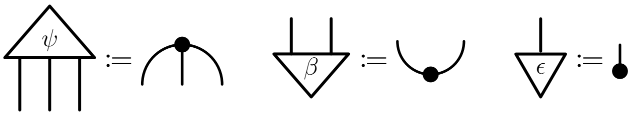
(4.6)

Now, we are ready to show connection between quantum states and commutative Frobenius algebras.

Theorem 4.5 ([9])**.** *Let* $\mathcal{H}$ *be an object of* **FdHilb**. *The Frobenius trios on* $\mathcal{H}$ *are isomorphic to the CFAs on* $\mathcal{H}$. *An isomorphism is given as*



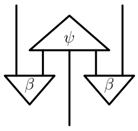
and



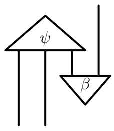
The readers may notice that the strongly SLOCC maximal condition is none other than the unit and counit conditions. Similarly, the symmetric condition leads the induced algebra to be commutative.

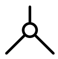
4.2 SLOCC Equivalence Classes of Qubits and Classes of CFAs

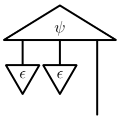
There are six SLOCC equivalence classes in three qubits, but classes that include SLOCC maximal states are just two (Figure. 2.1). Well-known representatives of them, namely $|GHZ\rangle$ and $|W\rangle$ are both Frobenius states. CFAs $\mathcal{G}_2$ and $\mathcal{W}_2$ in Example 3.41 and Example 3.51 are isomorphic to Frobenius trios $\langle|GHZ\rangle, \langle 00| + \langle 11|, \langle 0| + \langle 1|\rangle$ and $\langle |W\rangle, \langle 01| + \langle 10|, \langle 0|\rangle$, respectively. Indeed,

 $= ((\langle 00| + \langle 11|) \otimes I \otimes (\langle 00| + \langle 11|))(I \otimes (|000\rangle + |111\rangle) \otimes I)$

$= |0\rangle\langle 00| + |1\rangle\langle 11| =$ 

 $= (I \otimes I \otimes (\langle 00| + \langle 11|))((|000\rangle + |111\rangle) \otimes I)$

$= |00\rangle\langle 0| + |1\rangle\langle 11| =$ 

 $= ((\langle 0| + \langle 1|) \otimes (\langle 0| + \langle 1|) \otimes I)(|000\rangle + |111\rangle)$

$= |0\rangle + |1\rangle =$ 

 $= \langle 0| + \langle 1| =$ 

As shown in Example 3.50 and Example 3.51, these CFAs are an SCFA and an ACFA.

There is essentially no other kind of CFA on $\mathbb{C}^2$. It means any Frobenius state induces one of an SCFA and an ACFA. These classes of CFAs give another description about SLOCC classification of Frobenius states. More precisely, the following theorem shows the classification.

Theorem 4.6 ([9])**.** *A Frobenius state of three qubits is SLOCC equivalent to $|GHZ\rangle$ or $|W\rangle$, if and only if, the state induces SCFA or ACFA, respectively.*

4.3 SLOCC Equivalence Classes of Qutrits and Classes of CFAs

Unlike three qubits, there are uncountably infinite SLOCC equivalence classes in three qutrits. However, almost all SLOCC equivalence classes don't include any symmetric strongly SLOCC maximal state, much less Frobenius states.

Lemma 4.7 ([17])**.** *In three qubits, five SLOCC equivalence classes include symmetric and strongly SLOCC maximal state. The others don't.*

Representatives of these five SLOCC equivalence classes are the following.

1. $|\mathcal{G}\rangle := |000\rangle + |111\rangle + |222\rangle$
2. $|\mathcal{W}\rangle := |002\rangle + |020\rangle + |200\rangle + |011\rangle + |101\rangle + |110\rangle$
3. $|\mathcal{I}\rangle := |001\rangle + |010\rangle + |100\rangle + |222\rangle$
4. $|s_2\rangle := |000\rangle + |012\rangle + |021\rangle + |102\rangle + |120\rangle + |201\rangle + |210\rangle$
5. $|s_3\rangle := |012\rangle + |021\rangle + |102\rangle + |120\rangle + |201\rangle + |210\rangle$

The number of SLOCC equivalence classes including Frobenius states is much lower. The following lemma gives us a way to examine whether an SLOCC equivalence class contains any Frobenius state. It is a three qutrits version of the theorem in [23].

Lemma 4.8 ([17])**.** *Symmetric states of three qutrits $|\psi\rangle$ and $|\phi\rangle$ are SLOCC equivalent, if and only if, there is an invertible linear function L on $\mathbb{C}^3$ such that $|\psi\rangle = L^{\otimes 3}|\phi\rangle$.*

Proof. This is a summary. For the details, see Appendix A.1. A proof is similar to the original one. Since $|\psi\rangle$ and $|\phi\rangle$ are SLOCC equivalent and both symmetric, there is an invertible matrix B such that $|\psi\rangle = (B \otimes B^{-1} \otimes I)|\phi\rangle$. The Jordan normal form of B consists of one, two or three Jordan blocks. In any case, there is an invertible operator S such that $|\psi\rangle = S^{\otimes 3}|\psi_0\rangle$ where $|\psi_0\rangle$ is one of $|000\rangle$, $|000\rangle + |111\rangle$, $|001\rangle + |010\rangle + |100\rangle$, $|\mathcal{G}\rangle$, $|\mathcal{W}\rangle$ and $|\mathcal{I}\rangle$. These states are SLOCC inequivalent each other. Then, $|\psi\rangle$ and $|\phi\rangle$ can interconvertible with a symmetric operation via $|\psi_0\rangle$. □

Corollary 4.9 ([17])**.** *Any symmetric state SLOCC equivalent to a Frobenius state is a Frobenius state.*

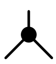
Checking a representative of each SLOCC equivalence class, we learn that there are just three SLOCC inequivalent Frobenius states. They give CFAs on $\mathbb{C}^3$ through Theorem 4.5.

The followings and $\mathcal{I}$ in Example 3.52 are commutative Frobenius algebra whose object is $\mathbb{C}^3$.

 $:= |0\rangle\langle 00| + |1\rangle\langle 11| + |2\rangle\langle 22|$  $:= |0\rangle + |1\rangle + |2\rangle$

 $:= |00\rangle\langle 0| + |11\rangle\langle 1| + |22\rangle\langle 2|$  $:= \langle 0| + \langle 1| + \langle 2|$

 $:= |0\rangle\langle 02| + |0\rangle\langle 11| + |0\rangle\langle 20| + |1\rangle\langle 12| + |1\rangle\langle 21| + |2\rangle\langle 22|$  $:= |2\rangle$

 $:= |00\rangle\langle 0| + |01\rangle\langle 1| + |10\rangle\langle 1| + |02\rangle\langle 2| + |11\rangle\langle 2| + |20\rangle\langle 2|$  $:= \langle 0|$

We call the above two CFAs $\mathcal{G}$ and $\mathcal{W}$. $\mathcal{G}$, $\mathcal{W}$ and $\mathcal{I}$ are isomorphic to $\langle|\mathcal{G}\rangle, \langle 00|+\langle 11|+\langle 22|, \langle 0|+\langle 1|+\langle 2|\rangle$, $\langle|\mathcal{W}\rangle, \langle 02|+\langle 11|+\langle 20|, \langle 0|\rangle$ and $\langle|\mathcal{I}\rangle, \langle 01|+\langle 10|+\langle 22|, \langle 0|+\langle 2|\rangle$. Moreover, as the colours of dots provides, they are special, anti-special and intermediate special. It shows classes of CFAs on $\mathbb{C}^3$ also have correspondence to SLOCC equivalence classes in three qutrits, like three qubits.

