University of Minho
School of Engineering

Bruna Filipa Martins Salgado

A Metric Equational System for Quantum Computation

October 2024

University of Minho
School of Engineering

Bruna Filipa Martins Salgado

A Metric Equational System for Quantum Computation

Master's Dissertation
Master in Physics Engineering

Work carried out under the supervision of
Renato Jorge Araújo Neves

October 2024

Acknowledgements

Write your acknowledgements here. Do not forget to mention the projects and grants that you have benefited from while doing your research, if any. Ask your supervisor about the specific textual format to use. (Funding agencies are quite strict about this.)

Statement of Integrity

I hereby declare having conducted this academic work with integrity.
I confirm that I have not used plagiarism or any form of undue use of information or falsification of results along the process leading to its elaboration.
I further declare that I have fully acknowledged the Code of Ethical Conduct of the University of Minho.

University of Minho, Braga, October 2024

Bruna Filipa Martins Salgado

Abstract

Noisy intermediate-scale quantum (NISQ) computers are expected to operate with severely limited hardware resources. Precisely controlling qubits in these systems comes at a high cost, is susceptible to errors, and faces scarcity challenges. Therefore, error analysis is indispensable for the design, optimization, and assessment of NISQ computing. Nevertheless, the analysis of errors in quantum programs poses a significant challenge. The overarching goal of the M.Sc. project is to provide a fully-fledged quantum programming language on which to study metric program equivalence in various scenarios, such as in quantum algorithmics and quantum information theory.

Keywords approximate equivalence, λ-calculus, metric equations

Resumo

Escrever aqui o resumo (pt)

Palavras-chave palavras, chave, aqui, separadas, por, vírgulas

Contents

List of Figures

Acronyms

NISQ Noisy Intermediate-Scale Quantum 1, 2, 3

BNF Backus-Naur Form 7, 8

CPTP Completely Positive Trace-Preserving 37, 38, 40, 44, 45, 53, 54, 55, 56, 88

OSR Operator Sum Representation 38

Notation

ρ, σ Typical designations for density matrices. 24

$\|.\|_2$ Euclidean norm. 24

$\|.\|_1$ Trace norm. 25

$\| \cdot \|_\infty$ Spectral norm. 25

$\|.\|_\sigma$ Operator norm. 25

$(-)^{\otimes n}$ N-fold tensor product. 27

$|\psi\rangle$ Quantum state. Also known as ket. 27

$\langle\psi|$ $|\psi\rangle^\dagger$. Also known as bra. 27

$\langle\psi|\phi\rangle$ Inner product between states $|\psi\rangle$ and $|\phi\rangle$. 27

$|\psi\rangle \otimes |\phi\rangle$ Tensor product of states $|\psi\rangle$ and $|\phi\rangle$. 29

$|\psi\rangle |\phi\rangle$ Tensor product of states $|\psi\rangle$ and $|\phi\rangle$. 29

$|\psi\phi\rangle$ Tensor product of states $|\psi\rangle$ and $|\phi\rangle$. 29

X Pauli operator σ_x. 31

Z Pauli operator σ_z. 31

H Hadamard gate 32

P Phase-shift gate 32

CNOT Controlled Not gate 32

$\| \cdot \|_\diamond$ Diamond norm. 39

Chapter 1

Introduction

1.1 Motivation and Context

Quantum computing dates back to 1982 when Nobel laureate Richard Feynman proposed the idea of constructing computers based on quantum mechanics principles to efficiently simulate quantum phenomena [1].

The field has since evolved into a multidisciplinary research area that combines quantum mechanics, computer science, and information theory. Quantum information theory, in particular, is based on the idea that if there are new physics laws, there should be new ways to process and transmit information. In classical information theory, all systems (computers, communication channels, etc.) are fundamentally equivalent, meaning they adhere to consistent scaling laws. These laws, therefore, govern the ultimate limits of such systems. For instance, if the time required to solve a particular problem, such as the factorization of a large number, increases exponentially with the size of the problem, this scaling behavior remains true irrespective of the computational power available. Such a problem, growing exponentially with the size of the object, is known as a "difficult problem". However, as demonstrated by Peter Shor, the use of a quantum computer with a sufficient number of quantum bits (qubits) could significantly accelerate the factorization of large numbers [2]. This advancement poses a significant threat to the security of confidential data transmitted over the Internet, as the RSA algorithm is based on the computational difficulty of factorizing large numbers.

The quantum computing paradigm holds immense promise, as evidenced by this compelling result in computational complexity theory. While hardware advancements have brought the scientific community closer to realizing this potential, the ultimate goal is yet to be accomplished. A **Noisy Intermediate-Scale Quantum** (**NISQ**) computer equipped with 50-100 qubits may surpass the capabilities of current classical computers, yet the impact of quantum noise, such as decoherence in entangled states, imposes limitations on the size of quantum circuits that can be executed reliably [3]. Unfortunately, general-purpose error correction techniques [4–6] consume a substantial number of qubits, making it difficult for **NISQ** devices to make use of them in the near term. For instance, the implementation of a single logical qubit may require between 10^3 and 10^4 physical qubits [7]. As a result, it is unreasonable to expect that the idealized quantum algorithm will run perfectly on a quantum device, instead only a mere approximation will be observed.

To reconcile quantum computation with **NISQ** computers, quantum compilers perform transformations for error mitigation [8] and noise-adaptive optimization [9]. Additionally, current quantum computers only support a restricted, albeit universal, set of quantum operations. As a result, nonnative operations must be decomposed into sequences of native operations before execution [10], [11]. In general, perfect computational universality is not sought, but only the ability to approximate any quantum algorithm, with a preference for minimizing the use of additional gates beyond the original requirements. The assessment of these compiler transformations necessitates a comparison of the error bounds between the source and compiled quantum programs. Additionally, in quantum information theory, it is essential to account for errors arising from malicious attacks or noisy channels [12].

This suggests the development of appropriate notions of approximate program equivalence, *in lieu* of the classical program equivalence and underlying theories that typically hinge on the idea that equivalence is binary, *i.e.* two programs are either equivalent or they are not [13].

As previously noted, Shor's algorithm has played a pivotal role in sparking heightened interest within the scientific community toward quantum computing research. Several quantum programming languages have surfaced over the past 25 years [14, 15]. These include imperative languages such as Qiskit [16] and Silq [17], as well as functional languages such as Quipper [18] and Q# [19]. On one hand, the design of quantum programming languages is strongly oriented towards implementing quantum algorithms. On the other hand, the definition of functional paradigmatic languages or functional calculi serves as a valuable tool for delving into theoretical aspects of quantum computing, particularly exploring the foundational basis of quantum computation [20].

Most of the current research on algorithms and programming languages assumes that addressing the challenge of noise during program execution will be resolved either by the hardware or through the implementation of fault-tolerant protocols designed independently of any specific application [21]. As previously stated, this assumption is not realistic in the **NISQ** era. Nonetheless, there have been efforts to address the challenge of approximate program equivalence in the quantum setting.

[22] and [23] reason about the issue of noise in a quantum while-language by developing a deductive system to determine how similar a quantum program is from its idealised, noise-free version. The former introduces the (Q,λ)-diamond norm which analyzes the output error given that the input quantum state satisfies some quantum predicate Q to degree λ. However, it does not specify any practical method for obtaining non-trivial quantum predicates. In fact, the methods used in [[22]] cannot produce any post conditions other than $(I, 0)$ (*i.e.*, the identity matrix I to degree 0, analogous to a "true" predicate) for large quantum programs. The latter specifically addresses and delves into this aspect.

An alternative approach was explored in [24], using linear λ-calculus as basis – *i.e* programs are written as linear λ-terms – which has deep connections to both logic and category theory [25], [26]. A notion of approximate equivalence is then integrated in the calculus via the so-called diamond norm , which induces a metric (roughly, a distance function) on the space of quantum programs (seen semantically as completely positive trace-preserving super-operators) [[12]]. The authors argue that their deductive system allows to compute an approximate distance between two quantum programs easily as opposed to computing an exact distance "semantically" which tends to involve quite complex operators. Some positive results were achieved in this setting, but much remains to be done.

Agora falta falar das copias : existe uma variedade de problemas in inf quantica que envolvem copias de estados, (discriminação, quantum hyp testing, metrology), e portanto o nosso framework deve ser capaz de lidar com isso.

1.2 Goals

1.3 Document Structure

Chapter 2

Metric Lambda Calculus

The Lambda Calculus, developed by Church and Curry in the 1930s, serves as a formal language capturing the key attribute of higher-order functional languages, treating functions as first-class citizens, allowing them to be passed as arguments [27]. Moreover, lambda calculus has been proven to be universal in the sense that any computable function can be represented as an expression within the language [28] . Beyond its foundational aspects, this calculus incorporates extensions for modeling side effects, including probabilistic or non-deterministic behaviors and shared memory. Higher-order functions form a pivotal abstraction in practical programming languages such as LISP, Scheme, ML, and Haskell.
This chapter introduces the metric lambda calculus as presented in [24]. The metric lambda calculus integrates notions of approximation into the equational system of affine lambda calculus, a variant of lambda calculus that restricts each variable to being used at most once. The metric lambda calculus incorporates a metric equational system, enabling reasoning about approximate program equivalence. This chapter offers a brief insight into lambda calculus and an overview of the syntax and metric equational system of the metric lambda calculus. For a more detailed study of lambda calculus theory, the reader is referred to [27].

2.1 The Lambda Calculus

The concept of a function takes a central role in the lambda calculus. But what exactly is a function? In most mathematics, the "functions as graphs" paradigm the "functions as graphs" paradigm is the most elegant and appropriate framework for understanding functions. Within this paradigm, each function f has a fixed domain X and a fixed codomain Y. The function f is then a subset of $X \times Y$ that satisfies the property that for each $x \in X$ there is a unique $y \in Y$ such that $(x, y) \in f$. Two functions f and g are equal if they yield the same output on each input, that is if $f(x) = g(x)$ for all $x \in X$. This perspective is known as the extensional view of functions, as it emphasizes that the only observable property of a function is how it maps inputs to outputs.

On the other hand, the "functions as rules" paradigm is more appropriate within computer science. In this context, defining a function involves specifying a rule or procedure for computing the function. Such a rule is often expressed in the form of a formula, for example, $f(x) = x^2$. As with the mathematical paradigm, two functions are considered extensionally equal if they exhibit the same input-output behavior. However, this view also introduces the notion of intensional equality: two functions are intensionally equal if they are defined by (essentially) the same formula.

In the lambda calculus, functions are described explicitly as formulae. The function $f : x \mapsto f(x)$ is represented as $\lambda x.f(x)$. Applying a function to an argument is done by juxtaposing the two expressions. For instance consider the function $f : x \mapsto x + 1$, to compute $f(2)$ one writes $(\lambda x.x + 1)(2)$.

The expression of higher-order functions - functions whose inputs and/or outputs are themselves functions- in a simple manner is an essential feature of lambda calculus. For example, the composition operator $f, g \mapsto f \circ g$ is written as $\lambda f.\lambda g.\lambda x.f(g(x))$. Considering the functions $f : x \mapsto x^2$ and $g : x \mapsto x + 1$, to compute $(f \circ g)(2)$ one writes

$$(\lambda f.\lambda g.\lambda x.f(g(x)))(\lambda x.x^2)(\lambda x.x + 1)(2).$$

As mentioned above, within the "functions as rules" paradigm, is not always necessary to specify the domain and codomain of a function in advance. For instance, the identity function $f : x \mapsto x$, can have any set X as its domain and codomain, provided that the domain and codomain are the same. In this case, one says that f has type $X \to X$. In the case of the composition operator, $h = \lambda f.\lambda g.\lambda x.f(g(x))$, the domain and codomain of the functions f and g must match. Specifically, f can have any set X as its domain and any set Y as its codomain, provided that Y is the domain of g. Similarly, g can have any set Z as its codomain. Thus, h has type

$$(X \to Y) \to (Y \to Z) \to (X \to Z).$$

This flexibility regarding domains and codomains enables operations on functions that are not possible in ordinary mathematics. For instance, if $f = \lambda x.x$ is the identity function, then one has that $f(x) = x$ for any x. In particular, by substituting f for x, one obtains $f(f) =$

$(\lambda x.x)(f) = f$. Note that the equation $f(f) = f$ is not valid in conventional mathematics, as it is not permissible, due to set-theoretic constraints, for a function to belong to its own domain.

Nevertheless, this remarkable aspect of lambda calculus, this work focuses on a more restricted version of the lambda calculus, known as the simply-typed lambda calculus. Here, each expression is always assigned a type, which is very similar to the situation in mathematics. A function may only be applied to an argument if the argument's type aligns with the function's expected domain. Consequently, terms such as $f(f)$ are not allowed, even if f represents the identity function.

2.2 Syntax

The grammar and term formation rules of the affine lambda calculus, discussed in [24], are presented in this subsection.

2.2.1 Type system

As previously mentioned, this work focuses on the simply-typed lambda calculus, this work focuses on the simply-typed lambda calculus, where each lambda term is assigned a *type*. Unlike sets, types are *syntactic* objects, meaning they can be discussed independently of their elements. One can conceptualize types as names or labels for set. The definition of the grammar of types for affine lambda calculus is as follows, where G represents a set of ground types, is given by the following **Backus-Naur Form** (**BNF**) [29].

$$\mathbb{A} ::= X \in G \mid \mathbb{I} \mid \mathbb{A} \otimes \mathbb{A} \mid \mathbb{A} \multimap \mathbb{A} \tag{2.1}$$

Note that this is an inductive definition. Ground types are things such as booleans, integers, and so forth. The type $\mathbb{I}$ is the unit/empty type, which has only one element. The type $\mathbb{A} \otimes \mathbb{A}$ correponds to the tensor of two types, while the type $\mathbb{A} \multimap \mathbb{B}$ is the type of linear maps one type to another.

2.2.2 (Raw)Terms

The expressions of the lambda calculus are called lambda terms. In the simply-typed lambda calculus, each lambda term is assigned a type. The terms without the specification of a type are called *raw typed lambda terms*. The grammar of *raw typed lambda terms* is given by the **BNF** below.

$$v, v_1, \dots, v_n, w \quad ::= \quad x \mid f(v_1, \dots, v_n) \mid * \mid (\lambda x : \mathbb{A}.v) \mid (vw) \mid v \otimes w \mid$$
$$\text{pm } v \text{ to } x \otimes y.w \mid v \text{ to } *.w \mid \text{dis}(v)$$

Here x ranges over an infinite set of variables. $f \in \Sigma$, where Σ corresponds to a class of sorted operation symbols, and $f(v_1, \dots, v_n)$ corresponds to the aplication of the function f to the arguments $v_1, \dots, v_n$. The symbol $*$ is the unit element of the type $\mathbb{I}$. The term $(\lambda x : \mathbb{A}.v)$ is the lambda abstraction term, which represents a function that takes an argument of type $\mathbb{A}$ and returns the value of v. The term (vw) is the application term, which applies the function v to the argument w. The term $v \otimes w$ is the tensor product of v and w. The term pm v to $x \otimes y.w$ is the pattern-matching construct, which is used to deconstruct a tensor product into components x and y. The term v to $*.w$ is used to discard a variable v of the unit type. The term dis(v) is the discard term, which is used to discard a term v.

Ver o que por antes do ::= porque v1,..., vn tb são termos

2.2.3 Free and Bound Variables

An occurrence of a variable x within a term of the form $\lambda x.v$ is referred to as *bound*. Similarly, the variables x and y in the term pm v to $x \otimes y.w$ are also bound. A variable occurrence that is not bound is said to be *free*. For example, in the term $\lambda x.xy$, the variable y is free, whereas the variable x is bound.

The set of free variables of a term v is denoted by $FV(v)$, and is defined inductively as follows:

$$\begin{aligned}
FV(x) &= \{x\}, & FV(*) &= \emptyset,\\
FV(f(v_1, \dots, v_n)), &= FV(v_1) \cup \ldots \cup FV(v_n) & FV(\lambda x : \mathbb{A}.v) &= FV(v) \backslash \{x\},\\
FV(vw) &= FV(v) \cup FV(w), & FV(v \otimes w) &= FV(v) \cup FV(w),\\
FV(\text{pm } v \text{ to } x \otimes y.w), &= FV(v) \cup (FV(w) \backslash \{x, y\}) & FV(\text{dis}(v)) &= FV(v),\\
FV(v \text{ to } *.w) &= FV(v) \cup FV(w).
\end{aligned}$$

2.2.4 Term formation rules

To prevent the formation of nonsensical terms within the context of lambda calculus, such as $(v \otimes w)(u)$, the *typing rules* are imposed.

A *typed* term is a pair consisting of a term and its corresponding type. The notation $v : \mathbb{A}$ denotes that the term v has type $\mathbb{A}$. Typing rules are formulated using *typing judgments*. A typing judgment is an expression of the form $x_1 : \mathbb{A}_1, \ldots, x_n : \mathbb{A}_n \triangleright v : \mathbb{A}$ (where $n \geq 1$), which asserts that the term v is a well-typed term of type $\mathbb{A}$ under the assumption that each variable variable x_i has type $\mathbb{A}_i$, for $1 \leq i \leq n$. The list $x_1 : \mathbb{A}_1, \ldots, x_n : \mathbb{A}_n$ of typed variables is called the *typing context* of the judgment, and it might be empty. Each variable x_i (where $1 \leq i \leq n$) must occur at most once in $x_1, \ldots, x_n$. The typing contexts are denoted by Greek letters Γ, Δ, E, and from now on, when referring to an abstract judgment, the notation $\Gamma \triangleright v : \mathbb{A}$ will be employed. The empty context is denoted by $-$. Note that in the affine lambda calculus, different contexts do not share variables. For example, if $\Gamma = x : \mathbb{A}, y : \mathbb{B}$ none of these variables can appear in any other context.

The concept of *shuffling* is employed to construct a linear typing system that ensures the admissibility of the exchange rule and enables unambiguous reference to judgment's denotation $[\![\Gamma \triangleright v : \mathbb{A}]\!]$. An admissible rule is not explicitly included in the formal definition of type theory, but its validity can be proven by demonstrating that whenever the premises can be derived, it is possible to construct a derivation of its conclusion. Shuffling is defined as a permutation of typed variables in a sequence of contexts, $\Gamma_1, \ldots, \Gamma_n$, preserving the relative order of variables within each Γ_i [30]. For instance, if $\Gamma_1 = x : \mathbb{A}, y : \mathbb{B}$ and $\Gamma_2 = z : \mathbb{D}$, then $z : \mathbb{D}, x : \mathbb{A}, y : \mathbb{B}$ is a valid shuffle of Γ_1, Γ_2. On the other hand, $y : \mathbb{B}, x : \mathbb{A}, z : \mathbb{D}$ is not a shuffle because it alters the occurrence order of x and y in Γ_1. The set of shuffles in $\Gamma_1, \ldots, \Gamma_n$ is denoted as Sf$(\Gamma_1, \ldots, \Gamma_n)$. A valid typing derivation is constructed using the inductive rules shown in Figure 1.

$$\frac{\Gamma_i \triangleright v_i : \mathbb{A}_i \quad f : \mathbb{A}_1, \ldots, \mathbb{A}_n \to \mathbb{A} \in \Sigma \quad E \in \mathsf{Sf}(\Gamma_1; \ldots; \Gamma_n)}{E \triangleright f(v_1, \ldots, v_n) : \mathbb{A}} \text{(ax)} \qquad \frac{}{x : \mathbb{A} \triangleright x : \mathbb{A}} \text{(hyp)}$$

$$\frac{}{- \triangleright * : \mathbb{I}} (\mathbb{I}_i) \quad \frac{\Gamma \triangleright v : \mathbb{A} \otimes \mathbb{B} \quad \Delta, x : \mathbb{A}, y : \mathbb{B} \triangleright w : \mathbb{D} \quad E \in \mathsf{Sf}(\Gamma; \Delta)}{E \triangleright \mathsf{pm}\ v\ \mathsf{to}\ x \otimes y.w : \mathbb{D}} (\otimes_e) \quad \frac{\Gamma \triangleright v : \mathbb{A}}{\Gamma \triangleright \mathsf{dis}(v) : \mathbb{I}} \text{(dis)}$$

$$\frac{\Gamma \triangleright v : \mathbb{A} \quad \Delta \triangleright w : \mathbb{B} \quad E \in \mathsf{Sf}(\Gamma; \Delta)}{E \triangleright v \otimes w : \mathbb{A} \otimes \mathbb{B}} (\otimes_i) \qquad \frac{\Gamma \triangleright v : \mathbb{I} \quad \Delta \triangleright w : \mathbb{A} \quad E \in \mathsf{Sf}(\Gamma; \Delta)}{E \triangleright v\ \mathsf{to}\ *.w : \mathbb{A}} (\mathbb{I}_e)$$

$$\frac{\Gamma, x : \mathbb{A} \triangleright v : \mathbb{B}}{\Gamma \triangleright \lambda x : \mathbb{A}.v : \mathbb{A} \multimap \mathbb{B}} (\multimap_i) \qquad \frac{\Gamma \triangleright v : \mathbb{A} \multimap \mathbb{B} \quad \Delta \triangleright w : \mathbb{A} \quad E \in \mathsf{Sf}(\Gamma; \Delta)}{E \triangleright vw : \mathbb{B}} (\multimap_e)$$

Figure 1: Term formation rules of affine lambda calculus.

The rule (ax) states that if there is a function $f \in \Sigma$ that has type $\mathbb{A}_1, \ldots, \mathbb{A}_n \to \mathbb{A}$ and a set of variables $v_1, \ldots, v_n$ whose types match the type of the arguments of f, then if that function is applied to v_1, ..., v_n the respective result is of type $\mathbb{A}$. The rule (hyp) is a tautology: under the assumption that x has type $\mathbb{A}$, x has type $\mathbb{A}$. The rule ($\mathbb{I}_i$) asserts that the unit element $*$ always has type $\mathbb{I}$. The rule ($\multimap_i$) expresses that if v is a term of type $\mathbb{B}$ with a variable x of type $\mathbb{A}$, then $\lambda x : \mathbb{A}.v$ is a function of type $\mathbb{A} \multimap \mathbb{B}$. The rule $(\multimap_e)$ states that a function of type $\mathbb{A} \multimap \mathbb{B}$ can be applied to an argument of type $\mathbb{A}$ to produce a result of type $\mathbb{B}$. The rule $(\otimes_i)$ asserts that if there is a term v of type $\mathbb{A}$ and a term w of type $\mathbb{B}$, then the tensor of these terms is of type $\mathbb{A} \otimes \mathbb{B}$. The rule $(\otimes_e)$ expresses if there is a term w of type $\mathbb{D}$ with variables x and y of types $\mathbb{A}$ and $\mathbb{B}$, respectively, and a term v of type $\mathbb{A} \otimes \mathbb{B}$, then v can be deconstructed into $x \otimes y$. The rule $(\mathbb{I}_e)$ states that if there is a term w of type $\mathbb{A}$ and a term v of type $\mathbb{I}$, then v can be discarded, and only the term w remains. Finally, the rule (dis) asserts that a term v of type $\mathbb{A}$ can be discarded, resulting in a term of type $\mathbb{I}$.

For a better understanding of the rules, a few straightforward programming examples are provided. For instance, the program that swaps the elements of a tensor product can be written as follows:

$$x : \mathbb{A}, y : \mathbb{B} \triangleright \mathsf{pm}\ x \otimes y\ \mathsf{to}\ a \otimes b.b \otimes a : \mathbb{B} \otimes \mathbb{A}$$

Now, to prove that this program is well-typed one can write the following typing derivation:

1	$x : \mathbb{A} \triangleright x : \mathbb{A}$	(hyp)
2	$y : \mathbb{B} \triangleright y : \mathbb{B}$	(hyp)
3	$x : \mathbb{A}, y : \mathbb{B} \triangleright x \otimes y : \mathbb{A} \otimes \mathbb{B}$	$(1, 2, \otimes_i)$
4	$b : \mathbb{B} \triangleright b : \mathbb{B}$	(hyp)
5	$a : \mathbb{A} \triangleright a : \mathbb{A}$	(hyp)
6	$b : \mathbb{B}, a : \mathbb{A} \triangleright b \otimes a : \mathbb{B} \otimes \mathbb{A}$	$(4, 5, \otimes_i)$
7	$x : \mathbb{A}, y : \mathbb{B} \triangleright \text{pm } x \otimes y \text{ to } a \otimes b.b \otimes a : \mathbb{B} \otimes \mathbb{A}$	$(3, 6, \otimes_e)$

Observe that in the notation of the third column, the numbers correspond to the premises utilized in the application of the rule.

Another example is the function that recieves a tensor product and returns first element and discards the second:

$$- \triangleright \lambda x : \mathbb{A} \otimes \mathbb{B}.\text{pm } x \text{ to } a \otimes b.\text{dis}(b) \ \text{ to } \ast .a : \mathbb{A}$$

To prove that this program is well-typed one can write the following typing derivation:

1	$b : \mathbb{B} \triangleright b : \mathbb{B}$	(hyp)
2	$b : \mathbb{B} \triangleright \text{dis}(b) : \mathbb{I}$	$(1, \text{dis})$
3	$a : \mathbb{A} \triangleright a : \mathbb{A}$	(hyp)
4	$a : \mathbb{A}, b : \mathbb{B} \triangleright \text{dis}(b) \ \text{ to } \ast .a$	$(2, 3, \mathbb{I}_e)$
5	$x : \mathbb{A} \otimes \mathbb{B} \triangleright x : \mathbb{A} \otimes \mathbb{B}$	(hyp)
6	$x : \mathbb{A} \otimes \mathbb{B} \triangleright \text{pm } x \text{ to } a \otimes b.\text{dis}(b) \ \text{ to } \ast .a : \mathbb{A}$	$(4, 5, \otimes I_e)$
7	$- \triangleright \lambda x : \mathbb{A} \otimes \mathbb{B}.\text{pm } x \text{ to } a \otimes b.\text{dis}(b) \ \text{ to } \ast .a : \mathbb{A}$	$(6, \multimap_i)$

Also fala-se de Type inference algorithm? Tipo existe...

2.2.5 α-equivalence

A natural notion of equivalence definition stems from the fact that terms that differ only in the names of their bound variables represent the same program. For instance, the functions $\lambda x : \mathbb{A}.x$ and $\lambda y : \mathbb{A}.y$ have the same input-output behavior, despite being represented by different lambda terms. This equivalence is called *α-equivalence*.

Definition 2.2.1. The α-equivalence is an equivalence relation on lambda terms that is used to rename bound variables. To rename a variable x as y in a term v, denoted by $v\{y/x\}$, is to replace all occurrences of x in v by y. Two terms v and w are α-equivalent, written $=_\alpha$, if one can be derived from the other by a series of changes of bound variables

Convention 2.2.2. Terms are considered up to α-equivalence from now on.

2.2.6 Substitution

The substitution of a variable x for a term w in a term v is denoted by $v[w/x]$. It is only permitted to replace free variables. For instance, $\lambda x.x\,[v/x]$ is $\lambda x.x$ and not $\lambda x.v$. Moreover, it is necessary to avoid the unintended binding of free variables. For example,

$$(\text{pm } x \otimes y \text{ to } a \otimes b.b \otimes a \otimes z)\,[z/\text{pm } c \otimes d \text{ to } e \otimes f.f \otimes e \otimes a]$$

is not the same as

$$\text{pm } x \otimes y \text{ to } a \otimes b.b \otimes a \otimes (\text{pm } c \otimes d \text{ to } e \otimes f.f \otimes e \otimes a).$$

Instead, the bounded variable a must be renamed before the substitution, and in this case, the proper substitution is

$$(\text{pm } x \otimes y \text{ to } t \otimes b.b \otimes t \otimes z)\,[z/\text{pm } c \otimes d \text{ to } e \otimes f.f \otimes e \otimes a]$$

which is equal to

$$\text{pm } x \otimes y \text{ to } t \otimes b.b \otimes t \otimes (\text{pm } c \otimes d \text{ to } e \otimes f.f \otimes e \otimes a).$$

Note that a simple way of ensuring these restrictions are satisfied is not allowing the variable x to occur in the context of w in $v[w/x]$. Since x is in the context of v, this is always the case in the affine lambda calculus.

Definition 2.2.3. Given the typings judgments $\Gamma, x : \mathbb{A} \triangleright v : \mathbb{B}$ and $\Delta \triangleright w : \mathbb{A}$, the substitution

$\Gamma, \Delta \triangleright v[w/x] : \mathbb{B}$ is defined below. The types of judgments are omitted as no ambiguity arises.

$$\Gamma, \Delta \triangleright y[w/x] = \Gamma, \Delta \triangleright y,$$

$$\Delta \triangleright *[w/x] = \Delta \triangleright *,$$

$$\Gamma, \Delta \triangleright (\lambda y : \mathbb{B}.v)[w/x] = \Gamma, \Delta \triangleright \lambda y : \mathbb{B}.v[w/x],$$

$$(\mathsf{dis}(v))[w/x] = \mathsf{dis}(v[w/x]),$$

In the next three cases, $\Gamma, x : \mathbb{A} \in \mathsf{Sf}(\Gamma_1, \ldots, \Gamma_i, \ldots, \Gamma_n)$ and $\Gamma_i \triangleright v_i$

$$\Gamma, \Delta \triangleright (f(v_1, \ldots, v_n))[w/x] = \Gamma, \Delta \triangleright f(v_1[w/x], \ldots, v_n), \qquad (\text{ if } x : \mathbb{A} \in \Gamma_1)$$

$$\Gamma, \Delta \triangleright (f(v_1, \ldots, v_i, \ldots, v_n))[w/x] = \Gamma, \Delta \triangleright f(v_1, \ldots, v_i[w/x], \ldots, v_n), \qquad (\text{ if } x : \mathbb{A} \in T_i)$$

$$\Gamma, \Delta \triangleright (f(v_1, \ldots, v_n))[w/x] = \Gamma, \Delta \triangleright f(v_1, \ldots, v_n[w/x]), \qquad (\text{ if } x : \mathbb{A} \in \Gamma_n)$$

In the next two cases, $\Gamma, x : \mathbb{A} \in \mathsf{Sf}(\Gamma_1, \Gamma_2), \Gamma_1 \triangleright v$, and $\Gamma_2 \triangleright u$

$$\Gamma, \Delta \triangleright (vu)[w/x] = \Gamma, \Delta \triangleright (v[w/x]u), \qquad (\text{ if } x : \mathbb{A} \in \Gamma_1)$$

$$\Gamma, \Delta \triangleright (vu)[w/x] = \Gamma, \Delta \triangleright (vu[w/x]), \qquad (\text{ if } x : \mathbb{A} \in \Gamma_2)$$

In the next two cases, $\Gamma, x : \mathbb{A} \in \mathsf{Sf}(\Gamma_1, \Gamma_2), \Gamma_1 \triangleright v$, and $\Gamma_2 \triangleright u$

$$\Gamma, \Delta \triangleright (v \otimes u)[w/x] = \Gamma, \Delta \triangleright v[w/x] \otimes u, \qquad (\text{ if } x : \mathbb{A} \in \Gamma_1)$$

$$\Gamma, \Delta \triangleright (v \otimes u)[w/x] = \Gamma, \Delta \triangleright v \otimes u[w/x], \qquad (\text{ if } x : \mathbb{A} \in \Gamma_2)$$

In the next two cases, $\Gamma, x : \mathbb{A} \in \mathsf{Sf}(\Gamma_1, \Gamma_2), \Gamma_1 \triangleright v$, and $\Gamma_2, y : \mathbb{D}, z : \mathbb{E} \triangleright u$

$$\Gamma, \Delta \triangleright (\mathsf{pm}\ v \ \mathsf{to}\ y \otimes z.u)[w/x] = \Gamma, \Delta \triangleright \mathsf{pm}\ v[w/x] \ \mathsf{to}\ y \otimes z.u, \qquad (\text{ if } x : \mathbb{A} \in \Gamma_1)$$

$$\Gamma, \Delta \triangleright (\mathsf{pm}\ v \ \mathsf{to}\ y \otimes z.u)[w/x] = \Gamma, \Delta \triangleright \mathsf{pm}\ v \ \mathsf{to}\ y \otimes z.u[w/x], \qquad (\text{ if } x : \mathbb{A} \in \Gamma_2)$$

In the next two cases, $\Gamma, x : \mathbb{A} \in \mathsf{Sf}(\Gamma_1, \Gamma_2), \Gamma_1 \triangleright v$, and $\Gamma_2 \triangleright u$

$$\Gamma, \Delta \triangleright (v \ \mathsf{to}\ * .u)[w/x] = \Gamma, \Delta \triangleright v[w/x] \ \mathsf{to}\ * .u \qquad (\text{ if } x : \mathbb{A} \in \Gamma_1),$$

$$\Gamma, \Delta \triangleright (v \ \mathsf{to}\ * .u)[w/x] = \Gamma, \Delta \triangleright v \ \mathsf{to}\ * .u[w/x] \qquad (\text{ if } x : \mathbb{A} \in \Gamma_2).$$

The sequential substitutions $M[M_i/x_i] \ldots [M_n/x_n]$ are writen as $M[M_i/x_i, \ldots, M_n/x_n]$.

2.2.7 Properties

The calculus defined in Figure 1 possesses several desirable properties, which are listed below. Before proceeding, it is necessary to introduce some auxiliary notation. Given a context Γ, $te(\Gamma)$ denotes context Γ with all types erased. The expression $\Gamma \simeq_\pi \Gamma'$ denotes that the contexts Γ is a permutation of context Γ'.This notation also applies to non-repetitive lists of untyped variables $te(\Gamma)$. Additionally, a judgment $\Gamma \triangleright v : \mathbb{A}$ will often be abbreviated into $\Gamma \triangleright v$ or even just v when no ambiguities arise.

The properties are as follows:

1. for all judgements $\Gamma \triangleright v$ and $\Gamma' \triangleright v$, $\mathrm{te}(\Gamma) \simeq_\pi \mathrm{te}(\Gamma')$;
2. additionally if $\Gamma \triangleright v : \mathbb{A}$, $\Gamma' \triangleright v : \mathbb{A}'$, and $\Gamma \simeq_\pi \Gamma'$, then $\mathbb{A}$ must be equal to $\mathbb{A}'$;
3. all judgements $\Gamma \triangleright v : \mathbb{A}$ have a unique derivation.
4. (exchange) For every judgement $\Gamma, x : \mathbb{A}, y : \mathbb{B}, \Delta \triangleright v : \mathbb{D}$ it is possible to derive $\Gamma, y : \mathbb{B}, x : \mathbb{A}, \Delta \triangleright v : \mathbb{D}$.
5. (substitution) For all judgements $\Gamma, x : \mathbb{A} \triangleright v : \mathbb{B}$ and $\Delta \triangleright w : \mathbb{A}$ it is possible to derive $\Gamma, \Delta \triangleright v[w/x] : \mathbb{B}$.

2.2.8 Equations-in-context

The simply typed lambda calculus is a formal language that captures operations like the application of a function to an argument and the elimination of variables. To express these operations there is a set of rules known as reduction rules. These rules fall into two primary categories: the β-*reductions*, which perform operations and enforce the implicit meaning of the term, and η-*reductions*, which simplify terms by exploiting the extensionality of functions. There is also a secondary class of reductions known as *commuting conversions*, which serve to disambiguate terms that, while equivalent, have different representations. As a result, affine λ-calculus comes equipped with the so-called equations-in-context $\Gamma \triangleright v = w : \mathbb{A}$, depicted in Figure 2.

$$
\begin{array}{llll}
(\beta) & \Gamma, \Delta \triangleright (\lambda x : \mathbb{A}.\, v) w = v[w/x] : \mathbb{B} & (\eta) & \Gamma \triangleright \lambda x : \mathbb{A}.(v x) = v : \mathbb{A} \multimap \mathbb{B} \\
(\beta_{\mathbb{I}_e}) & \Gamma \triangleright * \ \mathsf{to}\ * .\, v = v : \mathbb{A} & (\eta_{\mathbb{I}_e}) & \Delta, \Gamma \triangleright v \ \mathsf{to}\ * .\, w[*/z] = w[v/z] : \mathbb{A} \\
(\beta_{\otimes_e}) & \multicolumn{3}{c}{E, \Gamma, \Delta \triangleright \mathsf{pm}\ v \otimes w \ \mathsf{to}\ x \otimes y.\, u = u[v/x, w/y] : \mathbb{A}} \\
(\eta_{\otimes_e}) & \multicolumn{3}{c}{\Delta, \Gamma \triangleright \mathsf{pm}\ v \ \mathsf{to}\ x \otimes y.\, u[x \otimes y/z] = u[v/z] : \mathbb{A}} \\
(c_{\mathbb{I}_e}) & \multicolumn{3}{c}{\Delta, \Gamma, E \triangleright u[v \ \mathsf{to}\ * .w/z] = v \ \mathsf{to}\ * .u[w/z] : \mathbb{A}} \\
(c_{\otimes_e}) & \multicolumn{3}{c}{\Delta, \Gamma, E \triangleright u[\mathsf{pm}\ v \ \mathsf{to}\ x \otimes y.\, w/z] = \mathsf{pm}\ v \ \mathsf{to}\ x \otimes y.\, u[w/z] : \mathbb{A}} \\
(\eta_{\mathsf{dis}}) & \multicolumn{3}{c}{x_1 : \mathbb{A}_1, \dots, x_n : \mathbb{A}_n \triangleright v = \mathsf{dis}(x_1) \ \mathsf{to}\ * \dots .\, \mathsf{dis}(x_{n-1}) \ \mathsf{to}\ * \ \mathsf{dis}(x_n) : \mathbb{I}}
\end{array}
$$

Figure 2: Equations-in-context for affine lambda calculus

It is evident that, for example, equation (β) enforces the meaning of $(\lambda x : \mathbb{A}.\, v)\, w$, which is interpreted as "v with w in place of x". The equation (η), on the other hand, is a simplification rule that states that a function that applies another function v to an argument x can be simplified to the function v itself. The remaining β e η equations follow similar reasoning. The commuting conversion $(c_{\mathbb{I}_e})$ expresses that substituting a variable z by a term that maps a term v to the unit element $*$ in a term w is equivalent to mapping a term v to the unit element $*$ and then replacing z by w. The other commuting conversion has a similar interpretation.

2.3 Metric equational system

Mete-se contexto e tipo nas eqs métricas?

Metric equations [31], [32] are a strong candidate for reasoning about approximate program equivalence. These equations take the form of $t =_\epsilon s$, where ϵ is a non-negative rational representing the "maximum distance" between the two terms t and s. The metric equational system for linear lambda calculus is depicted in Figure 3.

$$\frac{}{v =_0 v}\,(\text{refl}) \qquad \frac{v =_q w \quad w =_r u}{v =_{q+r} u}\,(\text{trans}) \qquad \frac{v =_q w \quad r \geq q}{v =_r w}\,(\text{weak})$$

$$\frac{\forall r > q.\ v =_r w}{v =_q w}\,(\text{arch}) \qquad \frac{\forall i \leq n.\ v =_{q_i} w}{v =_{\wedge q_i} w}\,(\text{join}) \qquad \frac{v =_q w}{w =_q v}\,(\text{sym})$$

$$\frac{v =_q w \quad v' =_r w'}{v \otimes v' =_{q+r} w \otimes w'} \qquad \frac{\forall i \leq n.\ v_i =_{q_i} w_i}{f(v_1, \ldots, v_n) =_{\Sigma q_i} f(w_1, \ldots, , w_n)} \qquad \frac{v =_q w}{\lambda x : \mathbb{A}.\ v =_q \lambda x : \mathbb{A}.\ w}$$

$$\frac{v =_q w \quad v' =_r w'}{\mathsf{pm}\ v\ \mathsf{to}\ x \otimes y.\ v' =_{q+r} \mathsf{pm}\ w\ \mathsf{to}\ x \otimes y.\ w'} \qquad \frac{v =_q w}{\mathsf{dis}(v) =_q \mathsf{dis}(w)} \qquad \frac{v =_q w \quad v' =_r w'}{v v' =_{q+r} w w'}$$

$$\frac{\Gamma \triangleright v =_q w : \mathbb{A} \quad \Delta \in \mathsf{perm}(\Gamma)}{\Delta \triangleright v =_q w : \mathbb{A}} \qquad \frac{v =_q w \quad v' =_r w'}{v\ \mathsf{to}\ *.v' =_{q+r} w\ \mathsf{to}\ *.w'} \qquad \frac{v =_q w \quad v' =_r w'}{v[v'/x] =_{q+r} w[w'/x]}$$

Figure 3: Metric equational system

Here, perm(Γ) denotes the set of possible permutions of context Γ. The rules (refl), (trans), and (sym) generalize the properties of reflexivity, transitivity, and symmetry of equality.

Rule (weak) asserts that if two terms are at a maximum distance q from each other, then they are also separated by any $r \geq q$. Rule (arch) states that if $v =_r w$ for all approximations r of q, then it necessarily follows that $v =_q w$. The rule (join) expresses that if several maximum distances between two terms are known, the actual maximum distance between them is the minimum of these distances. The rule that follows conveys that if the maximum distance between two terms v and w is q, and the maximum distance between terms v' and w' is r, then the maximum distance between the tensor products $v \otimes v'$ and $w \otimes w'$ is $q + r$. The remaining rules follow similar reasoning.

To ilustrate the usefulness of these equations, consider the program P that recieves a tensor product, swaps its elements and then applies a function f to to the new second element of the tensor pair:

$$P = x : \mathbb{A}, y : \mathbb{B} \triangleright \text{pm } x \otimes y \text{ to } a \otimes b.b \otimes f(a) : \mathbb{D} \otimes \mathbb{A}$$

Now, consider the case where f is an idealized version of function f^ϵ mapping a to $f(a)^\epsilon$. The program that applies the "real" function f to the first element of the tensor pair is P^ϵ:

$$P^\epsilon = x : \mathbb{A}, y : \mathbb{B} \triangleright \text{pm } x \otimes y \text{ to } a \otimes b.b \otimes f(a)^\epsilon : \mathbb{D} \otimes \mathbb{A}$$

Knowing that $f(a)^\epsilon =_\epsilon f(a)$, it is possible to show that $P^\epsilon =_\epsilon P$ using the metric equational system. The prove is as follows. The types and contexts are omitted for brevity as no ambiguity arises.

1	$f(a)^\epsilon =_\epsilon f(a)$	
2	$b =_0 b$	(refl)
3	$b \otimes f(a)^\epsilon =_\epsilon b \otimes f(a)$	$(1, 2, \otimes_i)$
4	$x \otimes y =_0 x \otimes y$	(refl)
5	pm $x \otimes y$ to $a \otimes b.b \otimes f(a)^\epsilon =_\epsilon$ pm $x \otimes y$ to $a \otimes b.b \otimes f(a)$	$(3, 4, \otimes_e)$

Chapter 3

Quantum Meets Lambda Calculus

Quantum lambda calculus integrates quantum computation with higher-order functions, thereby emerging as a powerful tool for formal reasoning about quantum programs within a functional programming framework. This functional paradigm, with a static type system, offers the significant advantage of ensuring the absence of run-time errors, *i.e.*, potential errors can be detected at compile-time, when the program is written, rather than during execution.
The principal distinction between the quantum lambda calculus introduced in this section and the formulation proposed by Selinger [33, 34] lies in the handling of data duplication. In this aproach, as dictated by the type system in Figure 1, duplication of any data is strictly prohibited. In contrast, Selinger's approach permits the duplication of classical data while strictly forbidding the duplication of quantum data. Nonetheless, the controlled duplication of both classical and quantum data will be addressed in Chapter 5.
The first two sections of this chapter present the mathematical and quantum computing preliminaries necessary for understanding the theory of quantum computation. It should be noted that the concept of a norm, as well as the properties of some norms, are relevant here, as the existence of a metric system implies that operators have a well-defined norm. The introduction to quantum computing is primarily based on [12, 35], while the mathematical foundations are also based on [36] and [37]. The subsequent section delves into how the terms of quantum lambda calculus, which are constructed using Figure 1, are interpreted in the "quantum world".

3.1 Mathematical Preliminaries

It is impossible to present the theory of quantum computation without introducing some concepts of linear algebra within finite-dimensional spaces. This section provides a brief overview of the aspects of linear algebra that are most pertinent to the study of quantum computation.

3.1.1 Complex vector spaces

The basic objects of linear algebra are vector spaces. The vector spaces of interest in this work are the complex vector spaces, such as $\mathbb{C}^n$ and $\mathbb{C}^{n\times m}$ therefore, the following definition is given in the context of complex vector spaces.

Definition 3.1.1. A *vector space* (over $\mathbb{C}$) consists of a set V whose elements are called vectors, together with two operations:

- An operation called vector addition that takes two vectors $v, w \in V$, and results in a third vector, written $v + w \in V$;
- An operation called scalar multiplication that takes a scalar $a \in \mathbb{C}$ and a vector $v \in V$, and results in a new vector, written $r \cdot v \in V$

which satisfy the following conditions (called axioms), for all $u, v, w \in V$ and $a_1, a_2 \in \mathbb{C}$:

1. Vector addition is commutative: $u + v = v + u$;
2. Vector addition is associative: $(u + v) + w = u + (v + w)$;
3. There is a zero vector $0 \in V$ such that $v + 0 = v$ for all $v \in V$;
4. Each $v \in V$ has an additive inverse $w \in V$ such that $w + v = 0$;
5. Scalar multiplication distributes over scalar addition, $(a_1 + a_2) \cdot v = a_1 \cdot v + a_2 \cdot v$;
6. Scalar multiplication distributes over vector addition, $a_1 \cdot (v + w) = a_1 \cdot v + a_1 \cdot w$;
7. Ordinary multiplication of scalars associates with scalar multiplication, $(a_1 a_2) \cdot v = a_1 \cdot (a_2 \cdot v)$;
8. Multiplication by the scalar 1 is the identity operation, $1 \cdot v = v$.

The letters R, V, W will often be used to refer to vector spaces. All vector spaces are assumed to be finite dimensional, unless otherwise noted.

In the case of the vector space $\mathbb{C}^n$, the space of all n-tuples of complex numbers, $(a_1, \ldots, a_n)$, addition and scalar multiplication are defined in the following standard way:

- Addition: for vectors $u = (a_1, \ldots, a_n), v = (b_1, \ldots, b_n) \in \mathbb{C}^n$, the vector $u + v \in \mathbb{C}^n$ is defined by the equation $(u + v) = (a_1 + b_1, \ldots, a_n + b_n)$.
- Scalar multiplication: for a scalar $a \in \mathbb{C}$ and a vector $v = (b_1, \ldots, b_n) \in \mathbb{C}^n$, the vector $a \cdot v \in \mathbb{C}^n$ is defined by the equation $a \cdot v = (a \cdot b_1, \ldots, a \cdot b_n)$.

The zero vector in $\mathbb{C}^n$ is the vector with all entries equal to zero.

Sometimes, the column matrix notation is used to represent vectors in $\mathbb{C}^n$, that is, a vector $v \in \mathbb{C}^n$ is written as a column matrix

$$v = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Other times for readability the format $(a_1, \ldots, a_n)$ is used. The latter should be interpreted as a shorthand for a column vector.

$\mathbb{C}^{n \times m}$ is a vector space when addition is defined as matrix addition and scalar multiplication is defined as multiplication of each component by the scalar. The zero vector is the zero matrix, *i.e.*, the matrix with all entries equal to zero.

Definition 3.1.2. A *vector subspace* of a vector space V is a subset W of V such that W is also a vector space, that is, W must be closed under scalar multiplication and addition.

Definition 3.1.3. A *spanning set* of a vector space is a set of vectors $v_1, \ldots, v_n$ such that any vector v in the vector space can be written as a linear combination $v = \sum_i a_i v_i$ of vectors in that set, where a_i are scalars.

Definition 3.1.4. A set of non-zero vectors $v_1, \ldots, v_n$ are *linearly dependent* if there exists a set of complex numbers $a_1, \ldots, a_n$ with $a_i \neq 0$ for at least one value of i, such that

$$a_1 v_1 + a_2 v_2 + \ldots a_n v_n = 0.$$

Definition 3.1.5. A set of vectors $v_1, \ldots, v_n$ are *linearly independent* if they are not linearly dependent.

Definition 3.1.6. A *basis* for a vector space is a sequence of vectors that is linearly independent and that spans the space.

Definition 3.1.7. The number of elements in the basis is defined to be the *dimension* of V, denoted **dim** (V).

3.1.2 Linear operators

A *linear operator* between vector spaces V and W is defined to be any function $A : V \to W$ which is linear in its inputs, *i.e.*

$$A\left(\sum_i a_i v_i\right) = \sum_i a_i A(v_i)$$

Usually $A(v)$ is just denoted Av.

Suppose $V, W,$ and R are vector spaces, and $A : V \to R$ and $B : W \to R$ are linear operators. Then the notation BA is used to denote the *composition* of B with A, defined by $(BA)(v) \equiv B(A(v))$. Once again, $(BA)(v)$. is abbreviated as BAv.