Theorem 4.10 ([17])**.** *A Frobenius state of three qutrits is SLOCC equivalent to $|\mathcal{G}\rangle$, $|\mathcal{W}\rangle$ or $|\mathcal{I}\rangle$, if and only if, the state induces SCFA, ACFA or ISCFA, respectively.*

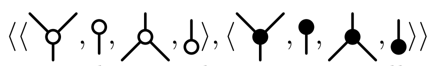
Chapter 5

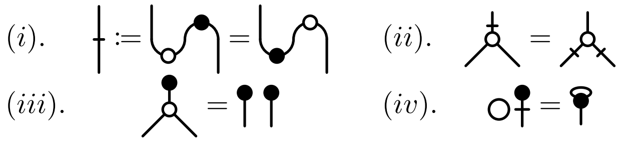
Graphical Calculus for Qutrits

We present a new graphical calculus for qutrits, G/W/I calculus. The calculus is based on GHZ/W calculus, a graphical calculus for qubits. In the beginning of this chapter, we explain GHZ/W calculus briefly. Next, we show the definition of G/W/I calculus and properties of them. Interestingly, although this calculus is an extension of GHZ/W calculus, a property of GHZ/W calculus on $\mathbb{C}^2$ doesn't hold in our calculus.

5.1 GHZ/W calculus

Theorem 4.6 means the SCFAs and the ACFAs on $\mathbb{C}^2$ represent all Frobenius states of three qubits. Interestingly, if we take a CFA from each class with some conditions, then they form a graphical calculus that is able to express not only three, but also n qubits.

Definition 5.1. Let  be a pair of an SCFA and an ACFA with the same Frobenius object a. We call it a **GHZ/W pair (on a)** when it satisfies the following axioms :



Example 5.2. As the name suggests, $\langle \mathcal{G}_2, \mathcal{W}_2 \rangle$ is a GHZ/W pair on $\mathbb{C}^2$.

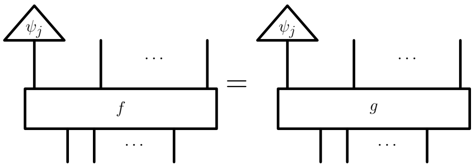
The axioms allow us to prove various equations. We will see several examples of them in Proposition 5.7. Before that, we pay attention to a Frobenius object of a GHZ/W pair. We are mainly interested in an object in **FdHilb** such as $\mathbb{C}^2$ and $\mathbb{C}^3$. Since their dimensions are finite, it is possible to prove equations on them using their bases.

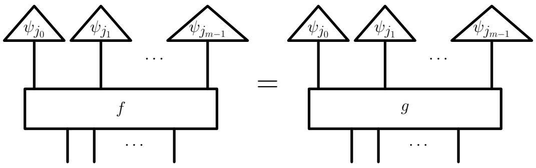
Definition 5.3. Let a be an object. A set $\{\psi_j : e \to a\}_{j \in J}$ is a **plugging set for** a when for any object b and arrows $f, g : a \to b$, the followings are equivalent.

1. $f = g$
2. For all $j \in J$, $f \circ \psi_j = g \circ \psi_j$

Proposition 5.4 ([10])**.** *Let a be an object, $\{\psi_j\}_{j \in J}$ be a plugging set for a and $f, g : a^{\square m} \to a^{\square n}$ be arrows. The followings are equivalent.*

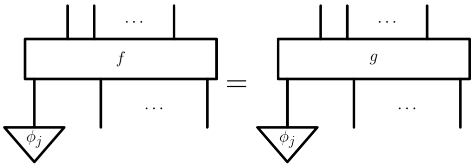
1. $f = g$

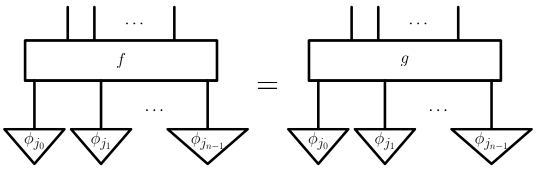
2. *For all $j \in J$,* 

3. *For all $j_0, j_1, \ldots, j_{m-1} \in J$,* 

Moreover, there exists a set $\{\phi_j : a \to e\}_{j \in J}$ making the followings equivalent.

1. $f = g$

2. *For all $j \in J$,* 

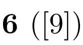
3. *For all $j_0, j_1, \ldots, j_{n-1} \in J$,* 

We also refer to a plugging set for a as a set $\{\phi_j\}_{j \in J}$.

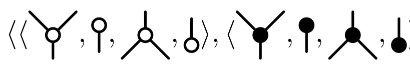
Remark. Although an equation proved using just the axioms of a GHZ/W pair holds in any GHZ/W pair, an equation proved using a plugging set is not always true. We show an example of it in Section 5.3.

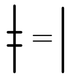
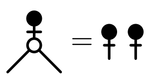
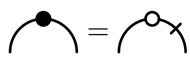
A GHZ/W pair provides a plugging set for $\mathbb{C}^2$.

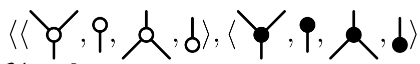
Proposition 5.5 ([9]). *If the dimension of $\mathcal{H}$ is larger than one, then* *. In particular,*  *is a plugging set for $\mathbb{C}^2$.*

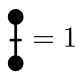
Corollary 5.6 ([9]).  *is a plugging set for $\mathbb{C}^2$.*

Now, we give several graphical equations as promised above. Note the equation 7 in the following proposition is specific to GHZ/W pairs on $\mathbb{C}^2$, since it is proved using a plugging set for $\mathbb{C}^2$.

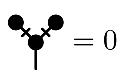
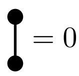
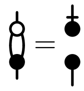
Proposition 5.7 ([9, 18]). *Let*  *be a GHZ/W pair on $\mathcal{H}$.*

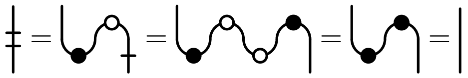
1.  2.  3. 

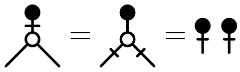
Suppose  *is a GHZ/W pair on $\mathcal{H}$ in* **FdHilb** *and* $\dim \mathcal{H} > 0$.

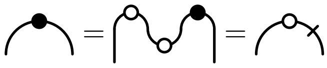
4. 

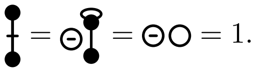
Moreover, suppose $\dim \mathcal{H} > 1$.

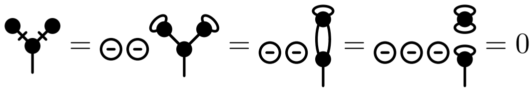
5.  6.  7. *If $\mathcal{H} = \mathbb{C}^2$, then* 

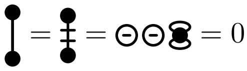
Proof. 1. 

2. 

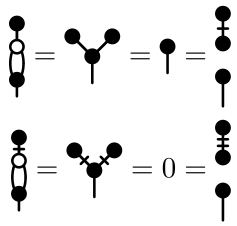
3. 

4. 

5. 

6. 

7. Plugging  and  into the inputs,



□

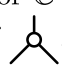
The axioms of a GHZ/W pair consist of only four equations. However, it is shown in the above proposition that the axioms are enough to prove various equations. Moreover, given an SCFA or an ACFA on $\mathbb{C}^2$, the axioms can determine the GHZ/W pair on $\mathbb{C}^2$ including the CFA.

Theorem 5.8 ([9])**.** *A GHZ/W pair on $\mathbb{C}^2$ is unique up to change of a basis. In particular, when a component of a GHZ/W pair on $\mathbb{C}^2$ is fixed, the other is uniquely determined up to permutation of bases.*

A GHZ/W pair has a power to express any state of qubits with the help of single qubits.