For any choice of complex spaces $V \in \mathbb{C}^n$ and $W \in \mathbb{C}^m$, there is a bijective linear correspondence between the set of operators from V to W and the set of $n \times m$ matrices. The claim that the matrix $A \in \mathbb{C}^{m \times n}$ is a linear operator just means that

$$A\left(\sum_i a_i v_i\right) = \sum_i a_i A(v_i)$$

is true as an equation where the operation is matrix multiplication of A by a collumn vector in $\mathbb{C}^n$. Clearly, this is true! On the other hand, suppose $A : V \to W$ is a linear operator between vector spaces V and W, such that $V \in \mathbb{C}^n$ and $W \in \mathbb{C}^m$. Suppose $v_1, \ldots, v_n$ is a basis for V and $w_1, \ldots, w_n$ is a basis for W. Then for each j in the range $1, \ldots, m$, there exist complex numbers A_{1j} through A_{nj} such that

$$Av_j = \sum_i A_{ij} w_i.$$

The matrix whose entries are the values A_{ij} is said to form a *matrix representation* of the operator A. This matrix representation of A is completely equivalent to the operator A. As a result, when considering operators on vector spaces of the form $\mathbb{C}^n$ it is common to refer to the operator A and its matrix representation interchangeably.

3.1.3 Inner product

Definition 3.1.8. The *inner product* $\langle \cdot, \cdot \rangle$ is a function from a vector space V to the complex numbers, $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$, that satisfies the following properties for all $v, w \in V$ and $r \in \mathbb{C}$:

1. Linearity in the second argument,

$$\left\langle v, \sum_i a_i w_i \right\rangle = \sum_i a_i \langle v, w_i \rangle.$$

2. $\langle v, w \rangle = \langle w, v \rangle^\dagger$, where $(-)^*$ is the complex conjugate operation.

3. $\langle v, w \rangle \geq 0$ with equality if and only if $v = 0$.

The inner product $\langle v, w \rangle$ of two vectors $v = (a_1, \ldots, a_n), w = (b_1, \ldots, b_n) \in \mathbb{C}^n$ is defined as

$$\langle v, w \rangle = \sum_i a_i^* b_i.$$

Trace

In order to define inner product of a matrix, it is necessary to first define the trace of a matrix. The trace of a square matrix $A \in \mathbb{C}^{n \times n}$ defined to be the sum of its diagonal elements,

$$\text{tr}(A) = \sum_i A_{ii}.$$

The trace is *cyclic*, that is, $\text{tr}(AB) = \text{tr}(BA)$, and *linear*, $\text{tr}(A+B) = \text{tr}(A)+\text{tr}(B)$, $\text{tr}(a \cdot A) = a \cdot \text{tr}(A)$, where matrices $A, B \in \mathbb{C}^{n \times n}$, and a is a complex number.
By means of the trace, one defines the inner product of two operators $A, B \in \mathbb{C}^{m \times n}$ as follows

$$\langle A, B \rangle = \text{tr}(A^\dagger B). \tag{3.1}$$

In the *finite* dimensional complex vector spaces relevant to quantum computation and quantum information, a *Hilbert space* is is equivalent to an inner product space. As a result, both $\mathbb{C}^n$ and $\mathbb{C}^{n \times m}$ are Hilbert spaces.

3.1.4 Norm and normed spaces

Definition 3.1.9. A *norm* $\|\cdot\|$ is a function that associates an element of a vector space V with a non-negative real number, such that the following properties hold:

1. Positive definiteness: $\|v\| \geq 0$ for all $v \in V$, with $\|v\| = 0$ if and only if $v = 0$;

2. Positive scalability: $\|av\| = |a|\|v\|$ for all $v \in V$ scalar a;

3. The triangle inequality: $\|v+w\| \leq \|v\| + \|w\|$ for all $v, w \in V$.

Definition 3.1.10. A vector space together with a norm is called a *normed vector space*.

Every normed space may be regarded as a metric space, in which the distance $d(x, y)$ between vectors x and y is $\|x-y\|$. The relevant properties of d are

1. $0 < d(x, y) < \infty$ for all x and y,

2. $d(x, y) = 0$ if and only if $x = y$,

3. $d(x, y) = d(y, x)$ for all x and y,

4. $d(x, z) < d(x, y) + d(y, z)$ for all x, y, z.

Every inner product space is a normed space, where the norm of a vector v is defined as $\|v\| = \sqrt{\langle v, v\rangle}$.

Definition 3.1.11. Two vector u, v are said to be *orthogonal* if $\langle v, u\rangle$. An *orthogonal set* is a set of orthogonal vectors of the same vector space.

Definition 3.1.12. A *unit vector* is a vector v such that $\|v\| = 1$. It is also said that v is *normalized* if $\|v\| = 1$

Definition 3.1.13. An orthogonal set of unit vectors is called an *orthonormal set*, and when such a set forms a basis it is called an *orthonormal basis*.

3.1.5 Eigenvectors and eigenvalues

Definition 3.1.14. An *n-permutation* is a function on the first n positive integers $\pi = \{1, \ldots, n\} \to \{1, \ldots, n\}$ that is one-to-one and onto. In a permutation each number $1, \ldots, n$ appears as output for one and only one input.

Definition 3.1.15. The *sign* of a permutation $\operatorname{sgn}(\pi)$ is -1 if the number of inversions in π is odd and is $+1$ if the number of inversions is even.

Definition 3.1.16. The *determinant* of a square matrix $A \in \mathbb{C}^{n\times n}$ is defined as

$$\det(A) = \sum_{\pi\in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} A_{i\sigma(i)},$$

Here S_n is the set of all n-permutations $\pi = \{1, \ldots, n\} \to \{1, \ldots, n\}$, and $\operatorname{sgn}(\pi)$ denotes the sign of the permutation π.

Definition 3.1.17. An *eigenvector* of a linear operator A on a vector space is a non-zero vector v such that $Av = \lambda v$, where λ is a complex number known as the *eigenvalue* of A corresponding to v.

The *characteristic polynomial* of a square operator A is the polynomial $p(\lambda) = \det(A - \lambda I)$, where I is the identity operator

$$\begin{aligned} I_V : & V \to V \\ & v \mapsto v. \end{aligned}$$

where V is a vector space. The subscript will be omitted unless ambiguity arises. It can be shown that the characteristic function depends only upon the operator A, and not on the specific matrix representation used for A. By the fundamental theorem of algebra, every polynomial has at least one complex root, so every operator A has at least one eigenvalue, and a corresponding eigenvector. The solutions of the *characteristic equation* $c(\lambda) = 0$ are the eigenvalues of the operator A.
A *diagonal representation* of an operator A on a vector space V is an expression of the form $A = \sum_i \lambda_i v_i v_i^\dagger$, where the vectors v_i form an orthonormal set of eigenvectors for A, with corresponding eigenvalues λ_i, and $(-)^\dagger$ is the adjoint operation.

3.1.6 Spectral theorem

Theorem 3.1.18. *[35] Every normal operator $A \in \mathbb{C}^{n\times n}$ can be expressed as a linear combination $\sum_i \lambda_i b_i b_i^\dagger$ where the set $\{b_i, \ldots, bn\}$ is an orthonormal basis on $\mathbb{C}^n$.*

Using this last result any function $f : \mathbb{C} \to \mathbb{C}$, can be extended to normal matrices via,

$$f(A) = \sum_i f(\lambda_i) b_i b_i^\dagger \tag{3.2}$$

where $A = \sum_i \lambda_i b_i b_i^\dagger$ is the spectral decomposition of A.

3.1.7 Important classes of operators/matrices

Linear operators mapping a complex space $\mathbb{C}^n$ or $\mathbb{C}^{n\times n}$ to itself will be called *square operators* due to the fact that their matrix representations are square matrices. Therefore, those definitions given in the context of square operators are also valid for square matrices.
The following classes of operators are of particular interest in quantum information theory.

Definition 3.1.19. *Normal operators.* A square operator A is *normal* if $AA^\dagger = A^\dagger A$.

Definition 3.1.20. *Hermitian operators.* A square operator A is *hermitian* if $A = A^\dagger$. Every Hermitian operator is a normal operator.

Definition 3.1.21. *Positive (semidefinite) operators*. A square operator $A : \mathbb{C}^n \to \mathbb{C}^\ltimes$ is *positive*, denoted $A \geq 0$, if $\langle v, Av \rangle \geq 0$ for all $v \in \mathbb{C}^n$. The sum of two positive semidefinite operators is positive semidefinite. Positive matrices are hermitian, and consequently, by the spectral decomposition, have diagonal representation $A = \sum_i \lambda_i v_i v_i^\dagger$, with non-negative eigenvalues λ_i [35].

Definition 3.1.22. *Unitary operators.* A square operator U is *unitary* if $U^\dagger U = UU^\dagger = I$. The letter U will often be used to refer to unitary operators.

Geometrically, unitary operators are important because they preserve inner products between vectors, $\langle Uv, Uw \rangle = \langle v, w \rangle$ for any two vectors v and w. Let $S_1 = \{v_i\}$ be any orthonormal basis set. Define $s_2 = \{w_i\} = \{Uv_i | v_i \in S\}$, so S_2 is also an orthonormal basis set, since unitary operators preserve inner products. Note that $U = \sum_i w_i v_i^\dagger$. Conversely, if $\{v_i\}$ are any two orthonormal bases, then it is easily checked that the operator U defined by $U = \sum_i w_i^\dagger v_i$ is unitary.

Definition 3.1.23. *Density operator*. Positive semidefinite operators that have trace equal to 1 are called *density operators*. Lowercase Greek letters, such as ρ, σ are conventionally used to denote density operators.

Definition 3.1.24. *Isometries*. An operator $A : \mathbb{C}^n \to \mathbb{C}^m$ is as isometry if $\|Av\| = \|v\|$ for all elements all elements $v \in \mathbb{C}^n$.

Definition 3.1.25. *Projectors*. A positive semidefinite operator P is a projector if $P^2 = P$. Equivalently, a projection operator is a Hermitian operator whose only eigenvalues are 0 and 1. The *orthogonal complement* of P is the operator $Q = I - P$.

Definition 3.1.26. *Diagonal operators*. A square operator A is *diagonal* if $A_{ij} = 0$ for all $i \neq j$.

3.1.8 Useful norms

Definition 3.1.27. The *euclidean norm*, $\|.\|_2$, of a vector $v \in \mathbb{C}^n$ is defined as:

$$\|v\|_2 = \sqrt{\langle v, v \rangle}.$$

Definition 3.1.28. The *trace norm*, $\|.\|_1$, of a matrix A is defined as:

$$\|A\|_1 = \text{tr}\sqrt{A^\dagger A} \tag{3.3}$$

This norm is also known as the Schatten 1-norm. The trace norm induces a metric on the set of density matrices which is defined by $d(\rho, \sigma) = \|\rho - \sigma\|_1$.

Alternatively, the trace norm of a square matrix $A \in \mathbb{C}^{n\times n}$ can be defined in the following way:

$$\|A\|_1 = \max\{|\langle U, A\rangle| \mid U \in \mathbb{C}^{n\times n} \text{ is a unitary operator}\}. \tag{3.4}$$

Proposition 3.1.29. *For all square matrices A and B, this norm enjoys the following properties:*

- *Submultiplicativity with respect to compositions: $\|AB\|_1 \leq \|A\|_1\|B\|_1$;*
- *Multiplicativity with respect to the tensor products: $\|A \otimes B\|_1 = \|A\|_1\|B\|_1$.*
- *Isometric invariance (and therefore unitarily invariance): for any unitary operators U_0 and U_1, $\|UAU_1^\dagger\|_1 = \|A\|_1$.*

Definition 3.1.30. The *spectral norm*, $\|\cdot\|_\infty$, of an operator $A : \mathbb{C}^n \to \mathbb{C}^m$ is defined as:

$$\|A\|_\infty = \max\{\|Av\|_2 \mid \|v\|_2 = 1\}.$$

Definition 3.1.31. Two norms on operators, $\| - \|_p$ and $\| - \|_{p*}$, are said to be *dual*, when for every operator $A : \mathbb{C}^n \to \mathbb{C}^m$, it holds that

$$\|A\|_p = \max\{|\langle B, A\rangle| \mid B : \mathbb{C}^n \to \mathbb{C}^m, \|B\|_{p*} = 1\}.$$

The trace norm and the spectral norm are dual.

Definition 3.1.32. Given normed vector spaces V and W, the operator,$\|.\|_\sigma$, norm for an operator $E : V \to W$ is defined as

$$\|E\|_\sigma = \sup\{\|E(A)\| \mid \|A\| = 1\}.$$

3.1.9 Tensor Products and Direct Sums of Complex spaces

Definition 3.1.33. The *direct sum* of two vector spaces V and W, denoted $V \oplus W$, is the space of all pairs (v, w) where $v \in V$ and $w \in W$.

The inner product in $V \oplus W$ is defined as follows:

$$\langle (v_1, w_1), (v_2, w_2) \rangle = \langle v_1, v_2 \rangle + \langle w_1, w_2 \rangle.$$

Definition 3.1.34. Consider two finite complex spaces spaces V and W with respective bases $(e_1, \ldots, e_n)$ and $(f_1, \ldots, f_k)$. The tensor product of V and W, denoted $V \otimes W$, is defined as the space generated by the basis of syntactic symbols:

$$(e_1 \otimes f_1, \ldots, e_1 \otimes f_k, \ldots, e_n \otimes f_1, \ldots, e_n \otimes f_k).$$

The tensor product of two elements $v = \sum_i \lambda_i \cdot e_i$ and w = $\sum_j \mu_j \cdot f_j$ is:

$$v \otimes w = \sum_{i,j} \lambda_i \mu_j \cdot e_i \otimes f_j.$$

The inner product in $V \otimes W$ is defined as follows

$$\langle e_i \otimes f_j, e_k \otimes f_l \rangle = \langle e_i, e_k \rangle \langle f_j, f_l \rangle.$$

The tensor product of two vectors $v = (v_1, \ldots, v_n) \in \mathbb{C}^n$ and $w = (w_1, \ldots, w_m) \in \mathbb{C}^m$ is defined as the vector $v \otimes w \in \mathbb{C}^{nm}$ such that

$$v \otimes w = \begin{pmatrix} v_1 w_1 \\ \vdots \\ v_1 w_m \\ \vdots \\ v_n w_1 \\ \vdots \\ v_n w_m \end{pmatrix}.$$

The tensor product of two operators $A \in \mathbb{C}^{n \times m}$ and $B \in \mathbb{C}^{p \times q}$ is defined as the operator $A \otimes B \in \mathbb{C}^{np \times mq}$ such that

$$(A \otimes B)(v \otimes w) = Av \otimes Bw.$$

The tensor product of two operators $P : \mathbb{C}^{n\times n} \to \mathbb{C}^{m\times m}$ and $Q \in \mathbb{C}^{o\times o} \to \mathbb{C}^{p\times p}$ is defined as the operator $P \otimes Q \in \mathbb{C}^{n\times n} \otimes \mathbb{C}^{o\times o} \to \mathbb{C}^{m\times m} \otimes \mathbb{C}^{p\times p}$ such that

$$(P \otimes Q)(A \otimes B) = P(A) \otimes Q(B).$$

The tensor product of two vector spaces corresponding to the direct sums of other vector spaces $V = V_1 \oplus \ldots \oplus V_n$ and $W = W_1 \oplus \ldots \oplus W_n$ is defined as

$$V \otimes W = V_1 \otimes W_1 \oplus \ldots \oplus V_1 \otimes W_n \oplus \ldots \oplus V_n \otimes W_1 \oplus \ldots \oplus \ldots \oplus W_n \otimes V_n.$$

The notation $(-)^{\otimes n}$ will be used to denote the tensor product of a vector space, vector, or operator with itself n times.
Considering vector spaces V, W, R, the following equalities hold:

$$v \otimes (w + r) = v \otimes w + v \otimes r, \text{ for all } v, w, r \in V, W, R;$$
$$(v + w) \otimes r = v \otimes r + w \otimes u, \text{ for all } v, w, r \in V, W, R;$$
$$(av) \otimes (bw) = ab(v \otimes w), \text{ for all } v, w \in V, W \text{ and scalars } a, b.$$

3.2 Quantum Computing Preliminaries

The basic unit of information in quantum computation is a quantum bit or qubit [38]. Just as classical bit, which can be in one of two states, 0 or 1, a qubit also has a state. Qubits are represented using *Dirac notation*, where the ket symbol $|\psi\rangle$ is used to denote a quantum state ψ. The corresponding bra symbol $\langle\psi|$ is used to denote the conjugate transpose of the state ψ. In this setting, the inner product of two states $|\psi\rangle$ and $|\phi\rangle$ is denoted $\langle\psi|\phi\rangle$ and is the same as $\langle\psi|\,|\phi\rangle$.

Definition 3.2.1. [35] Each isolated physical system is associated with a Hilbert space, known as the system's *state space*. The system's state is fully characterized by a *state vector*, which is a unit vector within this state space.

3.2.1 The 2-Dimensional Hilbert Space

The state of a single qubit is described by a normalized vector of the 2-dimensional Hilbert space $\mathbb{C}^2$. States $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are equivalent to the classical states 0 and 1, respectively. These states, known as the *computational basis* states, form an orthonormal basis for this vector space. Unlike classical bits, a qubit is not restricted to the states $|0\rangle$ and $|1\rangle$; it can exist in a linear combination of these states, commonly referred to as a *superposition*. Consequently, a general qubit state can be written as

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{3.5}$$

α and β are known as *amplitudes*. $|\alpha|^2$ and $|\beta|^2$ can be seen as the probabilities of measuring each state. Because $|\alpha|^2 + |\beta|^2 = 1$, Equation 3.5 and be rewritten as

$$|\psi\rangle = e^{i\gamma}\left(\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle\right), \tag{3.6}$$

where θ, ϕ and γ are real numbers. $e^{i\gamma}$ is known as a *global phase* and is often ignored because it has no observable effects, *i.e.*, it does not affect the probabilities of measurement outcomes. When disregarding the global phase, the quantum state can $|\psi\rangle$ be represented as:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{3.7}$$

which corresponds to a point in the unit sphere where θ marks the latitude (*i.e.* the polar angle) and ϕ marks the longitude (*i.e.* the azimuthal angle). This representation is traditionally called the Bloch sphere representation. A point in the latter representation corresponds to the vector in $\mathbb{R}^3$ defined by $(\cos\phi\sin\theta, \sin\phi\sin\theta, \cos\theta)$ and often called Bloch vector.

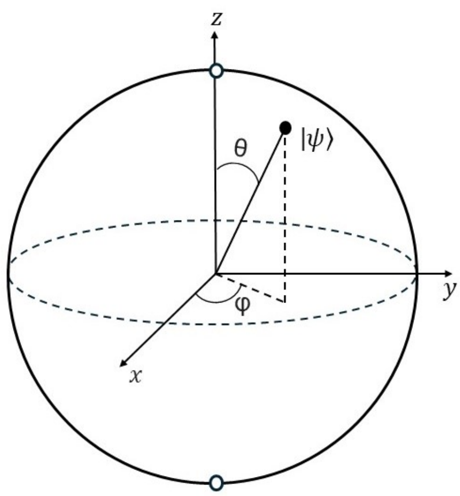


Figure 4: Bloch sphere representation of a qubit

The distance between two quantum states $|\psi\rangle$ and $|\psi'\rangle$ is their Euclidean distance in the Bloch sphere [8, 35].

There are infinite points in the Bloch sphere, which might suggest the possibility of encoding an infinite amount of information in the infinite binary expansion of the angle θ. However, when a qubit is measured, it collapses to one of the basis states, so only one bit of information can be extracted from a qubit. To accurately determine the amplitudes α and β, an infinite number of identical qubit copies would need to be measured. Nevertheless, it is still conceptually valid to think of these amplitudes as "hidden information". One could say that quantum computation is the art of manipulating this hidden information using phenomena such as interference and superposition to perform tasks that would be impossible or inefficient with classical computers.

3.2.2 Multi-qubit States

The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. As a result, an n-qubit state can be represented by a unit vector in 2^n-dimensional Hilbert space, $\mathbb{C}^{2^n}$. The notations $|\psi\rangle \otimes |\phi\rangle$, $|\psi\rangle\,|\phi\rangle$, and $|\psi\phi\rangle$ are used to denote the tensor product of two states $|\psi\rangle$ and $|\phi\rangle$. As for any complex vector, $|\psi\rangle^{\otimes n}$ denotes the n-fold tensor product of state $|\psi\rangle$ with itself. The computational basis states of an n-qubit system are of the form $|x_1 \dots x_n\rangle$ and so a quantum state of such a system is specified by 2^n amplitudes. For instance, a two-qubit state can be written as

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle\,.$$

It should be noted that unfortunately, no simple generalization of the Bloch sphere known for multiple qubits.

Entanglement

An interesting aspect of multi-qubit states is the phenomenon of *entanglement*. This term means strong intrinsic correlations between two (or more) particles when the quantum state of each of them cannot be described independently of the state of the other, i.e. cannot be written as a product of states of the individual qubits. Measuring one qubit of the entangled pair affects the state of the other qubit. This must happen even if the particles are far apart. In order to better understand this concept, consider the follow *Bell state* or *EPR pair*:

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Upon measuring the first qubit, there are two possible outcomes: 0 with probability $1/2$ and 1 with probability $1/2$. If the first qubit is measured to be 0, the second qubit will also be 0 with probability 1. If the first qubit is measured to be 1, the second qubit will also be 1 with probability 1. Therefore, the measurement outcomes are correlated.

These correlations prompted Einstein, Podolsky, and Rosen to publish a paper [39] questioning the completeness of quantum mechanics in 1935. The EPR paradox presented a dilemma: the existence of entanglement (i.e., correlations that persist regardless of distance) versus local realism and hidden variables. Einstein argued that if two objects, which have interacted in the past but are now separated, exhibit perfect correlation, they must possess a set of properties determined before their separation. These properties would persist in each object, dictating the outcomes of measurements on both sides. Einstein believed that the strong correlations predicted by quantum mechanics necessitate the existence of additional properties not accounted for by the quantum formalism that determine the measurement results. Therefore, he argued that quantum mechanics might require supplementation, as it may not represent a complete or ultimate description of reality.

In 1964, John Bell made a remarkable discovery: the measurement correlations in the Bell state are stronger than those that could ever occur between classical systems [40]. He explored the idea that each entangled particle might possess hidden properties — unaccounted for by quantum mechanics—that determine the measurement outcomes. Then, through mathematical reasoning, Bell demonstrated that the correlations predicted by any local hidden variable theory cannot exceed a specific level. There is an upper limit of correlations fixed by what today is called the “Bell inequalities”. He found that quantum theory sometimes predicts correlations that exceed this limit. Consequently, an experiment could settle the debate by testing whether or not correlations surpass the bounds he had found following Einstein’s position.

In 1982, Alain Aspect conducted an experiment that confirmed the violation of the Bell inequalities [41]. In this experiment, polarizers were placed more than twelve meters apart. This meant that the correlation obtained could not be explained by the fact that the particles carry within them unmeasured properties. Moreover, it proved that the outcome of the measurement is not determined until the moment of measurement. There seemed to be an instantaneous exchange between two particles at the time of measurement when they were twelve meters apart.

Sixteen years later, Nicolas Gisin [42] and Anton Zeilinger [43] conducted similar experiments, demonstrating that entanglement persists over distances of several kilometers. More recently, [44] extended these tests using entangled photon pairs sent from a satellite to verify Bell's inequalities over a distance of one thousand kilometers, further confirming that, regardless of the distance, entangled particles behave as an indivisible, inseparable whole. The connection between them is so profound that it appears to challenge the principles of relativity. This phenomenon is known as *quantum nonlocality*.

3.2.3 Unitary operators and Measurements

Pauli Matrices

The Pauli matrices are a set of three 2×2 hermitian matrices that are defined as follows:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The eigenvectors and eigenvalues of the Pauli matrices are as follows:

$$\sigma_x \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad \sigma_y \begin{pmatrix} 1 \\ i \end{pmatrix} = \begin{pmatrix} 1 \\ i \end{pmatrix}, \qquad \sigma_z \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$
$$\sigma_x \begin{pmatrix} 1 \\ -1 \end{pmatrix} = -\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \quad \sigma_y \begin{pmatrix} 1 \\ -i \end{pmatrix} = -\begin{pmatrix} 1 \\ -i \end{pmatrix}, \quad \sigma_z \begin{pmatrix} 0 \\ 1 \end{pmatrix} = -\begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

The normalized eigenvectors of σ_x are $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, and normalized eigenvectors of σ_y are $|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$ and $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$. The eigenvectors of σ_z are $|0\rangle$ and $|1\rangle$. These eigenvectors correspond to the $\hat{x}, \hat{y}$ and $\hat{z}$ axes of the Bloch sphere in Figure 4, respectively.

When matrices σ_x, σ_y or σ_z are applied to a state on the Bloch sphere, they rotate the state by π radians around the $\hat{x}, \hat{y}$ or $\hat{z}$ axis, respectively. For example, the action of σ_x on the state $|0\rangle$ is to rotate it to $|1\rangle$, and vice versa. Note that for the eigenstates of these matrices with eigenvalue -1, this still applies if considering a global phase of $-1 = e^{i\pi}$, given that two quantum states $|\psi\rangle$ and $e^{i\phi}\,|\psi\rangle$ are indistinguishable by any quantum measurement.

Matrices σ_x and σ_z will also be referred to as X and Z, respectively.

Unitary operators

Closed systems, i.e., systems that do not interact with other systems evolve according to unitary operators. In quantum computation, these unitary operators are also known as *gates*. For a state $|\psi\rangle$, a unitary operator U describes an evolution from $|\psi\rangle$ to $U|\psi\rangle$.
Pauli matrices are examples of unitary operators. The X and Z gates are often referred to as the *not* and *phase flip* gates, respectively. Other important unitary operators include *Hadamard gate*, denoted H, which maps $|0\rangle$ to $|+\rangle$ and $|1\rangle$ to $|-\rangle$, and the *phase-shift gate*, denoted P, which leaves $|0\rangle$ unaltered applies a phase shift of θ to the state $|1\rangle$:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad P = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}.$$

When the Pauli matrices are exponentiated, they result in three valuable classes of unitary matrices, corresponding to the rotation operators around the $\hat{x}$, $\hat{y}$, and $\hat{z}$ axes, which are defined as follows:

$$R_x(\theta) = e^{-i\theta\sigma_x/2} = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right)\sigma_x = \begin{pmatrix} \cos(\frac{\theta}{2}) & -i\sin(\frac{\theta}{2}) \\ -i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix},$$

$$R_y(\theta) = e^{-i\theta\sigma_y/2} = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right)\sigma_y = \begin{pmatrix} \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix},$$

$$R_z(\theta) = e^{-i\theta\sigma_z/2} = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right)\sigma_z = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}.$$

Theorem 3.2.2. *[35] Suppose U is a unitary operation on a single qubit. Then there exist real numbers α, β, γ and δ such that*

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta).$$

There are also multi-qubit gates, such as the *controlled-not* gate, denoted ***CNOT***, which leaves the states $|00\rangle$ and $|01\rangle$ unchanged, and maps $|10\rangle$ and $|11\rangle$ to each other:

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

In this case, as the state of the first qubit determines if the X gate is applied to the second qubit, the first qubit is called the *control qubit* and the second qubit the *target qubit*.
There is an "extension" of the controlled-not gate, the controlled-U gate, where U is a unitary gate acting on a single qubit. This gate applies the gate U to the target qubit if the control qubit is in state $|1\rangle$ and does nothing otherwise. It is defined as:

$$
\begin{aligned}
&\mathit{CU}(|0\rangle \otimes |\psi\rangle) = |0\rangle \otimes |\psi\rangle \\
&\mathit{CU}(|1\rangle \otimes |\psi\rangle) = |1\rangle \otimes U\,|\psi\rangle\,.
\end{aligned}
$$

It should be noted that no completely closed systems exist in the universe. Nevertheless, for many systems, the approximation of a closed system is valid.

Measurements

There are times when it necessary to observe the system to extract information. This interection leaves the system no longer closed and, consequently, the evolution of the system is no longer unitary.
The act of measuring a qubit is represented by a set of operators called *measurement operators*, denoted $\{M_m\}$. These operators act on the state space of the system being measured. The index m refers possible measurement outcomes. These measurement operators must satisfy the completeness equation $\sum_m M_m^\dagger M_m = I$, which ensures that the probabilities of all possible outcomes sum to 1. If a measurement M_m is performed on a state $|\psi\rangle$ the outcome m is observed with probability $p_m = \langle\psi|\, M_m^\dagger M_m\,|\psi\rangle$ for each m. Moreover, after a measurement yielding outcome m, the state collapses to $\frac{M_m|\psi\rangle}{\sqrt{p_m}}$.
In the case of the computational basis, the measurement operators are the projectors onto the basis states $|0\rangle$ and $|1\rangle$ denoted by $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$, respectively. Considering an arbitrary state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, the probabilities of measuring 0 and 1 are $p_0 = \langle\psi|\, M_0 M_0^\dagger\,|\psi\rangle = \langle\psi|\, M_0\,|\psi\rangle = |\alpha|^2$, and $p_1 = \langle\psi|\, M_1 M_1^\dagger\,|\psi\rangle = \langle\psi|\, M_1\,|\psi\rangle = |\beta|^2$. Consequently the states after measurement are $\frac{M_0|\psi\rangle}{|\alpha|} = \frac{\alpha}{|\alpha|}\,|0\rangle = |0\rangle$ (with $p = p_0$) and $\frac{M_1|\psi\rangle}{|\beta|} = \frac{\beta}{|\beta|}\,|1\rangle = |1\rangle$ (with $p = p_1$).
From now on, unless stated otherwise, any reference to measurement should be understood as pertaining to the computational basis.
As previously mentioned, any states $|\psi\rangle$ and $e^{i\phi}\,|\psi\rangle$ are indistinguishable by any quantum measurement. Consider a measurement operator M_m, the probabilities of obtaining out-

come m are $\langle\psi| M_m^\dagger M_m |\psi\rangle$ and $\langle\psi| e^{-i\theta} M_m^\dagger M_m e^{i\theta} |\psi\rangle = \langle\psi| M_m^\dagger M_m |\psi\rangle$. For this reason, it is said that these states are equal from an observational point of view.

3.2.4 Density operators

Until now the state vector formalism was used. However there is an alternative formulation using density operators. The density operator is often known as the *density matrix*, the two terms will be used interchangeably.

A quantum state $|\psi\rangle$ is said to be a *pure state* if it is completely known, i.e. if it can be written as a ket. In this case, the state can be written in the density operator formalism as $\rho = |\psi\rangle\langle\psi|$. On the other hand, a state that is a probabilistic mixture of pure states is designated a *mixed state*. A mixed state $\sum_i \alpha_i |\psi_i\rangle$ can be represented by a density operator $\rho = \sum_i |\alpha_i|^2 |\psi_i\rangle\langle\psi_i|$. Note that $|\alpha_i|^2$ is the probability of the system being in state $|\psi_i\rangle$.

With respect to density operators, when applying a unitary operator U to a state ρ, the resulting state is $U\rho U^\dagger$. Regarding measurements, given a collection of measurement operators, $\{M_m\}$, the probability of obtaining outcome m is $p(m) = \mathrm{Tr}(M_m \rho M_m^\dagger)$, and after a measurement yielding outcome m, the state collapes to $\frac{M_m^\dagger \rho M_m}{\mathrm{Tr}(M_m \rho M_m^\dagger)}$.

In subsection 3.2.1 it was shown how to determine the cartesian coordenates of a pure state in the Bloch Sphere from the state vector. For an arbitrary 2×2 density matrix, the following holds

$$\rho = \frac{1}{2}(I + r_x\sigma_x + r_y\sigma_y + r_z\sigma_z), \tag{3.8}$$

where $\vec{r} = (r_x, r_y, r_z)$ is a real three-dimensional vector such that $\|\vec{r}\|_2 \leq 1$. This vector is known as the Bloch vector for the state ρ. Since ρ is Hermitian. r_x, r_y and r_z are always real. The inverse map of Equation 3.8 is

$$r_\mu = \mathrm{Tr}(\rho\sigma_\mu) \tag{3.9}$$

Note that given that the trace is linear and matrix multiplication distributes over matrix addition, the cartesian coordinates of an operator consisting of the sum or subtraction of density operators can also be determined by Equation 3.9.

Reduced density operator

Density operators are particularly well-suited for describing individual subsystems of a composite quantum system. This type of description is provided by the *reduced density operator*

Given physical systems A and B whose composite system is given by the density operator ρ_{AB}, the reduced density operator for subsystem A is

$$\rho_A = \text{Tr}_B(\rho_{AB}),$$

where Tr_B is the partial trace over the Hilbert space of subsystem B, defined as

$$\begin{aligned}
\text{Tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) &= |a_1\rangle\langle a_2| \,\text{Tr}(|b_1\rangle\langle b_2|) \\
&= |a_1\rangle\langle a_2| \sum_\mu \langle\mu|\,|b_1\rangle\langle b_2|\,|\mu\rangle \\
&= |a_1\rangle\langle a_2| \sum_\mu \langle\mu|b_1\rangle\langle b_2|\mu\rangle \\
&= |a_1\rangle\langle a_2| \sum_\mu \langle b_2|\mu\rangle\langle\mu|b_1\rangle \\
&= |a_1\rangle\langle a_2| \langle b_2|b_1\rangle
\end{aligned}$$

where $|a_1\rangle$ and $|a_2\rangle$ are any two vectors in the state space of A, $|b_1\rangle$ and $|b_2\rangle$ are any two vectors in the state space of B, and $\{|\mu\rangle\}$, span the state space of B. Therefore, by linearly, the partial trace of $\rho_{AB} = \sum_{ijkl} p_{ijkl} |a_i\rangle\langle a_j| \otimes |b_k\rangle\langle b_l|$ is

$$\begin{aligned}
\text{Tr}_B(\rho_{AB}) &= \sum_{ijkl} p_{ijkl} \text{Tr}_B\left(|a_i\rangle\langle a_j| \otimes |b_k\rangle\langle b_l|\right) \\
&= \sum_{ijkl} p_{ijkl} |a_i\rangle\langle a_j| \sum_\mu \langle b_l|\mu\rangle\langle\mu|b_k\rangle = \sum_{ijkl} p_{ijkl} |a_i\rangle\langle a_j| \langle b_l|b_k\rangle
\end{aligned}$$

To demonstrate that this operator is a density operator, it must be shown that it possesses unit trace and is positive semidefinite. Given that the trace of ρ_{AB} corresponds to the sum of the diagonal elements of the density matrix, $\sum_i ikp_{iikk}$, and that that is also the case for the reduced density operator ρ_A, the sum of the diagonal elements is preserved by the partial trace. Thus, ρ_a has trace equal to 1. Moreover, considering that

$$\langle|\psi\rangle, \rho_{AB}|\psi\rangle\rangle = \langle\psi|\rho_{AB}|\psi\rangle = \langle\psi| \sum_{ijkl} p_{ijkl} |a_i\rangle\langle a_j| \otimes |b_k\rangle\langle b_l|\,|\psi\rangle$$

$$\begin{aligned}
&= \sum_{ijkl} p_{ijkl} \langle\psi|\,|a_i\rangle\langle a_j| \otimes |b_k\rangle\langle b_l|\,|\psi\rangle \\
&= \sum_{ijkl} p_{ijkl} \sum_m (\alpha_m^* \langle a_m| \otimes \langle b_m|)\,|a_i\rangle\langle a_j| \otimes |b_k\rangle\langle b_l| \sum_m (\alpha_m |a_m\rangle \otimes |b_m\rangle) \\
&= \sum_{ijklm} p_{ijkl} |\alpha_m|^2 \langle a_m|a_i\rangle\langle a_j|a_m\rangle\langle b_m|b_k\rangle\langle b_l|b_m\rangle
\end{aligned}$$

$$= \sum_{ijkl} p_{ijkl} \langle a_j|a_i\rangle \langle b_l|b_k\rangle$$

and that,

$$\langle |\psi\rangle , \rho_A |\psi\rangle\rangle = \langle\psi| \rho_A |\psi\rangle = \langle\psi| \sum_{ijkl} p_{ijkl} |a_i\rangle \langle a_j| \langle b_l|b_k\rangle |\psi\rangle$$

$$= \sum_{ijkl} p_{ijkl} \langle b_l|b_k\rangle \langle\psi| |a_i\rangle \langle a_j| |\psi\rangle =$$

$$= \sum_{ijklm} p_{ijkl} \langle b_l|b_k\rangle \sum_m (\alpha_m^* \langle a_m|) |a_i\rangle \langle a_j| \sum_m (\alpha_m |a_m\rangle)$$

$$= \sum_{ijklm} p_{ijkl} \langle b_l|b_k\rangle |\alpha_m|^2 \langle a_m|a_i\rangle \langle a_j|a_m\rangle = \sum_{ijkl} p_{ijkl} \langle b_l|b_k\rangle \langle a_j|a_i\rangle$$

$$= \sum_{ijkl} p_{ijkl} \langle a_j|a_i\rangle \langle b_l|b_k\rangle$$

where, $\{|a_m\rangle\}$ span the space of A and $\{|b_m\rangle\}$ span the space of B, it is possible to conclude that $\langle |\psi\rangle , \rho_{AB} |\psi\rangle\rangle = \langle |\psi\rangle , \rho_A |\psi\rangle\rangle$. Thus, since $\langle |\psi\rangle , \rho_{AB} |\psi\rangle\rangle \geq 0$, the same applies to $\langle |\psi\rangle , \rho_A |\psi\rangle\rangle$. Therefore, ρ_A is a positive semidefinite, and, consequently, a density operator.

In certain situations it is more advantageous to consider the reduced density operator for subsystem A defined as:

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}) = \sum_\mu \langle\mu| \rho_{AB} |\mu\rangle ,$$

where $\{|\mu\rangle\}$, span the state space of B and act only in the state space of B.

Similarly, the reduced density operator for subsystem B is $\rho_B = \mathrm{Tr}_A(\rho_{AB})$.

3.2.5 Quantum Channels

Thus far, only two types of quantum operations have been discussed: unitary operators, which describe the evolution of a closed quantum system, and measurements, which describe the act of observing a quantum system. Now, a new type of quantum operation that accounts for the more realistic notion of interaction between a quantum system and an environment will be introduced. Nonetheless, it is necessary to first introduce a few key concepts.

Definition 3.2.3. A *super-operator* Q is a linear map between the space of operators on a Hilbert space.

Definition 3.2.4. A super-operator Q is called *positive* if it sends positive matrices to positive matrices, *i.e.* $A \geq 0 \Rightarrow QA \geq 0$.

Definition 3.2.5. A super-operator Q is said to be *completely positive* if for all k,

$$Q \otimes I_{\mathbb{C}^{k\times k}} : \mathbb{C}^{n\times n} \otimes \mathbb{C}^{k\times k} \to \mathbb{C}^{m\times m} \otimes \mathbb{C}^{k\times k}$$

is positive.

Definition 3.2.6. A super-operator Q is called *trace-preserving* if Tr $(QA) =$ Tr(A).

Since density matrices are positive, any physically allowed transformation must be represented by a positive operator. Moreover, this is not sufficient on its own: since one can always extend the space $\mathbb{C}^{n\times n}$ to $\mathbb{C}^{n\times n} \otimes \mathbb{C}^{k\times k}$ by adjoining a new quantum system, any physically allowed transformation must be completely positive. Finally, since the trace of a density matrix is always 1, any physically allowed transformation must be trace-preserving. A **Completely Positive Trace-Preserving** (**CPTP**) operator is traditionally called a *quantum channel*.

Kraus operator sum representation

Assume that there is a quantum system S of interest which is a subsystem of a larger system which also includes an environment E. These systems have a joint unitary evolution described by a unitary operator U acting on the composite system, $U = \rho_{SE} \mapsto U\rho_{SE}U^\dagger$. Given that density matrices are positve operators, by (Definition 3.1.21), the density operator of the environment ρ_E initially can be written as

$$\rho_E = \sum_i p_i \left|i\right\rangle \left\langle i\right|$$

where $|i\rangle$ form an orthonormal basis for the state space of E and p_i are positive.
The state of the subsystem S after the unitary evolution corresponds to the partial trace of the joint state over the environment,

$$\begin{aligned}\rho_S =& \text{Tr}_E(U\rho_{SE}U^\dagger)\\ =& \sum_\mu \left\langle\mu\right| U\rho_{SE}U^\dagger \left|\mu\right\rangle\end{aligned}$$

where $\{|\mu\rangle\}$ span the state space of E.

Considering that initially both systems are completely decoupled, the initial state of the system can be written as $\rho_{SE} = \rho_S \otimes \rho_E$. Thus,

$$\begin{aligned}
\rho_S &= \sum_{\mu} \langle\mu| U \rho_S \otimes \sum_i p_i |i\rangle \langle i| U^\dagger |\mu\rangle \\
&= \sum_{\mu i} \sqrt{p_i} \langle\mu| U |i\rangle \rho_S \sqrt{p_i} \langle i| U^\dagger |\mu\rangle \\
&= \sum_{\mu i} \mathsf{K}_{\mu i} \rho_S \mathsf{K}_{\mu i}^\dagger
\end{aligned}$$

where the set of operators $\{\mathsf{K}_{\mu i}\}$ is designated *Kraus operators* and $\mathsf{K}_{\mu i} = \sqrt{p_i} \langle\mu| U |i\rangle$. Note that $\{|\mu\rangle\}$ and $\{|i\rangle\}$, act only in the state space of E. The equation $\rho_S = \sum_{\mu i} \mathsf{K}_{\mu i} \rho_S \mathsf{K}_{\mu i}^\dagger$ is called an ***Operator Sum Representation*** (***OSR***).

OSR can be thought of as a quantum channel that maps ρ_S to $\sum_{\mu i} \mathsf{K}_{\mu i} \rho_S \mathsf{K}_{\mu i}^\dagger$, given this map is **CPTP** [45].

Non-selective measurements

In the previously presented formalism to represent all the possible outcomes of a measurement, described by a set of operators $\{M_m\}$, on a state ρ, it would be necessary to write that state ρ collapse to state $\rho_m = \frac{M_m^\dagger \rho M_m}{\mathrm{Tr}(M_m \rho M_m^\dagger)}$ with probability $p(m) = \mathrm{Tr}(M_m \rho M_m^\dagger)$, for each possible outcome m. However, this is not appropriate for calculations. Consequently, to better represent the effect of a measurement on a quantum system *non-selective measurements* are used. In this case, the possible outcomes are not explicitly stated, and the state after the measurement is as follows:

$$\rho = \sum_m p_m \rho_m = \sum_m M_m \rho M_m^\dagger$$

This last equality corresponds to an Kraus operator sum representation, where the set of Kraus operators is $\{M_m\}$.

Norms on quantum channels

Definition 3.2.7. The norm of a super-operator $Q : \mathbb{C}^{n\times n} \to \mathbb{C}^{m\times m}$ is defined:

$$\|Q\|_1 = \max\{\|QA\|_1 \mid \|A\|_1 = 1\}, \tag{3.10}$$

where $A \in \mathbb{C}^{n\times n}$

Unfortunately, this norm is not stable under tensoring , given that the inequation $\|Q \otimes I_{\mathbb{C}^{n\times n}}\|_1 \leq \|Q\|_1$ does not hold [12]. As a result, the diamond norm, which is based on the trace norm, is used instead in the context of quantum channels.

Definition 3.2.8. Given a super-operator $Q : \mathbb{C}^{n\times n} \to \mathbb{C}^{m\times m}$, the diamond norm, $\|\cdot\|_\diamond$, is defined as:

$$\|Q\|_\diamond = \|Q \otimes I_{\mathbb{C}^{n\times n}}\|_1 \tag{3.11}$$

For this norm it holds that for all super-operators $Q : \mathbb{C}^{n\times n} \to \mathbb{C}^{m\times m}$ and $S : \mathbb{C}^{m\times m} \to \mathbb{C}^{o\times o}$, if Q is a quantum channel then $\|SQ\|_\diamond \leq \|S\|_\diamond$ [12, Proposition 3.44 and Proposition 3.48], and if S is a quantum channel, then $\|SQ\|_\diamond \leq \|Q\|_\diamond$. This is a desireble property, as is guarantees that quantum operations do not increase the distance between states, and as a consequence, composition of programs is valid.

Consider an operator r : $(\mathbb{C}^n \to \mathbb{C}^m) \to (\mathbb{C}^{n\times n} \to \mathbb{C}^{m\times m})$ that sends an operator T to the mapping $A \mapsto TAT^\dagger$. The exact calculation of distances induced by $\|\|_\diamond$ tends to be quite complicated, but a useful property for calculating the distance between quantum channels in the image of r is provided in [12]. Consider two operators $T, S : n \to m$. There exists a unit vector $v \in \mathbb{C}^n$ such that,

$$\|r(T)(vv^\dagger) - r(S)(vv^\dagger)\|_1 = \|r(T) - r(S)\|_\diamond \tag{3.12}$$

3.2.6 Quantum circuits

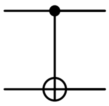
As quantum computation remains in its early stages of development, programming is primarily based on the use of *quantum circuits*. A quantum circuit consists of wires and *quantum gates*, which serve to transmit and manipulate quantum information. Each wire corresponds to a qubit, while the gates represent operations that can be applied to these qubits.

In this subsection the notation for the quantum gates used in this work will be introduced. Wires in parallel represent the tensor product of the respective qubits. For instance, $\psi_0 \otimes \psi_1$ corresponds to

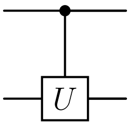
$$\begin{array}{l} |\psi_0\rangle \ \text{———} \\ |\psi_1\rangle \ \text{———} \end{array}$$

The single bit gates presented in Section 3.2.3 are represented as a box with the symbom of the gate inside. For example, the Hadamard gate is represented as

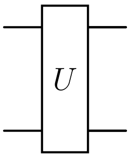
The controlled-not gate, which is a two-qubit gate, is represented as



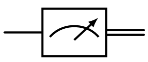
Similarly, the controlled-U gate, where U is an unitary single-qubit gate, is represented as



An arbitrary unitary operator acting on n qubits is represented as a box acting on n wires. For instance, the operator U acting on two qubits is represented as



CPTP maps are depicted as boxes containing the corresponding map symbols. The relevant **CPTP** operators will be introduced in section 4.8.
The measurement operation is representes by a "meter" symbol. Given that output of a measurement is a classical bit, the wire representing the output of a measurement is a classical wire, representes by a double line.



3.2.7 No-cloning theorem

The no-cloning theorem states that it is impossible to duplicate an unknown quantum bit [46]. In this subsection, an elementary proof of this theorem will be presented.
Suppose that there exists a unitary operator U that recieves a qubit $|\psi\rangle$ and some standard pure state $|s\rangle$ as input and oututs the state $|\psi\rangle \otimes |\psi\rangle$. The action of U can be written as

$$U\left(|\psi\rangle \otimes |s\rangle\right) = |\psi\rangle \otimes |\psi\rangle$$

Consider the aplication of U to two pure states $|\psi_0\rangle$ and $|\psi_1\rangle$,

$$U\left(|\psi_0\rangle \otimes |s\rangle\right) = |\psi_0\rangle \otimes |\psi_0\rangle$$
$$U\left(|\psi_1\rangle \otimes |s\rangle\right) = |\psi_1\rangle \otimes |\psi_1\rangle .$$

Given that unitary operators preserve inner products, the following equality should hold:

$$\langle\psi_0|\psi_1\rangle = \left(\langle\psi_0|\psi_1\rangle\right)^2$$

This equation is only satisfied if $\langle\psi_0|\psi_1\rangle = 0$ or $\langle\psi_0|\psi_1\rangle = 1$. The first case implies that $|\psi_0\rangle$ and $|\psi_1\rangle$ are orthogonal, and the second case implies that they are in the same state. Therefore, it is only possible to clone orthogonal states. These are the states perfectly distinguishable by measurement and thus are equivalent to copying classical information. For instance, it is impossible to the clone qubits $\psi_0 = |0\rangle$ and $\psi_1 = |-\rangle$, since they are not orthogonal.

It should be noted that this principle is upheld by the type system outlined in Figure 1, which does not allow the repeated use of a variable (seen as a quantum resource).

3.3 Interpretation

The syntax of the metric lambda calculus was presented in Chapter 2. Now, it is necessary to define the *model* of the "reality" of interest, *i.e.*, what the terms of the calculus mean within the "reality" considered. In the case of quantum lambda calculus, the model is based on quantum channels. The interpretation introduced in this subsection is based on the work of [24] with the addition of the measurement operation.

In order to define the interpretation of judgments $\Gamma \triangleright v : \mathbb{A}$, it is necessary to establish some notation first. Considering $v \in V$, $w \in W$, and $r \in R$ where V, W, R represent vector spaces, $\mathsf{sw}_{V,W} : V \otimes W \to W \otimes V$, denotes the swap operator, defined as $\mathsf{sw}_{V,W} = v \otimes w \mapsto w \otimes v$; $\lambda_V : \mathbb{C} \otimes V \to V$ is the left unitor defined as $\lambda_V = 1 \otimes v \mapsto v$; $\rho_V : V \otimes \mathbb{C} \to V$ is the right unitor defined as $\rho_V = v \otimes 1 \mapsto v$; and $\alpha_{V,W,R} : V \otimes (W \otimes R) \to (V \otimes W) \otimes R$ is the left associator, defined as $\alpha_{V,W,R} = v \otimes (w \otimes r) \mapsto (v \otimes w) \otimes r$. Moreover, for all operators $f : V \otimes W \to R$, the operator $\overline{f} : V \to (W \multimap R)$ denotes the corresponding curried version, defined as $\overline{f}(v) = w \mapsto f(v, w)$. On the other hand, the application operator denoted $\mathsf{app} : (V \multimap W) \otimes V \to W$, is defined as $f\,v = w$, where $f : V \multimap W$. The subscripts in these operators will be omitted unless ambiguity arises.

For all ground types $X \in G$ the interpretation of $[\![X]\!]$ is postulated as a vector space V. Types are interpreted inductively using the unit $\mathbb{I}$, the tensor $\otimes$, and the linear map $\multimap$. Given a non-empty context $\Gamma = \Gamma', x : \mathbb{A}$, its interpretation is defined by $[\![\Gamma', x : \mathbb{A}]\!] = [\![\Gamma']\!] \otimes [\![\mathbb{A}]\!]$ if Γ' is non-empty and $[\![\Gamma', x : \mathbb{A}]\!] = [\![\mathbb{A}]\!]$ otherwise. The empty context $-$ is interpreted as $[\![-]\!] = [\![\mathbb{I}]\!] = \mathbb{C}$. Given $X_1, ..., X_n \in V$, the n-tensor $(\ldots(X_1 \otimes X_2) \otimes \ldots) \otimes X_n$ is denoted as $X_1 \otimes \ldots \otimes X_n$, and similarly for operators.

"Housekeeping" operators are employed to handle interactions between context interpretation and the vectorial model. Given $\Gamma_1, \ldots, \Gamma_n$, the operator that splits $[\![\Gamma_1, \ldots, \Gamma_n]\!]$ into $[\![\Gamma_1]\!] \otimes \ldots \otimes [\![\Gamma_n]\!]$ is denoted by $\mathsf{sp}_{\Gamma_1;\ldots;\Gamma_n} : [\![\Gamma_1, \ldots, \Gamma_n]\!] \to [\![\Gamma_1]\!] \otimes \ldots \otimes [\![\Gamma_n]\!]$. For $n = 1$, $\mathsf{sp}_{\Gamma_1} = \mathrm{id}$. Let Γ_1 and Γ_2 be two contexts, $\mathsf{sp}_{\Gamma_1,\Gamma_2} \to \Gamma_1 \otimes \Gamma_2$ is defined as:

$$\mathsf{sp}_{-;\Gamma_2} = \lambda^{-1} \qquad \mathsf{sp}_{\Gamma_1;-} = \rho^{-1} \qquad \mathsf{sp}_{\Gamma_1;x:\mathbb{A}} = I \qquad \mathsf{sp}_{\Gamma_1;\Delta,x:\mathbb{A}} = \alpha \cdot (\mathsf{sp}_{\Gamma_1;\Delta} \otimes I)$$

For $n > 2$, $\mathsf{sp}_{\Gamma_1;\ldots;\Gamma_n}$ is is defined recursively based on the previous definition, using induction on n:

$$\mathsf{sp}_{\Gamma_1;\ldots;\Gamma_n} = (\mathsf{sp}_{\Gamma_1;\ldots;\Gamma_{n-1}} \otimes I) \cdot \mathsf{sp}_{\Gamma_1,\ldots,\Gamma_{n-1};\Gamma_n}$$

On the other hand, $\mathsf{jn}_{\Gamma_1;\ldots;\Gamma_n}$ denotes the inverse of $\mathsf{sp}_{\Gamma_1;\ldots;\Gamma_n}$. Next, given $\Gamma, x : \mathbb{A}, y : \mathbb{B}, \Delta$, the operator permuting x and y is denoted by $\mathsf{exch}_{\Gamma,x:\mathbb{A},y:\mathbb{B},\Delta} : [\![\Gamma, \underline{x : \mathbb{A}, y : \mathbb{B}}, \Delta]\!] \to [\![\Gamma, y : \mathbb{B}, x : \mathbb{A}, \Delta]\!]$ and defined as:

$$\mathsf{exch}_{\Gamma,\underline{x:\mathbb{A},y:\mathbb{B}},\Delta} = \mathsf{jn}_{\Gamma;y:\mathbb{B},x:\mathbb{A};\Delta} \cdot (I \otimes \mathsf{sw} \otimes I) \cdot \mathsf{sp}_{\Gamma;x:\mathbb{A},y:\mathbb{B};\Delta}$$

The shuffling operator $\mathsf{sh}_E : [\![E]\!] \to [\![\Gamma_1, \ldots, \Gamma_n]\!]$ is defined as a suitable composition of exchange operators.

For every operation symbol $f : \mathbb{A}_1, \ldots, \mathbb{A}_n \to \mathbb{A}$ it is assumed the existence of an operator $[\![f]\!] : [\![\mathbb{A}_1]\!] \otimes \ldots \otimes [\![\mathbb{A}_n]\!] \to [\![\mathbb{A}]\!]$. The interpretation of judgments is defined by induction over derivations according to the rules in Figure 5 [24].

$$\frac{[\![\Gamma_i \triangleright v_i : \mathbb{A}_i]\!] = m_i \quad f : \mathbb{A}_1, \dots, \mathbb{A}_n \to \mathbb{A} \in \Sigma \quad E \in \mathsf{Sf}(\Gamma_1; \dots; \Gamma_n)}{[\![E \triangleright f(v_1, \dots, v_n) : \mathbb{A}]\!] = [\![f]\!] \cdot (m_1 \otimes \dots \otimes m_n) \cdot \mathsf{sp}_{\Gamma_1;\dots;\Gamma_n} \cdot \mathsf{sh}_E} \qquad \frac{}{[\![x : \mathbb{A} \triangleright x : \mathbb{A}]\!] = \mathsf{I}_{[\![\mathbb{A}]\!]}}$$

$$\frac{}{[\![- \triangleright * : \mathbb{I}]\!] = \mathsf{I}_{[\![\mathbb{I}]\!]}} \qquad \frac{[\![\Gamma \triangleright v : \mathbb{A} \otimes \mathbb{B}]\!] = m \quad [\![\Delta, x : \mathbb{A}, y : \mathbb{B} \triangleright w : \mathbb{D}]\!] = n \quad E \in \mathsf{Sf}(\Gamma; \Delta)}{[\![E \triangleright \mathsf{pm}\ v\ \mathsf{to}\ x \otimes y.w : \mathbb{D}]\!] = n \cdot \mathsf{jn}_{\Delta;\mathbb{A};\mathbb{B}} \cdot \alpha \cdot \mathsf{sw} \cdot (m \otimes \mathsf{I}) \cdot \mathsf{sp}_{\Gamma;\Delta} \cdot \mathsf{sh}_E}$$

$$\frac{[\![\Gamma \triangleright v : \mathbb{A}]\!] = m \quad [\![\Delta \triangleright w : \mathbb{B}]\!] = n \quad E \in \mathsf{Sf}(\Gamma; \Delta)}{[\![E \triangleright v \otimes w : \mathbb{A} \otimes \mathbb{B}]\!] = (m \otimes n) \cdot \mathsf{sp}_{\Gamma;\Delta} \cdot \mathsf{sh}_E}$$

$$\frac{[\![\Gamma \triangleright v : \mathbb{I}]\!] = m \quad [\![\Delta \triangleright w : \mathbb{A}]\!] = n \quad E \in \mathsf{Sf}(\Gamma; \Delta)}{[\![E \triangleright v\ \mathsf{to}\ *.w : \mathbb{A}]\!] = n \cdot \lambda \cdot (m \otimes \mathsf{I}) \cdot \mathsf{sp}_{\Gamma;\Delta} \cdot \mathsf{sh}_E} \qquad \frac{[\![\Gamma, x : \mathbb{A} \triangleright v : \mathbb{B}]\!] = m}{[\![\Gamma \triangleright \lambda x : \mathbb{A}.\, v : \mathbb{A} \multimap \mathbb{B}]\!] = \overline{m \cdot \mathsf{jn}_{\Gamma;\mathbb{A}}}}$$

$$\frac{[\![\Gamma \triangleright v : \mathbb{A} \multimap \mathbb{B}]\!] = m \quad [\![\Delta \triangleright w : \mathbb{A}]\!] = n \quad E \in \mathit{Sf}(\Gamma; \Delta)}{[\![E \triangleright vw : \mathbb{B}]\!] = \mathsf{app} \cdot (m \otimes n) \cdot \mathsf{sp}_{\Gamma;\Delta} \cdot \mathsf{sh}_E} \qquad \frac{[\![\Gamma \triangleright v : \mathbb{A}]\!] = f}{[\![\Gamma \triangleright \mathsf{dis}(v) : \mathbb{I}]\!] = \mathsf{Tr} \cdot f}$$

Figure 5: Judgment interpretation

The following diagrams are useful to better understand the interpretation of judgements given in Figure 5.

$[\![\mathsf{ax}]\!]$: $[\![E]\!] \xrightarrow{\mathsf{sh}_E} [\![\Gamma_1, \dots, \Gamma_n]\!] \xrightarrow{\mathsf{sp}_{\Gamma;\Delta}} [\![\Gamma_1]\!] \otimes \dots \otimes [\![\Gamma_n]\!]$
$\xrightarrow{m_1 \otimes \dots \otimes m_n} [\![\mathbb{A}_1]\!] \otimes \dots \otimes [\![\mathbb{A}_n]\!] \xrightarrow{[\![f]\!]} [\![\mathbb{A}]\!]$

$[\![\mathsf{hyp}]\!]$: $[\![\mathbb{A}]\!] \xrightarrow{I_{[\![\mathbb{A}]\!]}} [\![\mathbb{A}]\!]$

$[\![\mathbb{I}_i]\!]$: $[\![\mathbb{I}]\!] \xrightarrow{I_{[\![\mathbb{I}]\!]}} [\![\mathbb{I}]\!]$

$[\![\otimes_e]\!]$: $[\![E]\!] \xrightarrow{\mathsf{sh}_E} [\![\Gamma, \Delta]\!] \xrightarrow{\mathsf{sp}_{\Gamma;\Delta}} [\![\Gamma]\!] \otimes [\![\Delta]\!] \xrightarrow{m \otimes \mathsf{I}} ([\![\mathbb{A}]\!] \otimes [\![\mathbb{B}]\!]) \otimes [\![\Delta]\!]$
$\xrightarrow{\mathsf{sw}} [\![\Delta]\!] \otimes ([\![\mathbb{A}]\!] \otimes [\![\mathbb{B}]\!]) \xrightarrow{\alpha} ([\![\Delta]\!] \otimes [\![\mathbb{A}]\!]) \otimes [\![\mathbb{B}]\!] \xrightarrow{\mathsf{jn}_{\Delta;\mathbb{A};\mathbb{B}}} [\![\Delta, \mathbb{A}, \mathbb{B}]\!]$
$\xrightarrow{n} [\![\mathbb{D}]\!]$

$[\![\otimes_i]\!]$: $[\![E]\!] \xrightarrow{\mathsf{sh}_E} [\![\Gamma, \Delta]\!] \xrightarrow{\mathsf{sp}_{\Gamma;\Delta}} [\![\Gamma]\!] \otimes [\![\Delta]\!] \xrightarrow{m \otimes n} [\![\mathbb{A}]\!] \otimes [\![\mathbb{B}]\!]$

$[\![\mathbb{I}_e]\!]$: $[\![E]\!] \xrightarrow{\mathsf{sh}_E} [\![\Gamma, \Delta]\!] \xrightarrow{\mathsf{sp}_{\Gamma;\Delta}} [\![\Gamma]\!] \otimes [\![\Delta]\!] \xrightarrow{m \otimes \mathsf{I}} [\![\mathbb{I}]\!] \otimes [\![\Delta]\!] \xrightarrow{\lambda} [\![\Delta]\!] \xrightarrow{n} [\![\mathbb{A}]\!]$

$[\![\multimap_i]\!]$: $[\![\Gamma]\!] \otimes [\![\mathbb{A}]\!] \xrightarrow{\overline{m \cdot \mathsf{jn}_{\Gamma;\mathbb{A}}}} [\![\mathbb{A}]\!] \multimap [\![\mathbb{B}]\!] \qquad ([\![\Gamma]\!] \otimes [\![\mathbb{A}]\!] \xrightarrow{\mathsf{jn}_{\Gamma;\mathbb{A}}} [\![\Gamma, \mathbb{A}]\!] \xrightarrow{m} [\![\mathbb{B}]\!])$

$[\![\multimap_e]\!]$: $[\![E]\!] \xrightarrow{\mathsf{sh}_E} [\![\Gamma, \Delta]\!] \xrightarrow{\mathsf{sp}_{\Gamma;\Delta}} [\![\Gamma]\!] \otimes [\![\Delta]\!] \xrightarrow{m \otimes n} [\![\mathbb{A}]\!] \multimap [\![\mathbb{B}]\!] \otimes [\![\mathbb{A}]\!] \xrightarrow{\mathsf{app}} [\![\mathbb{B}]\!]$

$[\![\mathsf{dis}]\!]$: $[\![\Gamma]\!] \xrightarrow{f} [\![\mathbb{A}]\!] \xrightarrow{\mathsf{Tr}} [\![\mathbb{I}]\!]$

Regarding the interpretation of the exhange and substitution properties, for any judgements

$\Gamma, x : \mathbb{A}, y : \mathbb{B}, \Delta \triangleright v : \mathbb{D}$, $\Gamma, x : \mathbb{A} \triangleright v : \mathbb{B}$, and $\Delta \triangleright w : \mathbb{A}$, the following equations hold:

$$\begin{aligned} [\![\Gamma, x : \mathbb{A}, y : \mathbb{B}, \Delta \triangleright v : \mathbb{D}]\!] &= [\![\Gamma, y : \mathbb{B}, x : \mathbb{A}, \Delta \triangleright v : \mathbb{D}]\!] \cdot \mathsf{exch}_{\Gamma, \underline{x:\mathbb{A}, y:\mathbb{B}}, \Delta} \\ [\![\Gamma, \Delta \triangleright v[w/x] : \mathbb{B}]\!] &= [\![\Gamma, x : \mathbb{A} \triangleright v : \mathbb{B}]\!] \cdot \mathsf{jn}_{\Gamma;\mathbb{A}} \cdot (\mathsf{I} \otimes [\![\Delta \triangleright w : \mathbb{A}]\!]) \cdot \mathsf{sp}_{\Gamma;\Delta} \end{aligned} \tag{3.13}$$

Types and operations in quantum lambda calculus

In the case of quantum lambda calculus, it is natural to consider a type *qbit* of quantum bits. The interpretation of this type is defined as $[\![qbit]\!] = \mathbb{C}^{2\times 2}$.

The following operations are considered: the creation of a new qubit in the state $|0\rangle$, *new* $0 : \mathbb{I} \multimap$ *qbit*, the creation of a new qubit in the state $|1\rangle$ (*new* $1 : \mathbb{I} \multimap$ *qbit*), measuring a qubit, *meas* : *qbit* $\multimap$ *qbit*, applying a unitary operation to a qubit, *U* : *qbit*$^{\otimes n}$ $\multimap$ *qbit*$^{\otimes n}$, and performing a **CPTP** operation on a qubit, *CPTP* : *qbit*$^{\otimes n}$ $\multimap$ *qbit*$^{\otimes n}$. These operations are defined in Figure 6.

$$[\![new\,0]\!] : \mathbb{C} \multimap [\![bit]\!] \qquad [\![new\,1]\!] : \mathbb{C} \multimap [\![bit]\!] \qquad [\![meas]\!] : [\![qbit]\!] \multimap [\![bit]\!]$$
$$1 \mapsto \left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right) \qquad 1 \mapsto \left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right) \qquad \rho \mapsto M_0\rho M_0^\dagger + M_1\rho M_1^\dagger$$
$$[\![U]\!] : [\![qbit]\!]^{\otimes n} \multimap [\![qbit]\!]^{\otimes n} \qquad [\![CPTP]\!] : [\![qbit]\!]^{\otimes n} \multimap [\![qbit]\!]^{\otimes n}$$
$$\rho \mapsto U\rho U^\dagger \qquad \rho \mapsto CPTP(\rho)$$

Figure 6: Interpretation of the operations in quantum lambda calculus.

The chosen model requires that all operators considered are **CPTP** maps. The identity I, the swap operator sw, the left and right unitors ρ and λ, the left associator α,the trace operation !, the split operator sp, the join operator jn, the exhange exch and shuffle sh are all **CPTP** maps [24]. However, the operators curry $\overline{f}$ and application app are not **CPTP** maps, which means that they are not allowed in this model. On the other hand the measurement operator $[\![meas]\!]$ and the unitary operator $[\![U]\!]$ are **CPTP** maps (Section 3.2.5, [12, page 73]).

Proposition 3.3.1. *The operators* $[\![new\,0]\!]$ *and* $[\![new\,1]\!]$ *are trace-preserving completely positive super-operators.*

Proof. It is straightforward to verify that the operators $[\![new\,0]\!]$ and $[\![new\,1]\!]$ are trace-preserving. Given that matrices $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$ correspond to the projectors $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$, one has that

$$\langle\psi| |0\rangle \langle 0| \otimes I^{\otimes n} |\psi\rangle = \langle\psi| |0\rangle \langle 0| \otimes \left(\frac{|0\rangle \langle 0| + |1\rangle \langle 1|}{2} \right)^{\otimes n} |\psi\rangle \tag{3.14}$$

$$= \sum_i |\alpha_i|^2 \langle\psi_{0i}|0\rangle \langle 0|\psi_{0i}\rangle \langle\psi_{1i}| \left(\frac{|0\rangle \langle 0| + |1\rangle \langle 1|}{2} \right) |\psi_{1i}\rangle \dots \langle\psi_{ni}| \left(\frac{|0\rangle \langle 0| + |1\rangle \langle 1|}{2} \right) |\psi_{ni}\rangle$$

(3.15)

$$= \sum_i |\alpha_i|^2 | \langle 0|\psi_{0i}\rangle |^2 \left(\frac{(| \langle 0|\psi_{1i}\rangle |^2 + | \langle 1|\psi_{1i}\rangle |^2) \dots (| \langle 0|\psi_{ni}\rangle |^2 + | \langle 1|\psi_{ni}\rangle |^2)}{2} \right) \tag{3.16}$$

(3.17)

Considering that the squared absolute value of a real number is always non-negative, the expression above is always non-negative. Therefore, the operator $[\![$*new* $0]\!]$ is positive. The same reasoning can be applied to the operator $[\![$*new* $1]\!]$. Therefore, attending to Definition 3.2.5 and Definition 3.2.4, it is possible to conclude that both operators $[\![$*new* $0]\!]$ and $[\![$*new* $1]\!]$ are completely positive super-operators. As a result, both operators are **CPTP** maps.

□

3.3.1 Example: Deutsch's Algorithm

In 1985, David Deutsch presented an algorithm that determines whether a function f is constant for a single-bit input (*i.e.*, either equal to 1 for all x or equal to 0 for all x) or balanced (*i.e.*, equal to 1 for half of the values of x and equal to 0 for the other half) [47]. Classically, to determine which case holds requires running f twice. Quantumly, it suffices to run f once. The Deutsch-Jozsa Algorithm is a simple example of a quantum algorithm that outperforms its classical counterpart. The algorithm is based on the concept of a quantum oracle, which is a black box that implements a unitary transformation U_f such that $U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$, where $\oplus$ denotes addition modulo 2. The quantum circuit implementing Deutsch's algorithm is presented in Figure 7.

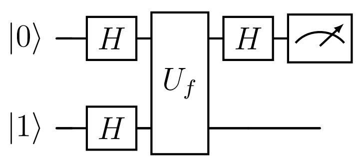


Figure 7: Quantum circuit implementing Deutsch's algorithm

Using lambda calculus, the Deutsch-Jozsa Algorithm can be expressed as:

$$\text{Deutsch} = -\triangleright \text{ pm } U_f(H\,(\textit{new}\,0\,(*)) \otimes H\,(\textit{new}\,1\,(*)))\ \textit{to}\ q_1 \otimes q_2\,.$$
$$\textit{meas}(H(q_1)) \otimes q_2 : \textit{qbit} \otimes \textit{qbit}$$

The proper interpretation of this term will be provided, but before that, an interpretation based on the quantum circuit in Figure 7 will be presented.

Attending to the circuit in Figure 7, one has that

$$\begin{aligned} & |0\rangle \otimes |1\rangle \\ \xmapsto{H\otimes H}\quad & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |-\rangle \end{aligned} \tag{3.18}$$

With respecto to quantum oracle U_f, it is possible to show that:

$$\begin{aligned} & |x\rangle \otimes |-\rangle = |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(|x\rangle \otimes |0\rangle - |x\rangle \otimes |1\rangle)) \\ \xmapsto{U_f}\ & \frac{1}{\sqrt{2}}(|x\rangle \otimes |0 \oplus f(x)\rangle - |x\rangle \otimes |1 \oplus f(x)\rangle) && \{\text{Defn. of } U_f\} \\ =\ & \frac{1}{\sqrt{2}}(|x\rangle\,|f(x)\rangle - |x\rangle\,|\neg f(x)\rangle) && \{0 \oplus x = x, 1 \oplus x = \neg x\} \\ =\ & \frac{1}{\sqrt{2}}(|x\rangle \otimes (|f(x)\rangle - |\neg f(x)\rangle)) \end{aligned} \tag{3.19}$$

Proceding by case distinction:

$$\frac{1}{\sqrt{2}}(|x\rangle \otimes (|f(x)\rangle - |\neg f(x)\rangle) = \begin{cases} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & \text{if } f(x) = 0 \\ |x\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) & \text{if } f(x) = 1 \end{cases} \tag{3.20}$$

It follows that:

$$|x\rangle \otimes \frac{1}{\sqrt{2}}(|f(x)\rangle - |\neg f(x)\rangle) = (-1)^{f(x)}\,|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = (-1)^{f(x)}\,|x\rangle \otimes |-\rangle \tag{3.21}$$

Returning to the interpretation of the Deutsch Algorithm, one has that:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |-\rangle \tag{3.22}$$

$$\xmapsto{U_f}\quad \frac{1}{\sqrt{2}}(U_f\,|0\rangle \otimes |-\rangle + U_f\,|1\rangle \otimes |-\rangle)) \tag{3.23}$$

$$=\quad \frac{1}{\sqrt{2}}((-1)^{f(0)}\,|0\rangle \otimes |-\rangle + (-1)^{f(1)}\,|1\rangle \otimes |-\rangle) \tag{3.24}$$

$$= \begin{cases} (\pm 1)\,|+\rangle \otimes |-\rangle & \text{if } f(0) = f(1) \\ (\pm 1)\,|-\rangle \otimes |-\rangle & \text{if } f(0) \neq f(1) \end{cases} \tag{3.25}$$

$$\xmapsto{H\otimes I} \begin{cases} (\pm 1)\,|0\rangle \otimes |-\rangle & \text{if } f(0) = f(1) \\ (\pm 1)\,|1\rangle \otimes |-\rangle & \text{if } f(0) \neq f(1) \end{cases} \tag{3.26}$$

Ignoring the global phase, the final state of the system is:

$$\xmapsto{\mathit{meas}\otimes I} \begin{cases} |0\rangle \otimes |-\rangle & \text{if } f(0) = f(1) \\ |1\rangle \otimes |-\rangle & \text{if } f(0) \neq f(1) \end{cases} \tag{3.27}$$

Now, regarding the interpretation of the lambda term Deutch,

$$\begin{aligned}
&[\![\text{Deutch}]\!] \\
&= [\![- \triangleright \text{pm } U_f(H\,(\mathit{new}\,0\,(*)) \otimes H\,(\mathit{new}\,1\,(*)))\ \mathit{to}\ q_1 \otimes q_2\,. \\
&\quad \mathit{meas}(H(q_1)) \otimes q_2 : \mathit{qbit} \otimes \mathit{qbit}]\!] \\
&= [\![q_1 : \mathit{qbit} \otimes q_2 : \mathit{qbit} \triangleright \mathit{meas}(H(q_1)) \otimes q_2 : \mathit{qbit} \otimes \mathit{qbit}]\!] \cdot \mathsf{jn}_{-;\mathit{qbit};\mathit{qbit}} && \{[\![\otimes_e]\!]\} \\
&\quad \cdot \alpha \cdot \mathsf{sw} \cdot ([\![- \triangleright U_f(H\,(\mathit{new}\,0\,(*)) \otimes H\,(\mathit{new}\,1\,(*))) : \mathit{qbit} \otimes \mathit{qbit}]\!] \\
&\quad \otimes I_{\mathbb{C}}) \cdot \mathsf{sp}_{-;-} \cdot \mathsf{sh}_{-;-} \\
&= ([\![q_1 : \mathit{qbit} \triangleright \text{meas}(H(q_1)) : \mathit{qbit}]\!] \otimes [\![q_2 : \mathit{qbit} \triangleright q_2 : \mathit{qbit}]\!]) && \{[\![\otimes_i]\!], \\
&\quad \cdot \mathsf{sp}_{\mathit{qbit};\mathit{qbit}} \cdot \mathsf{sh}_{\mathit{qbit};\mathit{qbit}} \cdot \mathsf{jn}_{-;\mathit{qbit};\mathit{qbit}} \cdot \alpha \cdot \mathsf{sw} \cdot ([\![- \triangleright U_f(H\,(\mathit{new}\,0\,(*)) && \text{Def. sp and sh}\} \\
&\quad \otimes H\,(\mathit{new}\,1\,(*))) : \mathit{qbit} \otimes \mathit{qbit}]\!] \otimes I_{\mathbb{C}}) \cdot I_{\mathbb{C}} \otimes I_{\mathbb{C}} \cdot I_{\mathbb{C}} \otimes I_{\mathbb{C}} \\
&= ([\![\text{meas}]\!] \cdot [\![H]\!] \cdot [\![q_1 : \mathit{qbit} \triangleright q_1 : \mathit{qbit}]\!] \cdot \mathsf{sp}_{\mathit{qbit}} \cdot \mathsf{sh}_{\mathit{qbit}} \otimes I_{[\![\mathit{qbit}]\!]}) && \{[\![\text{ax}]\!], [\![\text{hyp}]\!]\} \\
&\quad \cdot \mathsf{sp}_{\mathit{qbit};\mathit{qbit}} \cdot \mathsf{sh}_{\mathit{qbit};\mathit{qbit}} \cdot \mathsf{jn}_{-;\mathit{qbit};\mathit{qbit}} \cdot \alpha \cdot \mathsf{sw} \cdot ([\![U_f]\!] \cdot ([\![H]\!] \otimes [\![H]\!] \\
&\quad \cdot [\![\mathit{new}\,0]\!] \cdot [\![- \triangleright * : \mathbb{I}]\!] \cdot [\![\mathit{new}\,1]\!] \cdot [\![- \triangleright * : \mathbb{I}]\!]) \cdot \mathsf{sp}_{-;-} \cdot \mathsf{sh}_{-} \otimes I_{\mathbb{C}}) \\
&= ([\![\text{meas}]\!] \cdot [\![H]\!] \cdot I_{[\![\mathit{qbit}]\!]} \cdot I_{[\![\mathit{qbit}]\!]} \otimes I_{[\![\mathit{qbit}]\!]}) \cdot \mathsf{sp}_{\mathit{qbit};\mathit{qbit}} \cdot \mathsf{sh}_{\mathit{qbit};\mathit{qbit}} && \{[\![\text{hyp}]\!], [\![\mathbb{I}_i]\!], \\
&\quad \cdot \mathsf{jn}_{-;\mathit{qbit};\mathit{qbit}} \cdot \alpha \cdot \mathsf{sw} \cdot (([\![U_f]\!] \cdot ([\![H]\!] \cdot [\![\mathit{new}\,0]\!] \cdot I_{\mathbb{C}} \otimes [\![H]\!] \cdot [\![\mathit{new}\,1]\!] && \text{Def. sp and sh}\} \\
&\quad \cdot I_{\mathbb{C}}) \cdot I_{\mathbb{C}} \otimes I_{\mathbb{C}} \cdot I_{\mathbb{C}} \otimes I_{\mathbb{C}}) \otimes I_{\mathbb{C}}) \\
&= ([\![\text{meas}]\!] \cdot [\![H]\!] \otimes I_{[\![\mathit{qbit}]\!]}) \cdot \mathsf{sp}_{\mathit{qbit};\mathit{qbit}} \cdot \mathsf{sh}_{\mathit{qbit};\mathit{qbit}} \cdot \mathsf{jn}_{-;\mathit{qbit};\mathit{qbit}} \cdot \alpha \cdot \mathsf{sw} && \{\text{Figure 6}\} \\
&\quad \cdot (U_f\,(H\,|0\rangle\,\langle 0|\,H^\dagger \otimes H\,|1\rangle\,\langle 1|\,H^\dagger)\,U_f^\dagger \otimes I_{\mathbb{C}}) \\
&= ([\![\text{meas}]\!] \cdot [\![H]\!] \otimes I_{[\![\mathit{qbit}]\!]}) \cdot \mathsf{sp}_{\mathit{qbit};\mathit{qbit}} \cdot \mathsf{sh}_{\mathit{qbit};\mathit{qbit}} \cdot \mathsf{jn}_{-;\mathit{qbit};\mathit{qbit}} \cdot \alpha \cdot \mathsf{sw} && \{\text{Equation 3.18}, \\
&\quad \cdot \Bigg(\bigg(\frac{1}{\sqrt{2}}((-1)^{f(0)}\,|0\rangle\,\langle 0| \otimes |-\rangle\,\langle -| + (-1)^{f(1)}\,|1\rangle\,\langle 1| \otimes |-\rangle\,\langle -|)\bigg) && \text{Equation 3.24}\}
\end{aligned}$$

$$
\begin{aligned}
&\otimes I_{\mathbb{C}}\Big)\\
&= (\llbracket \mathsf{meas} \rrbracket \cdot \llbracket H \rrbracket \otimes I_{\llbracket qbit \rrbracket}) \cdot \mathsf{sp}_{qbit;qbit} \cdot \mathsf{sh}_{qbit;qbit} \cdot \lambda \otimes I_{\mathbb{C}} \cdot \alpha && \{\text{Def. jn}\}\\
&\quad \cdot \Big(I_{\mathbb{C}} \otimes \Big(\frac{1}{\sqrt{2}}((-1)^{f(0)} |0\rangle \langle 0| \otimes |-\rangle \langle -| + (-1)^{f(1)} |1\rangle \langle 1|\\
&\quad \otimes |-\rangle \langle -|)\Big)\Big)\\
&= (\llbracket \mathsf{meas} \rrbracket \cdot \llbracket H \rrbracket \otimes I_{\llbracket qbit \rrbracket}) \cdot \Big(\frac{1}{\sqrt{2}}((-1)^{f(0)} |0\rangle \langle 0| \otimes |-\rangle \langle -| && \{\text{Def. sp and sh}\}\\
&\quad + (-1)^{f(1)} |1\rangle \langle 1| \otimes |-\rangle \langle -|)\Big)\Big)\\
&= \begin{cases}
(M_0 \otimes I_{\llbracket qbit \rrbracket}) \cdot (H |+\rangle \langle +| H^\dagger \otimes |-\rangle \langle -|) & \text{if } f(0) = f(1)\\
\cdot (M_0^\dagger \otimes I_{\llbracket qbit \rrbracket}) + (M_1 \otimes I_{\llbracket qbit \rrbracket}) & \\
\cdot (H |+\rangle \langle +| H^\dagger \otimes |-\rangle \langle -|)(M_1^\dagger \otimes I_{\llbracket qbit \rrbracket}) & \\
(M_0 \otimes I_{\llbracket qbit \rrbracket}) \cdot (H |-\rangle \langle -| H^\dagger \otimes |-\rangle \langle -|) & \text{if } f(0) \neq f(1)\\
\cdot (M_0^\dagger \otimes I_{\llbracket qbit \rrbracket}) + (M_1 \otimes I_{\llbracket qbit \rrbracket}) & \\
\cdot (H |-\rangle \langle -| H^\dagger \otimes |-\rangle \langle -|)(M_1^\dagger \otimes I_{\llbracket qbit \rrbracket}) &
\end{cases} && \{\text{Equation 3.25, Figure 6}\}\\
&= \begin{cases}
|0\rangle \langle 0| \otimes |-\rangle \langle -| & \text{if } f(0) = f(1)\\
|1\rangle \langle 1| \otimes |-\rangle \langle -| & \text{if } f(0) \neq f(1)
\end{cases} && \{\text{Equation 3.26, Equation 3.27}\}
\end{aligned}
$$

Deutsch's Algorithm with Measurement Errors

A measurement error is characterized by reading a "1" as a "0" or vice versa. Measurement errors do not impact all states uniformly [48]. Consequently, there is a discrepancy in how frequently the state "1" is incorrectly read as "0" compared to how often the state "0" is measured as "1" or vice versa.

Given probabilities p_1 and p_2 of measuring a "0" as a "1" and a "1" as a "0", respectively, a measurement featuring this type of error, denoted meas^ϵ, is defined as follows:

$$
\begin{aligned}
&\mathsf{meas}^\epsilon : \llbracket qbit \rrbracket \to \llbracket qbit \rrbracket\\
&\qquad \rho \mapsto (1-p_1) M_0 \rho M_0^\dagger + (1-p_2) M_1 \rho M_1^\dagger + p_1 M_1 X \rho X^\dagger M_1^\dagger + p_2 M_0 X \rho X^\dagger M_0^\dagger
\end{aligned} \tag{3.28}
$$

Considering an arbitrary state $\rho = |\alpha|^2 |0\rangle\langle 0| + \alpha\beta^* |0\rangle\langle 1| + \alpha^* \beta |1\rangle\langle 0| + |\beta|^2 |1\rangle\langle 1|$, the resulting state after measurement is:

$$\begin{aligned}\text{meas}^{\epsilon}(\rho) &= (1-p_1)|\alpha|^2|0\rangle\langle 0| + (1-p_2)|\beta|^2|1\rangle\langle 1| + p_1|\alpha|^2|1\rangle\langle 1| + p_2|\beta|^2|0\rangle\langle 0| \\ &= ((1-p_1)|\alpha|^2 + p_2|\beta|^2)|0\rangle\langle 0| + ((1-p_2)|\beta|^2 + p_1|\alpha|^2)|1\rangle\langle 1|\end{aligned} \tag{3.29}$$

Given that

$$\begin{aligned}\text{Tr}(\text{meas}^{\epsilon}(\rho)) =& \text{Tr}(((1-p_1)|\alpha|^2 + p_2|\beta|^2)|0\rangle\langle 0| + ((1-p_2)|\beta|^2 + p_1|\alpha|^2)|1\rangle\langle 1|) \\ =&(1-p_1)|\alpha|^2 + p_2|\beta|^2 + (1-p_2)|\beta|^2 + p_1|\alpha|^2 = |\alpha|^2 + |\beta|^2 = \text{Tr}(\rho)\end{aligned} \tag{3.30}$$

this operator is trace-preserving. Attending to Equation 3.14 and to the fact that the sum of positive semidefinite matrices is semidefinite (Definition 3.1.21), it is straightforward to prove that the operator meas^{ϵ} is completely positive. As a result, meas^{ϵ} is a quantum channel and, consequently, a valid operation in the model considered.

For example, considering $p_1 = 0.1$ and $p_2 = 0.3$ the resulting state after measurement is:

$$\rho' = \begin{cases} 0.9\,|0\rangle\langle 0|\,|-\rangle\langle -| + 0.1\,|1\rangle\langle 1|\,|-\rangle\langle -| & \text{if } f(0) = f(1) \\ 0.3\,|0\rangle\langle 0|\,|-\rangle\langle -| + 0.7\,|1\rangle\langle 1|\,|-\rangle\langle -| & \text{if } f(0) \neq f(1) \end{cases} \tag{3.31}$$

As a result, the discrepancy between the ideal and actual measurement results, $[\![\rho - \rho']\!]_{\diamond}$, corresponds to:

$$\begin{aligned} &[\![\rho - \rho']\!]_{\diamond} \\ =& \begin{cases} \|(|0\rangle\langle 0|\,|-\rangle\langle -|) - (0.9\,|0\rangle\langle 0|\,|-\rangle\langle -| + 0.1\,|1\rangle\langle 1|\,|-\rangle\langle -|)\|_{\diamond} & \text{if } f(0) = f(1) \\ \|(|1\rangle\langle 1|\,|-\rangle\langle -|) - (0.3\,|0\rangle\langle 0|\,|-\rangle\langle -| + 0.7\,|1\rangle\langle 1|\,|-\rangle\langle -|)\|_{\diamond} & \text{if } f(0) \neq f(1) \end{cases} \\ =& \begin{cases} \|0.1\,|0\rangle\langle 0|\,|-\rangle\langle -| - 0.1\,|1\rangle\langle 1|\,|-\rangle\langle -|\|_{\diamond} & \text{if } f(0) = f(1) \\ \|-0.3\,|0\rangle\langle 0|\,|-\rangle\langle -| + 0.3\,|1\rangle\langle 1|\,|-\rangle\langle -|\|_{\diamond} & \text{if } f(0) \neq f(1) \end{cases} \\ =& \begin{cases} \|0.1\,(|0\rangle\langle 0| - |1\rangle\langle 1|)\,|-\rangle\langle -|\|_{\diamond} & \text{if } f(0) = f(1) \\ \|0.3\,(|1\rangle\langle 1| - |0\rangle\langle 0|)\,|-\rangle\langle -|\|_{\diamond} & \text{if } f(0) \neq f(1) \end{cases} \end{aligned} \tag{3.32}$$

Attending to Definition 3.1.9 and the multiplicativity of the diamond norm with respect to tensor products, it follows that:

$$[\![\rho - \rho']\!]_{\diamond} = \begin{cases} 0.1\||0\rangle\langle 0| - |1\rangle\langle 1|\|_{\diamond}\,\||-\rangle\langle -|\|_{\diamond} & \text{if } f(0) = f(1) \\ 0.3\|(|1\rangle\langle 1| - |0\rangle\langle 0|)\|_{\diamond}\,\||-\rangle\langle -|\|_{\diamond} & \text{if } f(0) \neq f(1) \end{cases} \tag{3.33}$$

Employing Equation 3.9, it is easily concluded that the Bloch vectors of the states $|0\rangle\langle 0|$, $|1\rangle\langle 1|$, and $|-\rangle\langle -|$ are $(-1,0,0)$, $(0,0,1)$, and $(0,0,-1)$, respectively. Consequently, and considering Definition 3.1.9 the discrepancy between the ideal and actual measurement results is:

$$
\begin{aligned}
[\![\rho - \rho']\!]_\diamond &= \begin{cases} 0.1\|(0,0,1)\|_2\|(1,0,0)\|_2 & \text{if } f(0) = f(1) \\ 0.3\|(0,0,-2)\|_2\|(1,0,0)\|_2 & \text{if } f(0) \neq f(1) \end{cases} \\
&= \begin{cases} 0.2\sqrt{1^2+0^2+0^2} \cdot \sqrt{1^2+0^2+0^2} & \text{if } f(0) = f(1) \\ 0.6\sqrt{(-1)^2+0^2+0^2} + \sqrt{1^2+0^2+0^2} & \text{if } f(0) \neq f(1) \end{cases} \\
&= \begin{cases} 0.2 & \text{if } f(0) = f(1) \\ 0.6 & \text{if } f(0) \neq f(1) \end{cases}
\end{aligned}
\tag{3.34}
$$

For an arbitray distance ϵ, between the ideal post-measurement state ρ he erroneous post-measurement stat ρ', using the metric deductive system in Figure 3 one can write:

$$
\begin{aligned}
&-\triangleright \text{ pm } U_f(H(\mathit{new}\,0(*)) \otimes H(\mathit{new}\,1(*))) \text{ to } q_1 \otimes q_2 \,. \\
&\quad \mathit{meas}(H(q_1)) \otimes q_2 : \mathit{qbit} \otimes \mathit{qbit} \\
&=_\epsilon \\
&-\triangleright \text{ pm } U_f(H(\mathit{new}\,0(*)) \otimes H(\mathit{new}\,1(*))) \text{ to } q_1 \otimes q_2 \,. \\
&\quad \mathit{meas}^\epsilon(H(q_1)) \otimes q_2 : \mathit{qbit} \otimes \mathit{qbit}
\end{aligned}
$$

Therefore, Deutsch $=_\epsilon$ Deutsch$^{\mathit{meas}^\epsilon}$, and consequently, for scenario under consideration, if f is a constant function, Deutsch $=_{0.2}$ Deutsch$^{\mathit{meas}^\epsilon}$; otherwise, Deutsch $=_{0.6}$ Deutsch$^{\mathit{meas}^\epsilon}$.

3.3.2 Example: Proving an equivalence using equations-in-context

This subsection aims to illustrate how to prove that creating a new qubit, discarding it, and then creating a new qubit is equivalent to just creating a new qubit, *i.e.*,

$$
-\triangleright \text{disc } \mathit{new}\,0(*) \text{ to } * \,.\, \mathit{new}\,0(*) : \mathit{qbit} = -\triangleright \mathit{new}\,0(*) : \mathit{qbit} \tag{3.35}
$$

syntactically, using equations-in-context.

The discard equation in the bottom line in Figure 2 states that all judgements $\Gamma \triangleright v : \mathbb{I}$ (with

$\Gamma = x_1 : \mathbb{A}_1, ..., x_n : \mathbb{A}_n$) carry no different information than that of just discarding all variables available in context Γ. Therefore,

$$- \triangleright * = \text{disc } \textit{new}0(*) \text{to} * : \mathbb{I} \tag{3.36}$$

Consequently,

$$- \triangleright \text{disc } \textit{new}0(*) \text{to} * . \textit{new}0(*) : \textit{qbit} = - \triangleright * \text{to} * . \textit{new}0(*) : \textit{qbit} \tag{3.37}$$

Subsequently applying the rule $\beta_{\mathbb{I}_e}$ in Figure 2, it holds that

$$\begin{aligned} - \triangleright \text{disc } \textit{new}0(*) \text{to} * . \textit{new}0(*) : \textit{qbit} &= - \triangleright * \text{ to } * . \textit{new}0(*) : \textit{qbit} \\ &= - \triangleright \textit{new}0(*) : \textit{qbit} \end{aligned} \tag{3.38}$$

Chapter 4

Conditionals

The notion of approximate equivalence for quantum programming explored in [24] does not encompass classical control flow, *i.e.*, the execution of operations conditioned on measurement outcomes.

This chapter presents the syntax, interpretation, and metric equations for the conditionals in quantum lambda calculus, along with several properties of the calculus. The syntax and interpretation are based on [34, 49, 50]. Although there is a notion of conditionals arising from the definition of measurement in Figure 6 based on the direct sum of super-operators [12, page 540], its emphasis is on the direct sum and not on the notion of conditionals. Since the goal of this work is to use a programming language to reason about quantum programs, it makes more sense to have an operator that is more focused on the notion of conditionals. As a result, a slightly different model for operations is introduced that draws inspiration from [51]. This model is based on direct sums of vector spaces and **CPTP** operators. Consequently, the concept of a **CPTP** operator is extended within this framework, and a new norm in the associated vector space is introduced, referred to as the *gen-norm*. The metric equations arise naturally from the definition of the gen-norm and are proven to be sound. At last, the utility of this framework is demonstrated through a series of examples of erroneous implementations of the quantum teleportation protocol.

4.1 A slightly different model for operations

Within the model of quantum lambda calculus, introduced in section 3.3, the measurement operation is defined in accordance with the standard approach in physics [12]. However, within this definiton the distinction between classical and quantum states is made through the elements of the spaces and not the spaces themselves, in the sense that both the result of measuring a quantum state, which is a classical bit, and the quantum state itself are elements of the same space, $\mathbb{C}^{2\times 2}$. Thus, now a new model based on the direct sums of vector spaces of square matrices is introduced.

As a result, it is necessary to define the operators considered in Figure 5 for direct sums of vector spaces. Consider the following complex vector spaces that are not the direct sum of other vector spaces $V_1, \ldots, V_n$, $W_1, \ldots, W_n$, and $R_1, \ldots, R_n$ and vectors $v_1 \in V_1, \ldots, v_n \in V_n, w_1 \in W_1, \ldots, w_m \in W_m, r_1 \in R_1, \ldots, r_t \in R_t$. These operators are defined as follows:

$$
\begin{aligned}
\mathsf{sw}_{V_1\oplus\ldots\oplus V_n, W_1\oplus\ldots\oplus W_n} :& V_1 \otimes W_1 \oplus \ldots \oplus V_n \otimes W_m \to W_1 \otimes V_1 \oplus \ldots \oplus W_m \otimes V_n \\
& (v_1 \otimes w_1, \ldots, v_n \otimes w_m) \mapsto (\mathsf{sw}_{V_1,W_1}(v_1 \otimes w_1), \ldots, \mathsf{sw}_{V_n,W_m}(v_n \otimes w_m))
\end{aligned}
$$

$$
\begin{aligned}
\lambda_{V_1\oplus\ldots\oplus V_n} :& \mathbb{C} \otimes V_1 \oplus \ldots \oplus \mathbb{C} \otimes V_n \to V_1 \oplus \ldots \oplus V_n \\
& (1 \otimes v_1, \ldots, 1 \otimes v_n) \mapsto (\lambda_{V_1}(1 \otimes v_1), \ldots, \lambda_{V_n}(1 \otimes v_n))
\end{aligned}
$$

$$
\begin{aligned}
\rho_{V_1\oplus\ldots\oplus V_n} :& V_1 \otimes \mathbb{C} \oplus \ldots \oplus V_n \otimes \mathbb{C} \to V_1 \oplus \ldots \oplus V_n \\
& (v_1 \otimes 1, \ldots, v_n \otimes 1) \mapsto (\rho_{V_1}(v_1 \otimes 1), \ldots, \rho_{V_n}(v_n \otimes 1))
\end{aligned}
$$

$$
\begin{aligned}
\alpha_{V_1\oplus\ldots\oplus V_n, W_1\oplus\ldots\oplus W_m, R_1\oplus\ldots\oplus R_t} :& V_1 \otimes (W_1 \otimes R_1) \oplus \ldots \oplus V_n \otimes (W_m \otimes R_t) \to \\
& (V_1 \otimes W_1) \otimes R_1 \oplus \ldots \oplus (V_n \otimes W_m) \otimes R_t \\
& (v_1 \otimes (w_1 \otimes r_1), \ldots, v_n \otimes (w_m \otimes r_t)) \mapsto \\
& (\alpha_{V_1,W_1,R_1}(v_1 \otimes (w_1 \otimes r_1)), \ldots, \alpha_{V_n,W_m,R_t}(v_n \otimes (w_m \otimes r_t)))
\end{aligned}
$$

Figure 8: Definition of the operators swap (sw), left unitor (λ), right unitor (ρ) and left associtor (α).

Within this model two distinct basic data types are considered: a type *bit* of classical bits and a type *qbit* of quantum bits. The interpretation of these types is defined as $[\![\mathit{bit}]\!] = \mathbb{C} \oplus \mathbb{C}$ and $[\![\mathit{qbit}]\!] = \mathbb{C}^{2\cdot 2}$. The type $\mathbb{I}$ is interpreted as $[\![\mathbb{I}]\!] = \mathbb{C}$.

The following operations are considered: the creation of a new bit $(1, 0)$, *new* $0 : \mathbb{I} \multimap \mathit{bit}$, the creation of a new bit $(0, 1)$, *new* $1 : \mathbb{I} \multimap \mathit{bit}$, the conversion of a bit into a qubit, $q : \mathit{bit} \multimap \mathit{qbit}$, measuring a qubit, $\mathit{meas} : \mathit{qbit} \to \mathit{bit}$, applying a unitary operation to a qubit $U : \mathit{qbit}, \ldots, \mathit{qbit} \to \mathit{qbit}^{\otimes n}$, and performing a **CPTP** operation on a qubit, $\mathit{CPTP} : \mathit{qbit}^{\otimes n} \multimap \mathit{qbit}^{\otimes n}$. These operations are defined in Figure 9.

$$\llbracket \textit{new}\, 0 \rrbracket : \mathbb{C} \multimap \llbracket \textit{bit} \rrbracket \qquad\qquad \llbracket \textit{new}\, 1 \rrbracket : \mathbb{C} \multimap \llbracket \textit{bit} \rrbracket$$
$$1 \mapsto (1,0) \qquad\qquad 1 \mapsto (0,1)$$
$$\llbracket q \rrbracket : \llbracket \textit{bit} \rrbracket \multimap \llbracket \textit{qbit} \rrbracket \qquad\qquad \llbracket \textit{meas} \rrbracket : \llbracket \textit{qbit} \rrbracket \multimap \llbracket \textit{bit} \rrbracket$$
$$(a,b) \mapsto \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \qquad\qquad \rho \mapsto (\mathrm{Tr}(M_0 \rho M_0^\dagger), \mathrm{Tr}(M_1 \rho M_1^\dagger))$$
$$\llbracket U \rrbracket : \llbracket \textit{qbit} \rrbracket^{\otimes n} \multimap \llbracket \textit{qbit} \rrbracket^{\otimes n} \qquad\qquad \llbracket \textit{CPTP} \rrbracket : \llbracket \textit{qbit} \rrbracket^{\otimes n} \multimap \llbracket \textit{qbit} \rrbracket^{\otimes n}$$
$$\rho \mapsto U \rho U^\dagger \qquad\qquad \rho \mapsto \textit{CPTP}(\rho)$$

Figure 9: Interpretation of the operations in quantum lambda calculus.