Theorem 5.9 ([9])**.** *Using a GHZ/W pair on $\mathbb{C}^2$ and states of single qubits, we can write any state of any composite system of qubits.*

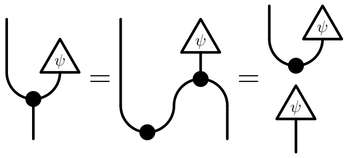
5.2 Graphical Calculus for Qutrits

Now, we move from the two dimensional complex space to the three dimensional complex space. The definition of a GHZ/W pair is independent from the dimension of the base space. Indeed, a GHZ/W pair on $\mathbb{C}^3$ gives a plugging set for $\mathbb{C}^3$ as discussed in the next section. However, this set is a bit complicated. Unlike for $\mathbb{C}^2$, a GHZ/W pair doesn't naturally provide a plugging set for $\mathbb{C}^3$. Recall a GHZ/W pair on $\mathbb{C}^2$ gives a plugging set as the copiable points of .

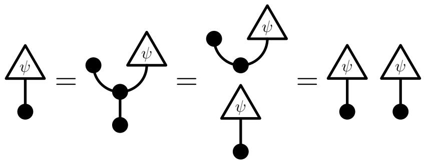
Definition 5.10. A **copiable point** or **copiable vector** of $f : a \to a\Box a$ is a vector $\psi : e \to a$ such that $f \circ \psi \circ \lambda_e = \psi\Box\psi$. Similarly, a **cocopiable functional** of $g : a\Box a \to a$ is a functional $\phi : a \to e$ such that $\phi \circ g = \lambda_e \circ \phi\Box\phi$.

Proposition 5.11. *Let* ⟨ , , , ⟩ *be a CFA and* $|\psi\rangle$ *be a copiable vector of* . *Then,* = . *Moreover, if* $|\psi\rangle \neq 0$, *then* $= 1$.

Proof.



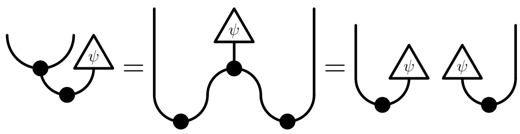
Furthermore,



Then, is 0 or 1. If $= 0$, then = = = $= 0$. □

Proposition 5.12. *Let* ⟨ , , , ⟩ *be a CFA and* $: e \to a$ *be an arrow.* *is a copiable vector of* , *if and only if,* *is a cocopiable functional of* .

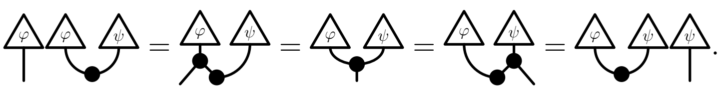
Proof. Assume is copiable. Then,



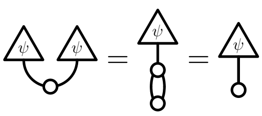
Similarly, noting that = , the converse also holds. □

Proposition 5.13. *Let* ⟨ , , , ⟩ *be a CFA and* , *be a copiable vector of* *such that* $\neq 0$. *Then,* = . *Moreover, if the CFA is special, then* = $= 1$.

Proof.



Assume a CFA is special.



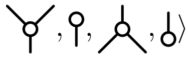
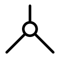
$= 1$.

□

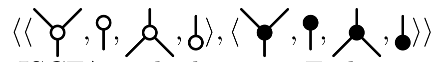
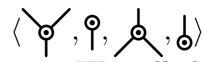
The copiable elements form a basis of the space spanned by them.

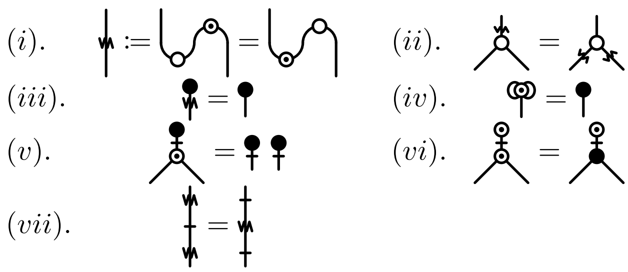
Lemma 5.14. *Let $\mathcal{H}$ be an object and $f : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$ be an arrow of* $\mathbf{Vect}_{\mathbb{C}}$*. The copiable vectors of f are linearly independent.* □

If the number of the copiable vectors is equal to the dimension of the base space, then they form a basis for the space. The set of copiable vectors of  is an example of it.

Theorem 5.15 ([11])**.** *Let* ⟨$\mathcal{H}$, ⟩ *be an SCFA in* **FdHilb**. *The copiable vectors of*  *forms a plugging set for $\mathcal{H}$.*

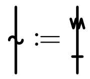
Now, we study a graphical calculus especially for $\mathbb{C}^3$ using CFAs. Recall a GHZ/W pair arises from the classification of SLOCC equivalence of Frobenius states on $\mathbb{C}^2$. It is natural to extend a GHZ/W pair using the classification on $\mathbb{C}^3$, namely, an SCFA, an ACFA and an ISCFA.

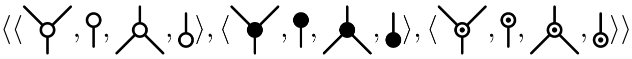
Definition 5.16. Let ⟨⟩ and ⟨⟩ be a GHZ/W pair and an ISCFA with the same Frobenius object a. We call them a **G/W/I trio (on** a**)** when it satisfies the following axioms :

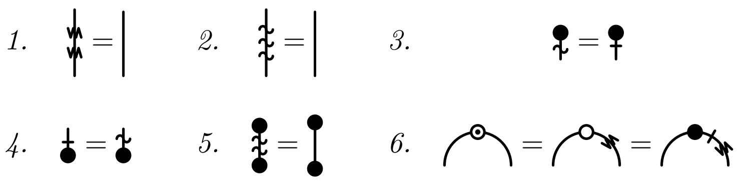


Example 5.17. $\langle \mathcal{G}, \mathcal{W}, \mathcal{I} \rangle$ is a G/W/I trio on $\mathbb{C}^3$.

Notation 5.18. For simplicity, we give syntactic sugar for G/W/I calculus, named **wave notation**.



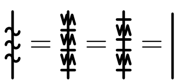
Proposition 5.19. *Let* ⟨⟨⟩⟩ *be a G/W/I trio on $\mathcal{H}$.*

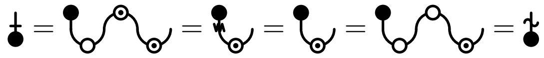


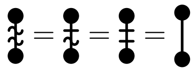
Suppose the G/W/I trio is in **FdHilb**.

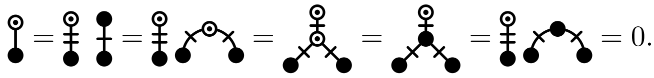
7. *If* $\dim \mathcal{H} > 0$*, then*  $= 1$ 8. *If* $\dim \mathcal{H} > 1$*, then*  $= 0$

Proof. 1., 3. , 6. and 7. are straightforward results of Proposition 5.7 and the axioms of G/W/I calculus.

2. 

4. 

5. 

8. 

□

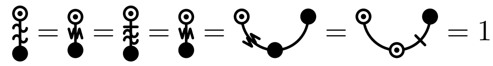
As mentioned above, a G/W/I trio naturally provides a basis for three dimensional space, which is the copiable vectors of .

Proposition 5.20. *If the dimension of $\mathcal{H}$ is larger than two, $\{\ ,\ ,\ \}$ spans a three dimensional space.*

Proof. $\nsim$ is a straightforward result of Propositions 5.5 and 5.19. $\nsim$ and $\nsim$ follows from $\nsim$ and $=$. Because of Theorem 5.15 and the fact $\{\ ,\ ,\ \}$ are copiable vectors of , $\{\ ,\ ,\ \}$ are linearly independent. □

Proposition 5.21. *The followings are plugging sets for $\mathbb{C}^3$.*

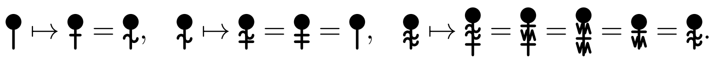
Proof. 1. and 2. are easy. The following equation

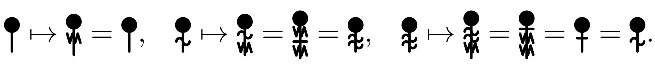


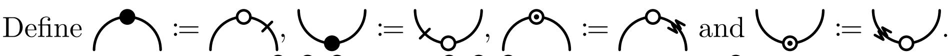
follows from Proposition 5.11. Since $= = 0$, $\neq 0$ and $\neq 0$ imply both and are linearly independent from $\{\ ,\ \}$. □

Theorem 5.22. *Let $\mathcal{F}$ be either an SCFA on $\mathbb{C}^3$, an ACFA or an ISCFA. A G/W/I trio on $\mathbb{C}^3$ that includes $\mathcal{F}$ is unique up to permutation and inverse of bases.*

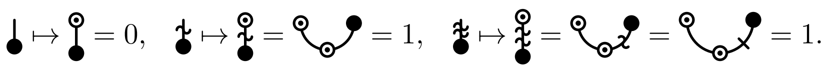
Proof. 1. Assume $\mathcal{F} = \langle\ ,\ ,\ ,\ \rangle$ is an SCFA. Take the copiable vectors of and name them , and . Then, define and as follows.