Furthermore, it is necessary to formally define certain concepts related to operators and super-operators within this context.

Definition 4.1.1. The trace of a vector $v = (v_1, \dots, v_n) \in \mathbb{C}^{o_1 \times o_1} \oplus \dots \oplus \mathbb{C}^{o_n \times o_n}$, is defined as

$$\mathrm{Tr}(v) = \sum_{i=1}^{n} \mathrm{Tr}(v_i) \tag{4.1}$$

Definition 4.1.2. An operator $A = (A_1, \dots, A_n) \in \mathbb{C}^{o_1 \times o_1} \oplus \dots \oplus \mathbb{C}^{o_n \times o_n}$ is said to be *positive* if A_i is positive for all $1 \le i \le n$.

Definition 4.1.3. An operator $U = (U_1, \dots, U_n) \in \mathbb{C}^{o_1 \times o_1} \oplus \dots \oplus \mathbb{C}^{o_n \times o_n}$ is *unitary* if U_i is unitary for all $1 \le i \le n$.

Definition 4.1.4. An super-operator $Q : \mathbb{C}^{o_1 \times o_1} \oplus \dots \oplus \mathbb{C}^{o_n \times o_n} \to \mathbb{C}^{p_1 \times p_1} \oplus \dots \oplus \mathbb{C}^{p_m \times p_m}$ is said to be *positive* if, for any $A \in \mathbb{C}^{o_1 \times o_1} \oplus \dots \oplus \mathbb{C}^{o_n \times o_n}$, the operator $Q(A)$ is also positive.

Definition 4.1.5. A super-operator $Q : \mathbb{C}^{o_1 \times o_1} \oplus \dots \oplus \mathbb{C}^{o_n \times o_n} \to \mathbb{C}^{p_1 \times p_1} \oplus \dots \oplus \mathbb{C}^{p_m \times p_m}$ is said to be *completely positive* if for all $k_1, \dots, k_t$,

$$\begin{aligned} Q \otimes I_{\mathbb{C}^{k_1 \times k_1} \oplus \dots \oplus \mathbb{C}^{k_t \times k_t}} :& (\mathbb{C}^{o_1 \times o_1} \oplus \dots \oplus \mathbb{C}^{o_n \times o_n}) \otimes (\mathbb{C}^{k_1 \times k_1} \oplus \dots \oplus \mathbb{C}^{k_t \times k_t}) \\ & \to (\mathbb{C}^{p_1 \times p_1} \oplus \dots \oplus \mathbb{C}^{p_m \times p_m}) \otimes (\mathbb{C}^{k_1 \times k_1} \oplus \dots \oplus \mathbb{C}^{k_t \times k_t}) \end{aligned}$$

is positive.

This new model further requires that all operators be **CPTP** maps. Consequently, it is necessary to prove that operators defined in Figure 8, as well as the interpretation of the operations *new* 0, *new* 1, q, and meas in Figure 9 are **CPTP** maps.

Proposition 4.1.6. *The operators swap* (sw)*, left unitor* (λ)*, right unitor* (ρ)*, and left associtor* (α) *defined in Figure 8 are* ***CPTP*** *maps.*

Proof. Attending to Definition 4.1.1 and given that the swap operator is trace-preserving when acting on complex vector spaces without direct sums, one has:

$$\mathsf{Tr}(\mathsf{sw}_{V_1,W_1}(v_1 \otimes w_1), \ldots, \mathsf{sw}_{V_n,W_m}(v_n \otimes w_m)) = \sum_{i=1}^{n}\sum_{j=1}^{m} \mathsf{Tr}(v_i \otimes w_j) = \mathsf{Tr}(v_1 \otimes w_1, \ldots, v_n \otimes w_m). \tag{4.2}$$

Therefore, considering Figure 8 the swap operator is trace-preserving.
Given that, for any arbitrary complex space $R_1 \oplus \ldots \oplus R_t$, it holds that

$$\begin{aligned} &\mathsf{sw}_{V_1 \oplus \ldots \oplus V_n, W_1 \oplus \ldots \oplus W_m} \otimes I_{R_1 \oplus \ldots \oplus R_t}((v_1 \otimes w_1, \ldots, v_n, \ldots, w_n) \otimes (r1, \ldots, r_t)) \\ &= (\mathsf{sw}_{V_1,W_1}(v_1 \otimes w_1), \ldots, \mathsf{sw}_{V_n,W_m}(v_n \otimes w_m)) \otimes (r_1, \ldots, r_t) \\ &= (\mathsf{sw}_{V_1,W_1}(v_1 \otimes w_1) \otimes r_1, \ldots, \mathsf{sw}_{V_n,W_m}(v_n \otimes w_m) \otimes r_n) \\ &= (\mathsf{sw}_{V_1,W_1} \otimes I_{R_1}(v_1 \otimes w_1 \otimes r_1), \ldots, \mathsf{sw}_{V_n,W_m} \otimes I_{R_t}(v_n \otimes w_m \otimes r_t)) \end{aligned} \tag{4.3}$$

Considering that the swap operator is completely positive when acting on complex vector spaces without direct sums, it follows that the expression in the last line of Equation 4.3 is positive. Consequently, attending to Definition 4.1.5, the swap operator is completely positive.
The proof that the left unitor, right unitor, and left associtor are **CPTP** maps follows the same reasoning used for the swap operator. □

Proposition 4.1.7. *The operators* $[\![$*new* $0]\!]$ *and* $[\![$*new* $1]\!]$ *are trace-preserving completely positive super-operators.*

Proof. Attending to Definition 4.1.1, one has that:

$$\mathsf{Tr}\left([\![\mathit{new}\ 0]\!]\right)(1) = \mathsf{Tr}((1,0)) = 1 \tag{4.4}$$

As a result, considering Figure 9, the operator $[\![$*new* $0]\!]$ is trace-preserving.

□

provas

The first step is to demonstrate that for any super-operators P and Q the following holds:

Lemma 4.1.8. $\|[P,Q]\|_\sigma \leq \max\{\|P\|_\sigma, \|Q\|_\sigma\}$

Proof. Employing the definition of the operator norm in **??**, it follows that:

$$
\begin{aligned}
&\mathsf{sup}\{\|[P,Q](v)\| \mid \|v\|=1\} \leq \mathsf{max}\{\mathsf{sup}\{\|P(w)\| \mid \|w\|=1\}, \mathsf{sup}\{\|Q(u)\| \mid \|u\|=1\}\} \\
&= \mathsf{sup}\{\|[P,Q](w,u)\| \mid \|w\|+\|u\|=1\} \leq \mathsf{max}\{\mathsf{sup}\{\|P(w)\| \mid \|w\|=1, \|Q(u)\| \mid \|u\|=1\}\} \\
&= \mathsf{sup}\{\|P(w)+Q(u)\| \mid \|w\|+\|u\|=1\|=1\} \leq \mathsf{max}\{\mathsf{sup}\{\|P(w)\| \mid \|w\|=1, \|Q(u)\| \mid \|u\|=1\}\} \\
&= \mathsf{sup}\{\|P(w)+Q(u)\| \mid \|w\|+\|u\|=1\} \leq \mathsf{sup}\{\mathsf{max}\{\|P(w)\| \mid \|w\|=1, \|Q(u)\| \mid \|u\|=1\}\}
\end{aligned} \tag{4.5}
$$

Therefore, by the triangle inequality, proving the inequality in Equation 4.6 suffices to establish Lemma 4.1.8.

$$
\mathsf{sup}\{\|P(w)\|+\|Q(u)\| \mid \|w\|+\|u\|=1\} \leq \mathsf{sup}\{\mathsf{max}\{\|P(w)\| \mid \|w\|=1, \|Q(u)\| \mid \|u\|=1\}\} \tag{4.6}
$$

This can be rewritten as:

$$
\|w\|+\|u\|=1 \land \mathsf{sup}\{\|P(w)\|+\|Q(u)\|\} \leq \mathsf{max}\left\{\frac{1}{\|w\|}\|P(w)\|, \frac{1}{\|u\|}\|Q(u)\|\right\} \tag{4.7}
$$

As a result,

$$
\|w\|+\|u\|=1 \land \mathsf{sup}\{\|P(w)\|+\|Q(u)\|\} \leq \mathsf{max}\left\{\left\|P\left(\frac{1}{\|w\|}w\right)\right\|, \left\|Q\left(\frac{1}{\|u\|}u\right)\right\|\right\} \tag{4.8}
$$

This is equivalent to demonstrating that for $a+b=1$,

$$
x+y \leq \max\left\{\frac{1}{a}x, \frac{1}{b}y\right\} \tag{4.9}
$$

This is done by arguing by *reductio ad absurdum*, *i.e.*, supposing otherwise leads to a contradiction:

$$
\begin{aligned}
&x+y > \max\left\{\frac{1}{a}x, \frac{1}{b}y\right\} \\
&\Rightarrow x+y > \frac{1}{a}x \land x+y > \frac{1}{b}y \\
&\Rightarrow a(x+y) > x \land b(x+y) > y \\
&\Rightarrow ax+ay > x \land bx+by > y \\
&\Rightarrow ax+ay > x \land (1-a)x+(1-a)y > y \\
&\Rightarrow ax+ay > x \land x-ax+y-ay > y \\
&\Rightarrow x < ax+ay \land x > ax+ay
\end{aligned} \tag{4.10}
$$

4.2 Syntax

The term formation rules for conditionals are depicted in Figure 10.

$$\frac{\Gamma \triangleright v : \mathbb{A}}{\Gamma \triangleright \mathsf{inl}_{\mathbb{B}}(v) : \mathbb{A} \oplus \mathbb{B}}\,(\mathsf{inl}) \qquad \frac{\Gamma \triangleright v : \mathbb{B}}{\Gamma \triangleright \mathsf{inr}_{\mathbb{A}}(v) : \mathbb{A} \oplus \mathbb{B}}\,(\mathsf{inr})$$

$$\frac{\Gamma \triangleright v : \mathbb{A} \oplus \mathbb{B} \quad \Delta, x : \mathbb{A} \triangleright w : \mathbb{D} \quad \Delta, y : \mathbb{B} \triangleright u : \mathbb{D} \quad E \in \mathsf{Sf}(\Gamma; \Delta)}{E \triangleright \mathsf{case}\; v\, \{\mathsf{inl}_{\mathbb{B}}(x) \Rightarrow w; \mathsf{inr}_{\mathbb{A}}(y) \Rightarrow u\} : \mathbb{D}}\,(\mathsf{case})$$

Figure 10: Term formation rules for conditionals

Properties

The rules presented in Figure 10 are subject the properties in Theorem 4.2.1.

Theorem 4.2.1. *Lambda calculus with conditionals has the following properties:*

1. *for all judgements $\Gamma \triangleright v$ and $\Gamma' \triangleright v$, te(Γ) $\simeq_\pi$ te(Γ');*
2. *additionally if $\Gamma \triangleright v : \mathbb{A}, \Gamma' \triangleright v : \mathbb{A}'$, and $\Gamma \simeq_\pi \Gamma'$, then $\mathbb{A}$ must be equal to $\mathbb{A}'$;*
3. *all judgements $\Gamma \triangleright v : \mathbb{A}$ have a unique derivation.*

Proof Regarding the first property, for the injections, taking into account the inl and inr derivations in Figure 10 and

$$\frac{\Gamma' \triangleright v : \mathbb{A}}{\Gamma' \triangleright \mathsf{inl}_{\mathbb{B}}(v) : \mathbb{A} \oplus \mathbb{B}} \qquad \frac{\Gamma' \triangleright v : \mathbb{B}}{\Gamma' \triangleright \mathsf{inr}_{\mathbb{A}}(v) : \mathbb{A} \oplus \mathbb{B}}$$

, it is necessary to prove that te(Γ) $\simeq_\pi$ te(Γ'). By induction hypothesis, te(Γ) $\simeq_\pi$ te(Γ') and te(Γ) $\simeq_\pi$ te(Γ'). Therefore, te(Γ) $\simeq_\pi$ te(Γ').

Concerning the case statement, considering Figure 10 and

$$\frac{\Gamma' \triangleright v : \mathbb{A} \oplus \mathbb{B} \quad \Delta', x : \mathbb{A} \triangleright w : \mathbb{D} \quad \Delta', y : \mathbb{B} \triangleright u : \mathbb{D} \quad E' \in \mathsf{Sf}(\Gamma'; \Delta')}{E' \triangleright \mathsf{case}\; v\, \{\mathsf{inl}_{\mathbb{B}}(x) \Rightarrow w; \mathsf{inr}_{\mathbb{A}}(y) \Rightarrow u\} : \mathbb{D}}$$

we want to prove that $\mathsf{te}(E) \simeq_\pi \mathsf{te}(E')$. By induction hypothesis, $\mathsf{te}(\Gamma) \simeq_\pi \mathsf{te}(\Gamma)$, $\mathsf{te}(\Delta, x) \simeq_\pi \mathsf{te}(\Delta', x)$ and $\mathsf{te}(\Delta, y) \simeq_\pi \mathsf{te}(\Delta', y)$. This implies that $\mathsf{te}(\Delta) \simeq_\pi \mathsf{te}(\Delta')$. Since, $E \in \mathsf{Sf}(\Gamma; \Delta)$ and $E' \in \mathsf{Sf}(\Gamma'; \Delta')$, one has that $\mathsf{te}(E) \simeq_\pi \mathsf{te}(\Gamma, \Delta)$ and $\mathsf{te}(E') \simeq_\pi \mathsf{te}(\Gamma', \Delta')$. Consequently, $\mathsf{te}(E)$ $\simeq_\pi \mathsf{te}(E')$.

With respect to the second property, for the injections, taking into account the inl and inr derivations in Figure 10 and

$$\frac{\Gamma' \triangleright v : \mathbb{A}'}{\Gamma' \triangleright \mathsf{inl}_{\mathbb{B}}(v) : \mathbb{A}' \oplus \mathbb{B}} \qquad \frac{\Gamma' \triangleright v : \mathbb{B}'}{\Gamma' \triangleright \mathsf{inr}_{\mathbb{A}}(v) : \mathbb{A} \oplus \mathbb{B}'}$$

concerning the left injection it is neccessary to prove that if $\Gamma \triangleright \mathsf{inl}_{\mathbb{B}}(v) : \mathbb{A} \oplus \mathbb{B}, \Gamma' \triangleright \mathsf{inl}_{\mathbb{B}}(v) : \mathbb{A}' \oplus \mathbb{B}$, and $\Gamma \simeq_\pi \Gamma'$, then $\mathbb{A} \oplus \mathbb{B}$ must be equal to $\mathbb{A}' \oplus \mathbb{B}$. By induction hypothesis over the premises it follows that $\mathbb{A}$ must be equal to $\mathbb{A}'$. Consequentlty, $\mathbb{A} \oplus \mathbb{B}$ must be equal $\mathbb{A}' \oplus \mathbb{B}$ The same reasoning can be applied to the right injection.

Regarding the case statement in considering Figure 10 and

$$\frac{\Gamma \triangleright v : \mathbb{A} \oplus \mathbb{B} \quad \Delta', x : \mathbb{A} \triangleright w : \mathbb{C}' \quad \Delta', y : \mathbb{B} \triangleright u : \mathbb{C}' \quad E' \in \mathsf{Sf}(\Gamma'; \Delta')}{E' \triangleright \mathsf{case}\, v\, \{\mathsf{inl}_{\mathbb{B}}(x) \Rightarrow w; \mathsf{inr}_{\mathbb{A}}(y) \Rightarrow u\} : \mathbb{C}'}$$

we want to prove that if $E \triangleright \mathsf{case}\, v\, \{\mathsf{inl}(x) \Rightarrow w; \mathsf{inr}(y) \Rightarrow u\} : \mathbb{D}; \Gamma' \triangleright \mathsf{case}\, v\, \{\mathsf{inl}(x) \Rightarrow w; \mathsf{inr}(y) \Rightarrow u\} : \mathbb{D}'$, and $E \simeq_\pi E'$, then $\mathbb{D}$ must be equal to $\mathbb{D}'$. Assuming, that $E \simeq_\pi E'$ and knowing that $E \in \mathsf{Sf}(\Gamma; \Delta)$ and $E' \in \mathsf{Sf}(\Gamma'; \Delta')$, one has that

$$\begin{aligned}
& x : \mathbb{A} \in \Delta & \\
\Longrightarrow\ & x : \mathbb{A} \in E & \{E \in \mathsf{Sf}(\Gamma; \Delta)\} \\
\Longrightarrow\ & x : \mathbb{A} \in E' & \{E \simeq_\pi E'\} \\
\Longrightarrow\ & x : \mathbb{A} \in \Delta' & \{\text{All terms are well typed and contexts do not share variables}\}
\end{aligned}$$

This proves that $\Delta \simeq_\pi \Delta'$. Therefore, by induction hypothesis on the premises of the conditional statement, one has that $\mathbb{D}$ must be equal to $\mathbb{D}'$.

Finally, concerning the third property, firstly it is necessary to demonstrate that the injections have unique derivations. This means proving that the premises of the inl and inr rules in Figure 10 and in

$$\frac{\Gamma' \rhd v : \mathbb{A}'}{\Gamma \rhd \mathsf{inl}_{\mathbb{B}}(v) : \mathbb{A}' \oplus \mathbb{B}} \qquad \frac{\Gamma' \rhd v : \mathbb{B}'}{\Gamma \rhd \mathsf{inr}_{\mathbb{A}}(v) : \mathbb{A} \oplus \mathbb{B}'}$$

are equal, which means proving that $\Gamma = \Gamma'$. In both cases, the derivation in Figure 10 enforces that $\Gamma = \Gamma'$.

Now, it is necessary to demonstrate that the case statement in Figure 10 has a unique derivation. This means proving that the premises in Figure 10 and in

$$\frac{\Gamma' \rhd v : \mathbb{A} \oplus \mathbb{B} \quad \Delta', x : \mathbb{A} \rhd w : \mathbb{C}' \quad \Delta', y : \mathbb{B} \rhd u : \mathbb{D} \quad E' \in \mathsf{Sf}(\Gamma'; \Delta')}{E \rhd \mathsf{case}\, v\, \{\mathsf{inl}_{\mathbb{B}}(x) \Rightarrow w; \mathsf{inr}_{\mathbb{A}}(y) \Rightarrow u\} : \mathbb{D}}$$

are equal, more concretely that $\Gamma = \Gamma'$ and $\Delta = \Delta'$.

$$\begin{aligned}
& x : \mathbb{A} \in \Gamma \\
\Longrightarrow\ & x : \mathbb{A} \in E \wedge te(x : \mathbb{A}) \in \Gamma' && \{E \in \mathsf{Sf}(\Gamma; \Delta), te(\Gamma) \simeq_\pi te(\Gamma')\} \\
\Longrightarrow\ & x : \mathbb{A} \in E \wedge x : \mathbb{A} \in \Gamma' && \{E \in \mathsf{Sf}(\Gamma; \Delta), E \in \mathsf{Sf}(\Gamma'; \Delta')\}
\end{aligned}$$

This last implication is related with the fact that in E, there can only exist one variable designated by x. Given that a shuffle preserves the relative order of the variables in each context, it follows that $\Gamma = \Gamma'$. The same reasoning can be applied to Δ and Δ', which concludes the proof.

□

Lemma 4.2.2. *(Exchange and Substitution) For every judgement $\Gamma, x : \mathbb{A}, y : \mathbb{B}, \Delta \rhd v : \mathbb{D}$ it is possible to derive $\Gamma, y : \mathbb{B}, x : \mathbb{A}, \Delta \rhd v : \mathbb{D}$. For all judgements $\Gamma, x : \mathbb{A} \rhd v : \mathbb{B}$ and $\Delta \rhd w : \mathbb{A}$ it is possible to derive $\Gamma, \Delta \rhd v[w/x] : \mathbb{B}$.*

Proof Regarding the exchange property, for the left injection, it is necessary to demonstrate that for every judgement $\Gamma, x : \mathbb{A}, y : \mathbb{B}, \Delta \triangleright \mathsf{inl}_{\mathbb{D}}(v) : \mathbb{D} \oplus \mathbb{D}$, it is possible to derive $\Gamma, y : \mathbb{B}, x : \mathbb{A}, \Delta \triangleright \mathsf{inl}_{\mathbb{D}}(v) : \mathbb{D} \oplus \mathbb{D}$. By induction hypothesis on the premises of $\Gamma, x : \mathbb{A}, y : \mathbb{B}, \Delta \triangleright \mathsf{inl}_{\mathbb{D}}(v) : \mathbb{D} \oplus \mathbb{D}$ and applying the inl rule, one has that:

$$\dfrac{\dfrac{\Gamma, x : \mathbb{A}, y : \mathbb{B}, \Delta \triangleright v : \mathbb{D}}{\Gamma, y : \mathbb{B}, x : \mathbb{A}, \Delta \triangleright v : \mathbb{D}}}{\Gamma, y : \mathbb{B}, x : \mathbb{A}, \Delta \triangleright \mathsf{inl}_{\mathbb{D}}(v) : \mathbb{D} \oplus \mathbb{D}}$$

For the right injection the proof is analogous.

With respect to the case statement it is necessary to prove that for every judgment $\Gamma, x : \mathbb{A}, y : \mathbb{B}, \Delta \triangleright$ case $v\,\{\mathsf{inl}_{\mathbb{E}}\ (a) \Rightarrow w; \mathsf{inr}_{\mathbb{D}}\ (b) \Rightarrow u\} : \mathbb{D}$, it is possible to derive $\Gamma, y : \mathbb{B}, x : \mathbb{A}, \Delta \triangleright$ case $v\,\{\mathsf{inl}_{\mathbb{E}}(a) \Rightarrow w; \mathsf{inr}_{\mathbb{D}}(b) \Rightarrow u\} : \mathbb{D}$. It is necessary to consider three scenarios:

1. $x : \mathbb{A}, y : \mathbb{B}$ are variables in the context of v;

2. $x : \mathbb{A}, y : \mathbb{B}$ are variables in the context of w and u;

3. $x : \mathbb{A}$ is a variable in the context of v and $y : \mathbb{B}$ is a variable in the context of w and u.

With respect to the first case, by induction hypothesis and applying the case rule, one has that:

$$\dfrac{\dfrac{\Gamma_1, x : \mathbb{A}, y : \mathbb{B}, \Gamma_2 \triangleright v : \mathbb{D} \oplus \mathbb{E} \quad \begin{array}{c} E, a : \mathbb{D} \triangleright w : \mathbb{D} \\ E, b : \mathbb{E} \triangleright u : \mathbb{D} \end{array} \quad \Gamma, y : \mathbb{B}, x : \mathbb{A}; \Delta \in \mathsf{Sf}(\Gamma_1, x : \mathbb{A}, y : \mathbb{B}, \Gamma_2; E)}{\Gamma_1, y : \mathbb{B}, x : \mathbb{A}, \Gamma_2 \triangleright v : \mathbb{D} \oplus \mathbb{E} \quad \begin{array}{c} E, a : \mathbb{D} \triangleright w : \mathbb{D} \\ E, b : \mathbb{E} \triangleright u : \mathbb{D} \end{array} \quad \Gamma, y : \mathbb{B}, x : \mathbb{A}; \Delta \in \mathsf{Sf}(\Gamma_1, y : \mathbb{B}, x : \mathbb{A}, \Gamma_2; E)}}{\Gamma, y : \mathbb{B}, x : \mathbb{A}, \Delta \triangleright \text{ case } v\,\{\mathsf{inl}_{\mathbb{E}}(a) \Rightarrow w; \mathsf{inr}_{\mathbb{D}}(b) \Rightarrow u\} : \mathbb{D}}$$

Next, for the second case, by induction hypothesis and applying the case rule, one has that:

$$\dfrac{\dfrac{E \triangleright v : \mathbb{D} \oplus \mathbb{E} \quad \begin{array}{c}\Delta_1, x : \mathbb{A}, y : \mathbb{B}, \Delta_2, a : \mathbb{D} \triangleright w : \mathbb{D} \\ \Delta_1, x : \mathbb{A}, y : \mathbb{B}, \Delta_2, b : \mathbb{E} \triangleright u : \mathbb{D}\end{array} \quad \Gamma, x : \mathbb{A}, y : \mathbb{B}; \Delta \in \mathsf{Sf}(E; \Delta_1, x : \mathbb{A}, y : \mathbb{B}, \Delta_2)}{E \triangleright v : \mathbb{D} \oplus \mathbb{E} \quad \begin{array}{c}\Delta_1, y : \mathbb{B}, x : \mathbb{A}, \Delta_2, a : \mathbb{D} \triangleright w : \mathbb{D} \\ \Delta_1, y : \mathbb{B}, x : \mathbb{A}, \Delta_2, b : \mathbb{E} \triangleright u : \mathbb{D}\end{array} \quad \Gamma, y : \mathbb{B}, x : \mathbb{A}; \Delta \in \mathsf{Sf}(E; \Delta_1, y : \mathbb{B}, x : \mathbb{A}, \Delta_2)}}{\Gamma, y : \mathbb{B}, x : \mathbb{A}, \Delta \triangleright \mathsf{case}\, v \, \{\mathsf{inl}_{\mathbb{E}}(a) \Rightarrow w; \mathsf{inr}_{\mathbb{D}}(b) \Rightarrow u\} : \mathbb{D}}$$

Finally, for the third case, considering the premises

$$\Gamma_1, x : \mathbb{A}, \Gamma_2 \triangleright v : \mathbb{D} \oplus \mathbb{E} \quad \begin{array}{c}\Delta_1, y : \mathbb{B}, \Delta_2, a : \mathbb{D} \triangleright w : \mathbb{D} \\ \Delta_1, y : \mathbb{B}, \Delta_2, b : \mathbb{E} \triangleright u : \mathbb{D}\end{array} \quad \begin{array}{c}\Gamma, x : \mathbb{A}, y : \mathbb{B}, \Delta \in \\ \mathsf{Sf}(\Gamma_1, x : \mathbb{A}, \Gamma_2; \Delta_2, y : \mathbb{B}, \Delta_1)\end{array}$$

and attending to the definition of shuffle, a possibility for $\Gamma, y : \mathbb{B}, x : \mathbb{A}, \Delta \in \mathsf{Sf}(\Gamma_1, x : \mathbb{A}, \Gamma_2; \Delta_2, y : \mathbb{B}, \Delta_1)$, given that in exchanging these variables the relative order of the variables in $\Gamma_1, x : \mathbb{A}, \Gamma_2$ and $\Delta_2, y : \mathbb{B}, \Delta_1$ is preserved. As a result, it is possible to derive $\Gamma, y : \mathbb{B}, x : \mathbb{A}, \Delta \triangleright \mathsf{case}\, v \, \{\mathsf{inl}_{\mathbb{E}}(a) \Rightarrow w; \mathsf{inr}_{\mathbb{D}}(b) \Rightarrow u\} : \mathbb{D}$.

With respect to the substitution property, for the left injection is necessary to demonstrate that for all judgements $\Gamma, x : \mathbb{D} \triangleright \mathsf{inl}_{\mathbb{B}}(v) : \mathbb{A} \oplus \mathbb{B}$ and $\Delta \triangleright w : \mathbb{D}$ it is possible to derive $\Gamma, \Delta \triangleright \mathsf{inl}_{\mathbb{B}}(v[w/x]) : \mathbb{A} \oplus \mathbb{B}$. By induction hypothesis, and applying the inl rule, one has that:

$$\dfrac{\dfrac{\dfrac{\Gamma, x : \mathbb{D} \triangleright v : \mathbb{A} \quad \Delta \triangleright w : \mathbb{D}}{\Gamma, \Delta \triangleright v[w/x] : \mathbb{A}}}{\Gamma, \Delta \triangleright \mathsf{inl}_{\mathbb{B}}(v[w/x]) : \mathbb{A} \oplus \mathbb{B}}}{\Gamma, \Delta \triangleright \mathsf{inl}_{\mathbb{B}}(v)[w/x] : \mathbb{A} \oplus \mathbb{B}}$$

For the right injection the proof is analogous.

Regarding the case statement it is necessary to prove that for all judgements $E, z : \mathbb{D} \triangleright \mathsf{case}\, v \, \{\mathsf{inl}_{\mathbb{A}}(x) \Rightarrow w; \mathsf{inr}_{\mathbb{B}}(y) \Rightarrow u\} : \mathbb{D}$ and $\Sigma \triangleright a : \mathbb{D}$ it is possible to derive $E, \Sigma \triangleright \mathsf{case}\, v \, \{\mathsf{inl}_{\mathbb{A}}(x) \Rightarrow w; \mathsf{inr}_{\mathbb{B}}(y) \Rightarrow u\}[a/z] : \mathbb{D}$. In this case, it is necessary to consider two scenarios:

1. $z : \mathbb{D}$ is a variable in the context of v;

2. $z : \mathbb{D}$ is a variable in the context of w and u.

Regarding the first case, by induction and applying the case rule, one has that:

$$\cfrac{\cfrac{\cfrac{\Gamma_1, z : \mathbb{D} \triangleright v : \mathbb{A} \oplus \mathbb{B} \quad \Gamma_2, x : \mathbb{A} \triangleright w : \mathbb{D} \quad \Gamma_2, y : \mathbb{B} \triangleright u : \mathbb{D} \quad E, z : \mathbb{D} \in \mathsf{Sf}(\Gamma_1, z : \mathbb{D}; \Gamma_2) \quad \Delta \triangleright a : \mathbb{D}}{\Gamma_1, \Delta \triangleright v[a/z] : \mathbb{A} \oplus \mathbb{B} \quad \Gamma_2, x : \mathbb{A} \triangleright w : \mathbb{D} \quad \Gamma_2, y : \mathbb{B} \triangleright u : \mathbb{D} \quad E, \Delta \in \mathsf{Sf}(\Gamma_1, \Delta; \Gamma_2)}}{E, \Delta \triangleright \mathsf{case}\ v\ \{\mathsf{inl}_{\mathbb{B}}(x) \Rightarrow w[a/z]; \mathsf{inr}_{\mathbb{A}}(y) \Rightarrow u[a/z]\} : \mathbb{D}}}{E, \Delta \triangleright \mathsf{case}\ v\ \{\mathsf{inl}_{\mathbb{B}}(x) \Rightarrow w; \mathsf{inr}_{\mathbb{A}}(y) \Rightarrow u\}[a/z] : \mathbb{D}}$$

The second case is similar to the first one, applying the exchange property, then the induction,followed by the exchange property once more, and finally the case rule, one has that

$$\cfrac{\cfrac{\cfrac{\cfrac{\begin{array}{c}\Gamma_2, z : \mathbb{D}, y : \mathbb{B} \triangleright u : \mathbb{D} \\ \Gamma_1 \triangleright v : \mathbb{A} \oplus \mathbb{B} \quad \Gamma_2, z : \mathbb{D}, x : \mathbb{A} \triangleright w : \mathbb{D} \quad E, z : \mathbb{D} \in \mathsf{Sf}(\Gamma_1; \Gamma_2, z : \mathbb{D}) \quad \Delta \triangleright a : \mathbb{D}\end{array}}{\begin{array}{c}\Gamma_2, y : \mathbb{B}, z : \mathbb{D} \triangleright u : \mathbb{D} \\ \Gamma_1 \triangleright v : \mathbb{A} \oplus \mathbb{B} \quad \Gamma_2, x : \mathbb{A}, z : \mathbb{D} \triangleright w : \mathbb{D} \quad E, z : \mathbb{D} \in \mathsf{Sf}(\Gamma_1; \Gamma_2, z : \mathbb{D}) \quad \Delta \triangleright a : \mathbb{D}\end{array}}}{\Gamma_1 \triangleright v : \mathbb{A} \oplus \mathbb{B} \quad \Gamma_2, x : \mathbb{A}, \Delta \triangleright w[a/z] : \mathbb{D} \quad \Gamma_2, y : \mathbb{B}, \Delta \triangleright u[a/z] : \mathbb{D} \quad E, \Delta \in \mathsf{Sf}(\Gamma_1; \Gamma_2, \Delta)}}{\Gamma_1 \triangleright v : \mathbb{A} \oplus \mathbb{B} \quad \Gamma_2, \Delta, x : \mathbb{A} \triangleright w[a/z] : \mathbb{D} \quad \Gamma_2, \Delta, y : \mathbb{B} \triangleright u[a/z] : \mathbb{D} \quad E, \Delta \in \mathsf{Sf}(\Gamma_1; \Gamma_2, \Delta)}}{\cfrac{E, \Delta \triangleright \mathsf{case}\ v[a/z]\ \{\mathsf{inl}_{\mathbb{B}}(x) \Rightarrow w; \mathsf{inr}_{\mathbb{A}}(y) \Rightarrow u\} : \mathbb{D}}{E, \Delta \triangleright \mathsf{case}\ v\ \{\mathsf{inl}_{\mathbb{B}}(x) \Rightarrow w; \mathsf{inr}_{\mathbb{A}}(y) \Rightarrow u\}[a/z] : \mathbb{D}}}$$

□

4.3 Interpretation

Considering $v \in V$, $w \in W$, and $u \in U$ where V, W, U represent vector spaces, $\mathsf{IL}_V : V \to V \oplus W$, denotes the left injection operator, defined as $\mathsf{IL}_V = v \mapsto (v, 0)$; $\mathsf{IR}_V : V \to W \oplus V$, denotes the right injection operator, defined as $\mathsf{IR}_V = v \mapsto (0, v)$; and $\mathsf{dist}_{V,W,U} : V \otimes (W \oplus U) \to (V \otimes W) \oplus (V \otimes U)$, denotes the distributive property of the tensor product over the direct sum, defined as $\mathsf{dist}_{V,W,U} = v \otimes (w, u) \mapsto (v \otimes w, v \otimes u)$. The subscripts in these operators will be omitted unless ambiguity arises. Moreover, the operation either corresponds to:

$$\frac{\begin{array}{c} T : V \to U \\ S : W \to U \end{array}}{[T,S] : V \oplus W \to U} \qquad [T,S] = (v,w) \mapsto T(v) + S(w) \tag{4.11}$$

The interpretation of conditionals is illustrated in Figure 11.

$$\frac{[\![\Gamma \triangleright v : \mathbb{A}]\!] = m}{[\![\Gamma \triangleright \mathsf{inl}(v) : \mathbb{A} \oplus \mathbb{B}]\!] = \mathsf{I_L} \cdot m} \qquad \frac{[\![\Gamma \triangleright v : \mathbb{B}]\!] = m}{[\![\Gamma \triangleright \mathsf{inr}(v) : \mathbb{A} \oplus \mathbb{B}]\!] = \mathsf{I_R} \cdot m}$$
$$\frac{[\![\Gamma \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] = b \quad [\![\Delta, x : \mathbb{A} \triangleright w : \mathbb{D}]\!] = p \quad [\![\Delta, y : \mathbb{B} \triangleright u : \mathbb{D}]\!] = q \quad E \in \mathsf{Sf}(\Gamma; \Delta)}{[\![E \triangleright \mathsf{case}\ v\ \{\mathsf{inl}(x) \Rightarrow w; \mathsf{inr}(y) \Rightarrow u\} : \mathbb{D}]\!] = [p \cdot \mathsf{jn}_{\Delta;\mathbb{A}}, q \cdot \mathsf{jn}_{\Delta;\mathbb{B}}] \cdot \mathsf{dist} \cdot \mathsf{sw} \cdot (b \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma;\Delta} \cdot \mathsf{sh}_E} \tag{4.12}$$

Figure 11: Judgment interpretation for conditionals

Proof In order to validate the judgment interpretation for conditionals, it is necessary to demonstrate its correctness.

For the booleans:

$$\begin{array}{l} [\![\Gamma]\!] \xrightarrow{m} [\![\mathbb{A}]\!] \xrightarrow{\mathsf{I_L}} [\![\mathbb{A} \oplus \mathbb{B}]\!] \\ [\![\Gamma]\!] \xrightarrow{m} [\![\mathbb{B}]\!] \xrightarrow{\mathsf{I_R}} [\![\mathbb{A} \oplus \mathbb{B}]\!] \end{array} \tag{4.13}$$

Now, for the case statement:

$$\begin{array}{l} [\![E]\!] \xrightarrow{\mathsf{sh}_E} [\![\Gamma, \Delta]\!] \xrightarrow{\mathsf{sp}_{\Gamma;\Delta}} [\![\Gamma]\!] \otimes [\![\Delta]\!] \xrightarrow{b \otimes \mathsf{id}} ([\![\mathbb{A}]\!] \oplus [\![\mathbb{B}]\!]) \otimes [\![\Delta]\!] \xrightarrow{\mathsf{sw}} [\![\Delta]\!] \otimes ([\![\mathbb{A}]\!] \oplus [\![\mathbb{B}]\!]) \\ \xrightarrow{\mathsf{dist}} ([\![\Delta]\!] \otimes [\![\mathbb{A}]\!]) \oplus ([\![\Delta]\!] \otimes [\![\mathbb{B}]\!]) \xrightarrow{[p \cdot \mathsf{jn}_{\Delta;\mathbb{A}}, q \cdot \mathsf{jn}_{\Delta;\mathbb{B}}]} [\![\mathbb{D}]\!] \end{array} \tag{4.14}$$

Next, it is necessary to demonstrate that the interpretation of exchange and substitution holds for injections and the case statement.

Lemma 4.3.1. *(Exchange) For all judgements $\Gamma, x : \mathbb{A}, y : \mathbb{B}, \Delta \triangleright v : \mathbb{D}$, the following equation holds: $[\![\Gamma, x : \mathbb{A}, y : \mathbb{B}, \Delta \triangleright v : \mathbb{D}]\!] = [\![\Gamma, y : \mathbb{B}, x : \mathbb{A}, \Delta \triangleright v : \mathbb{D}]\!] \cdot \mathsf{exch}_{\Gamma,\underline{\mathbb{A},\mathbb{B}},\Delta}$*

Proof Firstly, for the left injection,

$$
\begin{aligned}
&[\![\Gamma, x:\mathbb{A}, y:\mathbb{B}, \Delta \triangleright \mathsf{inl}_{\mathbb{D}}(v):\mathbb{D}\oplus\mathbb{D}]\!]\\
=&\mathsf{IL}\cdot[\![\Gamma, x:\mathbb{A}, y:\mathbb{B}, \Delta \triangleright v:\mathbb{D}]\!]\\
=&\mathsf{IL}\cdot[\![\Gamma, y:\mathbb{B}, x:\mathbb{A}, \Delta \triangleright v:\mathbb{D}]\!]\cdot\mathsf{exch}_{\Gamma,\underline{\mathbb{A},\mathbb{B}},\Delta} && \{\text{by induction hypothesis}\}\\
=&[\![\Gamma, y:\mathbb{B}, x:\mathbb{A}, \Delta \triangleright \mathsf{inl}_{\mathbb{D}}(v):\mathbb{D}\oplus\mathbb{D}]\!]
\end{aligned}
$$

The proof for the right injection is analogous.

Regarding the case statement, it is necessary to consider three scenarios:

1. $x:\mathbb{A}, y:\mathbb{B}$ are variables in the context of v;
2. $x:\mathbb{A}, y:\mathbb{B}$ are variables in the context of w and u;
3. $x:\mathbb{A}$ is a variable in the context of v and $y:\mathbb{B}$ is a variable in the context of w and u.

For the first case,

$$
\begin{aligned}
&[\![\Gamma, x:\mathbb{A}, y:\mathbb{B}, \Delta \triangleright \ \mathsf{case}\ \{\mathsf{inl}_{\mathbb{E}}(a)\Rightarrow w; \mathsf{inr}_{\mathbb{E}}(b)\Rightarrow u\}:\mathbb{D}]\!]\\
=&\left[[\![E, a:\mathbb{D}\triangleright w]\!]\cdot\mathsf{jn}_{E;\mathbb{D}}, [\![E, b:\mathbb{E}\triangleright u]\!]\cdot\mathsf{jn}_{E;\mathbb{E}}\right]\cdot\mathsf{dist}\cdot\mathsf{sw}\\
&\cdot([\![\Gamma_1, x:\mathbb{A}, y:\mathbb{B}, \Gamma_2\triangleright v:\mathbb{D}\oplus\mathbb{E}]\!]\otimes\mathsf{id})\cdot\mathsf{sp}_{\Gamma_1,\mathbb{A},\mathbb{B},\Gamma_2;E}\cdot\mathsf{sh}_{\Gamma,\mathbb{A},\mathbb{B},\Delta}\\
=&\left[[\![E, a:\mathbb{D}\triangleright w]\!]\cdot\mathsf{jn}_{E;\mathbb{D}}, [\![E, b:\mathbb{E}\triangleright u]\!]\cdot\mathsf{jn}_{E;\mathbb{E}}\right]\cdot\mathsf{dist}\cdot\mathsf{sw}\\
&\cdot([\![\Gamma_1, y:\mathbb{B}, x:\mathbb{A}, \Gamma_2\triangleright v:\mathbb{D}]\!]\cdot\mathsf{exch}_{\Gamma_1,\underline{\mathbb{A},\mathbb{B}},\Gamma_2}\otimes\mathsf{id})\cdot\mathsf{sp}_{\Gamma_1,\mathbb{A},\mathbb{B},\Gamma_2;E}\cdot\mathsf{sh}_{\Gamma,\mathbb{A},\mathbb{B},\Delta}\\
=&\left[[\![E, a:\mathbb{D}\triangleright w]\!]\cdot\mathsf{jn}_{E;\mathbb{D}}, [\![E, b:\mathbb{E}\triangleright u]\!]\cdot\mathsf{jn}_{E;\mathbb{E}}\right]\cdot\mathsf{dist}\cdot\mathsf{sw}\\
&\cdot([\![\Gamma_1, y:\mathbb{B}, x:\mathbb{A}, \Gamma_2\triangleright v:\mathbb{D}\oplus\mathbb{E}]\!]\otimes\mathsf{id})\cdot\mathsf{sp}_{\Gamma_1,\mathbb{B},\mathbb{A},\Gamma_2;E}\cdot\mathsf{exch}_{\Gamma_1,\underline{\mathbb{A},\mathbb{B}},\Gamma_2,E}\cdot\mathsf{jn}_{\Gamma_1,\mathbb{A},\mathbb{B},\Gamma_2;E}\\
&\cdot\mathsf{sp}_{\Gamma_1,\mathbb{A},\mathbb{B},\Gamma_2;E}\cdot\mathsf{sh}_{\Gamma,\mathbb{A},\mathbb{B},\Delta}\\
=&\left[[\![E, a:\mathbb{D}\triangleright w]\!]\cdot\mathsf{jn}_{E;\mathbb{D}}, [\![E, b:\mathbb{E}\triangleright u]\!]\cdot\mathsf{jn}_{E;\mathbb{E}}\right]\cdot\mathsf{dist}\cdot\mathsf{sw}\\
&\cdot([\![\Gamma_1, y:\mathbb{B}, x:\mathbb{A}, \Gamma_2\triangleright v:\mathbb{D}\oplus\mathbb{E}]\!]\otimes\mathsf{id})\cdot\mathsf{sp}_{\Gamma_1,\mathbb{B},\mathbb{A},\Gamma_2;E}\cdot\mathsf{exch}_{\Gamma,\underline{\mathbb{A},\mathbb{B}},\Delta}\cdot\mathsf{sh}_{\Gamma,\mathbb{A},\mathbb{B},\Delta}\\
=&\left[[\![E, a:\mathbb{D}\triangleright w]\!]\cdot\mathsf{jn}_{E;\mathbb{D}}, [\![E, b:\mathbb{E}\triangleright u]\!]\cdot\mathsf{jn}_{E;\mathbb{E}}\right]\cdot\mathsf{dist}\cdot\mathsf{sw}\\
&\cdot([\![\Gamma_1, y:\mathbb{B}, x:\mathbb{A}, \Gamma_2\triangleright v:\mathbb{D}\oplus\mathbb{E}]\!]\otimes\mathsf{id})\cdot\mathsf{sp}_{\Gamma_1,\mathbb{B},\mathbb{A},\Gamma_2;E}\cdot\mathsf{sh}_{\Gamma,\mathbb{B},\mathbb{A},\Delta}\cdot\mathsf{exch}_{\Gamma,\underline{\mathbb{A},\mathbb{B}},\Delta}\\
=&[\![\Gamma, y:\mathbb{B}, x:\mathbb{A}, \Delta \triangleright \ \mathsf{case}\ \{\mathsf{inl}_{\mathbb{E}}(a)\Rightarrow w; \mathsf{inr}_{\mathbb{E}}(b)\Rightarrow u\}:\mathbb{D}]\!]\cdot\mathsf{exch}_{\Gamma,\underline{\mathbb{A},\mathbb{B}},\Delta}
\end{aligned}
$$

Now, for the second case,

$$
\begin{aligned}
&[\![\Gamma, x:\mathbb{A}, y:\mathbb{B}, \Delta \triangleright \text{ case } \{\mathsf{inl}_{\mathbb{E}}(a) \Rightarrow w; \mathsf{inr}_{\mathbb{E}}(b) \Rightarrow u\} : \mathbb{D}]\!]\\
&= \big[[\![\Delta_1, x:\mathbb{A}, y:\mathbb{B}, \Delta_2, a:\mathbb{D} \triangleright w]\!] \cdot \mathsf{jn}_{\Delta_1,\mathbb{A},\mathbb{B},\Delta_2,\mathbb{D}}, [\![\Delta_1, x:\mathbb{A}, y:\mathbb{B}, \Delta_2, b:\mathbb{E} \triangleright u]\!] \cdot \mathsf{jn}_{\Delta_1,\mathbb{A},\mathbb{B},\Delta_2,\mathbb{D}}\big]\\
&\quad \cdot \mathsf{dist} \cdot \mathsf{sw} \cdot ([\![E \triangleright v : \mathbb{D} \oplus \mathbb{E}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{E;\Delta_1,\mathbb{A},\mathbb{B},\Delta_2} \cdot \mathsf{sh}_{\Gamma;\mathbb{A},\mathbb{B},\Delta}\\
&= [[\![\Delta_1, y:\mathbb{B}, x:\mathbb{A}, \Delta_2, a:\mathbb{D} \triangleright w]\!] \cdot \mathsf{exch}_{\Delta_1,\underline{\mathbb{A},\mathbb{B}},\Delta_2,\mathbb{D}} \cdot \mathsf{jn}_{\Delta_1,\mathbb{A},\mathbb{B},\Delta_2,\mathbb{D}},\\
&\quad [\![\Delta_1, y:\mathbb{B}, x:\mathbb{A}, \Delta_2, b:\mathbb{E} \triangleright w]\!] \cdot \mathsf{exch}_{\Delta_1,\underline{\mathbb{A},\mathbb{B}},\Delta_2,\mathbb{E}} \cdot \mathsf{jn}_{\Delta_1,\mathbb{A},\mathbb{B},\Delta_2,\mathbb{E}}] \cdot \mathsf{dist} \cdot \mathsf{sw}\\
&\quad \cdot ([\![E \triangleright v : \mathbb{D} \oplus \mathbb{E}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{E;\Delta_1,\mathbb{A},\mathbb{B},\Delta_2} \cdot \mathsf{sh}_{\Gamma,\mathbb{A},\mathbb{B},\Delta}\\
&= [[\![\Delta_1, y:\mathbb{B}, x:\mathbb{A}, \Delta_2, a:\mathbb{D} \triangleright w]\!] \cdot \mathsf{jn}_{\Delta_1,\mathbb{B},\mathbb{A},\Delta_2,\mathbb{D}}, [\![\Delta_1, y:\mathbb{B}, x:\mathbb{A}, \Delta_2, b:\mathbb{E} \triangleright w]\!] \cdot \mathsf{jn}_{\Delta_1,\mathbb{B},\mathbb{A},\Delta_2,\mathbb{E}}]\\
&\quad \cdot \mathsf{dist} \cdot \mathsf{sp}_{\Delta_1,\mathbb{B},\mathbb{A},\Delta_2;\mathbb{D}\oplus\mathbb{E}} \cdot \mathsf{exch}_{\Delta_1,\underline{\mathbb{A},\mathbb{B}},\Delta_2,\mathbb{D}\oplus\mathbb{E}} \cdot \mathsf{jn}_{\Delta_1,\mathbb{A},\mathbb{B},\Delta_2;\mathbb{D}\oplus\mathbb{E}} \cdot \mathsf{sw} \cdot ([\![E \triangleright v : \mathbb{D} \oplus \mathbb{E}]\!] \otimes \mathsf{id})\\
&\quad \cdot \mathsf{sp}_{E;\Delta_1,\mathbb{A},\mathbb{B},\Delta_2} \cdot \mathsf{sh}_{\Gamma,\mathbb{A},\mathbb{B},\Delta}\\
&= [[\![\Delta_1, y:\mathbb{B}, x:\mathbb{A}, \Delta_2, a:\mathbb{D} \triangleright w]\!] \cdot \mathsf{jn}_{\Delta_1,\mathbb{B},\mathbb{A},\Delta_2,\mathbb{D}}, [\![\Delta_1, y:\mathbb{B}, x:\mathbb{A}, \Delta_2, b:\mathbb{E} \triangleright w]\!] \cdot \mathsf{jn}_{\Delta_1,\mathbb{B},\mathbb{A},\Delta_2,\mathbb{E}}]\\
&\quad \cdot \mathsf{dist} \cdot \mathsf{sw} \cdot ([\![E \triangleright v : \mathbb{D} \oplus \mathbb{E}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma;\Delta_1,\mathbb{B},\mathbb{A},\Delta_2} \cdot \mathsf{exch}_{\Gamma,\Delta_1,\underline{\mathbb{A},\mathbb{B}},\Delta_2} \cdot \mathsf{jn}_{\Gamma;\Delta_1,\mathbb{A},\mathbb{B},\Delta_2}\\
&\quad \cdot \mathsf{sp}_{E;\Delta_1,\mathbb{A},\mathbb{B},\Delta_2} \cdot \mathsf{sh}_{\Gamma,\mathbb{A},\mathbb{B},\Delta}\\
&= [[\![\Delta_1, y:\mathbb{B}, x:\mathbb{A}, \Delta_2, a:\mathbb{D} \triangleright w]\!] \cdot \mathsf{jn}_{\Delta_1,\mathbb{B},\mathbb{A},\Delta_2,\mathbb{D}}, [\![\Delta_1, y:\mathbb{B}, x:\mathbb{A}, \Delta_2, b:\mathbb{E} \triangleright w]\!] \cdot \mathsf{jn}_{\Delta_1,\mathbb{B},\mathbb{A},\Delta_2,\mathbb{E}}]\\
&\quad \cdot \mathsf{dist} \cdot \mathsf{sw} \cdot ([\![E \triangleright v : \mathbb{D} \oplus \mathbb{E}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{E;\Delta_1,\mathbb{B},\mathbb{A},\Delta_2} \cdot \mathsf{sh}_{\Gamma,\mathbb{B},\mathbb{A},\Delta} \cdot \mathsf{exch}_{\Gamma,\underline{\mathbb{A},\mathbb{B}},\Delta}\\
&= [\![\Gamma, y:\mathbb{B}, x:\mathbb{A}, \Delta \triangleright \text{ case } \{\mathsf{inl}_{\mathbb{E}}(a) \Rightarrow w; \mathsf{inr}_{\mathbb{E}}(b) \Rightarrow u\} : \mathbb{D}]\!] \cdot \mathsf{exch}_{\Gamma,\underline{\mathbb{A},\mathbb{B}},\Delta}
\end{aligned}
$$

Finally, for the third case, note that, the shuffle operator is permutation of typed variables that preserves the relative order of the variables in both contexts, and, as a result, $\Gamma, \mathbb{B}, \mathbb{A}, \Delta \in \mathsf{Sf}(\Gamma_1, x:\mathbb{A}, \Gamma_2; \Delta_2, y:\mathbb{B}, \Delta_1)$. Thus, the proof is as follows:

$$
\begin{aligned}
&[\![\Gamma, x:\mathbb{A}, y:\mathbb{B}, \Delta \triangleright \text{ case } \{\mathsf{inl}_{\mathbb{E}}(a) \Rightarrow w; \mathsf{inr}_{\mathbb{E}}(b) \Rightarrow u\} : \mathbb{D}]\!]\\
&= \big[[\![\Delta_2, y:\mathbb{B}, \Delta_1, a:\mathbb{D} \triangleright w]\!] \cdot \mathsf{jn}_{\Delta_2,\mathbb{B},\Delta_1;\mathbb{D}}, [\![\Delta_2, y:\mathbb{B}, \Delta_1, b:\mathbb{E} \triangleright u]\!] \cdot \mathsf{jn}_{\Delta_2,\mathbb{B},\Delta_1;\mathbb{E}}\big] \cdot \mathsf{dist} \cdot \mathsf{sw}\\
&\quad \cdot ([\![\Delta_2, y:\mathbb{B}, \Delta_1 \triangleright v : \mathbb{D} \oplus \mathbb{E}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma_1,x:\mathbb{A},\Gamma_2;\Delta_2,y:\mathbb{B},\Delta_1} \cdot \mathsf{sh}_{\Gamma,\mathbb{A},\mathbb{B},\Delta}\\
&= \big[[\![\Delta_2, y:\mathbb{B}, \Delta_1, a:\mathbb{D} \triangleright w]\!] \cdot \mathsf{jn}_{\Delta_2,\mathbb{B},\Delta_1;\mathbb{D}}, [\![\Delta_2, y:\mathbb{B}, \Delta_1, b:\mathbb{E} \triangleright u]\!] \cdot \mathsf{jn}_{\Delta_2,\mathbb{B},\Delta_1;\mathbb{E}}\big] \cdot \mathsf{dist} \cdot \mathsf{sw}\\
&\quad \cdot ([\![\Delta_2, y:\mathbb{B}, \Delta_1 \triangleright v : \mathbb{D} \oplus \mathbb{E}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma_1,x:\mathbb{A},\Gamma_2;\Delta_2,y:\mathbb{B},\Delta_1} \cdot \mathsf{sh}_{\Gamma,\mathbb{A},\mathbb{B},\Delta} \cdot \mathsf{exch}_{\Gamma,\underline{\mathbb{A},\mathbb{B}},\Delta}\\
&= [\![\Gamma, y:\mathbb{B}, x:\mathbb{A}, \Delta \triangleright \text{ case } \{\mathsf{inl}_{\mathbb{E}}(a) \Rightarrow w; \mathsf{inr}_{\mathbb{E}}(b) \Rightarrow u\} : \mathbb{D}]\!] \cdot \mathsf{exch}_{\Gamma,\underline{\mathbb{A},\mathbb{B}},\Delta}
\end{aligned}
$$

$\square$

Lemma 4.3.2. *(Substitution) For all judgements $\Gamma, x : \mathbb{A} \triangleright v : \mathbb{B}$ and $\Delta \triangleright w : \mathbb{A}$ the following equation holds:* $[\![\Gamma, \Delta \triangleright v[w/x] : \mathbb{B}]\!] = [\![\Gamma, x : \mathbb{A} \triangleright v : \mathbb{B}]\!] \cdot jn_{\Gamma;\mathbb{A}} \cdot (id \otimes [\![\Delta \triangleright w : \mathbb{A}]\!]) \cdot sp_{\Gamma;\Delta}$

Regarding the left injection,

$$
\begin{aligned}
&[\![\Gamma, \Delta \triangleright \mathsf{inl}_{\mathbb{B}}(v)[w/x] : \mathbb{A} \oplus \mathbb{B}]\!] \\
=&\mathsf{IL} \cdot [\![\Gamma, \Delta \triangleright v[w/x] : \mathbb{A}]\!] \\
=&\mathsf{IL} \cdot [\![\Gamma, x : \mathbb{D} \triangleright v : \mathbb{A}]\!] \cdot \mathsf{jn}_{\Gamma;\mathbb{D}} \cdot (\mathsf{id} \otimes [\![\Delta \triangleright w : \mathbb{D}]\!]) \cdot \mathsf{sp}_{\Gamma;\Delta} \\
=&[\![\Gamma, x : \mathbb{D} \triangleright \mathsf{inl}_{\mathbb{B}}(v)[w/x] : \mathbb{A} \oplus \mathbb{B}]\!] \cdot \mathsf{jn}_{\Gamma;\mathbb{D}} \cdot (\mathsf{id} \otimes [\![\Delta \triangleright w : \mathbb{D}]\!]) \cdot \mathsf{sp}_{\Gamma;\Delta}
\end{aligned}
$$

The proof for the right injection is analogous.

With respect to the case statement, in this case, it is necessary to consider two scenarios:

1. $z : \mathbb{D}$ is a variable in the context of v;
2. $z : \mathbb{D}$ is a variable in the context of w and u.

For the first case,

Por as coisas direitas

$$
\begin{aligned}
&[\![E, \Delta \triangleright \text{ case } \{\mathsf{inl}_{\mathbb{B}}(x) \Rightarrow w; \mathsf{inr}_{\mathbb{A}}(y) \Rightarrow u\}[a/z] : \mathbb{D}]\!] \\
=& \left[[\![\Gamma_2, x : \mathbb{A} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Gamma_2;\mathbb{A}}, [\![\Gamma_2, y : \mathbb{B} \triangleright u]\!] \cdot \mathsf{jn}_{\Gamma_2;\mathbb{B}}\right] \cdot \mathsf{dist} \cdot \mathsf{sw} \cdot ([\![\Gamma_1, \Delta \triangleright v[a/z] : \mathbb{A} \oplus \mathbb{B}]\!] \\
&\otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma_1,\Delta;\Gamma_2} \cdot \mathsf{sh}_{E,\Delta} \\
=& \left[[\![\Gamma_2, x : \mathbb{A} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Gamma_2;\mathbb{A}}, [\![\Gamma_2, y : \mathbb{B} \triangleright u]\!] \cdot \mathsf{jn}_{\Gamma_2;\mathbb{B}}\right] \cdot \mathsf{dist} \cdot \mathsf{sw} \cdot (([\![\Gamma_1, z : \mathbb{D} \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] \\
&\cdot \mathsf{jn}_{\Gamma_1;\mathbb{D}} \cdot (\mathsf{id} \otimes [\![\Delta \triangleright a : \mathbb{D}]\!]) \cdot \mathsf{sp}_{\Gamma_1;\Delta}) \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma_1,\Delta;\Gamma_2} \cdot \mathsf{sh}_{E,\Delta} \\
=& \left[[\![\Gamma_2, x : \mathbb{A} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Gamma_2;\mathbb{A}}, [\![\Gamma_2, y : \mathbb{B} \triangleright u]\!] \cdot \mathsf{jn}_{\Gamma_2;\mathbb{B}}\right] \cdot \mathsf{dist} \cdot \mathsf{sw} \cdot ([\![\Gamma_1, z : \mathbb{D} \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] \\
&\otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma_1,\mathbb{D};\Gamma_2} \cdot \mathsf{jn}_{\Gamma_1;\mathbb{D};\Gamma_2} \cdot (\mathsf{id} \otimes [\![\Delta \triangleright a : \mathbb{D}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma_1;\Delta;\Gamma_2} \cdot \mathsf{sh}_{E,\Delta} \\
=& \left[[\![\Gamma_2, x : \mathbb{A} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Gamma_2;\mathbb{A}}, [\![\Gamma_2, y : \mathbb{B} \triangleright u]\!] \cdot \mathsf{jn}_{\Gamma_2;\mathbb{B}}\right] \cdot \mathsf{dist} \cdot \mathsf{sw} \cdot ([\![\Gamma_1, z : \mathbb{D} \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] \\
&\otimes \mathsf{id}) \ldots \\
=& \left[[\![\Gamma_2, x : \mathbb{A} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Gamma_2;\mathbb{A}}, [\![\Gamma_2, y : \mathbb{B} \triangleright u]\!] \cdot \mathsf{jn}_{\Gamma_2;\mathbb{B}}\right] \cdot \mathsf{dist} \cdot \mathsf{sw} \cdot ([\![\Gamma_1, z : \mathbb{D} \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] \\
&\otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma_1,\mathbb{D};\Gamma_2} \cdot \mathsf{sh}_{E,\mathbb{D}} \cdot \mathsf{jn}_{E;\mathbb{D}} \cdot (\mathsf{id} \otimes [\![\Delta \triangleright a : \mathbb{D}]\!]) \cdot \mathsf{sp}_{E;\Delta} \\
=& [\![E, z : \mathbb{D} \triangleright \text{ case } \{\mathsf{inl}_{\mathbb{B}}(x) \Rightarrow w; \mathsf{inr}_{\mathbb{A}}(y) \Rightarrow u\} : \mathbb{D}]\!] \cdot \mathsf{jn}_{E;\mathbb{D}} \cdot (\mathsf{id} \otimes [\![\Delta \triangleright a : \mathbb{D}]\!]) \cdot \mathsf{sp}_{E;\Delta}
\end{aligned}
$$

For the second case,

$$
\begin{aligned}
&[\![E, \Delta \triangleright \text{ case } \{\mathsf{inl}_{\mathbb{B}}(x) \Rightarrow w; \mathsf{inr}_{\mathbb{A}}(y) \Rightarrow u\}[a/z] : \mathbb{D}]\!]\\
= &\left[[\![\Gamma_2, \Delta, x : \mathbb{A} \triangleright w[a/z] : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Gamma_2,\Delta,\mathbb{A}}, [\![\Gamma_2, \Delta, y : \mathbb{B} \triangleright u[a/z] : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Gamma_2,\Delta,\mathbb{B}}\right] \cdot \mathsf{dist} \cdot \mathsf{sw}\\
&\cdot ([\![\Gamma_1 \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma_1;\Delta,\Gamma_2} \cdot \mathsf{sh}_{E,\Delta}\\
= &[[\![\Gamma_2, x : \mathbb{A}, \Delta \triangleright w[a/z] : \mathbb{D}]\!] \cdot \mathsf{exch}_{\Gamma_2,\Delta,\mathbb{A}} \cdot \mathsf{jn}_{\Gamma_2,\Delta,\mathbb{A}}, [\![\Gamma_2, y : \mathbb{B}, \Delta \triangleright u[a/z] : \mathbb{D}]\!] \cdot \mathsf{exch}_{\Gamma_2,\Delta,\mathbb{B}}\\
&\cdot \mathsf{jn}_{\Gamma_2,\Delta,\mathbb{B}}] \cdot \mathsf{dist} \cdot \mathsf{sw} \cdot ([\![\Gamma_1 \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma_1;\Delta,\Gamma_2} \cdot \mathsf{sh}_{E,\Delta}\\
= &[[\![\Gamma_2, x : \mathbb{A}, z : \mathbb{D} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Gamma_2,\mathbb{A};\mathbb{D}} \cdot (\mathsf{id} \otimes [\![\Delta \triangleright a : \mathbb{D}]\!]) \cdot \mathsf{sp}_{\Gamma_2,\mathbb{A};\Delta} \cdot \mathsf{exch}_{\Gamma_2,\Delta,\mathbb{A}} \cdot \mathsf{jn}_{\Gamma_2,\Delta,\mathbb{A}},\\
&[\![\Gamma_2, y : \mathbb{B}, z : \mathbb{D} \triangleright u : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Gamma_2,\mathbb{A};\mathbb{D}} \cdot (\mathsf{id} \otimes [\![\Delta \triangleright a : \mathbb{D}]\!]) \cdot \mathsf{sp}_{\Gamma_2,\mathbb{B};\Delta} \cdot \mathsf{exch}_{\Gamma_2,\Delta,\mathbb{B}}] \cdot \mathsf{jn}_{\Gamma_2,\Delta,\mathbb{B}}\\
&\cdot \mathsf{dist} \cdot \mathsf{sw} \cdot ([\![\Gamma_1 \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma_1;\Delta,\Gamma_2} \cdot \mathsf{sh}_{E,\Delta}\\
= &[[\![\Gamma_2, x : \mathbb{A}, z : \mathbb{D} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{exch}_{\Gamma_2,\mathbb{D},\mathbb{A}} \cdot \mathsf{jn}_{\Gamma_2,\mathbb{D},\mathbb{A}}, [\![\Gamma_2, y : \mathbb{B}, z : \mathbb{D} \triangleright u : \mathbb{D}]\!] \cdot \mathsf{exch}_{\Gamma_2,\mathbb{D},\mathbb{B}}\\
&\cdot \mathsf{jn}_{\Gamma_2,\mathbb{D},\mathbb{B}}] \cdot \mathsf{dist} \cdot \mathsf{sp}_{\Gamma_2,\mathbb{D};\mathbb{A}\oplus\mathbb{B}} \cdot \mathsf{jn}_{\Gamma_2;\mathbb{D};\mathbb{A}\oplus\mathbb{B}} \cdot (\mathsf{id} \otimes [\![\Delta \triangleright a : \mathbb{D}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma_2;\Delta,\mathbb{A}\oplus\mathbb{B}} \cdot \mathsf{sw}\\
&\cdot ([\![\Gamma_1 \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma_1;\Delta,\Gamma_2} \cdot \mathsf{sh}_{E,\Delta}\\
= &[[\![\Gamma_2, x : \mathbb{A}, z : \mathbb{D} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{exch}_{\Gamma_2,\mathbb{D},\mathbb{A}} \cdot \mathsf{jn}_{\Gamma_2,\mathbb{D},\mathbb{A}}, [\![\Gamma_2, y : \mathbb{B}, z : \mathbb{D} \triangleright u : \mathbb{D}]\!] \cdot \mathsf{exch}_{\Gamma_2,\mathbb{D},\mathbb{B}}\\
&\cdot \mathsf{jn}_{\Gamma_2,\mathbb{D},\mathbb{B}}] \cdot \mathsf{dist} \cdot \mathsf{sw} \cdot ([\![\Gamma_1 \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma_1;\Gamma_2,\mathbb{D}} \cdot \mathsf{jn}_{\Gamma_1;\Gamma_2;\mathbb{D}} \cdot (\mathsf{id} \otimes [\![\Delta \triangleright a : \mathbb{D}]\!] \otimes \mathsf{id})\\
&\cdot \mathsf{sp}_{\Gamma_1;\Delta;\Gamma_2} \cdot \mathsf{sh}_{E,\Delta}\\
= &[[\![\Gamma_2, x : \mathbb{A}, z : \mathbb{D} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{exch}_{\Gamma_2,\mathbb{D},\mathbb{A}} \cdot \mathsf{jn}_{\Gamma_2,\mathbb{D},\mathbb{A}}, [\![\Gamma_2, y : \mathbb{B}, z : \mathbb{D} \triangleright u : \mathbb{D}]\!] \cdot \mathsf{exch}_{\Gamma_2,\mathbb{D},\mathbb{B}}\\
&\cdot \mathsf{jn}_{\Gamma_2,\mathbb{D},\mathbb{B}}] \cdot \mathsf{dist} \cdot \mathsf{sw} \cdot ([\![\Gamma_1 \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma_1;\Gamma_2,\mathbb{D}} \cdot \mathsf{sh}_{E,\mathbb{D}} \cdot \mathsf{jn}_{E;\mathbb{D}} \cdot (\mathsf{id} \otimes [\![\Delta \triangleright a : \mathbb{D}]\!])\\
&\cdot \mathsf{sp}_{E;\Delta}\\
= &\left[[\![\Gamma_2, z : \mathbb{D}, x : \mathbb{A} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Gamma_2,\mathbb{D},\mathbb{A}}, [\![\Gamma_2, z : \mathbb{D}, y : \mathbb{B} \triangleright u : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Gamma_2,\mathbb{D},\mathbb{B}}\right] \cdot \mathsf{dist} \cdot \mathsf{sw}\\
&\cdot ([\![\Gamma_1 \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma_1;\Gamma_2,\mathbb{D}} \cdot \mathsf{sh}_{E,\mathbb{D}} \cdot \mathsf{jn}_{E;\mathbb{D}} \cdot (\mathsf{id} \otimes [\![\Delta \triangleright a : \mathbb{D}]\!]) \cdot \mathsf{sp}_{E;\Delta}\\
= &[\![E, z : \mathbb{D} \triangleright \text{ case } \{\mathsf{inl}_{\mathbb{B}}(x) \Rightarrow w; \mathsf{inr}_{\mathbb{A}}(y) \Rightarrow u\}[a/z] : \mathbb{D}]\!] \cdot \mathsf{jn}_{E;\mathbb{D}} \cdot (\mathsf{id} \otimes [\![\Delta \triangleright a : \mathbb{D}]\!]) \cdot \mathsf{sp}_{E;\Delta}
\end{aligned}
$$

□

4.4 β and η Equations

In this subsection it will be shown that the following equations hold for the model considered.

$$(\beta^{inl}_{case}):\ \Delta, \Gamma \triangleright \textsf{case inl}_{\mathbb{B}}(v)\,\{\textsf{inl}_{\mathbb{B}}(x) \Rightarrow w; \textsf{inr}_{\mathbb{A}}(y) \Rightarrow u\} = w[v/x] : \mathbb{D}$$

$$(\beta^{inr}_{case}):\ \Delta, \Gamma \triangleright \textsf{case inr}_{\mathbb{A}}(v)\,\{\textsf{inl}_{\mathbb{B}}(x) \Rightarrow w; \textsf{inr}_{\mathbb{A}}(y) \Rightarrow u\} = w[v/y] : \mathbb{D}$$

$$(\eta_{case}):\ \Delta, \Gamma \triangleright \textsf{case}\ (v)\ \{\textsf{inl}_{\mathbb{B}}(y) \Rightarrow w[\textsf{inl}_{\mathbb{B}}(y)/x]; \textsf{inr}_{\mathbb{A}}(z) \Rightarrow w[\textsf{inr}_{\mathbb{A}}(z)/x]\} = w[v/x] : \mathbb{D}$$

Proof It is necessary to demonstrate that

$$[\![\Delta, \Gamma \triangleright \textsf{case inl}_{\mathbb{B}}(v)\,\{\textsf{inl}_{\mathbb{B}}(x) \Rightarrow w; \textsf{inr}_{\mathbb{A}}(y) \Rightarrow u\} : \mathbb{D}]\!] = [\![\Delta, \Gamma \triangleright w[v/x] : \mathbb{D}]\!]$$

$$[\![\Delta, \Gamma \triangleright \textsf{case inr}_{\mathbb{A}}(v)\,\{\textsf{inl}_{\mathbb{B}}(x) \Rightarrow w; \textsf{inr}_{\mathbb{A}}(y) \Rightarrow u\} : \mathbb{D}]\!] = [\![\Delta, \Gamma \triangleright w[v/x] : \mathbb{D}]\!]$$

$$[\![\Delta, \Gamma \triangleright \textsf{case}\ (v)\,\{\textsf{inl}_{\mathbb{B}}(y) \Rightarrow w[\textsf{inl}_{\mathbb{B}}(y)/x]; \textsf{inr}_{\mathbb{A}}(z) \Rightarrow w[\textsf{inr}_{\mathbb{A}}(z)/x]\} : \mathbb{D}]\!] = [\![\Delta, \Gamma \triangleright w[v/x] : \mathbb{D}]\!]$$

Regarding the first equation,

$$\begin{aligned}
&[\![\Delta, \Gamma \triangleright \textsf{case inl}_{\mathbb{B}}(v)\,\{\textsf{inl}_{\mathbb{B}}(x) \Rightarrow w; \textsf{inr}_{\mathbb{A}}(y) \Rightarrow u\} : \mathbb{D}]\!] \\
=&[[\![\Delta, x : \mathbb{A} \triangleright w : \mathbb{D}]\!] \cdot \textsf{jn}_{\Delta;\mathbb{A}}, [\![\Delta, y : \mathbb{B} \triangleright u : \mathbb{D}]\!] \cdot \textsf{jn}_{\Delta;\mathbb{B}}] \cdot \textsf{dist} \cdot \textsf{sw} \cdot ([\![\Gamma \triangleright \textsf{inl}_{\mathbb{B}}(v) : \mathbb{A} \oplus \mathbb{B}]\!] \\
&\otimes \textsf{id}) \cdot \textsf{sp}_{\Gamma;\Delta} \cdot \textsf{sh}_{\Delta;\Gamma} \\
=&[[\![\Delta, x : \mathbb{A} \triangleright w : \mathbb{D}]\!] \cdot \textsf{jn}_{\Delta;\mathbb{A}}, [\![\Delta, y : \mathbb{B} \triangleright u : \mathbb{D}]\!] \cdot \textsf{jn}_{\Delta;\mathbb{B}}] \cdot \textsf{dist} \cdot \textsf{sw} \cdot (\textsf{IL} \cdot [\![\Gamma \triangleright v : \mathbb{A}]\!] \otimes \textsf{id}) \\
&\cdot \textsf{sp}_{\Gamma;\Delta} \cdot \textsf{sh}_{\Delta;\Gamma} \\
=&[[\![\Delta, x : \mathbb{A} \triangleright w : \mathbb{D}]\!] \cdot \textsf{jn}_{\Delta;\mathbb{A}}, [\![\Delta, y : \mathbb{B} \triangleright u : \mathbb{D}]\!] \cdot \textsf{jn}_{\Delta;\mathbb{B}}] \cdot \textsf{dist} \cdot \textsf{sw} \cdot (\textsf{IL} \otimes \textsf{id}) \cdot ([\![\Gamma \triangleright v : \mathbb{A}]\!] \\
&\otimes \textsf{id}) \cdot \textsf{sp}_{\Gamma;\Delta} \cdot \textsf{sh}_{\Delta;\Gamma} \\
=&[[\![\Delta, x : \mathbb{A} \triangleright w : \mathbb{D}]\!] \cdot \textsf{jn}_{\Delta;\mathbb{A}}, [\![\Delta, y : \mathbb{B} \triangleright u : \mathbb{D}]\!] \cdot \textsf{jn}_{\Delta;\mathbb{B}}] \cdot \textsf{dist} \cdot (\textsf{id} \otimes \textsf{IL}) \cdot \textsf{sw} \cdot ([\![\Gamma \triangleright v : \mathbb{A}]\!] \\
&\otimes \textsf{id}) \cdot \textsf{sp}_{\Gamma;\Delta} \cdot \textsf{sh}_{\Delta;\Gamma}
\end{aligned}$$

Given that $[\textsf{id} \otimes \textsf{IL}, \textsf{id} \otimes \textsf{IR}] \cdot \textsf{IL} = \textsf{id} \otimes \textsf{IL}$, it follows that the following diagram commutes.

$$\begin{tikzcd}
X \otimes Y \arrow[r, "\textsf{id} \otimes \textsf{IL}"] \arrow[d, "\textsf{IL}"'] & X \otimes (Y \oplus Y) \arrow[dl, bend right, "\textsf{dist}"'] \\
X \otimes Y \oplus X \otimes Z \arrow[ur, bend right, "{[\textsf{id} \otimes \textsf{IL}, \textsf{id} \otimes \textsf{IR}]}"'] &
\end{tikzcd}$$

And as a result, $\mathsf{dist} \cdot (\mathsf{id} \otimes \mathsf{Il}) = \mathsf{Il}$. Therefore,

$$
\begin{aligned}
&[[\![\Delta, x : \mathbb{A} \rhd w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}}, [\![\Delta, y : \mathbb{B} \rhd u : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{B}}] \cdot \mathsf{dist} \cdot (\mathsf{id} \otimes \mathsf{Il}) \cdot \mathsf{sw} \cdot ([\![\Gamma \rhd v : \mathbb{A}]\!] \\
&\quad \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma;\Delta} \cdot \mathsf{sh}_{\Delta;\Gamma} \\
=&[[\![\Delta, x : \mathbb{A} \rhd w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}}, [\![\Delta, y : \mathbb{B} \rhd u : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{B}}] \cdot \mathsf{Il} \cdot \mathsf{sw} \cdot ([\![\Gamma \rhd v : \mathbb{A}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma;\Delta} \\
&\quad \cdot \mathsf{sh}_{\Delta;\Gamma} \\
=&[\![\Delta, x : \mathbb{A} \rhd w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}} \cdot \mathsf{sw} \cdot ([\![\Gamma \rhd v : \mathbb{A}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma;\Delta} \cdot \mathsf{sh}_{\Delta;\Gamma} \\
=&[\![\Delta, x : \mathbb{A} \rhd w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}} \cdot (\mathsf{id} \otimes [\![\Gamma \rhd v : \mathbb{A}]\!]) \cdot \mathsf{sw} \cdot \mathsf{sp}_{\Gamma;\Delta} \cdot \mathsf{sh}_{\Delta;\Gamma} \\
=&[\![\Delta, x : \mathbb{A} \rhd w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}} \cdot (\mathsf{id} \otimes [\![\Gamma \rhd v : \mathbb{A}]\!]) \cdot \mathsf{sp}_{\Delta;\Gamma} \\
=&[\![w[v/x] : \mathbb{D}]\!]
\end{aligned}
$$

The proof for the second equation is analogous to the first one.
Taking into account that $[\mathsf{id} \otimes \mathsf{Il}, \mathsf{id} \otimes \mathsf{Ir}] \cdot \mathsf{Ir} = \mathsf{id} \otimes \mathsf{Ir}$, it follows that the following diagram commutes.

$$
\begin{tikzcd}
X \otimes Y \arrow[rr, "\mathsf{id} \otimes \mathsf{Ir}"] \arrow[d, "\mathsf{Ir}"'] & & X \otimes (Z \oplus Y) \arrow[dll, bend right, "\mathsf{dist}"'] \\
X \otimes Z \oplus X \otimes Y \arrow[urr, bend right, "{[\mathsf{id} \otimes \mathsf{Il}, \mathsf{id} \otimes \mathsf{Ir}]}"'] & &
\end{tikzcd}
$$

Consequentlty, $\mathsf{dist} \cdot (\mathsf{id} \otimes \mathsf{Ir}) = \mathsf{Ir}$. Thus,

$$
\begin{aligned}
&[\![\Delta, \Gamma \rhd \text{ case } \mathsf{inr}_{\mathbb{A}}(v)\, \{\mathsf{inl}_{\mathbb{B}}(x) \Rightarrow w; \mathsf{inr}_{\mathbb{A}}(y) \Rightarrow u\} : \mathbb{D}]\!] \\
=&[[\![\Delta, x : \mathbb{A} \rhd w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}}, [\![\Delta, y : \mathbb{B} \rhd u : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{B}}] \cdot \mathsf{dist} \cdot (\mathsf{id} \otimes \mathsf{Ir}) \cdot \mathsf{sw} \cdot ([\![\Gamma \rhd v : \mathbb{B}]\!] \\
&\quad \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma;\Delta} \cdot \mathsf{sh}_{\Delta;\Gamma} \\
=&[[\![\Delta, x : \mathbb{A} \rhd w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}}, [\![\Delta, y : \mathbb{B} \rhd u : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{B}}] \cdot \mathsf{Ir} \cdot \mathsf{sw} \cdot ([\![\Gamma \rhd v : \mathbb{B}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma;\Delta} \\
&\quad \cdot \mathsf{sh}_{\Delta;\Gamma} \\
=&[\![\Delta, y : \mathbb{B} \rhd w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{B}} \cdot (\mathsf{id} \otimes [\![\Gamma \rhd v : \mathbb{B}]\!]) \cdot \mathsf{sp}_{\Delta;\Gamma} \\
=&[\![w[v/y] : \mathbb{D}]\!]
\end{aligned}
$$

With respect to the third equation,

$$
\begin{aligned}
&[\![\Delta, \Gamma \triangleright \mathsf{case}\ (v)\ \{\mathsf{inl}_{\mathbb{B}}(y) \Rightarrow w[\mathsf{inl}_{\mathbb{B}}(y)/x]; \mathsf{inr}_{\mathbb{A}}(z) \Rightarrow w[\mathsf{inr}_{\mathbb{A}}(z)/x]\} : \mathbb{D}]\!]\\
=&[[\![\Delta, y : \mathbb{B} \triangleright w[\mathsf{inl}_{\mathbb{B}}(y)/x] : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}}, [\![\Delta, z : \mathbb{A} \triangleright w[\mathsf{inr}_{\mathbb{A}}(z)/x] : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{B}}] \cdot \mathsf{dist} \cdot \mathsf{sw}\\
&\cdot ([\![\Gamma \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma;\Delta} \cdot \mathsf{sh}_{\Delta;\Gamma}\\
=&[[\![\Delta, x : \mathbb{A} \oplus \mathbb{B} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}\oplus\mathbb{B}} \cdot (\mathsf{id} \otimes [\![y : \mathbb{A} \triangleright \mathsf{inl}_{\mathbb{B}}(y) : \mathbb{A} \oplus \mathbb{B}]\!]) \cdot \mathsf{sp}_{\Delta;\mathbb{A}} \cdot \mathsf{jn}_{\Delta;\mathbb{A}},\\
&[\![\Delta, x : \mathbb{A} \oplus \mathbb{B} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}\oplus\mathbb{B}} \cdot (\mathsf{id} \otimes [\![z : \mathbb{B} \triangleright \mathsf{inr}_{\mathbb{A}}(z) : \mathbb{A} \oplus \mathbb{B}]\!]) \cdot \mathsf{sp}_{\Delta;\mathbb{B}} \cdot \mathsf{jn}_{\Delta;\mathbb{B}}]\\
&\cdot \mathsf{dist} \cdot \mathsf{sw} \cdot ([\![\Gamma \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma;\Delta} \cdot \mathsf{sh}_{\Delta;\Gamma}\\
=&[[\![\Delta, x : \mathbb{A} \oplus \mathbb{B} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}\oplus\mathbb{B}} \cdot (\mathsf{id} \otimes \mathsf{IL} \cdot [\![y : \mathbb{A} \triangleright y : \mathbb{A}]\!]), [\![\Delta, x : \mathbb{A} \oplus \mathbb{B} \triangleright w : \mathbb{D}]\!]\\
&[\![\Delta, x : \mathbb{A} \oplus \mathbb{B} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}\oplus\mathbb{B}} \cdot (\mathsf{id} \otimes \mathsf{IR} \cdot [\![z : \mathbb{B} \triangleright z : \mathbb{B}]\!])] \cdot \mathsf{dist} \cdot \mathsf{sw} \cdot ([\![\Gamma \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!])\\
&\otimes \mathsf{id} \cdot \mathsf{sp}_{\Gamma;\Delta} \cdot \mathsf{sh}_{\Delta;\Gamma}\\
=&[[\![\Delta, x : \mathbb{A} \oplus \mathbb{B} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}\oplus\mathbb{B}} \cdot (\mathsf{id} \otimes \mathsf{IL} \cdot \mathsf{id}_{[\![\mathbb{A}]\!]}), [\![\Delta, x : \mathbb{A} \oplus \mathbb{B} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}\oplus\mathbb{B}}\\
&\cdot (\mathsf{id} \otimes \mathsf{IR} \cdot \mathsf{id}_{[\![\mathbb{B}]\!]})] \cdot \mathsf{dist} \cdot \mathsf{sw} \cdot ([\![\Gamma \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma;\Delta} \cdot \mathsf{sh}_{\Delta;\Gamma}\\
=&[\![\Delta, x : \mathbb{A} \oplus \mathbb{B} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}\oplus\mathbb{B}} \cdot (\mathsf{id} \otimes [\mathsf{IL} \cdot \mathsf{id}_{[\![\mathbb{A}]\!]}, \mathsf{IR} \cdot \mathsf{id}_{[\![\mathbb{B}]\!]}]) \cdot \mathsf{dist} \cdot \mathsf{sw} \cdot ([\![\Gamma \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!]\\
&\otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma;\Delta} \cdot \mathsf{sh}_{\Delta;\Gamma}
\end{aligned}
$$

Considering that $[\mathsf{IL} \cdot \mathsf{id}, \mathsf{IR} \cdot \mathsf{id}] = \mathsf{id} + \mathsf{id} = \mathsf{id}$, it follows that the following diagram commutes.

$$
\begin{tikzcd}
X \otimes (Y \oplus Y) \arrow[r, bend left, "{[\mathsf{id} \otimes \mathsf{IL}, \mathsf{id} \otimes \mathsf{IR}]}"] \arrow[d, "\mathsf{id} \otimes \mathsf{id}"'] & X \otimes Y \oplus X \otimes Z \arrow[l, bend left, "\mathsf{dist}"] \arrow[dl, "{\mathsf{id} \otimes [\mathsf{IL} \cdot \mathsf{id}, \mathsf{IR} \cdot \mathsf{id}]}"] \\
X \otimes (Y \oplus Y) &
\end{tikzcd}
$$

And as a result, one has that $\mathsf{id} \otimes [\mathsf{IL} \cdot \mathsf{id}_{[\![\mathbb{A}]\!]}, \mathsf{IR} \cdot \mathsf{id}_{[\![\mathbb{B}]\!]}] \cdot \mathsf{dist} = \mathsf{id} \otimes \mathsf{id}$. Therefore,

$$
\begin{aligned}
&[\![\Delta, x : \mathbb{A} \oplus \mathbb{B} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}\oplus\mathbb{B}} \cdot (\mathsf{id} \otimes [\mathsf{IL} \cdot \mathsf{id}_{[\![\mathbb{A}]\!]}, \mathsf{IR} \cdot \mathsf{id}_{[\![\mathbb{B}]\!]}]) \cdot \mathsf{dist} \cdot \mathsf{sw} \cdot ([\![\Gamma \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!]\\
&\otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma;\Delta} \cdot \mathsf{sh}_{\Delta;\Gamma}\\
=&[\![\Delta, x : \mathbb{A} \oplus \mathbb{B} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}\oplus\mathbb{B}} \cdot (\mathsf{id} \otimes \mathsf{id}) \cdot \mathsf{sw} \cdot ([\![\Gamma \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma;\Delta} \cdot \mathsf{sh}_{\Delta;\Gamma}\\
=&[\![\Delta, x : \mathbb{A} \oplus \mathbb{B} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}\oplus\mathbb{B}} \cdot \mathsf{sw} \cdot ([\![\Gamma \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Gamma;\Delta} \cdot \mathsf{sh}_{\Delta;\Gamma}\\
=&[\![\Delta, x : \mathbb{A} \oplus \mathbb{B} \triangleright w : \mathbb{D}]\!] \cdot \mathsf{jn}_{\Delta;\mathbb{A}\oplus\mathbb{B}} \cdot ([\![\Gamma \triangleright v : \mathbb{A} \oplus \mathbb{B}]\!] \otimes \mathsf{id}) \cdot \mathsf{sp}_{\Delta;\Gamma}\\
=&[\![w[v/x] : \mathbb{D}]\!]
\end{aligned}
$$

$\square$

4.5 Metric equations

The metric equations for conditionals are presented in Figure 12. Note that the first two equations are redundant.

$$\frac{v =_q w}{\mathsf{inl}(v) =_q \mathsf{inl}(w)} \qquad \frac{v =_q w}{\mathsf{inr}(v) =_q \mathsf{inr}(w)}$$

$$\frac{v =_q v' \quad w =_r w' \quad u =_s u'}{\mathsf{case}\ v\ \{\mathsf{inl}(x) \Rightarrow w; \mathsf{inr}(y) \Rightarrow u\} =_{q+\max(r,s)} \mathsf{case}\ v'\ \{\mathsf{inl}(x) \Rightarrow w'; \mathsf{inr}(y) \Rightarrow u'\}}$$

Figure 12: Metric equational system for condicionals

4.6 Generalized norm

Since the new model considered is based on direct sums of vector spaces, it is necessary to define a norm in these spaces.

Definition 4.6.1. Given $(v_1, \ldots, v_n) \in V_1 \oplus \ldots \oplus V_n$, the generalized norm is defined as:

$$\|(v_1, \ldots, v_n)\|_{\{V_1,\ldots,V_n\}\ \mathsf{gen}} = \sum_{i=1}^{n} \|v_i\|_{V_i} \tag{4.15}$$

where $\|\cdot\|_{V_i}$ is a norm associated with vector space V_i, for $1 \leq i \leq n$. When this norm is identical for all vector spaces $V_1, \ldots, V_n$, *i.e.*, $\|\cdot\|_{V_1} = \ldots = \|\cdot\|_{V_n} = \|\cdot\|_V$, the notation $\|\cdot\|_{\{V_1,\ldots,V_n\}\ \mathsf{gen}}$ is simplified to $\|\cdot\|_{V\ \mathsf{gen}}$. In this case, if $\|\cdot\|_V$ is also a generalized norm, the notation is further simplified to $\|\cdot\|_V$.
Now it is neccesary to prove that the generalized norm is a norm.

Proof. Attending to Definition 3.1.9, demonstrating that the generalized norm is a norm is equivalent to proving that it satisfies the following properties:

1. Positive definiteness: $\|(v_1, \ldots, v_n)\|_{\{V_1,\ldots,V_n\}\ \mathsf{gen}} \geq 0$ and $\|(v_1, \ldots, v_n)\|_{\{V_1,\ldots,V_n\}\ \mathsf{gen}} = 0$ if and only if $(v_1, \ldots, v_n) = 0$.

2. Positive scalability: $\|a(v_1, \ldots, v_n)\|_{\{V_1,\ldots,V_n\}\ \mathsf{gen}} = |a|\|(v_1, \ldots, v_n)\|_{\{V_1,\ldots,V_n\}\ \mathsf{gen}}$.

3. The triangle inequality: $\|(v_1,\ldots,v_n)+(w_1,\ldots,w_n)\|_{\{V_1,\ldots,V_n\}\text{ gen}} \leq \|(v_1,\ldots,v_n)\|_{\{V_1,\ldots,V_n\}\text{ gen}} + \|(w_1,\ldots,w_n)\|_{\{V_1,\ldots,V_n\}\text{ gen}}$.

Regarding the positive definiteness, for $1 \leq i \leq n$, given that $\|\cdot\|_{V_i}$ is a norm, it follows that $\|v_i\|_{V_i} \geq 0$ and $\|v_i\|_{V_i} = 0$ if and only if $v_i = 0$. Thus, $\|(v_1,\ldots,v_n)\|_{\{V_1,\ldots,V_n\}\text{ gen}} = \sum_i \|v_i\|_{V_i} \geq 0$ and $\|(v_1,\ldots,v_n)\|_{\{V_1,\ldots,V_n\}\text{ gen}} = \sum_i \|v_i\|_{V_i} = 0$ if and only if $(v_1,\ldots,v_n) = (0,\ldots,0) = 0$. With respect to the positive scalability, for $1 \leq i \leq n$, given that $\|\cdot\|_{V_i}$ is a norm, it follows that $\|v_i\|_{V_i}$ = $|a|\|v_i\|_{V_i}$. Therefore,

$$\begin{aligned}\|a(v_1,\ldots,v_n)\|_{\{V_1,\ldots,V_n\}\text{ gen}} &= \|(av_1,\ldots,av_n)\|_{\{V_1,\ldots,V_n\}} = \sum_i \|av_i\|_{V_i}\\ &= |a|\sum_i \|v_i\|_{V_i} = |a|\|(v_1,\ldots,v_n)\|_{\{V_1,\ldots,V_n\}\text{ gen}}\end{aligned}$$

Finally, concerning the triangle inequality, for $1 \leq i \leq n$, given that $\|\cdot\|_{V_i}$ is a norm, it follows that $\|v_i + w_i\|_{V_i} \leq \|v_i\|_{V_i} + \|w_i\|_{V_i}$. Hence, given that both terms of the inequation are non-negative, it follows that

$$\begin{aligned}\|(v_1,\ldots,v_n)+(w_1,\ldots,w_n)\|_{\{V_1,\ldots,V_n\}\text{ gen}} &= \|(v_1+w_1,\ldots,v_n+w_n)\|_{\{V_1,\ldots,V_n\}\text{ gen}}\\ &= \sum_i \|v_i + w_i\|_{V_i}\\ &\leq \sum_i \|v_i\|_{V_i} + \sum_i \|w_i\|_{V_i}\\ &= \|(v_1,\ldots,v_n)\|_{\{V_1,\ldots,V_n\}\text{ gen}} + \|(w_1,\ldots,w_n)\|_{\{V_1,\ldots,V_n\}\text{ gen}}\end{aligned}$$

□

Using Definition 4.6.1, it follows that the norms of the left and right injections, IL : $V \to V \oplus W$ and IR : $V \to W \oplus V$, applied to a vector $v \in V$, are defined as follows:

$$\begin{aligned}\|\text{IR}(v)\|_{\{V,W\}\text{ gen}} &= \|(v,0)\|_{\{V,W\}\text{ gen}} = \|v\|_V\\ \|\text{IL}(v)\|_{\{W,V\}\text{ gen}} &= \|(0,v)\|_{\{W,V\}\text{ gen}} = \|v\|_V\end{aligned} \tag{4.16}$$

where $\|\cdot\|_V$ is a norm in vector space V and $\|\cdot\|_W$ is a norm in vector space W.

Definition 4.6.2. An operator $A \in \mathbb{C}^{o_1\times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n\times o_n}$ can be decomposed as $A = (A_1,\ldots,A_n)$, where $A_i \in \mathbb{C}^{o_i\times o_i}$, for $1 \leq i \leq n$. The generalized trace norm of the operator A is defined as follows:

$$\|Q\|_{1\text{ gen}} = \sum_{i=1}^{n} \|A_i\|_1 \tag{4.17}$$

Within this model, the super-operators take the form $Q : V_1 \oplus \ldots \oplus V_n \quad \to W_1 \oplus \ldots \oplus W_m$, where each $V \in \{V_1, \ldots, V_n, W_1, \ldots, W_n\}$ is a vector space without direct sums.

Definition 4.6.3. For $Q : V_1 \oplus \ldots \oplus V_n \quad \to W, \exists Q_1 : V_1 \to W, \ldots, Q_n : V_n \to W$ such that

$$Q = [Q_1, \ldots, Q_n],$$

where $Q_i(v_i) = Q(\underbrace{\mathsf{I_L} \cdot \ldots \cdot \mathsf{I_L}}_{n-i\times} \cdot \underbrace{\mathsf{I_R} \cdot \ldots \cdot \mathsf{I_R}}_{i-1\times}(v_i))$, for $1 \leq i \leq n$.
The norm of the operator Q is defined as follows:

$$\|Q\|_{\{V_1\to W,\ldots,V_n\to W\}\,\mathsf{gen}} = \max\{\|Q_1\|_{V_1\to W}, \ldots, \|Q_n\|_{V_n\to W}\} \tag{4.18}$$

where, for $1 \leq i \leq n$, $\|\cdot\|_{V_i\to W}$ is a norm for an operator in the vector space $V_i \to W$.

As a result, now it is necessary to prove that the generalized norm for operators is a norm.