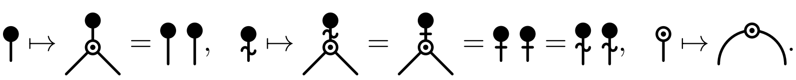


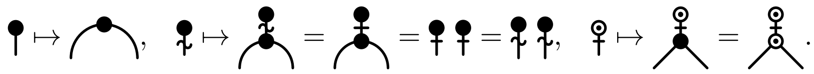


To use other bases, $\{\ ,\ ,\ \}$ and $\{\ ,\ ,\ \}$, we determine as follows.



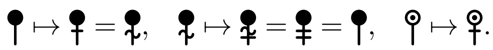
These bases determine and .



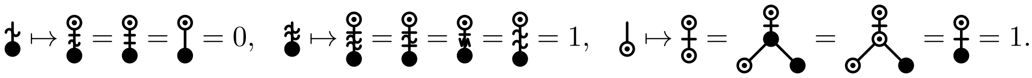


Then, the other components ⟨ := , , , := ⟩ , ⟨ := , , , := ⟩ are determined.

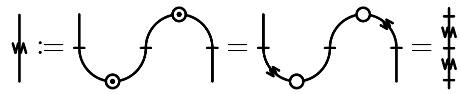
2. Assume $\mathcal{F} = \langle$, , , $\rangle$ is an ISCFA. Take the copiable vectors , of and , of . Notice there is no any other choice of them, and then no any permutation. The following mapping defines .



where is defined as follows.

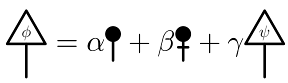


Then, is determined.

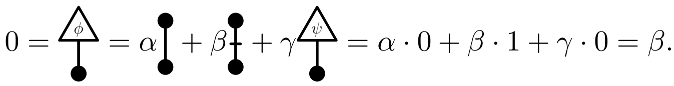


Now, we can get , and then the associated SCFA is uniquely determined.

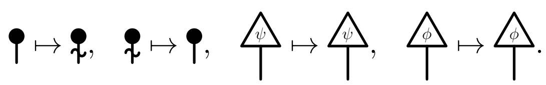
3. Assume $\mathcal{F} = \langle$, , , $\rangle$ is an ACFA. Let $\mathcal{S} = \langle$, , , $\rangle$ and $\mathcal{S}' = \langle$, , , $\rangle$ be SCFAs, and $\mathcal{I}$, $\mathcal{I}'$ be ISCFAs. Suppose $\langle \mathcal{S}, \mathcal{F}, \mathcal{I} \rangle$ and $\langle \mathcal{S}', \mathcal{F}, \mathcal{I}' \rangle$ are G/W/I trios. Take the copiable vectors , , ψ of , and , , ϕ of . By Theorem 5.15, ϕ can be written as



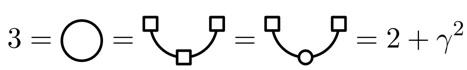
with complex numbers α, β and γ. Plugging into the both sides,



Similarly, $\alpha = 0$, and then $\phi \sim \psi$. Therefore, of $\langle \mathcal{S}, \mathcal{F}, \mathcal{I} \rangle$ and $\langle \mathcal{S}', \mathcal{F}, \mathcal{I}' \rangle$ are the same one defined as follows.



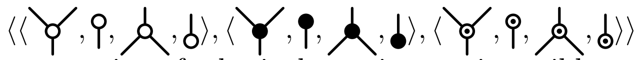
Equivalently, = := . Recall that the result of application of to any copiable vector of is one, and = + + ϕ = + + $\gamma\psi$.

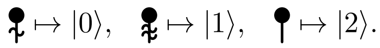


Therefore, $\gamma = \pm 1$. It means $\mathcal{S}$ is uniquely determined up to inverse of a basis.

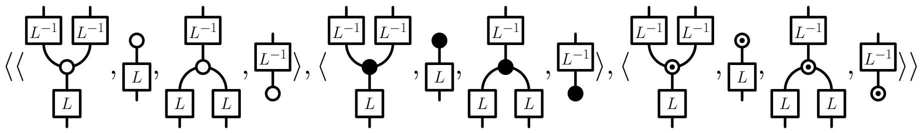
□

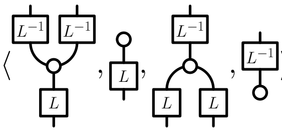
Theorem 5.23. *For any G/W/I trio on $\mathbb{C}^3$, there is an invertible matrix on $\mathbb{C}^3$ mapping it to a canonical G/W/I trio $\langle \mathcal{G}, \mathcal{W}, \mathcal{I} \rangle$.*

Proof. Let  be a G/W/I trio. The following mapping of a basis determines an invertible matrix L.



L induces another G/W/I trio as follows.



 is obviously $\mathcal{G}$, and then the above G/W/I trio is $\langle \mathcal{G}, \mathcal{W}, \mathcal{I} \rangle$.

□

Theorem 5.24. *Using a G/W/I trio and states of single qutrits, we can write any state of any composite system of qutrits.*

This theorem is proved by a similar way to the proof of Theorem 5.9. It is constructed of the following two lemmas.

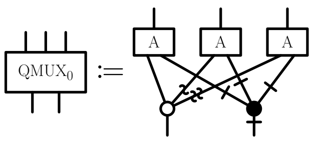
Lemma 5.25. *Any invertible matrix on $\mathbb{C}^3$ can be represented by a G/W/I trio and states of single qutrits.*

Lemma 5.26. *There is a linear function written using a G/W/I trio and states of single qutrits that maps $|\psi\rangle \otimes |\phi\rangle \otimes |\chi\rangle$ to a state SLOCC equivalent to $|0\psi\rangle + |1\phi\rangle + |2\chi\rangle$ where $|\psi\rangle$, $|\phi\rangle$ and $|\chi\rangle$ are states of single qutrits.*

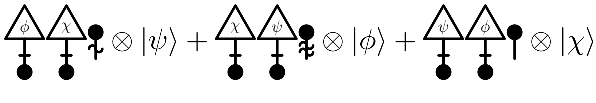
We will prove these lemmas ahead of Theorem 5.24.

Proof of Lemma 5.25. Take a G/W/I trio. There is an invertible matrix leading a canonical G/W/I trio $\langle \mathcal{G}, \mathcal{W}, \mathcal{I} \rangle$ to the G/W/I trio. Then, if we prove that we can write any invertible matrix using a canonical G/W/I trio $\langle \mathcal{G}, \mathcal{W}, \mathcal{I} \rangle$ and states of single qutrits, then it is sufficient for a proof of this lemma. It was proved in [17]. □

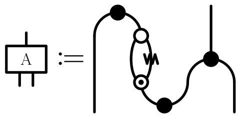
Proof of Lemma 5.26.



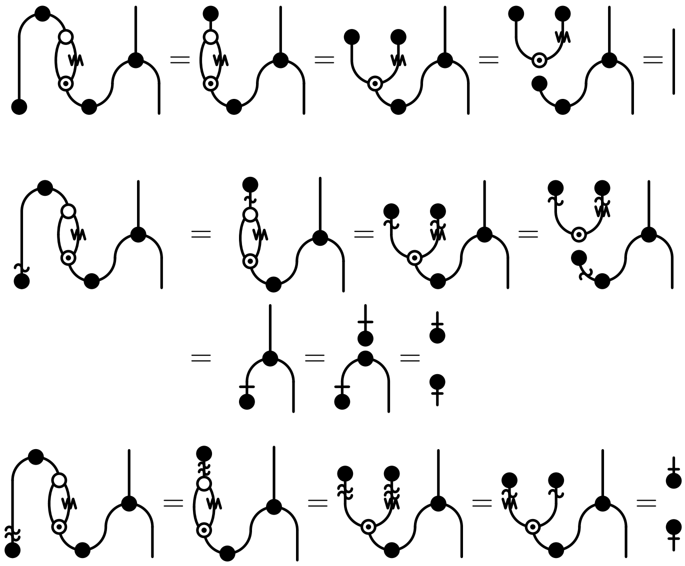
leads $|\psi\rangle \otimes |\phi\rangle \otimes |\chi\rangle$ to



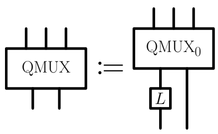
where



To prove it, we plug a basis {, , } into the left output of A.



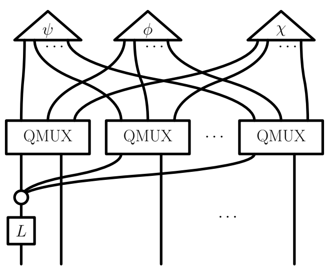
It is shown in Theorem 5.23 that there is a invertible matrix L mapping , and to $|0\rangle$, $|1\rangle$ and $|2\rangle$, respectively. Then,



is a linear function that we need. □

Now, we complete preparations for a proof of Theorem 5.24.

Proof of Theorem 5.24. Any state of a qutrit can be written using and an invertible matrix on $\mathbb{C}^3$. Let $|\psi\rangle$, $|\phi\rangle$ and $|\chi\rangle$ be states of N qutrits. Then,

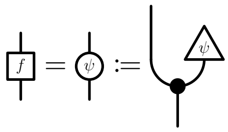


is $|0\psi\rangle + |1\phi\rangle + |2\chi\rangle$ with an appropriate invertible function L. By the induction hypothesis, $|\psi\rangle$, $|\phi\rangle$ and $|\chi\rangle$ can be written graphically. □

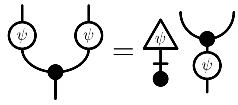
5.3 Embedding of GHZ/W Calculus

Now, we back to study a GHZ/W pair. Recently, it is shown that a GHZ/W pair on $\mathbb{C}^2$ satisfies "distributive law", and then an SCFA and an ACFA can be interpreted as $+$ and $\cdot$, respectively.

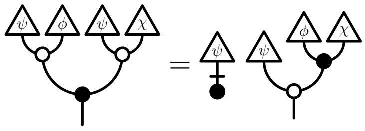
Definition 5.27 (Phase)**.** Let $\langle a,$, , , $\rangle$ be a CFA. An arrow $f : a \to a$ is a **phase** when there is an arrow $\psi : e \to a$ such that



Theorem 5.28 (Distributive Law [10])**.** *For any state $|\psi\rangle$ of a qubit,*

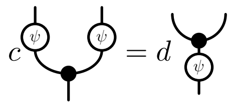


Equivalently, for any states $|\psi\rangle$, $|\phi\rangle$ and $|\chi\rangle$ of qubits,



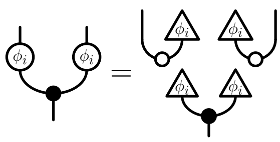
We move to $\mathbb{C}^3$ where we are mainly concerned. Does a GHZ/W pair on $\mathbb{C}^3$ satisfy the distributive law? The answer is no. Moreover, a GHZ/W pair on a space whose dimension is odd doesn't satisfy this law.

Lemma 5.29. *Let $\langle\langle$, , , $\rangle, \langle$, , , $\rangle\rangle$ be a GHZ/W pair on $\mathcal{H}$ in* **FdHilb**. *If* rank $\left(\;\right) > 1$*, then there is a vector $|\psi\rangle$ such that for any $c, d \in \mathbb{C}$, the following equation doesn't hold.*

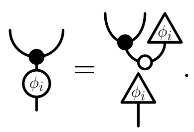


(5.1)

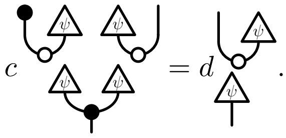
Proof. When $\dim \mathcal{H} = 0, 1, 2$, this lemma obviously holds. Assume $\dim \mathcal{H} > 2$. Take linearly independent copiable vectors $\{|\phi_i\rangle\}_{i=0}^{\dim \mathcal{H}-1}$ of where $|\phi_0\rangle :=$ and $|\phi_1\rangle :=$. The definition of $\{|\phi_i\rangle\}_{i=0}^{\dim \mathcal{H}-1}$ implies for any $i \in \{0, \dots, \dim \mathcal{H} - 1\}$,



and



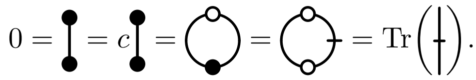
Because rank $\left(\;\right) > 1$, there are at least two numbers $j_0, j_1 \in \{0, \dots, \dim \mathcal{H} - 1\}$ such that $j_0 < j_1$, $\neq 0$ and $\neq 0$. Since we know $=$ $=$ and $=$ $=$ $= 0$, either or both of j_0 and j_1 are bigger than 1. Put $|\psi\rangle := |\phi_{j_1}\rangle$. This vector is a vector that we need. Assume $|\psi\rangle$ satisfies (5.1) with some complex numbers c, d. Take such complex numbers c, d. Since $|\psi\rangle$ make both sides of (5.1) nonzero, c and d are both nonzero. Putting in the left input of both sides, we get



It implies $\neq 0$. Therefore, by Proposition 5.13, $=$. However, it contradicts the definition of $|\psi\rangle$. □

Lemma 5.30. *If the dimension of $\mathcal{H}$ is odd and bigger than* 2, rank $\neq 1$.

Proof. Assume rank $= 1$. Since $=$ $=$ $\neq 0$, $\neq 0$. On the other hand, $=$ $=$ $\neq 0$. They imply there is a nonzero complex number c such that $= c$. Then,



However, there is no linear function on $\mathcal{H}$ such that it is an involution and trace of it is zero. □

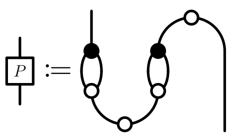
Corollary 5.31. *The distributive law doesn't hold in any GHZ/W pair on* $\mathbb{C}^3$*.*

Remark. Lemma 5.30 also implies {, , } is a plugging set for $\mathbb{C}^3$. They are purely written in a GHZ/W pair, and what they form a plugging set for $\mathbb{C}^3$ is a consequence of the axioms of a GHZ/W pair. From this viewpoint, a GHZ/W pair isn't simply specific to $\mathbb{C}^2$, but it also covers $\mathbb{C}^3$. However, as pointed out above, the plugging set isn't a canonical one. That is, isn't always a cocopiable functional of . Then, this plugging set is a bit hard to use. This is why we refer to a graphical calculus for qubits as a GHZ/W calculus, and define an extension of a GHZ/W pair.

It was shown in [10] that a GHZ/W pair on $\mathbb{C}^2$ satisfies the distributive law, and then rational arithmetic can be encoded regarding an SCFA as multiplication and an ACFA as addition. Since GHZ/W pairs on $\mathbb{C}^3$ and their extensions lack the distributive law, it is not known whether a G/W/I calculus contains rational arithmetic. Although a G/W/I trio on $\mathbb{C}^3$ is an extension of a GHZ/W pair on $\mathbb{C}^2$, is the power of a G/W/I trio less than the power of a GHZ/W pair?