Proof. Regarding the positive definiteness, given that $\|\cdot\|_{V_i\to W}$ is a norm, it follows that $\|Q_i\|_{V_i\to W} \geq 0$ and $\|Q_i\|_{V_i\to W} = 0$ if and only if $Q_i = 0$, for $1 \leq i \leq n$. Thus, $\|Q\|_{\{V_1\to W,\ldots,V_n\to W\}\,\mathsf{gen}} = \max\{\|Q_1\|_{V_1\to W}, \ldots, \|Q_n\|_{V_n\to W}\} \geq 0$ and $\|Q\|_{\{V_1\to W,\ldots,V_n\to W\}\,\mathsf{gen}} = 0$ if and only if $Q = [Q_1, \ldots, Q_n] = [0, \ldots, 0] = 0$.
With respect to the positive scalability, given that $\|\cdot\|_{V_i\to W}$ is a norm, it follows that $\|aQ_i\|_{V_i\to W} = |a|\|Q_i\|_{V_i\to W}$, for $1 \leq i \leq n$. Therefore,

$$\begin{aligned}
\|aQ\|_{\{V_1\to W,\ldots,V_n\to W\}\,\mathsf{gen}} &= \|\,[aQ_1, \ldots, aQ_n]\|_{\{V_1\to W,\ldots,V_n\to W\}\,\mathsf{gen}} \\
&= \max\{\|aQ_1\|_{V_1\to W}, \ldots, \|aQ_n\|_{V_1\to W}\} \\
&= \max\{|a|\|Q_1\|_{V_1\to W}, \ldots, |a|\|Q_n\|_{V_n\to W}\} \\
&= |a| \max\{\|Q_1\|_{V_1\to W}, \ldots, \|Q_n\|_{V_n\to W}\} \\
&= |a|\|Q\|_{\{V_1\to W,\ldots,V_n\to W\}\,\mathsf{gen}}
\end{aligned}$$

Finally, concerning the triangle inequality, given that $\|\cdot\|_{V_i\to W}$ is a norm, it follows that $\|Q_i + S_i\|_{V_i\to W} \leq \|Q_i\|_{V_i\to W} + \|S_i\|_{V_i\to W}$, for $1 \leq i \leq n$. Hence, given that both terms of the inequation are non-negative, it follows that

$$\begin{aligned}\|Q+S\|_{\{V_1\to W,\ldots,V_n\to W\}\text{ gen}} &= \|[Q_1+S_1,\ldots,Q_n+S_n]\|_{\{V_1,\ldots,V_n\}\text{ gen}}\\ &= \max\{\|Q_1+S_1\|_{V_1\to W},\ldots,\|Q_n+S_n\|_{V_1\to W}\}\\ &\leq \max\{\|Q_1\|_{V_1\to W}+\|S_1\|_{V_1\to W},\ldots,\|Q_n\|_{V_n\to W}+\|R_n\|_{V_1\to W}\}\\ &= \max\{\|Q_1\|_{V_1\to W},\ldots,\|Q_n\|_{V_n\to W}\}\\ &\quad+\max\{\|S_1\|_{V_1\to W},\ldots,\|S_n\|_{V_1\to W}\}\\ &= \|Q\|_{\{V_1\to W,\ldots,V_n\to W\}\text{ gen}}+\|S\|_{\{V_1\to W,\ldots,V_n\to W\}\text{ gen}}\end{aligned}$$

□

Definition 4.6.4. For $Q : V \to W_1 \oplus \ldots \oplus W_m$, (where $W_1,\ldots,W_m$ are not direct sum of vector spaces,) $\exists\, Q_1 : V \to W_1,\ldots,Q_2 : V \to W_m$ such that

$$Q = \sum_{i=1}^{m} \underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{m-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot Q_i,$$

where $Q_i = \underbrace{\mathsf{PL}\cdot\ldots\cdot\mathsf{PL}}_{m-i\times}\cdot\underbrace{\mathsf{PR}\cdot\ldots\cdot\mathsf{PR}}_{i-1\times}\cdot Q$, for $1 \leq i \leq n$. As a result, considering Definition 4.6.1, the norm of the operator Q correponds to:

$$\|Q\|_{\{V\to W_1,\ldots,V\to W_n\}\text{ gen}} = \max\left\{\sum_{i=1}^{m}\|Q_i(v)\|_{W_i} \mid \|v\|_V = 1\right\} \tag{4.19}$$

Note that this is equivalent to defining the norm of the operator Q as follows:

$$\|Q\|_{\{V\to W_1,\ldots,V\to W_n\}\text{ gen}} = \max\{\|Q(v)\|_{\{W_1,\ldots,W_n\}\text{ gen}} \mid \|v\|_V = 1\} \tag{4.20}$$

Provar que isto é uma norma

Leveraging Definition 4.6.3 and Definition 4.6.4, it is possible to define the norm of an operator $Q : V_1 \oplus \ldots \oplus V_n \ \to W = W_1 \oplus \ldots \oplus W_m$, where each $V \in \{V_1,\ldots,V_n,W_1,\ldots,W_n\}$ is a vector space without direct sums, as outlined below.

Definition 4.6.5. For $Q : V_1 \oplus \ldots \oplus V_n \ \to W_1 \oplus \ldots \oplus W_m \exists Q_{11} : V_1 \to W_1,\ldots Q_{1m} : V_1 \to W_n,\ldots,Q_{n1} : V_n \to W_1,\ldots,Q_{nm} : V_n \to W_m$ such that

$$Q = \left[\sum_{i=1}^{m} \underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{m-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot Q_{1i},\ \ldots\ ,\sum_{i=1}^{m} \underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{m-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot Q_{ni}\right],$$

where $Q_{ij} = \underbrace{\mathsf{PL}\cdot\ldots\cdot\mathsf{PL}}_{m-j\times}\cdot\underbrace{\mathsf{PR}\cdot\ldots\cdot\mathsf{PR}}_{j-1\times}\cdot Q(\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{n-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}(v_i))$, for $1 \leq i \leq n$ and $1 \leq j \leq m$.

The norm of the operator Q is defined in the following manner:

$$\|Q\|_{\{V_1\to W_1,\ldots,V_n\to W_m\}\,\mathsf{gen}} = \max\Bigg\{\max\left\{\sum_{i=1}^{m}\|Q_{1i}(v_1)\|_{W_i} \,|\, \|v_1\|_{V_1} = 1\right\} \\ ,\ldots,\max\left\{\sum_{i=1}^{m}\|Q_{ni}(v_n)\|_{W_i} \,|\, \|v_n\|_{V_n} = 1\right\}\Bigg\} \tag{4.21}$$

Attending to the fact that the norms defined in Definition 4.6.3 and Definition 4.6.4 are valid, it follows that so is the norm defined above.

Convention 4.6.6. From this point forward, unless stated otherwise, whenever the equality

$$Q = \left[\sum_{i=1}^{m}\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{m-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot Q_{1i},\ \ldots,\ \sum_{i=1}^{m}\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{m-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot Q_{ni}\right]$$

is used for a super-operator Q, it is understood that the operators $Q_{11},\ldots,Q_{1m},\ldots,Q_{n1},\ldots,Q_{nm}$ are defined as in Definition 4.6.5.

It should be noted that the coproduct of two operators $Q : V_1 \oplus \ldots \oplus V_n \to W$ and $S : R_1 \oplus \ldots \oplus R_n \to W$ defined as, respectively, $Q = [Q_1,\ldots,Q_n]$ and $S = [S_1,\ldots,S_n]$, corresponds to $[Q,S] = [Q_1,\ldots,Q_n,S_1,\ldots,S_n]$.

The tensor product of two operators $Q : V_1\oplus\ldots\oplus V_n \to W_1\oplus\ldots W_m$ and $S : R_1\oplus\ldots\oplus R_t \to Y_1 \oplus \ldots \oplus Y_s$, corresponds to

$$\begin{aligned} &Q\otimes S : (V_1\oplus\ldots\oplus V_m)\otimes(R_1\oplus\ldots\oplus R_n)\to(W_1\oplus\ldots W_m)\otimes(Y_1\oplus\ldots\oplus Y_s)\\ &Q\otimes S = \left[\sum_{i=1}^{m}\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{m-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot Q_{1i},\ \ldots,\ \sum_{i=1}^{m}\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{m-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot Q_{ni}\right]\\ &\qquad\otimes\left[\sum_{i=1}^{s}\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{s-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot S_{1i},\ \ldots,\ \sum_{i=1}^{s}\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{s-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot S_{ti}\right]. \end{aligned} \tag{4.22}$$

Attending to the definition of the tensor product of a direct sum of vector spaces, it follows that the tensor product of two operators is defined as follows:

$$\begin{aligned} &Q\otimes S : V_1\otimes R_1\oplus\ldots\oplus V_1\otimes R_t\oplus\ldots\oplus V_n\otimes R_1\oplus\ldots\oplus V_n\otimes R_t\to W_1\otimes Y_1\oplus\ldots\oplus\\ &\qquad W_1\otimes Y_s\oplus\ldots\oplus W_m\otimes Y_1\oplus\ldots\oplus W_m\otimes Y_s\\ &Q\otimes S = \Bigg[\sum_{i=1}^{m}\sum_{j=1}^{s}\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{m-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{s-j\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{j-1\times}\cdot Q_{1i}\otimes S_{1j},\ \ldots, \end{aligned}$$

$$\sum_{i=1}^{m}\sum_{j=1}^{s}\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{m-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{s-j\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{j-1\times}\cdot Q_{1i}\otimes S_{tj},\ \ldots\ ,$$
$$\sum_{i=1}^{m}\sum_{j=1}^{s}\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{m-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{s-j\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{j-1\times}\cdot Q_{ni}\otimes S_{1j},\ \ldots\ ,$$
$$\left.\sum_{i=1}^{m}\sum_{j=1}^{s}\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{m-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{s-j\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{j-1\times}\cdot Q_{ni}\otimes S_{tj}\right]$$

Consider the identity operator, $I_{V_1\oplus\ldots\oplus V_n} : V_1\oplus\ldots\oplus V_n \to V_1\oplus\ldots\oplus V_n$. Note that in the decomposition

$$I=\left[\sum_{i=1}^{m}\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{m-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot I_{1i},\ \ldots\ ,\sum_{i=1}^{m}\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{m-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot I_{ni}\right],$$

one has that:

$$\begin{cases} I_{ij}=0 & \text{if } i\neq j\\ I_{ij}=I_{V_i} & \text{if } i=j. \end{cases}$$

Therefore,

$$I=\left[\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{n-1\times}\cdot I_{V_1},\ldots,\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{n-1\times}\cdot I_{V_n}\right].$$

As a result, given a super-operator $Q : V_1\oplus\ldots\oplus V_n \to W_1\oplus\ldots\oplus W_m$, the super-operator $Q\otimes I_{R_1\oplus\ldots\oplus R_t}$ is defined as follows:

$$\begin{aligned}Q\otimes I=\Bigg[&\sum_{i=1}^{m}\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{m-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{t-1\times}\cdot Q_{1i}\otimes I_{R_1},\ \ldots\ ,\\ &\sum_{i=1}^{m}\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{m-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{t-1\times}\cdot Q_{1i}\otimes I_{R_t},\ \ldots\ ,\\ &\sum_{i=1}^{m}\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{m-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{t-1\times}\cdot Q_{ni}\otimes I_{R_1},\ \ldots\ ,\\ &\sum_{i=1}^{m}\underbrace{\mathsf{IL}\cdot\ldots\cdot\mathsf{IL}}_{m-i\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{i-1\times}\cdot\underbrace{\mathsf{IR}\cdot\ldots\cdot\mathsf{IR}}_{t-1\times}\cdot Q_{ni}\otimes I_{R_t}\Bigg].\end{aligned}\tag{4.23}$$

Definition 4.6.7. The norm generalized trace norm of a super-operator $Q : \mathbb{C}^{o_1\times o_1}\oplus\ldots\oplus\mathbb{C}^{o_n\times o_n} \to \mathbb{C}^{p_1\times p_1}\oplus\ldots\oplus\ \mathbb{C}^{p_m\times p_m}$, denoted $\|Q\|_{1\,\mathsf{gen}}$, is defined as follows:

$$\begin{aligned}\|Q\|_{1\,\mathsf{gen}}=\max\Bigg\{&\max\left\{\sum_{i=1}^{m}\|Q_{1i}(A_1)\|_1 \mid \|A_1\|_1=1\right\}\\ &,\ \ldots\ ,\max\left\{\sum_{i=1}^{m}\|Q_{ni}(A_n)\|_1 \mid \|A_n\|_1=1\right\}\Bigg\}\end{aligned}\tag{4.24}$$

Note that this definition is equivalent to the following:

$$\begin{aligned}\|Q\|_{1\,\mathsf{gen}} &= \max\{\|Q_1\|_{1\,\mathsf{gen}}, \ldots, \|Q_n(A_n)\|_{1\,\mathsf{gen}}\} \\ &= \max\{\max\{\|Q_1(A_1)\|_{1\,\mathsf{gen}} \mid \|A_1\|_1 = 1\}, \ldots, \max\{\|Q_n(A_n)\|_{1\,\mathsf{gen}} \mid \|A_n\|_1 = 1\}\},\end{aligned} \tag{4.25}$$

where

$$\|Q_i(A_i)\|_{1\,\mathsf{gen}} = \sum_j \|Q_{ij}(A_i)\|_1 \tag{4.26}$$

for $1 \le i \le n$.

Definition 4.6.8. Given a super-operator $Q : \mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n} \to \mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m \times p_m}$, denoted $\|Q\|_{\diamond\,\mathsf{gen}}$, its generalized diamond norm, denoted $\|Q\|_{\diamond\,\mathsf{gen}}$, of is defined as follows:

$$\|Q\|_{\diamond\,\mathsf{gen}} = \|Q \otimes I_{\mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n}}\|_{1\,\mathsf{gen}}$$

In order for the generalized diamond norm to be a suitable norm when reasoning about quantum programs, similarly to the diamond norm, it should satisfy the following properties:

1. Stability under tensoring with identity: $\|Q \otimes I\|_{\diamond\,\mathsf{gen}} \le \|Q\|_{\diamond\,\mathsf{gen}}$;
2. If Q is a quantum channel then $\|SQ\|_{\diamond\,\mathsf{gen}} \le \|S\|_{\diamond\,\mathsf{gen}}$, and if S is a quantum channel, then $\|SQ\|_{\diamond\,\mathsf{gen}} \le \|Q\|_{\diamond\,\mathsf{gen}}$.

In the proofs of the theorems, propositions, and lemmas that follow, certain sections or the entirety of the proof align precisely with the proofs of the corresponding results for the trace or diamond norm presented in [12]. In these instances, those sections are omitted, and the reader is referred to the relevant proof in [12].

Proposition 4.6.9. *For all super-operators $Q : \mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n} \to \mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m \times p_m}$, it holds that:*

$$\begin{aligned}\|Q\|_{1\,gen} = \max\Bigg\{ &\max\left\{\sum_{i=1}^{m} \|Q_{1i}(v_1 w_1^\dagger)\|_1 \mid \|v_1\|_2 = 1, \|w_1\|_2 = 1\right\} \\ &, \ldots, \max\left\{\sum_{i=1}^{m} \|Q_{ni}(v_n w_n^\dagger)\|_1 \mid \|v_n\|_1 = 1, \|w_n\|_1 = 1\right\}\Bigg\}\end{aligned} \tag{4.27}$$

definir função convexa nos preliminares matemáticos

Proof. Attending to triangle inequality and positive scalability properties of a norm, all norms are convex functions. Considering Definition 4.6.7, the argument for this equality is similar to the one presented in [12, Proof of Proposition 3.38], now taking into account that the generalized trace norm is a convex function □

Lemma 4.6.10. *Let* $Q_i : \mathbb{C}^{o\times o} \to \mathbb{C}^{p_1\times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m\times p_m}$ *be a super-operator. For every choice of a complex vector space* $\mathbb{C}^q$ *and unit vectors* $v_1, v_2 \in \mathbb{C}^o \otimes \mathbb{C}^q$*, there exist unit vectors* $w_1, w_2 \in \mathbb{C}^o \otimes \mathbb{C}^o$ *such that the following equalities hold:*

$$\sum_{j=1}^{m} \left\| Q_{ij} \otimes I_{\mathbb{C}^{q\times q}}(v_1 v_2^\dagger) \right\|_1 = \sum_{j=1}^{m} \left\| Q_{ij} \otimes I_{\mathbb{C}^{o\times o}}(w_1 w_2^\dagger) \right\|_1 \tag{4.28}$$

Proof. The proof of this Lemma follows form the one presented in [12, Proof of Lemma 3.45]. Considering that for $q \leq o$, if for any choice of an isometry $T \in \mathbb{C}^q \to \mathbb{C}^o$, the vectors $w_1 = (I_{\mathbb{C}^o} \otimes T)v_1$ and $w_2 = (I_{\mathbb{C}^o} \otimes T)v_2$ satisfy

$$\|Q_{ij} \otimes I_{\mathbb{C}^{q\times q}}(v_1 v_2^\dagger)\|_1 = \|Q_{ij} \otimes I_{\mathbb{C}^{o\times o}}(w_1 w_2^\dagger)\|_1, \tag{4.29}$$

consequentlty, for any choice of an isometry $T \in \mathbb{C}^q \to \mathbb{C}^o$ the vectors $w_1 = (I_{\mathbb{C}^o} \otimes T)v_1$ and $w_2 = (I_{\mathbb{C}^o} \otimes T)v_2$ satisfy Equation 4.28.

Furthermore, for $q > o$, given that the vectors w_1, w_2 which satisfy Equation 4.29 are defined solely based on the Schmidt decomposition of w_1, w_2, it follows that these same vectors satisfy Equation 4.28. □

Lemma 4.6.11. *Given two sets* $A = a_1, \ldots, a_n$ *and* $B = b_1, \ldots, b_m$*, if* $a_i \leq b_j$ *for all* $1 \leq j \leq m$*, then* $\max A \geq \max B$*.*

Proof. Since $a_i \leq b_j$ for all $1 \leq j \leq m$, given that the maximum element of a set belongs to the set, it follows that $\max a_i \geq \max B$. From the definition of the maximum of a set, it follows that $\max A \geq a_i$. Therefore, $\max A \geq \max B$. □

Lemma 4.6.12. *Given sets* $A_1, \ldots, A_n$*, it holds that* $\max\{\max A_1, \ldots, \max A_n\} = \max \cup_{i=1}^n A_i$*.*

Proof. Since $\max A_1 \in A_1, \ldots, \max A_n \in A_n$, it follows that $\{\max A_1, \ldots, \max A_n\} \in \cup_{i=1}^n A_i$. Consequentlty $\max\{\max A_1, \ldots, \max A_n\} \leq \max \cup_{i=1}^n A_i$. Considering that $\forall a_{1i} \in A_1, \ldots, a_{ni} \in A_n, \max A_i \geq a_{1i}, \ldots, \max A_n \geq a_{ni}$, it follows that

$$\forall a_{1i} \in A_1, \ldots, a_{ni} \in A_n, \max\{\max A_1, \ldots, \max A_n\} \geq a_{1i}, \ldots, \max\{\max A_1, \ldots, \max A_n\} \geq a_{ni}.$$

As a result, $\max\{\max A_1, \ldots, \max A_n\} \geq \max \cup_{i=1}^n A_i$. Therefore, $\max\{\max A_1, \ldots, \max A_n\} = \max \cup_{i=1}^n A_i$. □

Lemma 4.6.13. *Given sets $A_1, \dots, A_n$, with $\sum_{i=1}^n A_i = \{\sum_{i=1}^n a_i \mid a_i \in A_i\}$ it holds that $\sum_{i=1}^n \max A_i = \max\{\sum_{i=1}^n A_i\}$*

Proof. Since $\max A_1 \in A_1, \dots, \max A_n \in A_n$, it follows that $\sum_{i=1}^n \max A_i \in \{\sum_{i=1}^n A_i\}$. Consequentlty, $\sum_{i=1}^n \max A_i \leq \max\{\sum_{i=1}^n A_i\}$. Considering that $\forall a_{1i} \in A_1, \dots, a_{ni} \in A_n, \max A_1 \geq a_{1i}, \dots, \max A_n \geq a_{ni}$, it follows that $\sum_{i=1}^n \max A_i \geq \max\{\sum_{i=1}^n A_i\}$. Therefore, $\sum_{i=1}^n \max A_i = \max\{\sum_{i=1}^n A_i\}$. $\square$

Lemma 4.6.14. *Let $Q : \mathbb{C}^{o_1 \times o_1} \oplus \dots \oplus \mathbb{C}^{o_n \times o_n} \to \mathbb{C}^{p_1 \times p_1} \oplus \dots \oplus \mathbb{C}^{p_m \times p_m}$ be a super-operator, then for $O \in \mathbb{C}^{o_1 \times o_1} \oplus \dots \oplus \mathbb{C}^{o_m \times o_m}$ it holds that:*

$$\|Q(O)\|_{1\,gen} \leq \|Q\|_{1\,gen} \cdot \|O\|_{1\,gen}. \tag{4.30}$$

Proof. O can be written as $O = (O_1, \dots, O_n)$, where $O_i \in \mathbb{C}^{p_i \times p_i}$ and $O_i = \underbrace{\mathrm{PL} \cdot \dots \cdot \mathrm{PL}}_{n-i\times} \cdot \underbrace{\mathrm{PR} \cdot \dots \cdot \mathrm{PR}}_{i-1\times} \cdot O$ for $1 \leq i \leq n$. Considering Definition 4.6.1, it follows that:

$$\|O\|_{1\text{ gen}} = \|O_1\|_1 + \dots + \|O_n\|_1. \tag{4.31}$$

Considering the decomposition of Q as in Definition 4.6.3, applying O to Q results in:

$$Q(O) = [Q_1, \dots, Q_n](O_1, \dots, O_n) = \sum_{i=1}^n Q_i(O_i) \tag{4.32}$$

As a result, considering the triangle inequality, it follows that:

$$\|Q(O)\|_{1\text{ gen}} \leq \sum_{i=1}^n \|Q_i(O_i)\|_{1\text{ gen}}. \tag{4.33}$$

The generalized trace norm of Q is given by:

$$\begin{aligned}
\|Q\|_{1\text{ gen}} &= \max\{\max\{\|Q_1(A_1)\|_{1\text{ gen}} \mid \|A_1\|_1 = 1\} && \{\text{Definition 4.6.7}\} \\
&\qquad, \dots, \max\{\|Q_n(A_n)\|_{1\text{ gen}} \mid \|A_n\|_1 = 1\}\Big\} \\
&= \max\Big\{\|Q_1(A_1)\|_{1\text{ gen}}, \dots, \|Q_n(A_n)\|_{1\text{ gen}} \mid \|A_1\|_1 = 1 && \{\text{Lemma 4.6.12}\} \\
&\qquad, \dots, \|A_n\|_1 = 1\}
\end{aligned} \tag{4.34}$$

To prove that if $\|O\|_{1\text{ gen}} = 1$

$$\|Q(O)\|_{1\text{ gen}} \leq \|Q\|_{1\text{ gen}}, \tag{4.35}$$

is equivalent to demonstrating that,

$$\max\left\{\|Q(O)\|_{1\text{ gen}}\;\middle|\;\sum_{i=1}^{n}\|O_i\|_1=1\right\}\leq\|Q\|_{1\text{ gen}},\tag{4.36}$$

Given Equation 4.33 and Equation 4.34, if the following inequality holds, then Equation 4.35 also holds.

$$\begin{aligned}&\max\left\{\sum_{i=1}^{n}\|Q_i(O_i)\|_{1\text{ gen}}\;\middle|\;\sum_{i=1}^{n}\|O_i\|_1=1\right\}\\&\leq\max\{\|Q_1(A_1)\|_{1\text{ gen}},\ldots,\|Q_n(A_n)\|_{1\text{ gen}}\mid\|A_1\|_1=1,\ldots,\|A_n\|_1=1\}\end{aligned}\tag{4.37}$$

Considering $O_1,\ldots,O_n$ as the matrices that maximize the left-hand side of the inequality, it follows that:

$$\begin{aligned}&\max\{\|Q_1(A_1)\|_{1\text{ gen}},\ldots,\|Q_n(A_n)\|_{1\text{ gen}}\mid\|A_1\|_1=1,\ldots,\|A_n\|_1=1\}\\&\geq\max\left\{\|Q_1(O_1/\|O_1\|_1)\|_{1\text{ gen}},\ldots,\|Q_n(O_n/\|O_n\|_1)\|_{1\text{ gen}}\right\}.\end{aligned}\tag{4.38}$$

Consequentlty, proving the following inequality is equivalent to demonstrating that Equation 4.35 holds.

$$\begin{aligned}&\max\left\{\sum_{i=1}^{n}\|Q_i(O_i)\|_{1\text{ gen}}\right\}\leq\max\{\|Q_1(O_1/\|O_1\|_1)\|_{1\text{ gen}},\ldots,\|Q_n(O_n/\|O_n\|_1)\|_{1\text{ gen}}\}\\&\wedge\sum_{i=1}^{n}\|O_i\|_1=1\end{aligned}\tag{4.39}$$

This inequality can be rewritten as:

$$\begin{aligned}&\max\left\{\sum_{i=1}^{n}\|Q_i(O_i)\|_{1\text{ gen}}\right\}\leq\max\left\{(1/\|O_1\|_1)\|Q_1(O_1)\|_{1\text{ gen}},\ldots,(1/\|O_n\|_1)\|Q_n(O_n)\|_{1\text{ gen}}\right\}\\&\wedge\sum_{i=1}^{n}\|O_i\|_1=1.\end{aligned}\tag{4.40}$$

This is equivalent to demonstrating that for all $a_1,\ldots,a_n,x_1,\ldots,x_n\in\mathbb{R}_0^+$ with $a_1+\ldots+a_n=1$,

$$x_1+\ldots+x_n\leq\max\left\{\frac{1}{a_1}x_1,\ldots,\frac{1}{a_n}x_n\right\}\tag{4.41}$$

Designating $M=\max\left\{\frac{1}{a_1}x_1,\ldots,\frac{1}{a_n}x_n\right\}$, from the definition of maximum it follows that, for all $1\leq i\leq n$, $x_i\leq M\cdot a_i$, and consequently, $x_1+\ldots+x_n\leq M\cdot(a_1+\ldots+a_n)=M$. Therefore, it holds that:

$$\|Q(O)\|_{1\text{ gen}}\leq\|Q\|_{1\text{ gen}}.\tag{4.42}$$

As a result, it follows that for an operator $O \in \mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_m \times o_m}$, $\left\| Q \left(\frac{O}{\|O\|_{1 \text{ gen}}} \right) \right\|_{1 \text{ gen}}$ is upper bounded by $\|Q\|_{1 \text{ gen}}$. Thus, Equation 4.35 holds. $\square$

Theorem 4.6.15. *For all super-operators $Q : \mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n} \rightarrow \mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m \times p_m}$ and complex spaces $\mathbb{C}^{q_1 \times q_1} \oplus \ldots \oplus \mathbb{C}^{q_t \times q_t}$ it holds that:*

$$\|Q \otimes I_{\mathbb{C}^{q_1 \times q_1} \oplus \ldots \oplus \mathbb{C}^{q_t \times q_t}}\|_{1 \text{ gen}} \leq \|Q\|_{\diamond \text{ gen}} \tag{4.43}$$

with equality holding under the assumption that within the direct sum of vector spaces $\mathbb{C}^{q_1 \times q_1} \oplus \ldots \oplus \mathbb{C}^{q_t \times q_t}$, there exists a vector space $\mathbb{C}^{q_i \times q_i}$, where $1 \leq i \leq t$, such that for all $1 \leq j \leq n$, dim $\mathbb{C}^{q_i} \geq$ dim $\mathbb{C}^{o_j}$.

Proof. Attending to Equation 4.23, Definition 4.6.7 and Definition 4.6.8 , one has that

$$\begin{aligned}
\|Q\|_{\diamond \text{ gen}} &= \|Q \otimes I_{\mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n}}\|_{1 \text{ gen}} \\
&= \max \left\{ \max \left\{ \sum_{i=1}^{m} \|Q_{1i} \otimes I_{\mathbb{C}^{o_1 \times o_1}}(A_{11})\|_1 \mid \|A_{11}\|_1 = 1 \right\} \right. \\
&\quad , \ldots , \max \left\{ \sum_{i=1}^{m} \|Q_{1i} \otimes I_{\mathbb{C}^{o_n \times o_n}}(A_{1n})\|_1 \mid \|A_{1n}\|_1 = 1 \right\} \\
&\quad , \ldots , \max \left\{ \sum_{i=1}^{m} \|Q_{ni} \otimes I_{\mathbb{C}^{o_1 \times o_1}}(A_{n1})\|_1 \mid \|A_{n1}\|_1 = 1 \right\} \\
&\quad \left. , \ldots , \max \left\{ \sum_{i=1}^{m} \|Q_{ni} \otimes I_{\mathbb{C}^{q_t \times q_t}}(A_{nn})\|_1 \mid \|A_{nn}\|_1 = 1 \right\} \right\}
\end{aligned} \tag{4.44}$$

Applying the same principle as in [12, Proof of Theorem 3.36], considering Proposition 4.6.9, Lemma 4.6.10, and Equation 4.23, it follows that for unit vectors $v_{ij}, w_{ij} \in \mathbb{C}^{o_i} \otimes \mathbb{C}^{o_j}$, where $1 \leq i \leq n$ and $1 \leq j \leq n$, the following inequality holds:

$$\begin{aligned}
\|Q \otimes I_{\mathbb{C}^{q_1 \times q_1} \oplus \ldots \oplus \mathbb{C}^{q_t \times q_t}}\|_{1 \text{ gen}} = \max & \left\{ \sum_{i=1}^{m} \left\| Q_{1i} \otimes I_{\mathbb{C}^{o_1 \times o_1}}(v_{11} w_{11}^{\dagger}) \right\|_1 \right. \\
& , \ldots , \sum_{i=1}^{m} \left\| Q_{1i} \otimes I_{\mathbb{C}^{o_n \times o_n}}(v_{1n} w_{1n}^{\dagger}) \right\|_1 \\
& , \ldots , \sum_{i=1}^{m} \left\| Q_{ni} \otimes I_{\mathbb{C}^{o_1 \times o_1}}(v_{n1} w_{n1}^{\dagger}) \right\|_1 \\
& \left. , \ldots , \sum_{i=1}^{m} \left\| Q_{1i} \otimes I_{\mathbb{C}^{o_n \times o_n}}(v_{nn} w_{nn}^{\dagger}) \right\|_1 \right\}
\end{aligned} \tag{4.45}$$

Note that if the number of direct sums in the complex space $\mathbb{C}^{q_1 \times q_1} \oplus \ldots \oplus \mathbb{C}^{q_t \times q_t}$ is less than the number of direct sums in the complex space $\mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n}$, when considering

Lemma 4.6.10 it is always possible to choose the vector space in $\mathbb{C}^{o_1\times o_1}\oplus\ldots\oplus\mathbb{C}^{o_n\times o_n}$, $\mathbb{C}^{o_k\times o_k}$, such that $\sum_{j=1}^{m}\|Q_{ij}\otimes I_{\mathbb{C}^{o_k\times o_k}}(v_{ik}w_{ik}^{\dagger})\|$ is maximized, where $1\leq i\leq n$ and $1\leq k\leq n$. As a result, the equality above holds in this case. On the other hand if the number of direct sums in the complex space $\mathbb{C}^{q_1\times q_1}\oplus\ldots\oplus\mathbb{C}^{q_t\times q_t}$ is greater than the number of direct sums in the complex space $\mathbb{C}^{o_1\times o_1}\oplus\ldots\oplus\mathbb{C}^{o_n\times o_n}$, regarding the vector spaces $\mathbb{C}^{q_n\times q_n},\ldots,\mathbb{C}^{q_t\times q_t}$, when considering Lemma 4.6.10 it is possible to choose $\mathbb{C}^{o_1\times o_1}$ as the vector space where the identity operator acts. This corresponds to the elements $\sum_{j=1}^{m}|Q_{ij}\otimes I_{\mathbb{C}^{o_1\times o_1}}(v_{i1}w_{i1}^{\dagger})|$, where $1\leq i\leq n$, which were already in the set. Since a set cannot contain duplicate elements, the set remains unchanged, and therefore, the equality above holds in this case as well.

Attending to Definition 3.1.28, for unit vectors v_{ik} and w_{ik}, where $1\leq i\leq n$ and $1\leq k\leq n$, it follows that:

$$\sum_{j=1}^{m}\left\|Q_{ij}\otimes I_{\mathbb{C}^{o_k\times o_k}}(v_{ik}w_{ik}^{\dagger})\right\|_1\leq\max\left\{\sum_{j=1}^{m}\|Q_{ij}\otimes I_{\mathbb{C}^{o_k\times o_k}}(A_{ik})\|_1\mid\|A_{ik}=1\|_1\right\},\quad(4.46)$$

As a result, considering Equation 4.44 it holds that:

$$\|Q\otimes I_{\mathbb{C}^{q_1\times q_1}\oplus\ldots\oplus\mathbb{C}^{q_t\times q_t}}\|_{1\text{ gen}}\leq\|Q\|_{\diamond\text{ gen}}\quad(4.47)$$

If dim $\mathbb{C}^{q_k}\geq$ dim $\mathbb{C}^{o_i}$, there exists an isometry $T:\mathbb{C}^{o_i}\rightarrow\mathbb{C}^{q_k}$. Moreover, for $A\in\mathbb{C}^{o_i\otimes o_i}$, such that $\|A\|_1=1$, and $Q_{ij}:\mathbb{C}^{o_i\otimes o_i}\rightarrow\mathbb{C}^{p_j\otimes p_j}$, where $1\leq j\leq m$, considering [12, Proof of Theorem 3.36], it holds that:

$$\sum_{j=1}^{m}\|Q_{ij}\otimes I_{\mathbb{C}^{o_i\times o_i}}(A)\|_1=\sum_{j}\|(Q_{ij}\otimes I_{\mathbb{C}^{q_k\times q_k}})((I_{\mathbb{C}^{o_i\times o_i}}\otimes T)A(I_{\mathbb{C}^{o_i\times o_i}}\otimes T)^{\dagger})\|_1.\quad(4.48)$$

This can be rewritten as:

$$\sum_{j=1}^{m}\|Q_{ij}\otimes I_{\mathbb{C}^{o_i\times o_i}}(A)\|_1=\|(Q_i\otimes I_{\mathbb{C}^{q_k\times q_k}})((I_{\mathbb{C}^{o_i\times o_i}}\otimes T)A(I_{\mathbb{C}^{o_i\times o_i}}\otimes T)^{\dagger})\|_{1\text{ gen}}.\quad(4.49)$$

Consequentlty, by Lemma 4.6.14, it follows that:

$$\sum_{j=1}^{m}\|Q_{ij}\otimes I_{\mathbb{C}^{o_i\times o_i}}(A)\|_1\leq\|Q_i\otimes I_{\mathbb{C}^{q_k\times q_k}}\|_{1\text{ gen}}=\max\left\{\sum_{j=1}^{m}\|Q_{ij}\otimes I_{\mathbb{C}^{q_k\times q_k}}(B)\|_1\mid\|B\|=1\right\}.\quad(4.50)$$

And, as a result, considering Lemma 4.6.11, under the assumption that within the direct sum of vector spaces $\mathbb{C}^{q_1\times q_1}\oplus\ldots\oplus\mathbb{C}^{q_t\times q_t}$, there exists a vector space $\mathbb{C}^{q_i\times q_i}$, where $1\leq i\leq t$, such that for all $1\leq j\leq n$, dim $\mathbb{C}^{q_i}\geq$ dim $\mathbb{C}^{o_j}$, it holds that:

$$\|Q\|_{\diamond\text{ gen}}\leq\|Q\otimes I_{\mathbb{C}^{q_1\times q_1}\oplus\ldots\oplus\mathbb{C}^{q_t\times q_t}}\|_{1\text{ gen}}\quad(4.51)$$

which completes the proof. □

Corollary 4.6.16. *For all super-operators $Q : \mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n} \rightarrow \mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m \times p_m}$ and complex spaces $\mathbb{C}^{q_1 \times q_1} \oplus \ldots \oplus \mathbb{C}^{q_t \times q_t}$ it holds that:*

$$\|Q \otimes I_{\mathbb{C}^{q_1 \times q_1} \oplus \ldots \oplus \mathbb{C}^{q_t \times q_t}}\|_{\diamond \textit{ gen}} = \|Q\|_{\diamond \textit{ gen}} \tag{4.52}$$

Proposition 4.6.17. *The generalized trace norm is submultiplicative with respect to composition of super-operators, i.e., for all super-operators $Q : \mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n} \rightarrow \mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m \times p_m}$ and $S : \mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m \times p_m} \rightarrow \mathbb{C}^{q_1 \times q_1} \oplus \ldots \oplus \mathbb{C}^{q_t \times q_t}$, it holds that:*

$$\|SQ\|_{1 \textit{ gen}} \leq \|S\|_{1 \textit{ gen}} \|Q\|_{1 \textit{ gen}} \tag{4.53}$$

Proof. Considering the decomposition $Q = [Q_1, \ldots, Q_n]$, where $Q_1, \ldots, Q_n$ are defined as in Definition 4.6.3, and for $1 \leq i \leq n$ $Q_i = \sum_{j=1}^{m} \underbrace{\mathsf{IL} \cdot \ldots \cdot \mathsf{IL}}_{m-i\times} \cdot \underbrace{\mathsf{IR} \cdot \ldots \cdot \mathsf{IR}}_{i-1\times} \cdot Q_{ij}$, the composition $S \cdot Q$ can be defined as follows:

$$S \cdot Q = [S \cdot Q_1, \ldots, S \cdot Q_n]. \tag{4.54}$$

where,

$$S \cdot Q_i = \sum_{j=1}^{m} \sum_{k=1}^{t} \underbrace{\mathsf{IL} \cdot \ldots \cdot \mathsf{IL}}_{t-k\times} \cdot \underbrace{\mathsf{IR} \cdot \ldots \cdot \mathsf{IR}}_{k-1\times} \cdot S_{jk} \cdot Q_{ij} \tag{4.55}$$

Attending to Definition 4.6.3, it follows that:

$$\begin{aligned} \|S \cdot Q\|_{1 \text{ gen}} = \max\{&\max\{\|S \cdot Q_1(A_1)\|_{1 \text{ gen}} \mid \|A_1\|_1 = 1\} \\ &, \ldots, \max\{\|S \cdot Q_n(A_n)\|_{1 \text{ gen}} \mid \|A_n\|_1 = 1\}\}, \end{aligned} \tag{4.56}$$

where,

$$\|S \cdot Q_i(A_i)\|_{1 \text{ gen}} = \sum_{k=1}^{t} \left\| \sum_{j=1}^{m} S_{jk} \cdot Q_{ij}(A_i) \right\|_1 . \tag{4.57}$$

for all $1 \leq i \leq n$.

Let $P \in \mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m \times p_m}$, by Lemma 4.6.14 it follows that:

$$\|S(P)\|_{1 \text{ gen}} \leq \|S\|_{1 \text{ gen}} \cdot \|P\|_{1 \text{ gen}}. \tag{4.58}$$

As a result,

$$\|S(Q_i(A_i))\|_{1 \text{ gen}} \leq \|S\|_{1 \text{ gen}} \cdot \|Q_i(A_i)\|_{1 \text{ gen}}, \tag{4.59}$$

for all $O_i \in \mathbb{C}^{o_i \times o_i}$ and $1 \leq i \leq n$.

Given that

$$S \cdot Q_i(A_i) = \sum_{j=1}^{m} \sum_{k=1}^{t} \underbrace{\mathsf{I}_{\mathsf{L}} \cdot \ldots \cdot \mathsf{I}_{\mathsf{L}}}_{t-k\times} \cdot \underbrace{\mathsf{I}_{\mathsf{R}} \cdot \ldots \cdot \mathsf{I}_{\mathsf{R}}}_{k-1\times} \cdot S_{jk} \cdot Q_{ij}(A_i) \tag{4.60}$$

and that

$$Q_i(A_i) = \sum_{j=1}^{m} \underbrace{\mathsf{I}_{\mathsf{L}} \cdot \ldots \cdot \mathsf{I}_{\mathsf{L}}}_{m-j\times} \cdot \underbrace{\mathsf{I}_{\mathsf{R}} \cdot \ldots \cdot \mathsf{I}_{\mathsf{R}}}_{j-1\times} \cdot Q_{ij}(A_i), \tag{4.61}$$

considering Definition 4.6.2, Equation 4.59 can be rewritten as:

$$\sum_{k=1}^{t} \left\| \sum_{j=1}^{m} S_{jk} \cdot Q_{ij}(A_i) \right\|_1 \leq \|S\|_{1\,\mathsf{gen}} \cdot \sum_{j=1}^{m} \|Q_{ij}(A_i)\|_1 . \tag{4.62}$$

Taking the maximum over all $A \in \mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n}$ such that $\|A_i\|_1 = 1$ yields the following inequality

$$\begin{aligned} &\max \left\{ \sum_{k=1}^{t} \left\| \sum_{j=1}^{m} S_{jk} \cdot Q_{ij}(A_i) \right\|_1 \,\middle|\, \|A_i\|_1 = 1 \right\} \\ &\leq \|S\|_{1\,\mathsf{gen}} \cdot \max \left\{ \sum_{j=1}^{m} \|Q_{ij}(A_i)\|_1 \,\middle|\, \|O_i\|_1 = 1 \right\}. \end{aligned} \tag{4.63}$$

Attending to Equation 4.57 and Definition 4.6.4, this is equivalent to

$$\max\{\|S \cdot Q_i(A_1)\|_{1\,\mathsf{gen}} \mid \|A_1\|_1 = 1\} = \|SQ_i\|_{1\,\mathsf{gen}} \leq \|S\|_{1\,\mathsf{gen}} \cdot \|Q_i\|_{1\,\mathsf{gen}} \tag{4.64}$$

for all $1 \leq i \leq n$. Considering Definition 4.6.3, given the fact that for $a, b, c \in \mathbb{R}$ if $a \leq b$ and $b \leq c$, then $a \leq c$, it follows that:

$$\|SQ_i\|_{1\,\mathsf{gen}} \leq \|S\|_{1\,\mathsf{gen}} \|Q\|_{1\,\mathsf{gen}} \tag{4.65}$$

Attending to Equation 4.56, and the fact that if all elements of a set verify a certain property, then the maximum of the set also verifies the property, given it is an element of the set, it follows that:

$$\|SQ\|_{1\,\mathsf{gen}} \leq \|S\|_{1\,\mathsf{gen}} \|Q\|_{1\,\mathsf{gen}} \tag{4.66}$$

Therefore, the inequality in Equation 4.67 holds.

□

Proposition 4.6.18. *The generalized diamond norm is submultiplicative with respect to composition of super-operators, i.e., for all super-operators* $Q : \mathbb{C}^{o_1\times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n\times o_n} \rightarrow \mathbb{C}^{p_1\times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m\times p_m}$ *and* $S : \mathbb{C}^{p_1\times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m\times p_m} \rightarrow \mathbb{C}^{q_1\times q_1} \oplus \ldots \oplus \mathbb{C}^{q_t\times q_t}$*, it holds that:*

$$\|SQ\|_{\diamond\text{ gen}} \leq \|S\|_{\diamond\text{ gen}}\|Q\|_{\diamond\text{ gen}} \tag{4.67}$$

Proof. By Proposition 4.6.17, it is possible to state that:

$$\|SQ \otimes I_{\mathbb{C}^{o_1\times o_1}\oplus\ldots\oplus\mathbb{C}^{o_n\times o_n}}\|_{1\text{ gen}} \leq \|S \otimes I_{\mathbb{C}^{o_1\times o_1}\oplus\ldots\oplus\mathbb{C}^{o_n\times o_n}}\|_{1\text{ gen}} \cdot \|Q \otimes I_{\mathbb{C}^{o_1\times o_1}\oplus\ldots\oplus\mathbb{C}^{o_n\times o_n}}\|_{1\text{ gen}} \tag{4.68}$$

Attending to Definition 4.6.8, it follows that:

$$\|SQ\|_{\diamond\text{ gen}} \leq \|S \otimes I_{\mathbb{C}^{o_1\times o_1}\oplus\ldots\oplus\mathbb{C}^{o_n\times o_n}}\|_{1\text{ gen}} \cdot \|Q\|_{\diamond\text{ gen}} \tag{4.69}$$

Given Theorem 4.6.15, it holds that

$$\|S \otimes I_{\mathbb{C}^{o_1\times o_1}\oplus\ldots\oplus\mathbb{C}^{o_n\times o_n}}\|_{1\text{ gen}} \leq \|S\|_{\diamond\text{ gen}} \tag{4.70}$$

As a result, the inequality in Equation 4.67 holds. □

Lemma 4.6.19. *For all super-operators* $Q_i : \mathbb{C}^{n\times n} \rightarrow \mathbb{C}^{p_1\times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m\times p_m}$*, it holds that:*

$$\|Q_i\|_{1\text{ gen}} = \max\{\text{Tr}\left(Q_i(vv^\dagger)\right) \mid \|v\|_2 = 1\} \tag{4.71}$$

Proof. For $A \in \mathbb{C}^{n\times n}$, it holds that:

$$\begin{aligned}
\|Q_i\|_{1\text{ gen}} &= \sum_{j=1}^{m} \max\{\|Q_{ij}(A)\|_1 \mid \|A\|_1 = 1\} && \{\text{Definition 4.6.4}\}\\
&= \max\left\{\sum_{j=1}^{m}\|Q_{ij}(A)\|_1 \;\middle|\; \|A\|_1 = 1\right\} && \{\text{Lemma 4.6.13}\}\\
&= \max\left\{\sum_{j=1}^{m}|\langle U_j, Q_{ij}(A)\rangle| \;\middle|\; \|A\|_1 = 1, U_j \in \mathbb{C}^{n\times n}\right\} && \{\text{Equation 3.4}\}\\
&= \max\left\{\sum_{j=1}^{m}|\text{Tr}(U_j^\dagger Q_{ij}(A))| \;\middle|\; \|A\|_1 = 1, U_j \in \mathbb{C}^{n\times n}\right\} && \{\text{Equation 3.1}\}\\
&= \max\left\{\sum_{j=1}^{m}|\text{Tr}(A^\dagger Q_{ij}^\dagger U_j)| \;\middle|\; \|A\|_1 = 1, U_j \in \mathbb{C}^{n\times n}\right\}\\
&= \max\left\{\left|\text{Tr}\left(A^\dagger\left(\sum_{j=1}^{m} Q_{ij}^\dagger U_j\right)\right)\right| \;\middle|\; \|A\|_1 = 1, U_j \in \mathbb{C}^{n\times n}\right\}\\
&= \max\left\{\left|\left\langle A, \sum_{j=1}^{m} Q_{ij}^\dagger U_j\right\rangle\right| \;\middle|\; \|A\|_1 = 1, U_j \in \mathbb{C}^{n\times n}\right\} && \{\text{Equation 3.1}\}
\end{aligned} \tag{4.72}$$

Consequently, one has that:

$$\begin{aligned}
&\max\left\{\left\|\sum_{j=1}^{m} Q_{ij}^{\dagger} U_j\right\|_{\infty} \middle| U_j \in \mathbb{C}^{n\times n}\right\} \\
&= \max\left\{\max\left\{\left|\left\langle A, \sum_{j=1}^{m} Q_{ij}^{\dagger} U_j\right\rangle\right| \middle| A \in \mathbb{C}^{n\times n}, \|A\|_1 = 1\right\}\right. && \{\text{Definition 3.1.31}\} \\
&\qquad \left.\middle| U \in \mathbb{C}^{n\times n}\right\} \\
&= \max\left\{\left|\left\langle A, \sum_{j=1}^{m} Q_{ij}^{\dagger} U_j\right\rangle\right| \middle| A \in \mathbb{C}^{n\times n}, \|A\|_1 = 1, U_j \in \mathbb{C}^{n\times n}\right\} && \{\text{Lemma 4.6.12}\} \\
&= \|Q_i\|_{1\text{ gen}} && \{\text{Equation 4.72}\}
\end{aligned} \tag{4.73}$$

The rest of the proof follows the same reasoning as in [12, Proof of Theorem 3.39]. Attending to [12, Equation 3.236, Equation 3.237 and Lemma 3.3], along with the observation that the eigenvalues of $U_1, \ldots, U_m$ all lie on the unit circle, it follows that:

$$\left\|\sum_{j=1}^{m} Q_{ij}^{\dagger} U_j\right\|_{\infty} \leq \left\|\sum_{j=1}^{m} Q_{ij}^{\dagger} I_{\mathbb{C}^{p_j \otimes p_j}}\right\|_{\infty} \tag{4.74}$$

Given that the identity matrix is unitary, one has:

$$\|Q_i\|_{1\text{ gen}} = \left\|\sum_{j=1}^{m} Q_{ij}^{\dagger} I_{\mathbb{C}^{p_j \otimes p_j}}\right\|_{\infty} \tag{4.75}$$

Attending to the fact that $\left\|\sum_{j=1}^{m} Q_{ij}^{\dagger} I_{\mathbb{C}^{p_j \otimes p_j}}\right\|_{\infty}$ is positive-semidefinite, it holds that:

$$\|Q_i\|_{1\text{ gen}} = \max\left\{\left\langle vv^{\dagger}, \sum_{j=1}^{m} Q_{ij}^{\dagger} I_{\mathbb{C}^{p_j \otimes p_j}}\right\rangle \middle| \|v\|_2 = 1\right\} = \max\{\mathrm{Tr}\left(Q_i(vv^{\dagger})\right) \mid \|v\|_2 = 1\} \tag{4.76}$$

□

Proposition 4.6.20. *Let* $Q : \mathbb{C}^{o_1\times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n\times o_n} \rightarrow \mathbb{C}^{p_1\times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m\times p_m}$ *be a positive trace-preserving super-operator. Then, it holds that* $\|Q\|_{1\,gen} = 1$.

Proof. Consider the decomposition $Q = [Q_1, \ldots, Q_n]$, where $Q_1, \ldots, Q_n$ are defined as in Definition 4.6.4. In this case attending to Definition 4.6.7, one has:

$$\|Q\|_{1\text{ gen}} = \max\{\max\{\|Q_1(A_1)\|_{1\text{ gen}} \mid \|A_1\|_1 = 1\}, \ldots, \{\max\{\|Q_n(A_n)\|_{1\text{ gen}} \mid \|A_n\|_1 = 1\}\}$$

(4.77)

Note that for all $1 \leq i \leq m$, if Q is positive trace-preserving, then Q_i is also positive trace-preserving, considering its definition in Definition 4.6.5, and given that the composition of positive trace-preserving super-operators is also positive trace-preserving.

É necessário provar esta afirmação?