In the rest of this chapter, we will define a projector onto a GHZ/W pair on $\mathbb{C}^2$, and then prove that all equations of a GHZ/W pair on $\mathbb{C}^2$ can be embedded into a G/W/I trio on $\mathbb{C}^3$.

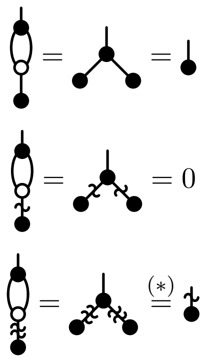
Proposition 5.32. *Let* ⟨⟨ , , , ⟩, ⟨ , , , ⟩, ⟨ , , , ⟩⟩ *be a G/W/I trio on* $\mathbb{C}^3$*.*



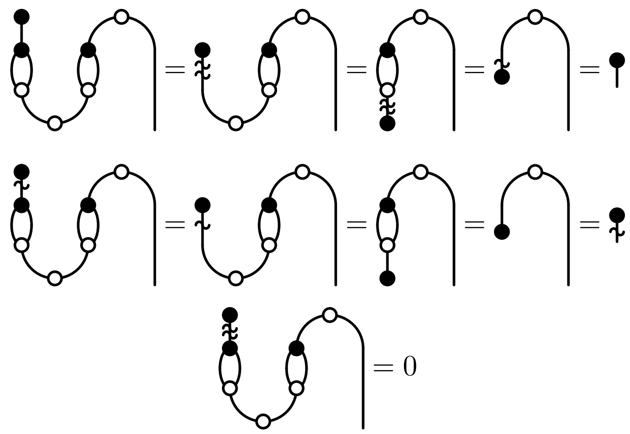
is a projector onto two dimensional space spanned by and . Explicitly, the projector P leads and to themselves, and to 0.

Proof. The following arrow, which is a part of the projector P,

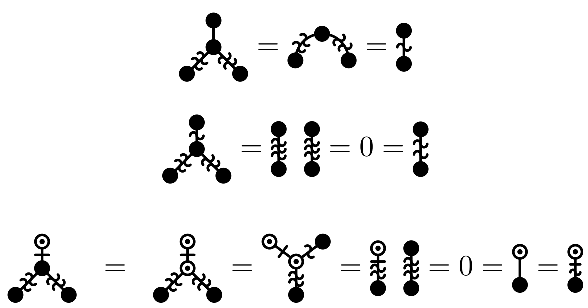
maps , and to , and 0, respectively. To prove this, we plug {, , } to the arrow.



Before giving a proof of the equation (∗), we prove this proposition using a plugging set {, , }.



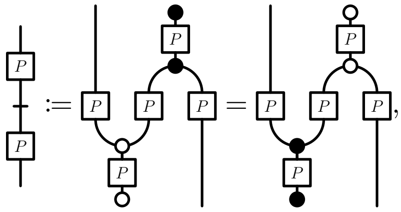
At the last of this proof, we prove the equation (∗) using a plugging set {, , }.



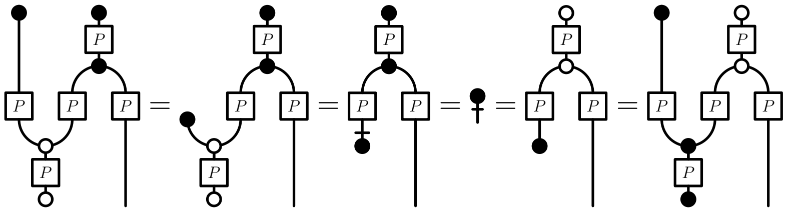
□

Theorem 5.33. *Let f, g be arrows on $\mathbb{C}^2$ consisting of a GHZ/W pair, and f', g' be arrows on $\mathbb{C}^3$ obtained by substituting the projector P for all wires in f and g, respectively. If $f = g$, then $f' = g'$.*

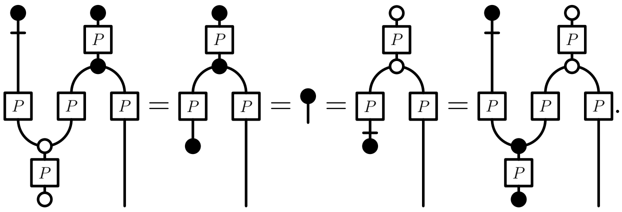
Proof. Any equation on $\mathbb{C}^3$ obtained by replacing all wires of an axiom of a GHZ/W pair or a CFA with  holds. For example,

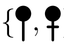


because

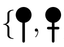
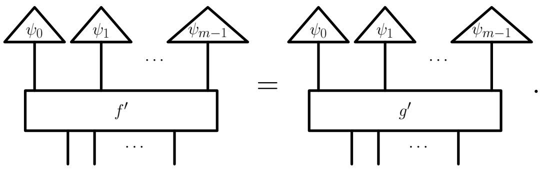


and



Moreover, {} is a plugging set for them. It means the followings are equivalent.

1. $f' = g'$.

2. For any $\psi_0, \dots, \psi_{m-1} \in$ {}, 

If $f = g$, then there are $n \in \mathbb{N}$ and $f_1, \dots, f_{n-1}$ such that $f_i = f_{i+1}$ for any $i \in \{0, \dots, n-1\}$ where $f_0 = f$, $f_n = g$, and $f_i = f_{i+1}$ is an axiom or a consequence of a plugging. Because of the above argument, any axiom and equation by a plugging hold in a G/W/I calculus. □

Therefore, any equation of a GHZ/W pair on $\mathbb{C}^2$ can be encoded using our G/W/I trio on $\mathbb{C}^3$.

Chapter 6

Related Works

As shown in the previous chapter, our calculus is based on GHZ/W calculus, which is mainly for two-dimensional complex space. Since GHZ/W calculus was introduced in [9], it and its extensions have been studied in several papers [15, 25, 18]. For example, using GHZ/W calculus on $\mathbb{C}^2$ with an operation such as the Pauli Z matrix, rational arithmetic can be encoded [10]. Another extension also contains rational arithmetic. GHZ/W calculus on $\mathbb{C}^2$ with an appropriate vector allows us to express complex numbers and perform complex arithmetic operations [14]. Our work is a new kind of extension of GHZ/W calculus, which focuses on another dimension $\mathbb{C}^3$. Through the study of $\mathbb{C}^3$, we found that the distributive law, which is a foundation of the above arithmetic, doesn't hold in GHZ/W calculus on $\mathbb{C}^3$.

Another famous graphical calculus based on commutative Frobenius algebra is the ZX-calculus, which is formed by a pair of complementary observables [7]. The calculus has a lot of application of quantum computing and protocols, such as measurement-based quantum computation [12], and the relation with GHZ/W calculus was shown [8]. However, this calculus also focuses on $\mathbb{C}^2$, and then it hasn't used to study qutrits.

Chapter 7

Conclusion

In this paper, we produced a new graphical calculus for qutrits. This calculus, named G/W/I calculus, is an extension of GHZ/W calculus, which focuses on qubits, and is based on SLOCC equivalence classes of three qubits.

At first, we completed classifying SLOCC equivalence classes of three qutrits by proving that any SLOCC equivalent symmetric states are connected via a symmetric invertible transformation. Although there are infinitely many SLOCC equivalence classes of three qutrits, just three classes contain Frobenius states, which are strongly SLOCC maximal and strongly symmetric states. Based on these classes, we defined G/W/I calculus. After that, we showed several properties of G/W/I calculus on $\mathbb{C}^3$ that GHZ/W calculus on $\mathbb{C}^2$ has. More specifically, the axioms of G/W/I calculus gives a basis of $\mathbb{C}^3$ naturally and determines representatives of three classes, and any state of any composite system of qutrits can be written using G/W/I calculus on $\mathbb{C}^3$ and states of single qutrits. These properties mean a G/W/I calculus on $\mathbb{C}^3$ and the axioms of it have enough power to express calculation for qutrits.

Since the axioms of G/W/I calculus contain the axioms of GHZ/W calculus, G/W/I calculus on $\mathbb{C}^3$ contains GHZ/W calculus on $\mathbb{C}^3$. Then, we also studied GHZ/W calculus on $\mathbb{C}^3$. It was shown in [10], that GHZ/W calculus on $\mathbb{C}^2$ can express rational arithmetic. We studied whether GHZ/W calculus on $\mathbb{C}^3$ has the same property, and found that GHZ/W calculus on an odd-dimensional space doesn't satisfy the distributive law, which is a foundation of the arithmetic. Although the result raised the question whether G/W/I calculus on $\mathbb{C}^3$ is more powerful than GHZ/W calculus on $\mathbb{C}^2$, we showed G/W/I calculus on $\mathbb{C}^3$ contains GHZ/W calculus on $\mathbb{C}^2$ by proving any equation holding in GHZ/W calculus on $\mathbb{C}^2$ holds in G/W/I calculus on $\mathbb{C}^3$ via a projector onto $\mathbb{C}^2$. Almost all properties of these graphical calculi are proved using a plugging set, which plays a role like a basis. The lack of distributivity also means there is an equation that cannot be proved without plugging. That is, existence of plugging sets increases the number of provable equations in these graphical calculi.

A part of future work is developing a graphical calculus for higher dimension. The dimension of $\mathbb{C}^3$ is the least dimension such that there are infinitely many orthonormal bases, even if a base vector is fixed. This property makes graphical calculation more difficult than $\mathbb{C}^2$. In $\mathbb{C}^4$ and higher dimensional spaces, there may be other difficulties of creating graphical calculus. In addition to that, more studies about G/W/I calculus are needed. We showed the lack of the distributive law, which is a relation between two CFAs. G/W/I calculus may satisfy another relation between two CFAs, or a relation between three CFAs. It will show us advantages of G/W/I calculus over GHZ/W calculus.

References

[1] S. Abramsky and B. Coecke. A categorical semantics of quantum protocols. In *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science: LICS 2004*, pages 415–425. IEEE Computer Society, 2004.

[2] H. Bechmann-Pasquinucci and A. Peres. Quantum cryptography with 3-state systems. *Physical Review Letters*, 85(15):3313–3316, October 2000.

[3] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India*, pages 175–179, December 1984.

[4] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895–1899, March 1993.

[5] M. Bourennane, A. Karlsson, and G. Björk. Quantum key distribution using multilevel encoding. *Physical Review A*, 64(1):012306, June 2001.

[6] D. Bruß and C. Macchiavello. Optimal eavesdropping in cryptography with three-dimensional quantum states. *Physical Review Letters*, 88(12):127901, March 2002.

[7] B. Coecke and R. Duncan. Interacting quantum observables: categorical algebra and diagrammatics. *New Journal of Physics*, 13(4):043016, 2011.

[8] B. Coecke and B. Edwards. Three qubit entanglement within graphical Z/X-calculus. *Electronic Proceedings in Theoretical Computer Science*, 52:22–33, 2011.

[9] B. Coecke and A. Kissinger. The compositional structure of multipartite quantum entanglement. In *Automata, Languages and Programming*, volume 37th International Colloquium, ICALP 2010, Bordeaux, France, July 6-10, 2010, Proceedings, Part II, 2010.

[10] B. Coecke, A. Kissinger, A. Merry, and S. Roy. The GHZ/W-calculus contains rational arithmetic. *Electronic Proceedings in Theoretical Computer Science*, 52:34–48, 2011.

[11] B. Coecke, D. Pavlovic, and J. Vicary. A new description of orthogonal bases. *Mathematical Structures in Computer Science*, FirstView:1–13.

[12] R. Duncan and S. Perdrix. Rewriting measurement-based quantum computations with generalised flow. In Samson Abramsky, Cyril Gavoille, Claude

Kirchner, Friedhelm Meyer auf der Heide, and PaulG. Spirakis, editors, *Automata, Languages and Programming*, volume 6199 of *Lecture Notes in Computer Science*, pages 285–296. Springer Berlin Heidelberg, 2010.

[13] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Physical Review A*, 62(6):062314, November 2000.

[14] B. Frot. Implementing and automating complex arithmetic in quantomatic. Master's thesis, The University of Oxford, 2011.

[15] M. Herrmann. Models of multipartite entanglement. Master's thesis, The University of Oxford, 2010.

[16] K. Honda. Graphical classification of entangled qutrits. Bachelor's Thesis, The University of Tokyo, 2011.

[17] K. Honda. Graphical classification of entangled qutrits. *Electronic Proceedings in Theoretical Computer Science*, 95:123–141, 2012.

[18] A. Kissinger. *Pictures of Processes: Automated Graph Rewriting for Monoidal Categories and Applications to Quantum Computing.* PhD thesis, The University of Oxford, 2011.

[19] J. Kock. *Frobenius Algebras and 2-D Topological Quantum Field Theories*, volume 59 of *London Mathematical Society Student Texts.* Cambridge University Press, December 2003.

[20] L. Lamata, J. León, D. Salgado, and E. Solano. Inductive classification of multipartite entanglement under stochastic local operations and classical communication. *Physical Review A*, 74(5):052336, November 2006.

[21] L. Lamata, J. León, D. Salgado, and E. Solano. Inductive entanglement classification of four qubits under stochastic local operations and classical communication. *Physical Review A*, 75(2):022318, February 2007.

[22] S. M. Lane. *Categories for the Working Mathematician.* Springer, 2nd edition, September 1998.

[23] P. Mathonet, S. Krins, M. Godefroid, L. Lamata, E. Solano, and T. Bastin. Entanglement equivalence of N-qubit symmetric states. *Physical Review A*, 81(5):052315, May 2010.

[24] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, October 2000.

[25] S. Roy. Towards normal forms for GHZ/W calculus. In D. Home, G. Kar, and A. S. Majumda, editors, *American Institute of Physics Conference Series*, volume 1384 of *American Institute of Physics Conference Series*, pages 112–119, September 2011.

[26] P. Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14:527–586, 2004.

[27] P. Selinger. Dagger compact closed categories and completely positive maps. *Electronic Notes in Theoretical Computer Science*, 170:139 – 163, 2007.

[28] P. Selinger. A survey of graphical languages for monoidal categories. In B. Coecke, editor, *New Structures for Physics*, volume 813 of *Lecture Notes in Physics*, chapter 4, pages 289–355. Springer, 1st edition, 2011.

[29] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 41(2):pp. 303–332, 1999.

[30] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85:441–444, July 2000.

[31] F. Verstraete, J. Dehaene, B. De Moor, and H. Verschelde. Four qubits can be entangled in nine different ways. *Physical Review A*, 65(5):052112, April 2002.

[32] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, October 1982.

[33] X. Yang, Z. Wang, X. Wang, and S. Fei. Classification of bipartite and tripartite qutrit entanglement under SLOCC. *Communications in Theoretical Physics*, 50(3):651–654, 2008.

Appendix A

Abbreviated Proof

A.1 Theorem 4.8

Proof. Since $|\phi\rangle$ and $|\psi\rangle$ are SLOCC equivalent, there are invertible matrices L_1, L_2, L_3 such that

$$|\phi\rangle = (L_1 \otimes L_2 \otimes L_3)|\psi\rangle \tag{A.1}$$

Moreover, since $|\phi\rangle$ and $|\psi\rangle$ are both symmetric, the above equation holds even if matrices are exchanged.

$$|\phi\rangle = (L_2 \otimes L_1 \otimes L_3)|\psi\rangle \tag{A.2}$$

Then,

$$|\psi\rangle = (L_2^{-1}L_1 \otimes L_1^{-1}L_2 \otimes L_3^{-1}L_3)|\psi\rangle = (L \otimes L^{-1} \otimes I)|\psi\rangle \tag{A.3}$$

where $L := L_2^{-1}L_1$. The proof is divided to the following three cases depending on the matrix L. More precisely, on the Jordan normal form J of L. The Jordan normal form J of L is a Jordan matrix J such that

$$L = S^{-1}JS \tag{A.4}$$

where S is an invertible matrix.