Attending to Lemma 4.6.19, it holds that:

$$\|Q_i\|_{1\text{ gen}} = \max\{\mathsf{Tr}\left(Q_i(vv^\dagger)\right) \mid \|v\|_2 = 1\}, \tag{4.78}$$

where $v \in \mathbb{C}^{o_i}$ and $1 \leq i \leq n$.
If Q_i is trace-preserving, then considering Definition 3.2.6, one has:

$$\mathsf{Tr}(Q_i(vv^\dagger)) = \mathsf{Tr}(vv^\dagger) \tag{4.79}$$

As a result, considering the definition of trace-norm for square matrices, Definition 3.1.28, for $\|v\|_2 = 1$ it follows that $\|Q_i\|_{1\text{ gen}} = \mathsf{Tr}(vv^\dagger) = 1$ for all $1 \leq i \leq n$. Given that if all elements of a set verify a certain property, then the maximum of the set also verifies the property it follows that $\|Q\|_{1\text{ gen}} = 1$.

□

Corollary 4.6.21. *Let $Q : \mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n} \to \mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m \times p_m}$ be a* ***CPTP*** *super-operator. Then, it holds that $\|Q\|_{\diamond\text{ gen}} = 1$.*

Proof. Given that Q is a **CPTP** super-operator, if follows that $Q \otimes I_{\mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n}}$ is a positive trace-preserving super-operator. As a result, attending to Proposition 4.6.20, it holds that $\|Q \otimes I_{\mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n}}\|_{1\text{ gen}} = 1$. As a result, considering Definition 4.6.8, it follows that $\|Q\|_{\diamond\text{ gen}} = 1$. □

Corollary 4.6.22. *Let $Q : \mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n} \to \mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m \times p_m}$ and $S : \mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m \times p_m} \to \mathbb{C}^{q_1 \times q_1} \oplus \ldots \oplus \mathbb{C}^{q_t \times q_t}$ be super-operators. If Q is a* ***CPTP*** *super-operator, then $\|SQ\|_{\diamond\text{ gen}} \leq \|S\|_{\diamond\text{ gen}}$, and if S is a quantum channel, then $\|SQ\|_{\diamond\text{ gen}} \leq \|Q\|_{\diamond\text{ gen}}$*

Proof. This result is an immediate consequence of Proposition 4.6.18 and Corollary 4.6.21.

□

Proposition 4.6.23. *For all super-operators $Q_0, Q_1 : \mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n} \to \mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m \times p_m}$ and $P_0, P_1 : \mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m \times p_m} \to \mathbb{C}^{q_1 \times q_1} \oplus \ldots \oplus \mathbb{C}^{q_t \times q_t}$, it holds that:*

$$\|P_0Q_0 - P_1Q_1\|_{\diamond\text{ gen}} \leq \|Q_0 - Q_1\|_{1\text{gen}} + \|P_0 - P_1\|_{\diamond\text{ gen}} \tag{4.80}$$

Proof. The proof follows the same reasoning as in [12, Proof of Theorem 3.41], following from the triangle inequality, Proposition 4.6.18 and Corollary 4.6.21. □

Proposition 4.6.24. *For all $O \in \mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n}$ and $P \in \mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m \times p_m}$ it holds that:*

$$\|O \otimes P\|_{1\,gen} = \|O\|_{1\,gen} \|P\|_{1\,gen} \tag{4.81}$$

Proof. Consider the decompositions $O = (O_1, \ldots, O_n)$ and $P = (P_1, \ldots, P_t)$. Given that the trace norm of matrices is multiplicative with respect to tensor products and attending to Definition 4.6.2, it follows

$$\begin{aligned}\|O \otimes P\|_{1\text{ gen}} &= \|(O_1, \ldots, O_n) \otimes (P_1, \ldots, P_t)\|_{1\text{ gen}} \\ &= \|(O_1 \otimes P_1, \ldots, O_1 \otimes P_t, \ldots, O_n \otimes P_1, \ldots, O_n \otimes P_t)\|_{1\text{ gen}} \\ &= \sum_{i=1}^{n} \sum_{j=1}^{t} \|O_i \otimes P_j\|_1 = \sum_{i=1}^{n} \sum_{j=1}^{t} \|O_i\|_1 \|P_j\|_1 = \sum_{i=1}^{n} \|O_i\|_1 \sum_{j=1}^{t} \|P_j\|_1 \\ &= \|O\|_{1\text{ gen}} \|P\|_{1\text{ gen}}\end{aligned} \tag{4.82}$$

□

Proposition 4.6.25. *Let $Q : \mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n} \to \mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m \times p_m}$ be a super-operator, let $U_0, U_1 \in \mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n}$ and $U_2, U_3 \in \mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m \times p_m}$ be unitary operators, and let $S : Q : \mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n} \to \mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_m \times p_m}$ be defined as:*

$$S(A) = U_2 Q(U_0 A U_1) U_3 \tag{4.83}$$

for all $A \in \mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n}$. Then, it holds that $\|S\|_{1\,gen} = \|Q\|_{1\,gen}$

Proof. Considering the decompositions $Q = [Q_1, \ldots, Q_n]$, $S = [S_1, \ldots, S_n]$, with $Q_i = (Q_{i1}, \ldots, Q_{im})$ and $S_i = (S_{i1}, \ldots, S_{im})$, $U_0 = (U_{01}, \ldots, U_{0n})$, $U_1 = (U_{11}, \ldots, U_{1n})$, $U_2 = (U_{21}, \ldots, U_{2m})$,$U_3 = (U_{31}, \ldots, U_{3m})$, and $A = (A_1, \ldots, A_n)$ one has that:

$$\begin{aligned}S(A) &= U_2 \cdot (Q_1(U_{01} A_1 U_{11}),\ \ldots\ , Q_n(U_{0n} A_n U_{1n})) \cdot U_3 \\ &= \sum_{i=1}^{n} (U_{21} Q_{i1}(U_{0i} A_i U_{1i}) U_{31},\ \ldots\ , U_{2m} Q_{im}(U_{0i} A_i U_{1i}) U_{3m}) \\ &= \sum_{i=1}^{n} (S_{i1}(A),\ \ldots\ , S_{im}(A)) = \sum_{i=1}^{n} S_i(A)\end{aligned} \tag{4.84}$$

Given that U_0, U_1, U_2, U_3 are unitary operators, it follows that, $Qij = U_{2j}^\dagger S_{ij}(U_{0i}^\dagger A U_{1i}^\dagger) U_{3j}^\dagger$, and consequently:

$$Q(A) = \sum_{i=1}^{n} \left(U_{21}^\dagger S_{i1}(U_{0i}^\dagger A_i U_{1i}^\dagger) U_{31}^\dagger, \; \ldots \; , U_{2m}^\dagger S_{im}(U_{0i}^\dagger A_i U_{1i}^\dagger) U_{3m}^\dagger \right) = \sum_{i=1}^{n} Q_i(A) \tag{4.85}$$

Applying the same reasoning as in [12, Proof of Proposition 3.41], considering Definition 4.6.1 , by the unitary invariance of the trace norm, Lemma 4.6.14 and Definition 4.6.7, it follows that for $1 \leq i \leq n$:

$$\begin{aligned} \|S_i(A_i)\|_{1\text{ gen}} &= \sum_{j=1}^{m} \|U_{2j} Q_{i1}(U_{0i} A_i U_{1i}) U_{3j}\|_1 = \sum_{j=1}^{m} \|Q_{ij}(U_{0i} A_i U_{1i})\|_1 = \|Q_i(U_{0i} A_i U_{1i})\|_{1\text{ gen}} \\ &\leq \|Q_i\|_{1\text{ gen}} \|A_i\|_1 \leq \|Q\|_{1\text{ gen}} \|A_i\|_1 \end{aligned} \tag{4.86}$$

As a result, given Definition 4.6.4 it follows that $\|S_i\|_{1\text{ gen}} \leq \|Q\|_{1\text{ gen}}$ for all $1 \leq i \leq n$. Thus, attending to Definition 4.6.7, it holds that,

$$\|Q\|_{1\text{ gen}} \geq \max\{\|S_1\|_{1\text{ gen}}, \ldots, \|S_n\|_{1\text{ gen}}\} = \|S\|_{1\text{ gen}} \tag{4.87}$$

Considering Equation 4.85 the same approach can be taken to find that $\|S\|_{1\text{ gen}} \leq \|Q\|_{1\text{ gen}}$, which concludes the proof. ☐

Theorem 4.6.26. *For all* $Q : \mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n} \to \mathbb{C}^{q_1 \times q_1} \oplus \ldots \oplus \mathbb{C}^{q_m \times q_m}$ *and* $S : \mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_t \times p_t} \to \mathbb{C}^{r_1 \times r_1} \oplus \ldots \oplus \mathbb{C}^{r_s \times r_s}$*, it holds that:*

$$\|Q \otimes S\|_{\diamond\text{ gen}} = \|Q\|_{\diamond\text{ gen}} \|S\|_{\diamond\text{ gen}} \tag{4.88}$$

Proof. This prove follows the same reasoning as [12, Proof of Theorem 3.49]. By Proposition 4.6.18 and Corollary 4.6.16, one has:

$$\begin{aligned} \|Q \otimes S\|_{\diamond\text{ gen}} &= \|(Q \otimes I_{\mathbb{C}^{r_1 \times r_1} \oplus \ldots \oplus \mathbb{C}^{r_s \times r_s}})(I_{\mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n}} \otimes S)\|_{\diamond\text{ gen}} \\ &\leq \|Q \otimes I_{\mathbb{C}^{r_1 \times r_1} \oplus \ldots \oplus \mathbb{C}^{r_s \times r_s}}\|_{\diamond\text{ gen}} \|I_{\mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n}} \otimes S\|_{\diamond\text{ gen}} \\ &= \|Q\|_{\diamond\text{ gen}} \|S\|_{\diamond\text{ gen}} \end{aligned} \tag{4.89}$$

Consider operators $O \in (\mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n}) \otimes (\mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n})$ and $P \in (\mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_t \times p_t}) \otimes (\mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_t \times p_t})$ such that $\|O\|_{1\text{ gen}} = 1$ and $\|P\|_{1\text{ gen}} = 1$, and such that these equalities hold:

$$\begin{aligned} \|Q\|_{\diamond\text{ gen}} &= \|Q \otimes I_{\mathbb{C}^{o_1 \times o_1} \oplus \ldots \oplus \mathbb{C}^{o_n \times o_n}}(O)\|_{1\text{ gen}} \\ \|S\|_{\diamond\text{ gen}} &= \|S \otimes I_{\mathbb{C}^{p_1 \times p_1} \oplus \ldots \oplus \mathbb{C}^{p_t \times p_t}}(P)\|_{1\text{ gen}} \end{aligned} \tag{4.90}$$

Attending do Proposition 4.6.24, it follows that:

$$\|O \otimes P\|_{1\text{ gen}} = \|O\|_{1\text{ gen}}\|P\|_{1\text{ gen}} = 1 \tag{4.91}$$

Attending to Definition 4.6.8 and Proposition 4.6.25, which implies that this norm is invariant under permuting the ordering of tensor factors of super-operadores, one has

$$\begin{aligned}\|Q \otimes S\|_{\diamond\text{ gen}} &= \left\|Q \otimes S \otimes I_{(\mathbb{C}^{o_1\times o_1}\oplus\ldots\oplus\mathbb{C}^{o_n\times o_n})\otimes(\mathbb{C}^{p_1\times p_1}\oplus\ldots\oplus\mathbb{C}^{p_t\times p_t})}\right\|_{1\text{gen}} \\ &= \|Q \otimes S \otimes I_{\mathbb{C}^{o_1\times o_1}\oplus\ldots\oplus\mathbb{C}^{o_n\times o_n}} \otimes I_{\mathbb{C}^{p_1\times p_1}\oplus\ldots\oplus\mathbb{C}^{p_t\times p_t}}\|_{1\text{gen}} \\ &= \|Q \otimes I_{\mathbb{C}^{o_1\times o_1}\oplus\ldots\oplus\mathbb{C}^{o_n\times o_n}} \otimes S \otimes I_{\mathbb{C}^{p_1\times p_1}\oplus\ldots\oplus\mathbb{C}^{p_t\times p_t}}\|_{1\text{gen}}\end{aligned} \tag{4.92}$$

Attending to Lemma 4.6.14 and Equation 4.91, one has that:

$$\begin{aligned}&\|Q \otimes I_{\mathbb{C}^{o_1\times o_1}\oplus\ldots\oplus\mathbb{C}^{o_n\times o_n}} \otimes S \otimes I_{\mathbb{C}^{p_1\times p_1}\oplus\ldots\oplus\mathbb{C}^{p_t\times p_t}}\|_{1\text{ gen}} \\ \geq\ &\|Q \otimes I_{\mathbb{C}^{o_1\times o_1}\oplus\ldots\oplus\mathbb{C}^{o_n\times o_n}} \otimes S \otimes I_{\mathbb{C}^{p_1\times p_1}\oplus\ldots\oplus\mathbb{C}^{p_t\times p_t}}(O \otimes P)\|_{1\text{gen}}\end{aligned} \tag{4.93}$$

Considering Equation 4.92, this can be rewritten as:

$$\|Q \otimes S\|_{\diamond\text{ gen}} \geq \|Q \otimes I_{\mathbb{C}^{o_1\times o_1}\oplus\ldots\oplus\mathbb{C}^{o_n\times o_n}} \otimes S \otimes I_{\mathbb{C}^{p_1\times p_1}\oplus\ldots\oplus\mathbb{C}^{p_t\times p_t}}(O \otimes P)\|_{1\text{gen}} \tag{4.94}$$

By Proposition 4.6.24 and Equation 4.90, it holds that:

$$\begin{aligned}\|Q \otimes S\|_{\diamond\text{ gen}} &\geq \|Q \otimes I_{\mathbb{C}^{o_1\times o_1}\oplus\ldots\oplus\mathbb{C}^{o_n\times o_n}} \otimes S \otimes I_{\mathbb{C}^{p_1\times p_1}\oplus\ldots\oplus\mathbb{C}^{p_t\times p_t}}(O \otimes P)\|_{1\text{gen}} \\ &= \|Q \otimes I_{\mathbb{C}^{o_1\times o_1}\oplus\ldots\oplus\mathbb{C}^{o_n\times o_n}}(O)\|_{1\text{ gen}}\|P \otimes I_{\mathbb{C}^{o_1\times o_1}\oplus\ldots\oplus\mathbb{C}^{o_n\times o_n}}(O)\|_{1\text{ gen}} \\ &= \|Q\|_{\diamond\text{ gen}}\|S\|_{\diamond\text{ gen}}\end{aligned} \tag{4.95}$$

which completes the proof. □

Now, with respect to the metric equations in Figure 12, considering the interpretation of the booleans defined in Figure 11, demonstrating the soundness of the metric equations for the booleans is equivalent to proving the theorem below. It should be noted that in the quantum paradigm, the distance between two super-operators Q and Q' corresponds to the generalized diamond norm between Q and Q'.

Theorem 4.6.27. *For any non-negative rational q and super-operators Q and Q' such that $d(Q, Q') \leq q$ the following holds:*

$$d(\mathsf{IL}(Q), \mathsf{IL}(Q')) \leq q \tag{4.96}$$

$$d(\mathsf{IR}(Q), \mathsf{IR}(Q')) \leq q \tag{4.97}$$

Proof. Considering Definition 4.6.1, it holds that:

$$\|\mathsf{IL}(Q) - \mathsf{IL}(Q')\|_{\diamond\,\text{gen}} = \|(Q - Q', 0)\|_{\diamond\,\text{gen}} = \|Q - Q'\|_{\diamond\,\text{gen}} = d(Q, Q') \leq q \tag{4.98}$$

Applying the same reasoning to $\|\mathsf{IR}(Q) - \mathsf{IR}(Q')\|_{\diamond\,\text{gen}}$, it follows that Equation 4.97 holds. ☐

Regarding the metric equation for the case statement, considering its interpretation in Figure 11 its soundness follows from the following theorem.

Theorem 4.6.28. *For any non-negative rationals q, r e s and super-operators $Q, Q', S_0, S_0', S_1, S_1'$ such that $d(Q, Q') \leq q$, $d(S_0, S_0') \leq r$, and $d(S_1, S_1') \leq r$, it holds that:*

$$d([S_0, S_1] \cdot Q, [S_0', S_1'] \cdot Q') \leq q + \max\{r, s\} \tag{4.99}$$

Proof. Considering Definition 4.6.3, it holds that:

$$\begin{aligned} d([S_0, S_1], [S_0', S_1']) &= \|[S_0, S_1] - [S_0', S_1']\|_{\diamond\,\text{gen}} = \|[S_0 - S_0', S_1 - S_1']\|_{\diamond\,\text{gen}} \\ &= \max\{\|S_0 - S_0'\|_{\diamond\,\text{gen}}, \|S_1 - S_1'\|_{\diamond\,\text{gen}}\} = \max\{d(S_0, S_0'), d(S_1, S_1')\} = \max\{r, s\} \end{aligned} \tag{4.100}$$

Given Proposition 4.6.23, it follows that:

$$\begin{aligned} &d([S_0, S_1] \cdot Q, [S_0', S_1'] \cdot Q) = \|[S_0, S_1] \cdot Q - [S_0', S_1'] \cdot Q'\|_{\diamond\,\text{gen}} \\ &\leq \|Q - Q'\|_{\diamond\,\text{gen}} + \|[S_0, S_1] - [S_0', S_1']\|_{\diamond\,\text{gen}} \leq d(Q, Q') + d([S_0, S_1], [S_0', S_1']) \leq q + \max\{r, s\} \end{aligned} \tag{4.101}$$

☐

4.7 Ilustration: Quantum Teleportation

[52] introduced the concept of quantum teleportation, which is a protocol that allows the transfer of unknown quantum states between distant parties. The quantum teleportation protocol is a fundamental building block for quantum communication, quantum computation, and quantum networks, its applications ranging from secure quantum communication to distributed quantum computing [53–55].

Conceptually the protocol can be described as follows: Alice and Bob share an entangled pair of qubits, which are in a Bell state. Alice keeps the first qubit and Bob the second. Moreover, Alice has a qubit in an unknown state $|\psi\rangle$ that she wants to send to Bob. Alice entangles her qubit and the firt qubit of the Bell state, and then measures them. The result of this measurement is two classical bits that Alice sends to Bob though a classical channel. Based on the measurement results, Bob applies a correction to his qubit so it matches the initial state $|\psi\rangle$. The circuit corresponding to the implementation of the quantum teleportation protocol is depicted in Figure 13.

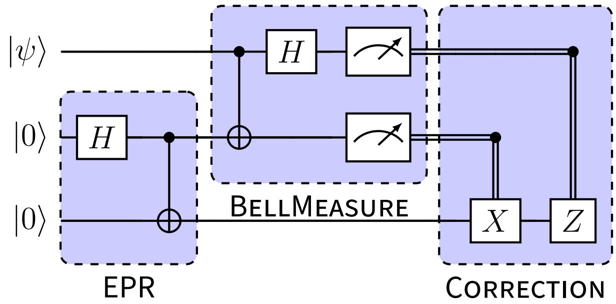


Figure 13: Quantum Teleportation Protocol

When formalizing the quantum teleportation protocol within the lambda calculus framework, each part of the protocol is instantiated as a distinct function. This entails the definition of three specific programs:

$$\begin{aligned}
&\textbf{EPR}: \ \mathbb{I} \multimap (\textit{qbit} \otimes \textit{qbit}) \\
&\textbf{BellMeasure}: \ \textit{qbit} \otimes \textit{qbit} \multimap \textit{bit} \otimes \textit{bit} \\
&\textbf{Correction}: \ \textit{qbit} \otimes \textit{bit} \otimes \textit{bit} \multimap \textit{qbit}
\end{aligned}$$

Considering the unitary operations $H : \textit{qbit} \rightarrow \textit{qbit}$, $X : \textit{qbit} \rightarrow \textit{qbit}$, $Z : \textit{qbit} \rightarrow \textit{qbit}$, $I : \textit{qbit} \rightarrow \textit{qbit}$, and $\textit{CNOT} : \textit{qbit}, \textit{qbit} \rightarrow \textit{qbit} \otimes \textit{qbit}$, these functions are defined as follows:

$$\begin{aligned}
&\textbf{EPR} = - \triangleright \textit{CNOT}\,(H\,(q\,(\textit{new}\,0\,(*))), (q\,(\textit{new}\,0\,(*)))) \\
&\textbf{BellMeasure} = q_1 : \textit{qbit}, q_2 : \textit{qbit} \triangleright (\text{pm}\ \ \textit{CNOT}(q_1, q_2)\ \text{to}\ x \otimes y.\, \textit{meas}(H(x)) \otimes \textit{meas}(y)) \\
&\textbf{Correction} = q : \textit{qbit}, x : \text{bit}, y : \text{bit} \triangleright\ \text{case}\ x\,\{\text{inl}(x_0) \Rightarrow (\text{cond}\,y\,\{\text{inl}(y_0) \Rightarrow I(q); \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \text{inr}(y_1) \Rightarrow X(q))\}; \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \text{inr}(x_1) \Rightarrow (\text{cond}\,y\,\{\text{inl}(y_0) \Rightarrow Z(q); \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \text{inr}(y_1) \Rightarrow Z(X(q))\})\}
\end{aligned}$$

Designating the qubit to be teleported as q_0, one can conceptualize the teleportation procedure as follows:

$$q_0 : qbit \triangleright \mathsf{pm}\ \textbf{EPR}(*)\ \mathsf{to}\ q_1 \otimes q_2.$$
$$\mathsf{pm}\ \textbf{BellMeasure}(q_0, q_1)\ \mathsf{to}\ c_0 \otimes c_1.$$
$$\mathsf{pm}\ \textbf{Correction}(q_2, c_0, c_1)\ \mathsf{to}\ q.\, q$$

Regarding the interpretation of the quantum teleportation protocol, considering $\rho = |\phi\rangle\langle\phi|$ as the state of the system before measurement, $|\phi\rangle$ is calculated as follows, where $|\psi\rangle$ is the state of the qubit to be teleported:

$$\begin{aligned}
& |\psi\rangle \otimes |0\rangle \otimes |0\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle \otimes |0\rangle \\
\xmapsto{I\otimes H \otimes I}\quad & (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\
\xmapsto{I\otimes CNOT}\quad & (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle) \\
\xmapsto{CNOT\otimes I}\quad & \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle) \\
\xmapsto{H\otimes I \otimes I}\quad & \frac{1}{2}(\alpha|000\rangle + \alpha|001\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|110\rangle + \beta|101\rangle - \beta|001\rangle) \\
= \quad & \frac{1}{2}(|00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) + |01\rangle \otimes (\alpha|1\rangle + \beta|0\rangle) + |10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) \\
& + |11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle)) \\
= \quad & |00\rangle \otimes |\psi\rangle + |01\rangle \otimes X|\psi\rangle + |10\rangle \otimes Z|\psi\rangle + |11\rangle \otimes XZ|\psi\rangle = |\phi\rangle
\end{aligned} \tag{4.102}$$

Regarding the remaining steps of the protocol,

$$\begin{aligned}
|\phi\rangle\langle\phi| = \quad & \frac{1}{4}(|00\rangle\langle 00| \otimes |\psi\rangle\langle\psi| + |00\rangle\langle 01| \otimes |\psi\rangle\langle\psi|X + |00\rangle\langle 10| \otimes |\psi\rangle\langle\psi|Z \\
& + |00\rangle\langle 11| \otimes |\psi\rangle\langle\psi|ZX + X|01\rangle\langle 00| \otimes |\psi\rangle\langle\psi| + |01\rangle\langle 01| \otimes X|\psi\rangle\langle\psi|X \\
& + |01\rangle\langle 10| \otimes X|\psi\rangle\langle\psi|Z + |01\rangle\langle 11| \otimes X|\psi\rangle\langle\psi|ZX + |10\rangle\langle 00| \otimes Z|\psi\rangle\langle\psi| \\
& + |10\rangle\langle 01| \otimes Z|\psi\rangle\langle\psi|X + |10\rangle\langle 10| \otimes Z|\psi\rangle\langle\psi|Z + |10\rangle\langle 11| \otimes Z|\psi\rangle\langle\psi|ZX \\
& + |00\rangle\langle 11| \otimes |\psi\rangle\langle\psi|ZX + |01\rangle\langle 11| \otimes X|\psi\rangle\langle\psi|ZX + |10\rangle\langle 11| \otimes Z|\psi\rangle\langle\psi|ZX \\
& + |11\rangle\langle 11| \otimes ZX|\psi\rangle\langle\psi|ZX) \\
\xmapsto{\mathsf{meas}\otimes\mathsf{meas}\otimes I}\quad & \Big(\Big(\frac{1}{4}|\psi\rangle\langle\psi|, \frac{1}{4}X|\psi\rangle\langle\psi|X\Big), \Big(\frac{1}{4}Z|\psi\rangle\langle\psi|Z, \frac{1}{4}XZ|\psi\rangle\langle\psi|ZX\Big)\Big)
\end{aligned} \tag{4.103}$$

With respect to the final step of the protocol, attending to the interpretation of the conditional statement (Figure 11), the state of the system after the application of the correction function is given by:

$$
\begin{aligned}
&\frac{1}{4}|\psi\rangle\langle\psi| + \frac{1}{4}XX|\psi\rangle\langle\psi|XX + \frac{1}{4}ZZ|\psi\rangle\langle\psi|ZZ + \frac{1}{4}ZXXZ|\psi\rangle\langle\psi|ZXXZ \\
=&\frac{1}{4}\left(|\psi\rangle\langle\psi| + |\psi\rangle\langle\psi| + |\psi\rangle\langle\psi| + |\psi\rangle\langle\psi|\right) = |\psi\rangle\langle\psi|
\end{aligned} \tag{4.104}
$$

4.8 Ilustration: Noisy Quantum Teleportation

4.8.1 Noisy Quantum Teleportation: Decoherence

Realistic quantum systems are never isolated, but are immersed in the surrounding environment and interact continuously with it [56]. Decoherence can be seen as the consequence of that 'openness' of quantum systems to their environments . To study decoherence in a quantum channel within the presented metric deductive system, one can consider the application of a dephasing channel in the quantum teleportation protocol with a certain probability p.

The Kraus operators of the dephasing channel with probability p are expressed as:

$$D_0 = \frac{\sqrt{2-p}}{\sqrt{2}} I, D_1 = \frac{\sqrt{p}}{\sqrt{2}} Z \tag{4.105}$$

Considering a density operator $\rho = |\alpha|^2|0\rangle\langle 0| + \alpha\beta^\dagger|0\rangle\langle 1| + \alpha^\dagger\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|$, using these Kraus operators, it is possible to easily verify that after applying the dephasing channel with probability p, the resulting operator ρ' is given by:

$$\rho' = A_0\rho A_0^\dagger + A_1\rho A_1^\dagger = |\alpha|^2|0\rangle\langle 0| + (1-p)\alpha\beta^\dagger|0\rangle\langle 1| + (1-p)\alpha^\dagger\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1| \tag{4.106}$$

This shows that the dephasing channel with probability p preserves the diagonal elements of the density matrix while attenuating the off-diagonal elements by a factor of $(1-p)$.

The circuit representing the introduction of decoherence after EPR is illustrated in Figure 14.

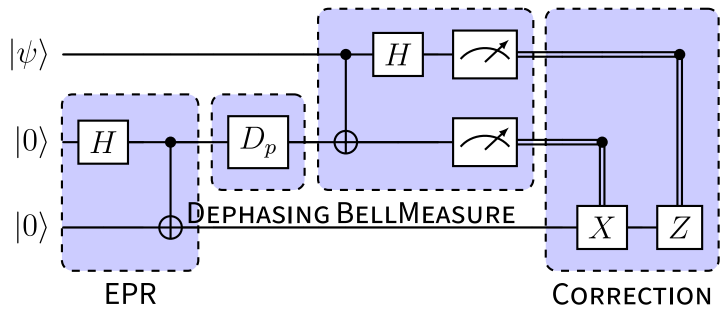


Figure 14: Quantum Teleportation Protocol: Dephasing with probability p after EPR pair creation.

In this case, to facilate the analysis, the quantum teleportion protocol is devided in four parts: EPR, BellMeasure, Identity and Correction. This entails the definition of an aditional function and respective version subjected to decoherence with probability p:

$$\textbf{Identity} : \textit{qbit} \multimap \textit{qbit}$$
$$\textbf{Identity}^p : \textit{qbit} \multimap \textit{qbit}$$

Considering the unitary operation I : *qbit* $\rightarrow$ *qbit*, and the operation D_p : *qbit* $\rightarrow$ *qbit* the ideal version of this function, **Identity**, and its respective version subjected to decoherence with probability p, **Identity**^{p}, are defined as follows:

$$\textbf{Identity} = q : \textit{qbit} \triangleright I(q) : \textit{qbit} \tag{4.107}$$
$$\textbf{Identity}^p = q : \textit{qbit} \triangleright D_p(q) : \textit{qbit} \tag{4.108}$$

Designating the qubit to be teleported as q_0, one can conceptualize the teleportation procedure as follows:

$$\begin{aligned}
&\text{pm } \textbf{EPR}(*) \text{ to } q_1 \otimes q_2. \\
&\text{pm } \textbf{Identity}(q_1) \text{ to } id_q_1. \\
&\text{pm } \textbf{BellMeasure}(q_0, id_q_1) \text{ to } c_0 \otimes c_1. \\
&\text{pm } \textbf{Correction}(q_2, c_0, c_1) \text{ to } q.\, q
\end{aligned}$$

To evaluate the disparity between the ideal implementation of the quantum teleportation protocol and its realization subjected to decoherence, the initial step involves computing the distance between the density operators of the ideal and noisy implementations of the EPR state, denoted as ρ and ρ', respectively.

$$\begin{aligned}
&|0\rangle\langle 0| \otimes |0\rangle\langle 0| \\
\xmapsto{\text{EPR}}\ &\frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|) = \rho \\
\xmapsto{D(p)\otimes I}\ &\frac{1}{2}(|00\rangle\langle 00| + (1-p)\,|00\rangle\langle 11| + (1-p)|11\rangle\langle 00| + |11\rangle\langle 11|) = \rho'
\end{aligned} \tag{4.109}$$

The distance between the r-image of the mapping $1 \mapsto \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$ and the mapping $1 \mapsto \frac{1}{2}(|00\rangle\langle 00| + (1-p)\,|00\rangle\langle 11| + (1-p)|11\rangle\langle 00| + |11\rangle\langle 11|)$ is given by: $f(p) = \|\frac{p}{2}(|00\rangle\langle 11| + |11\rangle\langle 00|)\|_1$. Therefore, attending to Equation 3.12, $\|\rho -$

$\rho'(p)\|_\diamond = f(p)$.

$$
\begin{aligned}
f(p) &= \left\| \frac{p}{2} \left(|00\rangle\langle 11| + |11\rangle\langle 00| \right) \right\|_1 \\
&= \mathrm{Tr}\left(\sqrt{\frac{p^2}{4}(|00\rangle\langle 11| + |11\rangle\langle 00|)(|00\rangle\langle 11| + |11\rangle\langle 00|)^\dagger} \right) && \{\|\|_1 \text{ defn. for matrices}\} \\
&= \mathrm{Tr}\left(\sqrt{\frac{p^2}{4}(|00\rangle\langle 00| + |11\rangle\langle 11|)} \right) \\
&= \mathrm{Tr}\left(\frac{p}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|) \right) && \{\text{Equation 3.2}\} \\
&= \frac{p}{2} + \frac{p}{2} = p
\end{aligned}
\tag{4.110}
$$

Therefore, the distance between the ideal and noisy implementations of the EPR state is given by $\|\rho - \rho'(p)\|_\diamond = p$.

Next, via the metric deductive system in Figure 3, it is easily verified that for an error p,

$$
q : \textit{qbit} \triangleright I(q) =_p q : \textit{qbit} \triangleright D_p(q) : \textit{qbit} \tag{4.111}
$$

Therefore **Identity** $=_p$ **Identity**^{p} and finally, considering the entirety of the quantum teleportation protocol denoted as **QTP**, it follows that **QTP** $=_p$ **QTP**^{p}. This final metric equation indicates that by bounding the error associated with the application of decoherence with a specified probability p to the initial qubit before measurement, it becomes feasible to limit the overall error of the entire quantum teleportation protocol. Moreover, it is interesting to observe that the error associated with the application of decoherence with a certain probability p in one of the qubits corresponds exactly to that probability p.

4.8.2 Noisy Quantum Teleportation: Amplitude Damping

Next, the amplitude-damping channel is considered as a source of noise in the quantum teleportation protocol. Similarly to the dephasing channel, the amplitude damping channel serves as a model illustrating the dissipation of energy between a qubit and its environment. An example of this type of noise is found in the spontaneous emission of a photon by a two-level atom into an electromagnetic field environment with either a finite or infinite number of modes at zero temperature [57, 58].

The amplitude damping channel with probability γ is described by the Kraus operators:

$$
A_0 = |0\rangle\langle 0| + \sqrt{1-\gamma}\,|1\rangle\langle 1|\,, A_1 = \sqrt{\gamma}\,|0\rangle\langle 1| \tag{4.112}
$$

Applying these Kraus operators to the density operator $\rho = |\alpha|^2|0\rangle\langle 0| + \alpha\beta^\dagger|0\rangle\langle 1| + \alpha^\dagger\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|$, the the resulting operator ρ' is given by:

$$\begin{aligned}\rho' &= A_0\rho A_0^\dagger + A_1\rho A_1^\dagger \\ &= (|\alpha|^2 + \gamma|\beta|^2)\,|0\rangle\langle 0| + \sqrt{1-\gamma}\,\alpha\beta^\dagger\,|0\rangle\langle 1| + \sqrt{1-\gamma}\,\alpha^\dagger\beta\,|1\rangle\langle 0| + (1-\gamma)|\beta|^2\,|1\rangle\langle 1|\end{aligned} \tag{4.113}$$

It is possible to observe that as γ increases, while the $|1\rangle\langle 1|$ component, alongside the non-diagonal elements, are attenuated, the $|0\rangle\langle 0|$ element is amplified.

The circuit representing the introduction of amplitude damping after the correction step is presented in Figure 15.

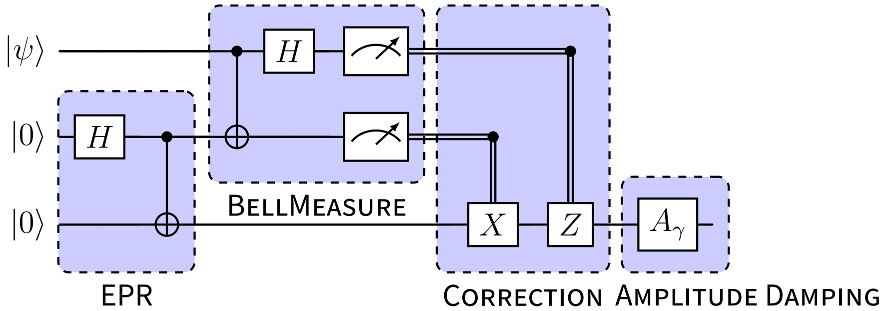


Figure 15: Quantum Teleportation Protocol: Amplitude Dampling with probability γ after Correction.

Once again, a fourth part of the teleportation protocol, the **Identity**, is considered to facilitate the error analysis. In this case, it is neccessay to define the erroneous version of **Identity**, **Identity**$^{A(\gamma)}$:

$$\textbf{Identity}^{A(\gamma)} : \textit{qbit} \multimap \textit{qbit} \tag{4.114}$$

Considering the operation $A_\gamma : \textit{qbit} \rightarrow \textit{qbit}$ the respective version of **Identity** subjected to amplitude damping with probability γ, **Identity**$^{A(\gamma)}$, is defined as follows:

$$\textbf{Identity}^{A(\gamma)} = q : \textit{qbit} \triangleright A_\gamma(q) : \textit{qbit} \tag{4.115}$$

Designating the qubit to be teleported as q_0, one can conceptualize the teleportation procedure as follows:

pm **EPR**$(*)$ to $q_1 \otimes q_2$.

pm **BellMeasure**(q_0, q_1) to $c_0 \otimes c_1$.

pm **Correction**(q_2, c_0, c_1) to q. **Identity**(q)

The first step to evaluate the distance between the ideal quantum teleportation protocol and the one subjected to amplitude damping with probability γ is to compute the distance between the density operators of the ideal and noisy implementations of the teleported qubit, denoted as ρ and ρ', respectively.

As shown in Equation 4.104, the state of the teleported qubit is $\rho = |\psi\rangle\langle\psi|$. Given Equation 4.113, the state of the teleported qubit after amplitude damping with probability γ is $(|\alpha|^2 + \gamma|\beta|^2)|0\rangle\langle 0| + \sqrt{1-\gamma}\alpha\beta^\dagger|0\rangle\langle 1| + \sqrt{1-\gamma}\alpha^\dagger\beta|1\rangle\langle 0| + (1-\gamma)|\beta|^2|1\rangle\langle 1|$, which is denoted as ρ'.

As a result,

$$\begin{aligned}\rho - \rho' =& |\alpha|^2|0\rangle\langle 0| + \alpha\beta^\dagger|0\rangle\langle 1| + \alpha^\dagger\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1| - \big((|\alpha|^2 + \gamma|\beta|^2)|0\rangle\langle 0| \\ &+ \sqrt{1-\gamma}\alpha\beta^\dagger|0\rangle\langle 1| + \sqrt{1-\gamma}\alpha^\dagger\beta|1\rangle\langle 0| + (1-\gamma)|\beta|^2|1\rangle\langle 1|\big) \\ =& \gamma|\beta|^2|0\rangle\langle 0| + (1-\sqrt{1-\gamma})(\alpha\beta^\dagger|0\rangle\langle 1| + \alpha^\dagger\beta|1\rangle\langle 0|) - \gamma|\beta|^2|1\rangle\langle 1|\end{aligned} \tag{4.116}$$

Employing Equation 3.9, the components of the Bloch vector of the state $\rho - \rho'$ are as follows:

$$\begin{aligned}
r_x =& \mathrm{Tr}\left[\begin{pmatrix}\gamma|\beta|^2 & (1-\sqrt{1-\gamma})\alpha\beta^\dagger \\ (1-\sqrt{1-\gamma})\alpha^\dagger\beta & -\gamma|\beta|^2\end{pmatrix}\cdot\begin{pmatrix}0 & 1 \\ 1 & 0\end{pmatrix}\right] \\
=& \mathrm{Tr}\left[\begin{pmatrix}(1-\sqrt{1-\gamma})\alpha\beta^\dagger & \gamma|\beta|^2 \\ -\gamma|\beta|^2 & (1-\sqrt{1-\gamma})\alpha^\dagger\beta\end{pmatrix}\right] = (1-\sqrt{1-\gamma})(\alpha\beta^\dagger + \alpha^\dagger\beta) \\
\\
r_y =& \mathrm{Tr}\left[\begin{pmatrix}\gamma|\beta|^2 & (1-\sqrt{1-\gamma})\alpha\beta^\dagger \\ (1-\sqrt{1-\gamma})\alpha^\dagger\beta & -\gamma|\beta|^2\end{pmatrix}\cdot\begin{pmatrix}0 & -i \\ i & 0\end{pmatrix}\right] \\
=& \mathrm{Tr}\left[\begin{pmatrix}i(1-\sqrt{1-\gamma})\alpha\beta^\dagger & -i\gamma|\beta|^2 \\ i\gamma|\beta|^2 & -i(1-\sqrt{1-\gamma})\alpha^\dagger\beta\end{pmatrix}\right] = i(1-\sqrt{1-\gamma})(\alpha\beta^\dagger - \alpha^\dagger\beta) \\
\\
r_z =& \mathrm{Tr}\left[\begin{pmatrix}\gamma|\beta|^2 & (1-\sqrt{1-\gamma})\alpha\beta^\dagger \\ (1-\sqrt{1-\gamma})\alpha^\dagger\beta & -\gamma|\beta|^2\end{pmatrix}\cdot\begin{pmatrix}1 & 0 \\ 0 & -1\end{pmatrix}\right] \\
=& \mathrm{Tr}\left[\begin{pmatrix}\gamma|\beta|^2 & -(1-\sqrt{1-\gamma})\alpha\beta^\dagger \\ (1-\sqrt{1-\gamma})\alpha^\dagger\beta & \gamma|\beta|^2\end{pmatrix}\right] = \gamma|\beta|^2 + \gamma|\beta|^2 = 2\gamma|\beta|^2
\end{aligned} \tag{4.117}$$

Consequently, and knowing that the distance between two vectors corresponds to their Euclidean distance, it follows that the distance between the ideal and noisy implementations of the teleported qubit corresponds to:

$$
\begin{aligned}
&\|\rho - \rho'\|_\diamond \\
&= \left\| \left((1-\sqrt{1-\gamma})(\alpha\beta^\dagger + \alpha^\dagger\beta), i(1-\sqrt{1-\gamma})(\alpha\beta^\dagger - \alpha^\dagger\beta), 2\gamma|\beta|^2 \right) \right\|_2 && \{\text{Equation 4.117}\} \\
&= \sqrt{\left((1-\sqrt{1-\gamma})(\alpha\beta^\dagger + \alpha^\dagger\beta)\right)^2 + \left(i(1-\sqrt{1-\gamma})(\alpha\beta^\dagger - \alpha^\dagger\beta)\right)^2 + (2\gamma|\beta|^2)^2} && \{\text{Definition 3.1.27}\} \\
&= \sqrt{\left((1-\sqrt{1-\gamma})(\alpha\beta^\dagger + \alpha^\dagger\beta)\right)^2 - \left((1-\sqrt{1-\gamma})(\alpha\beta^\dagger - \alpha^\dagger\beta)\right)^2 + (2\gamma|\beta|^2)^2} \\
&= \sqrt{4\cdot(1-\sqrt{1-\gamma})^2|\alpha|^2|\beta|^2 + 4\gamma^2|\beta|^4} \\
&= 2\cdot\sqrt{(1-\sqrt{1-\gamma})^2|\alpha|^2|\beta|^2 + \gamma^2|\beta|^4}
\end{aligned}
\tag{4.118}
$$

Note that, as expected when $\gamma \to 0$ or $\beta \to 0$,$\|\rho - \rho'\|_\diamond \to 0$, and when $\gamma \to 1$, $\|\rho - \rho'\|_\diamond \to 2\left(\sqrt{|\alpha|^2|\beta|^2 + \gamma^2|\beta|^4}\right)$.

From this result, it follows that **Identity** $=_{2\cdot\sqrt{(1-\sqrt{1-\gamma})^2|\alpha|^2|\beta|^2+\gamma^2|\beta|^4}}$ **Identity**$^{A(\gamma)}$. Thus, **QTP** $=_{2\cdot\sqrt{(1-\sqrt{1-\gamma})^2|\alpha|^2|\beta|^2+\gamma^2|\beta|^4}}$ **QTP**$^{A(\gamma)}$.

4.8.3 Noisy Quantum Teleportation: An imperfect implementation of the Hadamard gate

Now, it will be considered an imperfect implementation of a Hadamard gate, denoted as H^ϵ. Therefore, a new operation is added H^ϵ : *qbit* $\to$ *qbit* and it is postulated as an axiom that q : *qbit* $\triangleright H =_\epsilon H^\epsilon$: *qbit*. In this example, considering the Hadamard gate as the composition $R_y(\frac{\pi}{2}) \cdot P(\pi)$, H^ϵ is regarded as the composition $R_y(\frac{\pi}{2}) \cdot P(\pi + \delta)$. This imperfect implementation deviates from a precise rotation of π radians along the z-axis, rotating by $\pi + \delta$ radians instead. This type of imperfection is inevitable during the implementation of quantum gates. The circuit representing the introduction of an erroneous Hadamard gate is presented in Figure 16.

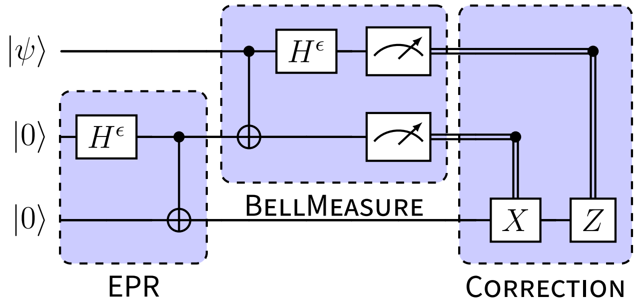


Figure 16: Quantum Teleportation Protocol: Erroneous implementation of the Hadamard gate. H^ϵ is regarded as the composition $R_y(\frac{\pi}{2}) \cdot P(\pi + \epsilon)$.

As usual, the initial step consists of evaluating the distance between the density operators of the ideal and noisy implementations of the Hadamard gate within each block. With respect to the EPR block, as presented in Equation 4.102 the ideal state of the EPR pair is $\frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$. Regarding, the imperfect Hadamard gate one has that:

$$\begin{aligned}
&|0\rangle \otimes |0\rangle \\
\xmapsto{H^\epsilon \otimes I} \quad & R_y\left(\frac{\pi}{2}\right) \cdot P(\pi + \epsilon)\,|0\rangle \otimes |0\rangle = R_y\left(\frac{\pi}{2}\right)|0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\
\xmapsto{CNOT} \quad & \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi\rangle
\end{aligned} \tag{4.119}$$

Therefore, the state of the EPR pair with an imperfect Hadamard gate is $|\Phi\rangle\langle\Phi| = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$. Hence, the imperfect Hadamard gate does not affect the state of the EPR pair and, as a result, the distance between the ideal and noisy implementations of the EPR pair is zero, **EPR** $=_0$ **EPR**$^{H(\epsilon)}$.