1. J is a diagonal matrix D, that is,

$$D = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \tag{A.5}$$

   with non-zero coefficients $\lambda_1, \lambda_2, \lambda_3$.

2. J is J_1 consisting of two Jordan blocks. A matrix expression of J_1 is

$$J_1 = \begin{bmatrix} \lambda_1 & 1 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{bmatrix} \tag{A.6}$$

   with non-zero coefficients λ_1, λ_2.

3. J is a Jordan block J_2, namely

$$J_2 = \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix} \tag{A.7}$$

   with non-zero coefficient λ.

We shall investigate each case. In the following, $|\psi'\rangle := S^{\otimes 3}|\psi\rangle$ where S is the invertible matrix defined above. Note $|\psi'\rangle$ is also symmetric and can be written as

$$|\psi'\rangle = \sum_{i=0}^{3}\sum_{j=0}^{3-i} a_i^j |\psi_i^j\rangle \tag{A.8}$$

where

$$|\psi_i^j\rangle = \sum_{\chi\in\sigma(1^j 2^i 0^{3-i-j})} |\chi\rangle. \tag{A.9}$$

and σ maps a string to the set of its permutations.

case 1

$$\begin{aligned}
&|\psi'\rangle = (D\otimes D^{-1}\otimes I)|\psi'\rangle \\
= \ & \left(\left(\frac{\lambda_1}{\lambda_2}-1\right)|01\rangle + \left(\frac{\lambda_2}{\lambda_1}-1\right)|10\rangle\right)\otimes(a_0^1|0\rangle + a_0^2|1\rangle + a_1^1|2\rangle) \\
+ \ & \left(\left(\frac{\lambda_1}{\lambda_3}-1\right)|02\rangle + \left(\frac{\lambda_3}{\lambda_1}-1\right)|20\rangle\right)\otimes(a_1^0|0\rangle + a_1^1|1\rangle + a_2^0|2\rangle) \\
+ \ & \left(\left(\frac{\lambda_2}{\lambda_3}-1\right)|12\rangle + \left(\frac{\lambda_3}{\lambda_2}-1\right)|21\rangle\right)\otimes(a_1^1|0\rangle + a_1^2|1\rangle + a_2^1|2\rangle) \\
+ \ & |\psi'\rangle
\end{aligned} \tag{A.10}$$

This case can be subdivided depending on the eigenvalues $\lambda_1, \lambda_2, \lambda_3$.

1. Assume $\lambda_1 = \lambda_2 = \lambda_3$. It means D is similar to identity matrix and $L_1 = \lambda L_2$. Then, we exchange the role of L_2 and L_3. If D is similar to identity matrix in spite of exchange, it means $|\psi\rangle$ and $|\phi\rangle$ are already connected by a symmetric translation.

2. Assume $\lambda_1, \lambda_2, \lambda_3$ are distinct. It follows $a_0^1 = a_0^2 = a_1^0 = a_1^1 = a_1^2 = a_2^0 = a_2^1 = 0$. Suppose two of the rest a_0^0, a_0^3, a_3^0 are zero. We assume a_0^0 is nonzero without loss of generality. Then,

   $$|\psi\rangle = S^{-1\otimes 3}|\psi'\rangle = (S^{-1}S_\psi)^{\otimes 3}|000\rangle. \tag{A.11}$$

   where

   $$S_\psi = \begin{bmatrix} \sqrt[3]{a_0^0} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \tag{A.12}$$

   Similarly, the both cases when one of the rest coefficients is zero and all coefficients are nonzero, there is an invertible matrix S_ψ such that

   $$|\psi\rangle = (S^{-1}S_\psi)^{\otimes 3}\left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)\right) \tag{A.13}$$

   and

   $$|\psi\rangle = (S^{-1}S_\psi)^{\otimes 3}|\mathcal{G}\rangle \tag{A.14}$$

3. Suppose just two of the eigenvalues are the same. We assume $\lambda_1 = \lambda_2$ and $\lambda_1 \neq \lambda_3$. It follows $a_1^0 = a_1^1 = a_1^2 = a_2^0 = a_2^1 = 0$. Then,

   $$|\psi\rangle = a_0^0|\psi_0^0\rangle + a_0^1|\psi_0^1\rangle + a_0^2|\psi_0^2\rangle + a_0^3|\psi_0^3\rangle + a_3^0|\psi_3^0\rangle \tag{A.15}$$

If $a_0^0 = a_0^1 = a_0^2 = a_0^3 = 0$,

$$|\psi\rangle = (S^{-1}S_\psi)^{\otimes 3}|000\rangle. \tag{A.16}$$

with an appropriate matrix S_ψ. Otherwise, we think of a symmetric state of three qubit $|\pi\rangle := \frac{1}{\sqrt{1-|a_3^0|^2}}(a_0^0|\psi_0^0\rangle + a_0^1|\psi_0^1\rangle + a_0^2|\psi_0^2\rangle + a_0^3|\psi_0^3\rangle)$. By the theorem in [23], there is a 2×2 invertible matrix M connecting $|\pi\rangle$ to one of $|000\rangle$, $|GHZ\rangle$ and $|W\rangle$. We define S_ψ as

$$S_\psi = \begin{bmatrix} p\sqrt[6]{1-|a_3^0|^2} & q\sqrt[6]{1-|a_3^0|^2} & 0 \\ r\sqrt[6]{1-|a_3^0|^2} & s\sqrt[6]{1-|a_3^0|^2} & 0 \\ 0 & 0 & \sqrt[3]{a_3^0} \end{bmatrix} \tag{A.17}$$

where

$$M = \begin{bmatrix} p & q \\ r & s \end{bmatrix}. \tag{A.18}$$

Then, S_ψ satisfies one of following equations.

$$\sqrt{2}S_\psi{}^{\otimes 3}(\frac{1}{\sqrt{2}}(|000\rangle + |222\rangle)) = |\psi'\rangle \tag{A.19}$$

$$\sqrt{3}S_\psi{}^{\otimes 3}(\frac{1}{\sqrt{3}}(|000\rangle + |111\rangle + |222\rangle)) = |\psi'\rangle \tag{A.20}$$

$$2S_\psi{}^{\otimes 3}(\frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |222\rangle)) = |\psi'\rangle \tag{A.21}$$

The same arguments *mutatis mutandis* show there is an invertible matrix S_ψ such that the tensor power of it connects $|\psi\rangle$ to one of $|000\rangle$, $|000\rangle + |111\rangle$, $|001\rangle + |010\rangle + |100\rangle$, $|\mathcal{G}\rangle$, $|\mathcal{W}\rangle$ and $|\mathcal{I}\rangle$ in Case 2 and Case 3.

Therefore, we find that for any symmetric state $|\psi\rangle$ of three qutrits, there is a 3×3 invertible matrix S such that one of the following equations holds.

$$|\psi\rangle = S^{\otimes 3}|000\rangle \tag{A.22}$$

$$|\psi\rangle = S^{\otimes 3}(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)) \tag{A.23}$$

$$|\psi\rangle = S^{\otimes 3}(\frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)) \tag{A.24}$$

$$|\psi\rangle = S^{\otimes 3}|\mathcal{G}\rangle \tag{A.25}$$

$$|\psi\rangle = S^{\otimes 3}|\mathcal{W}\rangle \tag{A.26}$$

$$|\psi\rangle = S^{\otimes 3}|\mathcal{I}\rangle \tag{A.27}$$

We know that $|000\rangle$, $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, $\frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$, $|\mathcal{G}\rangle$, $|\mathcal{W}\rangle$ and $|\mathcal{I}\rangle$ are SLOCC inequivalent each other. Therefore, via one of these states, $|\phi\rangle$ can be transformed $|\psi\rangle$ by the tensor power of a matrix. □