Next, it is necessary to repeat this exercise regarding the BellMeasure block. As shown in Equation 4.103, the ideal state of the BellMeasure block is
$\rho = \left(\left(\frac{1}{4}|\psi\rangle\langle\psi|, \frac{1}{4}X|\psi\rangle\langle\psi|X\right), \left(\frac{1}{4}Z|\psi\rangle\langle\psi|Z, \frac{1}{4}XZ|\psi\rangle\langle\psi|ZX\right)\right)$. Regarding the imperfect Hadamard gate, knowing that:

$$\begin{aligned}
&\alpha\,|0\rangle + \beta\,|1\rangle \\
\xmapsto{H^\epsilon} \quad & R_y\left(\frac{\pi}{2}\right) \cdot P(\pi + \epsilon)(\alpha\,|0\rangle + \beta\,|1\rangle) = R_y\left(\frac{\pi}{2}\right) \cdot \left(\alpha\,|0\rangle + e^{i(\pi+\epsilon)}\beta\,|1\rangle\right) \\
= \quad & R_y\left(\frac{\pi}{2}\right) \cdot \left(\alpha\,|0\rangle - e^{i\epsilon}\beta\,|1\rangle\right) = \frac{1}{\sqrt{2}}\left((\alpha + e^{i\epsilon}\beta)\,|0\rangle + (\alpha - e^{\epsilon}\beta)\,|1\rangle\right)
\end{aligned} \tag{4.120}$$

It follows, that:

$$
\begin{aligned}
& |\psi\rangle \otimes |0\rangle \otimes |0\rangle \\
\xmapsto{\text{EPR}} \quad & \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle) \\
\xmapsto{CNOT \otimes I} \quad & \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle) \\
\xmapsto{H^{\epsilon} \otimes I \otimes I} \quad & \frac{1}{2}\left(\alpha(|000\rangle + |100\rangle + |011\rangle + |111\rangle) + \beta e^{i\epsilon}(|010\rangle - |110\rangle + |001\rangle - |101\rangle)\right) \\
& = \frac{1}{2}\left(\alpha(|000\rangle + |100\rangle + |011\rangle + |111\rangle) + \beta e^{i\epsilon}(|010\rangle - |110\rangle + |001\rangle - |101\rangle)\right) \\
& = \frac{1}{2}(|00\rangle \otimes (\alpha|0\rangle + \beta e^{i\epsilon}|1\rangle) + |01\rangle \otimes (\alpha|1\rangle + e^{i\epsilon}\beta|0\rangle) + |10\rangle \otimes (\alpha|0\rangle - e^{i\epsilon}\beta|1\rangle)) \\
& + |11\rangle \otimes (\alpha|1\rangle - e^{i\epsilon}\beta|0\rangle)) \\
& = |00\rangle \otimes P(\epsilon)|\psi\rangle + |01\rangle \otimes XP(\epsilon)|\psi\rangle + |10\rangle \otimes ZP(\epsilon)|\psi\rangle + |11\rangle \otimes XZP(\epsilon)|\psi\rangle \\
& = |\phi'\rangle
\end{aligned}
\tag{4.121}
$$

Finally, measuring the first two qubits:

$$
\begin{aligned}
|\phi'\rangle\langle\phi'| \xmapsto{\text{meas} \otimes \text{meas} \otimes I} & \Big(\Big(\frac{1}{4}P(\epsilon)|\psi\rangle\langle\psi|P^{\dagger}(\epsilon), \frac{1}{4}XP(\epsilon)|\psi\rangle\langle\psi|XP^{\dagger}(\epsilon)\Big), \\
& \Big(\frac{1}{4}ZP(\epsilon)|\psi\rangle\langle\psi|P^{\dagger}(\epsilon)Z, \frac{1}{4}XZP(\epsilon)|\psi\rangle\langle\psi|P^{\dagger}(\epsilon)ZX\Big)\Big) = \rho'
\end{aligned}
\tag{4.122}
$$

Given that,

$$
\begin{aligned}
|\psi\rangle\langle\psi| - P(\epsilon)|\psi\rangle\langle\psi|P^{\dagger}(\epsilon) = & |\alpha|^2|0\rangle\langle 0| + \alpha\beta^{\dagger}|0\rangle\langle 1| + \alpha^{\dagger}\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1| - \\
& (|\alpha|^2|0\rangle\langle 0| + e^{-i\epsilon}\alpha\beta^{\dagger}|0\rangle\langle 1| + e^{i\epsilon}\alpha^{\dagger}\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|) \\
= & (1 - e^{-i\epsilon})\alpha\beta^{\dagger}|0\rangle\langle 1| + (1 - e^{i\epsilon})\alpha^{\dagger}\beta|1\rangle\langle 0|
\end{aligned}
\tag{4.123}
$$

$$
\begin{aligned}
X|\psi\rangle\langle\psi|X - XP(\epsilon)|\psi\rangle\langle\psi|XP^{\dagger}(\epsilon) = & |\alpha|^2|1\rangle\langle 1| + \alpha\beta^{\dagger}|1\rangle\langle 0| + \alpha^{\dagger}\beta|0\rangle\langle 1| + |\beta|^2|0\rangle\langle 0| - \\
& (|\alpha|^2|1\rangle\langle 1| + e^{-i\epsilon}\alpha\beta^{\dagger}|1\rangle\langle 0| + e^{i\epsilon}\alpha^{\dagger}\beta|0\rangle\langle 1| + |\beta|^2|0\rangle\langle 0|) \\
= & (1 - e^{-i\epsilon})\alpha\beta^{\dagger}|1\rangle\langle 0| + (1 - e^{i\epsilon})\alpha^{\dagger}\beta|0\rangle\langle 1|
\end{aligned}
\tag{4.124}
$$

$$
\begin{aligned}
Z|\psi\rangle\langle\psi|Z - ZP(\epsilon)|\psi\rangle\langle\psi|P^{\dagger}(\epsilon)Z = & |\alpha|^2|0\rangle\langle 0| - \alpha\beta^{\dagger}|0\rangle\langle 1| - \alpha^{\dagger}\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1| - \\
& (|\alpha|^2|0\rangle\langle 0| - e^{-i\epsilon}\alpha\beta^{\dagger}|0\rangle\langle 1| - e^{i\epsilon}\alpha^{\dagger}\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|) \\
= & (e^{-i\epsilon} - 1)\alpha\beta^{\dagger}|0\rangle\langle 1| + (e^{i\epsilon} - 1)\alpha^{\dagger}\beta|1\rangle\langle 0|
\end{aligned}
$$

(4.125)

$$XZ\,|\psi\rangle\,\langle\psi|\,ZX - XZP(\epsilon)|\psi\rangle\langle\psi|P^{\dagger}(\epsilon)ZX = |\alpha|^2|1\rangle\langle 1| - \alpha\beta^{\dagger}|1\rangle\langle 0| - \alpha^{\dagger}\beta|0\rangle\langle 1| + |\beta|^2|0\rangle\langle 0| - \\ (|\alpha|^2|1\rangle\langle 1| - e^{-i\epsilon}\alpha\beta^{\dagger}|1\rangle\langle 0| - e^{i\epsilon}\alpha^{\dagger}\beta|0\rangle\langle 1| + |\beta|^2|0\rangle\langle 0|) \\ = (e^{-i\epsilon} - 1)\alpha\beta^{\dagger}|1\rangle\langle 0| + (e^{i\epsilon} - 1)\alpha^{\dagger}\beta|0\rangle\langle 1| \tag{4.126}$$

Consequently,

$$\begin{aligned}\rho - \rho' =& \Big(\Big(\frac{1}{4}|\psi\rangle\langle\psi| - \frac{1}{4}P(\epsilon)|\psi\rangle\langle\psi|P^{\dagger}(\epsilon), \frac{1}{4}XP(\epsilon)|\psi\rangle\langle\psi|XP^{\dagger}(\epsilon) - \frac{1}{4}XP(\epsilon)|\psi\rangle\langle\psi|XP^{\dagger}(\epsilon)\Big), \\ & \Big(\frac{1}{4}ZP(\epsilon)|\psi\rangle\langle\psi|P^{\dagger}(\epsilon)Z - \frac{1}{4}ZP(\epsilon)|\psi\rangle\langle\psi|P^{\dagger}(\epsilon)Z, \\ & \frac{1}{4}P(\epsilon)XZ|\psi\rangle\langle\psi|P^{\dagger}(\epsilon)ZX - \frac{1}{4}XZP(\epsilon)|\psi\rangle\langle\psi|P^{\dagger}(\epsilon)ZX\Big)\Big) \\ =& \Big(\Big(\frac{1}{4}(1 - e^{-i\epsilon})\alpha\beta^{\dagger}|0\rangle\langle 1| + \frac{1}{4}(1 - e^{i\epsilon})\alpha^{\dagger}\beta|1\rangle\langle 0|, \frac{1}{4}(1 - e^{-i\epsilon})\alpha\beta^{\dagger}|1\rangle\langle 0| + \frac{1}{4}(1 - e^{i\epsilon})\alpha^{\dagger}\beta|0\rangle\langle 1|\Big), \\ & \Big(\frac{1}{4}(e^{-i\epsilon} - 1)\alpha\beta^{\dagger}|0\rangle\langle 1| + \frac{1}{4}(e^{i\epsilon} - 1)\alpha^{\dagger}\beta|1\rangle\langle 0|, \frac{1}{4}(e^{-i\epsilon} - 1)\alpha\beta^{\dagger}|1\rangle\langle 0| + \frac{1}{4}(e^{i\epsilon} - 1)\alpha^{\dagger}\beta|0\rangle\langle 1||\Big)\Big) \\ =& \left(\left(\frac{1}{4}\sigma, \frac{1}{4}\sigma'\right), \left(\frac{1}{4}\sigma'', \frac{1}{4}\sigma'''\right)\right)\end{aligned} \tag{4.127}$$

Employing Equation 3.9, the components of the Bloch vector of each state $\sigma, \sigma', \sigma'', \sigma'''$ are as follows:

$$
\begin{aligned}
r_x =& \mathsf{Tr}\left[\begin{pmatrix} 0 & (1-e^{-i\epsilon})\alpha\beta^\dagger \\ (1-e^{i\epsilon})\alpha^\dagger\beta & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right] \\
=& \mathsf{Tr}\left[\begin{pmatrix} (1-e^{-i\epsilon})\alpha\beta^\dagger & 0 \\ 0 & (1-e^{i\epsilon})\alpha^\dagger\beta \end{pmatrix}\right] = (1-e^{-i\epsilon})\alpha\beta^\dagger + (1-e^{i\epsilon})\alpha^\dagger\beta \\
r_y =& \mathsf{Tr}\left[\begin{pmatrix} 0 & (1-e^{-i\epsilon})\alpha\beta^\dagger \\ (1-e^{i\epsilon})\alpha^\dagger\beta & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\right] \\
=& \mathsf{Tr}\left[\begin{pmatrix} i(1-e^{-i\epsilon})\alpha\beta^\dagger & 0 \\ 0 & -i(1-e^{i\epsilon})\alpha^\dagger\beta \end{pmatrix}\right] = i(1-e^{-i\epsilon})\alpha\beta^\dagger - i(1-e^{i\epsilon})\alpha^\dagger\beta \\
r_z =& \mathsf{Tr}\left[\begin{pmatrix} 0 & (1-e^{-i\epsilon})\alpha\beta^\dagger \\ (1-e^{i\epsilon})\alpha^\dagger\beta & 0 \end{pmatrix}\cdot\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right] \\
=& \mathsf{Tr}\left[\begin{pmatrix} 0 & (1-e^{-i\epsilon})\alpha\beta^\dagger \\ -(1-e^{i\epsilon})\alpha^\dagger\beta & 0 \end{pmatrix}\right] = 0
\end{aligned}
\tag{4.128}
$$

$$
\begin{aligned}
r_x =& \mathsf{Tr}\left[\begin{pmatrix} 0 & (1-e^{i\epsilon})\alpha^\dagger\beta \\ (1-e^{-i\epsilon})\alpha\beta^\dagger & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right] \\
=& \mathsf{Tr}\left[\begin{pmatrix} (1-e^{i\epsilon})\alpha^\dagger\beta & 0 \\ 0 & (1-e^{-i\epsilon})\alpha\beta^\dagger \end{pmatrix}\right] = (1-e^{i\epsilon})\alpha^\dagger\beta + (1-e^{-i\epsilon})\alpha\beta^\dagger \\
r_y =& \mathsf{Tr}\left[\begin{pmatrix} 0 & (1-e^{i\epsilon})\alpha^\dagger\beta \\ (1-e^{-i\epsilon})\alpha\beta^\dagger & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\right] \\
=& \mathsf{Tr}\left[\begin{pmatrix} i(1-e^{i\epsilon})\alpha^\dagger\beta & 0 \\ 0 & -i(1-e^{-i\epsilon})\alpha\beta^\dagger \end{pmatrix}\right] = i(1-e^{i\epsilon})\alpha^\dagger\beta - i(1-e^{-i\epsilon})\alpha\beta^\dagger \\
r_z =& \mathsf{Tr}\left[\begin{pmatrix} 0 & (1-e^{i\epsilon})\alpha^\dagger\beta \\ (1-e^{-i\epsilon})\alpha\beta^\dagger & 0 \end{pmatrix}\cdot\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right] \\
=& \mathsf{Tr}\left[\begin{pmatrix} 0 & (1-e^{i\epsilon})\alpha^\dagger\beta \\ -(1-e^{-i\epsilon})\alpha\beta^\dagger & 0 \end{pmatrix}\right] = 0
\end{aligned}
\tag{4.129}
$$

$$
\begin{aligned}
r_x =& \mathrm{Tr}\left[\begin{pmatrix} 0 & (e^{-i\epsilon}-1)\alpha\beta^\dagger \\ (e^{i\epsilon}-1)\alpha^\dagger\beta & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right] \\
=& \mathrm{Tr}\left[\begin{pmatrix} (e^{-i\epsilon}-1)\alpha\beta^\dagger & 0 \\ 0 & (e^{i\epsilon}-1)\alpha^\dagger\beta \end{pmatrix}\right] = (e^{-i\epsilon}-1)\alpha\beta^\dagger + (e^{i\epsilon}-1)\alpha^\dagger\beta \\
r_y =& \mathrm{Tr}\left[\begin{pmatrix} 0 & (e^{-i\epsilon}-1)\alpha\beta^\dagger \\ (e^{i\epsilon}-1)\alpha^\dagger\beta & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\right] \\
=& \mathrm{Tr}\left[\begin{pmatrix} i(e^{-i\epsilon}-1)\alpha\beta^\dagger & 0 \\ 0 & -i(e^{i\epsilon}-1)\alpha^\dagger\beta \end{pmatrix}\right] = i(e^{-i\epsilon}-1)\alpha\beta^\dagger - i(e^{i\epsilon}-1)\alpha^\dagger\beta \\
r_z =& \mathrm{Tr}\left[\begin{pmatrix} 0 & (e^{-i\epsilon}-1)\alpha\beta^\dagger \\ (e^{i\epsilon}-1)\alpha^\dagger\beta & 0 \end{pmatrix}\cdot\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right] \\
=& \mathrm{Tr}\left[\begin{pmatrix} 0 & (e^{-i\epsilon}-1)\alpha\beta^\dagger \\ -(e^{i\epsilon}-1)\alpha^\dagger\beta & 0 \end{pmatrix}\right] = 0
\end{aligned}
\tag{4.130}
$$

$$
\begin{aligned}
r_x =& \mathrm{Tr}\left[\begin{pmatrix} 0 & (e^{i\epsilon}-1)\alpha^\dagger\beta \\ (e^{-i\epsilon}-1)\alpha\beta^\dagger & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right] \\
=& \mathrm{Tr}\left[\begin{pmatrix} (e^{i\epsilon}-1)\alpha^\dagger\beta & 0 \\ 0 & (e^{-i\epsilon}-1)\alpha\beta^\dagger \end{pmatrix}\right] = (e^{i\epsilon}-1)\alpha^\dagger\beta + (e^{-i\epsilon}-1)\alpha\beta^\dagger \\
r_y =& \mathrm{Tr}\left[\begin{pmatrix} 0 & (e^{i\epsilon}-1)\alpha^\dagger\beta \\ (e^{-i\epsilon}-1)\alpha\beta^\dagger & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\right] \\
=& \mathrm{Tr}\left[\begin{pmatrix} i(e^{i\epsilon}-1)\alpha^\dagger\beta & 0 \\ 0 & -i(e^{-i\epsilon}-1)\alpha\beta^\dagger \end{pmatrix}\right] = i(e^{i\epsilon}-1)\alpha^\dagger\beta - i(e^{-i\epsilon}-1)\alpha\beta^\dagger \\
r_z =& \mathrm{Tr}\left[\begin{pmatrix} 0 & (e^{i\epsilon}-1)\alpha^\dagger\beta \\ (e^{-i\epsilon}-1)\alpha\beta^\dagger & 0 \end{pmatrix}\cdot\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right] \\
=& \mathrm{Tr}\left[\begin{pmatrix} 0 & (e^{i\epsilon}-1)\alpha^\dagger\beta \\ -(e^{-i\epsilon}-1)\alpha\beta^\dagger & 0 \end{pmatrix}\right] = 0
\end{aligned}
\tag{4.131}
$$

As a result, and given that the distance between two vectors corresponds to their Euclidean distance, it follows that the distance between the ideal and noisy implementations of the

Hadamard gate in the BellMeasure block corresponds to:

$$
\begin{aligned}
\|\rho-\rho'\|_\diamond &= \left\| \left(\left(\frac{1}{4}\sigma, \frac{1}{4}\sigma'\right), \left(\frac{1}{4}\sigma'', \frac{1}{4}\sigma'''\right) \right) \right\|_\diamond \\
&= \left\|\frac{1}{4}\sigma\right\|_\diamond + \left\|\frac{1}{4}\sigma'\right\|_\diamond + \left\|\frac{1}{4}\sigma''\right\|_\diamond + \left\|\frac{1}{4}\sigma'''\right\|_\diamond \qquad \{\textbf{??}\} \\
&= \left\|\frac{1}{4}((1-e^{-i\epsilon})\alpha\beta^\dagger + (1-e^{i\epsilon})\alpha^\dagger\beta, i(1-e^{-i\epsilon})\alpha\beta^\dagger - i(1-e^{i\epsilon})\alpha^\dagger\beta)\right\|_2 + \\
&\quad \left\|\frac{1}{4}((1-e^{i\epsilon})\alpha^\dagger\beta + (1-e^{-i\epsilon})\alpha\beta^\dagger, i(1-e^{i\epsilon})\alpha^\dagger\beta - i(1-e^{-i\epsilon})\alpha\beta^\dagger)\right\|_2 + \\
&\quad \left\|\frac{1}{4}((e^{-i\epsilon}-1)\alpha\beta^\dagger + (e^{i\epsilon}-1)\alpha^\dagger\beta, i(e^{-i\epsilon}-1)\alpha\beta^\dagger - i(e^{i\epsilon}-1)\alpha^\dagger\beta)\right\|_2 + \\
&\quad \left\|\frac{1}{4}((e^{i\epsilon}-1)\alpha^\dagger\beta + (e^{-i\epsilon}-1)\alpha\beta^\dagger, i(e^{i\epsilon}-1)\alpha^\dagger\beta - i(e^{-i\epsilon}-1)\alpha\beta^\dagger)\right\|_2
\end{aligned}
\tag{4.132}
$$

Applying Definition 3.1.27 to each term, it follows that:

$$
\begin{aligned}
\|\rho-\rho'\|_\diamond =& \frac{1}{4}\sqrt{((1-e^{-i\epsilon})\alpha\beta^\dagger + (1-e^{i\epsilon})\alpha^\dagger\beta)^2 + (i((1-e^{-i\epsilon})\alpha\beta^\dagger - (1-e^{i\epsilon})\alpha^\dagger\beta))^2} \\
&+ \frac{1}{4}\sqrt{((1-e^{i\epsilon})\alpha^\dagger\beta + (1-e^{-i\epsilon})\alpha\beta^\dagger)^2 + (i((1-e^{i\epsilon})\alpha^\dagger\beta - (1-e^{-i\epsilon})\alpha\beta^\dagger))^2} \\
&+ \frac{1}{4}\sqrt{((e^{-i\epsilon}-1)\alpha\beta^\dagger + (e^{i\epsilon}-1)\alpha^\dagger\beta)^2 + (i((e^{-i\epsilon}-1)\alpha\beta^\dagger - (e^{i\epsilon}-1)\alpha^\dagger\beta))^2} \\
&+ \frac{1}{4}\sqrt{((e^{i\epsilon}-1)\alpha^\dagger\beta + (e^{-i\epsilon}-1)\alpha\beta^\dagger)^2 + (i((e^{i\epsilon}-1)\alpha^\dagger\beta - (e^{-i\epsilon}-1)\alpha\beta^\dagger))^2} \\
=& \frac{1}{4}\sqrt{((1-e^{-i\epsilon})\alpha\beta^\dagger + (1-e^{i\epsilon})\alpha^\dagger\beta)^2 + (i((1-e^{-i\epsilon})\alpha\beta^\dagger - (1-e^{i\epsilon})\alpha^\dagger\beta))^2} \\
&+ \frac{1}{4}\sqrt{((1-e^{-i\epsilon})\alpha\beta^\dagger + (1-e^{i\epsilon})\alpha^\dagger\beta)^2 + (-(i((1-e^{-i\epsilon})\alpha\beta^\dagger - (1-e^{i\epsilon})\alpha^\dagger\beta)))^2} \\
&+ \frac{1}{4}\sqrt{(-((1-e^{-i\epsilon})\alpha\beta^\dagger + (1-e^{i\epsilon})\alpha^\dagger\beta))^2 + (i((1-e^{-i\epsilon})\alpha\beta^\dagger - (1-e^{i\epsilon})\alpha^\dagger\beta))^2} \\
&+ \frac{1}{4}\sqrt{(-((1-e^{-i\epsilon})\alpha\beta^\dagger + (1-e^{i\epsilon})\alpha^\dagger\beta))^2 + (-(i((1-e^{-i\epsilon})\alpha\beta^\dagger - (1-e^{i\epsilon})\alpha^\dagger\beta)))^2} \\
&= \frac{1}{4}\sqrt{((1-e^{-i\epsilon})\alpha\beta^\dagger + (1-e^{i\epsilon})\alpha^\dagger\beta)^2 + (i((1-e^{-i\epsilon})\alpha\beta^\dagger - (1-e^{i\epsilon})\alpha^\dagger\beta))^2} \\
&= \sqrt{4(1-e^{-i\epsilon})(1-e^{i\epsilon})|\alpha|^2|\beta|^2} = 2\sqrt{(1-e^{i\epsilon}-e^{-i\epsilon}+1)|\alpha|^2|\beta|^2} \\
&= 2\sqrt{2(1-\cos(\epsilon))|\alpha|^2|\beta|^2} = 2\sqrt{2}\sqrt{(1-\cos(\epsilon))|\alpha|^2|\beta|^2}
\end{aligned}
\tag{4.133}
$$

It is possible to observe that when $\epsilon = 0$, the distance between the ideal and noisy implementations of the Hadamard gate in the BellMeasure block is zero, which is consistent with the fact that the ideal and noisy implementations are the same. The same goes for $\epsilon = \pi$, $\alpha = 0$ and $\beta = 0$ given that only the non-diagonal components of the density matrix are affected by an erroneous phase gate.

Given this result it is possible to conclude that **BellMeasure** $=_{2\sqrt{2}\sqrt{(1-\cos(\epsilon))|\alpha|^2|\beta|^2}}$ **BellMeasure**$^{H(\epsilon)}$. Hence, **QTP** $=_{0+2\sqrt{2}\sqrt{(1-\cos(\epsilon))|\alpha|^2|\beta|^2}}$ **QTP**$^{H(\epsilon)}$, *i.e.*, **QTP** $=_{2\sqrt{2}\sqrt{(1-\cos(\epsilon))|\alpha|^2|\beta|^2}}$ **QTP**$^{H(\epsilon)}$.

4.8.4 Ilustration: A malicious attack on the quantum teleportation protocol

Now, consider a malicious attack on the quantum teleportation protocol in the form of a bit-flip occurring with a 50% probability before measurement. More generally, one can define an operation T that applies a unitary operation U to the state given as input with 50% probability. Operation T can be defined as follows:

$$T: \ \textit{qbit}, ..., \textit{qbit} \multimap \textit{qbit}^{\otimes n}$$

$$T = q_1 : \textit{qbit}, ..., q_n : \textit{qbit} \triangleright \text{pm}\, CU(R_X^{\frac{\pi}{2}}(q(\textit{new}\,0(*))), q_1, ..., q_n) \text{ to } newq \otimes q.\, \textit{disc}(newq)$$

This operation is depicted in Figure 17.

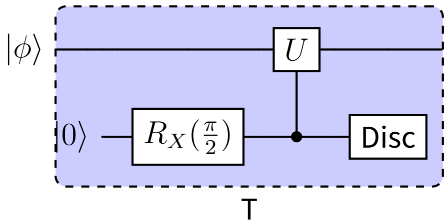


Figure 17: T operation

Regarding the calculations, applying operation T to the state $|\psi\rangle$, one has that:

$$\begin{aligned}
& |\phi\rangle\langle\phi| \\
\xmapsto{I\otimes q(\textit{new}\,0(*))} \quad & |\phi\rangle\langle\phi| \otimes |0\rangle\langle 0| \\
\xmapsto{I\otimes R_X(\frac{\pi}{2})} \quad & |\phi\rangle\langle\phi| \otimes \frac{1}{2}(|0\rangle\langle 0| - i|0\rangle\langle 1| + i|1\rangle\langle 0| + |1\rangle\langle 1|) \\
& = \frac{1}{2}(|\phi\rangle\langle\phi||0\rangle\langle 0| - i|\phi\rangle\langle\phi||0\rangle\langle 1| + i|\phi\rangle\langle\phi||1\rangle\langle 0| + |\phi\rangle\langle\phi||1\rangle\langle 1|) \\
\xmapsto{\text{CU}} \quad & \frac{1}{2}(|\phi\rangle\langle\phi||0\rangle\langle 0| - i|\phi\rangle\langle\phi||0\rangle\langle 1|U^\dagger + iU|\phi\rangle\langle\phi||1\rangle\langle 0| + U|\phi\rangle\langle\phi||1\rangle\langle 1|U^\dagger) \\
\xmapsto{I\otimes\text{Disc}} \quad & \frac{1}{2}(|\phi\rangle\langle\phi| + U|\phi\rangle\langle\phi|U^\dagger)
\end{aligned} \tag{4.134}$$

Revisiting the example at hand, the circuit that represents the quantum teleportation protocol with a 50% probability of occurring a bit flip prior to measurement is depicted in Figure 18.

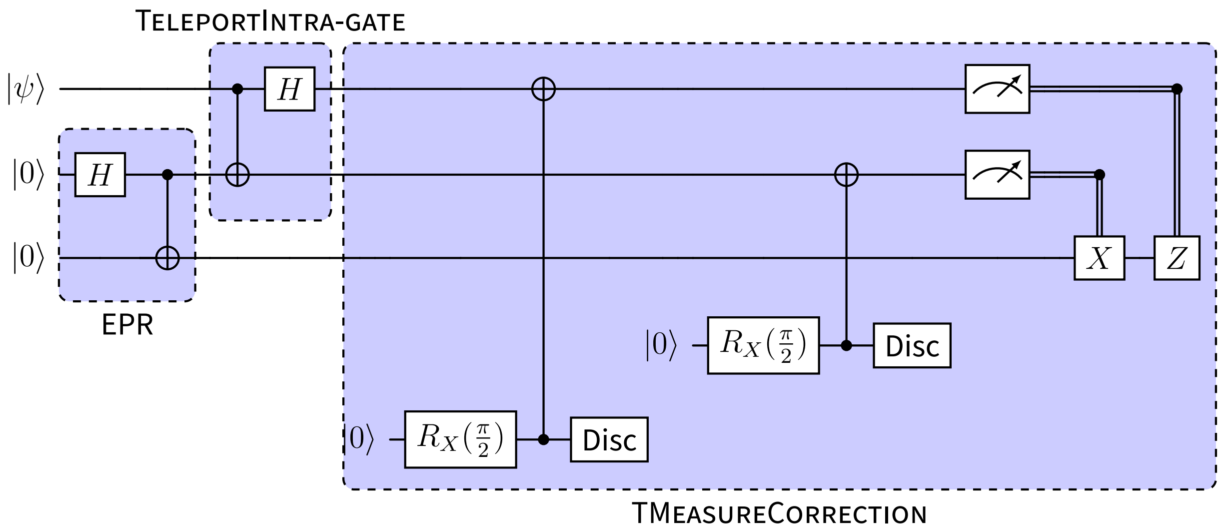


Figure 18: Quantum Teleportation Protocol: Bit flip with 50% probability before measurement.

In this case, the quantum teleportation protocol is divided into three parts: **EPR**, **TeleportIntra-gate** and **TMeasureCorrection**. As a result, it is necessary to define the new functions (note that the function **EPR** is the same as the one defined in section 4.7):

BellMeasure : $\quad$ *qbit* $\otimes$ *qbit* $\multimap$ *qbit* $\otimes$ *qbit*

TeleportIntra-gate : $\quad$ *qbit* $\otimes$ *qbit* $\otimes$ *qbit* $\multimap$ *qbit* $\otimes$ *qbit* $\otimes$ *qbit*

TMeasureCorrection : $\quad$ *qbit* $\otimes$ *qbit* $\otimes$ *qbit* $\multimap$ *qbit*

Considering the operation $T_{X\otimes I\otimes I}$ as the operation T with the unitary U represented by $X \otimes I \otimes I$, and similarly, $T_{I\otimes X\otimes I}$ as T with U denoted by $I \otimes U \otimes I$, these funtions can be defined as follows:

TeleportIntra-gate $= q_1 : \mathit{qbit}, q_2 : \mathit{qbit} \triangleright (\mathrm{pm}\ \ \mathit{CNOT}(q_1, q_2)\ \mathrm{to}\ x \otimes y.\, H(x) \otimes y)$

TMeasureCorrection $= q_1 : \mathit{qbit}, q_2 : \mathit{qbit}, q_3 : \mathit{qbit} \triangleright \mathrm{pm}\ T_{X\otimes I\otimes I}(q_1, q_2, q_3)\ \mathrm{to}\ a \otimes b \otimes c.$

$\mathrm{pm}\ T_{I\otimes X\otimes I}(a, b, c)\ \mathrm{to}\ d \otimes e \otimes q.$

$\mathrm{pm}\ \mathit{meas}(d) \otimes \mathit{meas}(e)\ \mathrm{to}\ x \otimes y.$

$\mathrm{case}\ \ x\,\{\mathrm{inl}(x_0) \Rightarrow (\mathrm{cond}\,y\,\{\mathrm{inl}(y_0) \Rightarrow \mathit{I}(q);\ \ \mathrm{inr}(y_1) \Rightarrow\ \mathit{X}(q))\};$

$\mathrm{inr}(x_1) \Rightarrow (\mathrm{cond}\,y\,\{\mathrm{inl}(y_0) \Rightarrow \mathit{Z}(q); \mathrm{inr}(y_1) \Rightarrow \mathit{Z}(\mathit{X}(q))\})\}$

Designating the qubit to be teleported as q_0, one can conceptualize he quantum teleportation protocol with a 50% probability of occurring a bit flip prior to measurement as follows:

$$\begin{aligned}
&\text{pm } \textbf{EPR}(*) \text{ to } q_1 \otimes q_2. \\
&\text{pm } \textbf{TeleportIntra-gate}(q_0, q_1) \text{ to } tiq_0 \otimes tiq_1. \\
&\text{pm } \textbf{TMeasureCorrection}(tiq_0, tiq_1, q_2) \text{ to } q.\, q
\end{aligned}$$

Per Equation 4.104, the state of the system post-teleportation protocol corresponds to $|\psi\rangle\langle\psi|$ in the absence of a malicious attack, denoted as ρ.
Regarding the first two parts of the teleportation protocol, given Equation 4.102, one has that:

$$\begin{aligned}
&|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0| \otimes |0\rangle\langle 0| \\
\xmapsto{\text{EPR}}\ &\frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle) \\
\xmapsto{\text{TeleportIntra-gate}}\ &|00\rangle \otimes |\psi\rangle + |01\rangle \otimes X|\psi\rangle + |10\rangle \otimes Z|\psi\rangle + |11\rangle \otimes XZ|\psi\rangle = |\phi\rangle
\end{aligned} \tag{4.135}$$

Consequently, the state of the system post-teleportation protocol corresponds to $|\phi\rangle\langle\phi|$. With respect to **TMeasureCorrection**, considering that,

$$\begin{aligned}
&|\phi\rangle = |00\rangle \otimes |\psi\rangle + |01\rangle \otimes X|\psi\rangle + |10\rangle \otimes Z|\psi\rangle + |11\rangle \otimes XZ|\psi\rangle \\
\xmapsto{X\otimes I\otimes I}\ &|10\rangle \otimes |\psi\rangle + |11\rangle \otimes X|\psi\rangle + |00\rangle \otimes Z|\psi\rangle + |01\rangle \otimes XZ|\psi\rangle \\
&= |00\rangle \otimes Z|\psi\rangle + |01\rangle \otimes XZ|\psi\rangle + |10\rangle \otimes |\psi\rangle + |11\rangle \otimes X|\psi\rangle = |\phi'\rangle
\end{aligned} \tag{4.136}$$

And,

$$\begin{aligned}
&|\phi\rangle = |00\rangle \otimes |\psi\rangle + |01\rangle \otimes X|\psi\rangle + |10\rangle \otimes Z|\psi\rangle + |11\rangle \otimes XZ|\psi\rangle \\
\xmapsto{I\otimes X\otimes I}\ &|01\rangle \otimes |\psi\rangle + |00\rangle \otimes X|\psi\rangle + |11\rangle \otimes Z|\psi\rangle + |10\rangle \otimes XZ|\psi\rangle \\
&= |00\rangle \otimes X|\psi\rangle + |01\rangle \otimes |\psi\rangle + |10\rangle \otimes XZ|\psi\rangle + |11\rangle \otimes Z|\psi\rangle = |\phi''\rangle
\end{aligned} \tag{4.137}$$

And finally,

$$\begin{aligned}
&|\phi'\rangle = |00\rangle \otimes Z|\psi\rangle + |01\rangle \otimes XZ|\psi\rangle + |10\rangle \otimes |\psi\rangle + |11\rangle \otimes X|\psi\rangle \\
\xmapsto{I\otimes X\otimes I}\ &|01\rangle \otimes Z|\psi\rangle + |00\rangle \otimes XZ|\psi\rangle + |11\rangle \otimes |\psi\rangle + |10\rangle \otimes X|\psi\rangle \\
&= |00\rangle \otimes XZ|\psi\rangle + |01\rangle \otimes Z|\psi\rangle + |10\rangle \otimes X|\psi\rangle + |11\rangle \otimes |\psi\rangle = |\phi'''\rangle
\end{aligned} \tag{4.138}$$

It follows that,

$$
\begin{aligned}
&|\phi\rangle\langle\phi| \\
\xmapsto{T_{X\otimes I\otimes I}}\quad & \frac{1}{2}\left(|\phi\rangle\langle\phi| + |\phi'\rangle\langle\phi'|\right) && \{\text{Equation 4.134}\} \\
\xmapsto{T_{I\otimes X\otimes I}}\quad & \frac{1}{4}\left(|\phi\rangle\langle\phi| + |\phi'\rangle\langle\phi'| + |\phi''\rangle\langle\phi''| + |\phi'''\rangle\langle\phi'''|\right) && \{\text{Equation 4.134}\} \\
\xmapsto{\text{meas}\otimes\text{meas}\otimes I}\quad & \frac{1}{4}\Bigg(\bigg(\Big(\frac{1}{4}|\psi\rangle\langle\psi|, \frac{1}{4}X|\psi\rangle\langle\psi|X\Big), \Big(\frac{1}{4}Z|\psi\rangle\langle\psi|Z, \frac{1}{4}XZ|\psi\rangle\langle\psi|ZX\Big)\bigg) \\
& + \bigg(\Big(\frac{1}{4}Z|\psi\rangle\langle\psi|Z, \frac{1}{4}XZ|\psi\rangle\langle\psi|XZ\Big), \Big(\frac{1}{4}|\psi\rangle\langle\psi|, \frac{1}{4}X|\psi\rangle\langle\psi|X\Big)\bigg) \\
& + \bigg(\Big(\frac{1}{4}X|\psi\rangle\langle\psi|X, \frac{1}{4}|\psi\rangle\langle\psi|\Big), \Big(\frac{1}{4}XZ|\psi\rangle\langle\psi|ZX, \frac{1}{4}Z|\psi\rangle\langle\psi|Z\Big)\bigg) \\
& + \bigg(\Big(\frac{1}{4}XZ|\psi\rangle\langle\psi|ZX, \frac{1}{4}Z|\psi\rangle\langle\psi|Z\Big), \Big(\frac{1}{4}X|\psi\rangle\langle\psi|X, \frac{1}{4}|\psi\rangle\langle\psi|\Big)\bigg)\Bigg)
\end{aligned}
\tag{4.139}
$$

Next, regarding the condicional statements, applying correction to $\Big(\big(\frac{1}{4}|\psi\rangle\langle\psi|, \frac{1}{4}X|\psi\rangle\langle\psi|X\big), \big(\frac{1}{4}Z|\psi\rangle\langle\psi|Z,$ results in the state $|\psi\rangle$ (Equation 4.104). Moreover, with respect to $\Big(\big(\frac{1}{4}|\psi\rangle\langle\psi|, \frac{1}{4}X|\psi\rangle\langle\psi|X\big), \big(\frac{1}{4}Z|\psi\rangle\langle\psi|Z, \frac{1}{4}$ one has that applying the condicional statements:

$$
\begin{aligned}
&\frac{1}{4}Z|\psi\rangle\langle\psi|Z + \frac{1}{4}XXZ|\psi\rangle\langle\psi|ZXX + \frac{1}{4}Z|\psi\rangle\langle\psi|Z + \frac{1}{4}ZXX|\psi\rangle\langle\psi|XXZ \\
=&\frac{1}{4}Z|\psi\rangle\langle\psi|Z + \frac{1}{4}Z|\psi\rangle\langle\psi|Z + \frac{1}{4}Z|\psi\rangle\langle\psi|Z + \frac{1}{4}Z|\psi\rangle\langle\psi|Z = Z|\psi\rangle\langle\psi|Z
\end{aligned}
\tag{4.140}
$$

Furthermore, applying correction to $\Big(\big(\frac{1}{4}X|\psi\rangle\langle\psi|X, \frac{1}{4}|\psi\rangle\langle\psi|\big), \big(\frac{1}{4}XZ|\psi\rangle\langle\psi|ZX, \frac{1}{4}Z|\psi\rangle\langle\psi|Z\big)\Big)$ results in

$$
\begin{aligned}
&\frac{1}{4}X|\psi\rangle\langle\psi|X + \frac{1}{4}X|\psi\rangle\langle\psi|X + \frac{1}{4}ZXZ|\psi\rangle\langle\psi|ZXZ + \frac{1}{4}ZXZ|\psi\rangle\langle\psi|ZXZ \\
=&\frac{1}{4}X|\psi\rangle\langle\psi|X + \frac{1}{4}X|\psi\rangle\langle\psi|X + \frac{1}{4}X|\psi\rangle\langle\psi|X + \frac{1}{4}X|\psi\rangle\langle\psi|X = X|\psi\rangle\langle\psi|X
\end{aligned}
\tag{4.141}
$$

And, at last, regarding $\Big(\big(\frac{1}{4}XZ|\psi\rangle\langle\psi|ZX, \frac{1}{4}Z|\psi\rangle\langle\psi|Z\big), \big(\frac{1}{4}X|\psi\rangle\langle\psi|X, \frac{1}{4}|\psi\rangle\langle\psi|\big)\Big)$,

$$
\begin{aligned}
&\frac{1}{4}XZ|\psi\rangle\langle\psi|ZX + \frac{1}{4}XZ|\psi\rangle\langle\psi|ZX + \frac{1}{4}ZX|\psi\rangle\langle\psi|XZ + \frac{1}{4}ZX|\psi\rangle\langle\psi|XZ \\
=&\frac{1}{4}XZ|\psi\rangle\langle\psi|ZX + \frac{1}{4}XZ|\psi\rangle\langle\psi|ZX + \frac{1}{4}XZ|\psi\rangle\langle\psi|ZX + \frac{1}{4}XZ|\psi\rangle\langle\psi|ZX \\
=&ZX|\psi\rangle\langle\psi|XZ
\end{aligned}
\tag{4.142}
$$

Consequentlty, applying the conditional statements to the state obtained in Equation 4.139, it follows that,

$$\begin{aligned}
&\frac{1}{4}\left(|\psi\rangle\langle\psi| + Z|\psi\rangle\langle\psi|Z + X|\psi\rangle\langle\psi|X + ZX|\psi\rangle\langle\psi|XZ\right)\\
=&\frac{1}{4}(|\alpha|^2|0\rangle\langle 0| + \alpha\beta^\dagger|0\rangle\langle 1| + \alpha^\dagger\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|\\
&+|\alpha|^2|0\rangle\langle 0| - \alpha\beta^\dagger|0\rangle\langle 1| - \alpha^\dagger\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|\\
&+|\beta|^2|0\rangle\langle 0| + \alpha^\dagger\beta|0\rangle\langle 1| + \alpha\beta^\dagger|1\rangle\langle 0| + |\alpha|^2|1\rangle\langle 1|\\
&+|\beta|^2|0\rangle\langle 0| - \alpha^\dagger\beta|0\rangle\langle 1| - \alpha\beta^\dagger|1\rangle\langle 0| + |\alpha|^2|1\rangle\langle 1|)\\
=&\frac{|\alpha|^2+|\beta|^2}{2}|0\rangle\langle 0| + \frac{|\alpha|^2+|\beta|^2}{2}|1\rangle\langle 1| = \rho'
\end{aligned} \tag{4.143}$$

Therefore, $\rho - \rho'$ corresponds to:

$$\begin{aligned}
\rho - \rho' =&|\alpha|^2|0\rangle\langle 0| + \alpha\beta^\dagger|0\rangle\langle 1| + \alpha^\dagger\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|\\
&-\left(\frac{|\alpha|^2+|\beta|^2}{2}|0\rangle\langle 0| + \frac{|\alpha|^2+|\beta|^2}{2}|1\rangle\langle 1|\right)\\
=&\frac{|\alpha|^2-|\beta|^2}{2}|0\rangle\langle 0| + \alpha\beta^\dagger|0\rangle\langle 1| + \alpha^\dagger\beta|1\rangle\langle 0| + \frac{|\beta|^2-|\alpha|^2}{2}|1\rangle\langle 1|
\end{aligned} \tag{4.144}$$

Employing Equation 3.9, the components of the Bloch vector of the state $\rho - \rho'$ are as follows:

$$\begin{aligned}
r_x =&\text{Tr}\left[\begin{pmatrix}\frac{|\alpha|^2-|\beta|^2}{2} & \alpha\beta^\dagger\\ \alpha^\dagger\beta & \frac{|\beta|^2-|\alpha|^2}{2}\end{pmatrix}\cdot\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\right] = \text{Tr}\left[\begin{pmatrix}\alpha\beta^\dagger & \frac{|\alpha|^2-|\beta|^2}{2}\\ \frac{|\beta|^2-|\alpha|^2}{2} & \alpha^\dagger\beta\end{pmatrix}\right] = \alpha\beta^\dagger + \alpha^\dagger\beta\\
r_y =&\text{Tr}\left[\begin{pmatrix}\frac{|\alpha|^2-|\beta|^2}{2} & \alpha\beta^\dagger\\ \alpha^\dagger\beta & \frac{|\beta|^2-|\alpha|^2}{2}\end{pmatrix}\cdot\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}\right] = \text{Tr}\left[\begin{pmatrix}i\alpha\beta^\dagger & \frac{|\alpha|^2-|\beta|^2}{2}\\ \frac{|\beta|^2-|\alpha|^2}{2} & -i\alpha^\dagger\beta\end{pmatrix}\right] = i(\alpha\beta^\dagger - \alpha^\dagger\beta)\\
r_z =&\text{Tr}\left[\begin{pmatrix}\frac{|\alpha|^2-|\beta|^2}{2} & \alpha\beta^\dagger\\ \alpha^\dagger\beta & \frac{|\beta|^2-|\alpha|^2}{2}\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\right] = \text{Tr}\left[\begin{pmatrix}\frac{|\alpha|^2-|\beta|^2}{2} & -\alpha\beta^\dagger\\ \alpha^\dagger\beta & -\frac{|\beta|^2-|\alpha|^2}{2}\end{pmatrix}\right] = |\alpha|^2 - |\beta|^2
\end{aligned} \tag{4.145}$$

Considering that the distance between two vectors corresponds to their Euclidean distance, it follows that the distance between the ideal state and its version subjected to the malicious attack is given by:

$$
\begin{aligned}
&\|\rho - \rho'\|_\diamond \\
&= \left\|\left(\alpha\beta^\dagger + \alpha^\dagger\beta, i(\alpha\beta^\dagger - \alpha^\dagger\beta), |\alpha|^2 - |\beta|^2\right)\right\|_2 && \{\text{Equation 4.145}\} \\
&= \sqrt{(\alpha\beta^\dagger + \alpha^\dagger\beta)^2 + (i(\alpha\beta^\dagger - \alpha^\dagger\beta))^2 + (|\alpha|^2 - |\beta|^2)^2} && \{\text{Definition 3.1.27}\} \\
&= \sqrt{(\alpha\beta^\dagger + \alpha^\dagger\beta)^2 + -(\alpha\beta^\dagger - \alpha^\dagger\beta)^2 + (|\alpha|^2 - |\beta|^2)^2} \\
&= \sqrt{4\alpha\beta^\dagger\alpha^\dagger\beta + |\alpha|^4 - 2|\alpha|^2|\beta|^2 + |\beta|^4} = \sqrt{4|\alpha|^2|\beta|^2 + |\alpha|^4 - 2|\alpha|^2|\beta|^2 + |\beta|^4} \\
&= \sqrt{|\alpha|^4 + 2|\alpha|^2|\beta|^2 + |\beta|^4} = \sqrt{(|\alpha|^2 + |\beta|^2)^2} = |\alpha|^2 + |\beta|^2 = 1
\end{aligned}
\tag{4.146}
$$

Chapter 5

Graded modalities

The linearity constraint is often deemed too restrictive, prompting research into relaxing it in various computational paradigms. In [59], the controlled use of a resource multiple times is explored within approximate program equivalence paradigms. Moreover, the grammar introduced allows the specification of how many times a resource can be used—a notion particularly relevant in quantum computation, especially within the NISQ era where resources are scarce.

Intro

5.1 Syntax

Here, the following grammar of types is used.

$$\mathbb{A} ::= X \mid \mathbb{I} \mid \mathbb{A} \otimes \mathbb{A} \mid \mathbb{A} \oplus \mathbb{A} \mid \mathbb{A} \multimap \mathbb{A} \mid\, !_r \mathbb{A} \qquad\qquad X \in G, r \in \mathbb{N}$$

$$\frac{\Gamma_i \triangleright v_i :!_{r \cdot s_i} \mathbb{A}_i \quad x_1 :!_{s_1} \mathbb{A}_1, \ldots, x_n :!_{s_n} \mathbb{A}_n \triangleright u : \mathbb{A} \quad E \in \mathsf{Sf}(\Gamma_1; \ldots; \Gamma_n)}{E \triangleright \mathsf{pr}_{(r,[s_1,\ldots,s_n])} v_1, \ldots, v_n \;\mathsf{fr}\; x_1, \ldots, x_n . u :!_r \mathbb{A}} (!_i) \qquad \frac{\Gamma \triangleright v :!_1 \mathbb{A}}{\Gamma \triangleright \mathsf{dr}\; v : \mathbb{A}} (!_e)$$

$$\frac{\Gamma \triangleright v :!_0 \mathbb{A} \quad \Delta \triangleright u : \mathbb{B} \quad E \in \mathsf{Sf}(\Gamma, \Delta)}{E \triangleright v.u : \mathbb{B}} (!_0) \qquad \frac{\Gamma \triangleright v :!_{n+m} \mathbb{A} \quad \Delta, x :!_n \mathbb{A}, y :!_m \mathbb{B} \triangleright u : \mathbb{B} \quad E \in \mathsf{Sf}(\Gamma, \Delta)}{E \triangleright \mathsf{cp}_{(n,m)} v \;\mathsf{to}\; x, y.u : \mathbb{B}} (!_{n+m})$$

Figure 19: Term formation rules of graded lambda calculus.

5.2 Interpretation

5.3 Quantum State Discrimination

Chapter 6

Conclusions and future work

Conclusions and future work.

6.1 Conclusions

6.2 Prospect for future work

Bibliography

[1] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6-7), 1982.

[2] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[3] John Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2:79, 2018.

[4] A Robert Calderbank and Peter W Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098, 1996.

[5] Daniel Gottesman. *Stabilizer codes and quantum error correction*. California Institute of Technology, 1997.

[6] Andrew M Steane. Error correcting codes in quantum theory. *Physical Review Letters*, 77(5):793, 1996.

[7] Austin G Fowler, Matteo Mariantoni, John M Martinis, and Andrew N Cleland. Surface codes: Towards practical large-scale quantum computation. *Physical Review A*, 86(3):032324, 2012.

[8] Joel J Wallman and Joseph Emerson. Noise tailoring for scalable quantum computation via randomized compiling. *Physical Review A*, 94(5):052325, 2016.

[9] Prakash Murali, Jonathan M Baker, Ali Javadi-Abhari, Frederic T Chong, and Margaret Martonosi. Noise-adaptive compiler mappings for noisy intermediate-scale quantum computers. In *Proceedings of the twenty-fourth international conference on architectural support for programming languages and operating systems*, pages 1015–1029, 2019.

[10] Aram W Harrow, Benjamin Recht, and Isaac L Chuang. Efficient discrete approximations of quantum gates. *Journal of Mathematical Physics*, 43(9):4445–4451, 2002.

[11] Lukas Burgholzer and Robert Wille. Advanced equivalence checking for quantum circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 40(9):1810–1824, 2020.

[12] John Watrous. *The theory of quantum information*. Cambridge university press, 2018.

[13] Glynn Winskel. *The formal semantics of programming languages: an introduction*. MIT press, 1993.

[14] Jianjun Zhao. Quantum software engineering: Landscapes and horizons. *arXiv preprint arXiv:2007.07047*, 2020.

[15] Manuel A Serrano, Jose A Cruz-Lemus, Ricardo Perez-Castillo, and Mario Piattini. Quantum software components and platforms: Overview and quality assessment. *ACM Computing Surveys*, 55(8):1–31, 2022.

[16] Qiskit contributors. Qiskit: An open-source framework for quantum computing, 2023.

[17] Benjamin Bichsel, Maximilian Baader, Timon Gehr, and Martin Vechev. Silq: A high-level quantum language with safe uncomputation and intuitive semantics. In *Proceedings of the 41st ACM SIGPLAN Conference on Programming Language Design and Implementation*, pages 286–300, 2020.

[18] Alexander S Green, Peter LeFanu Lumsdaine, Neil J Ross, Peter Selinger, and Benoît Valiron. Quipper: a scalable quantum programming language. In *Proceedings of the 34th ACM SIGPLAN conference on Programming language design and implementation*, pages 333–342, 2013.

[19] Krysta Svore, Alan Geller, Matthias Troyer, John Azariah, Christopher Granade, Bettina Heim, Vadym Kliuchnikov, Mariia Mykhailova, Andres Paz, and Martin Roetteler. Q# enabling scalable quantum computing and development with a high-level dsl. In *Proceedings of the real world domain specific languages workshop 2018*, pages 1–10, 2018.

[20] Margherita Zorzi. On quantum lambda calculi: a foundational perspective. *Mathematical Structures in Computer Science*, 26(7):1107–1195, 2016.

[21] Frederic T Chong, Diana Franklin, and Margaret Martonosi. Programming languages and compiler design for realistic quantum hardware. *Nature*, 549(7671):180–187, 2017.

[22] Shih-Han Hung, Kesha Hietala, Shaopeng Zhu, Mingsheng Ying, Michael Hicks, and Xiaodi Wu. Quantitative robustness analysis of quantum programs. *Proceedings of the ACM on Programming Languages*, 3(POPL):1–29, 2019.

[23] Runzhou Tao, Yunong Shi, Jianan Yao, John Hui, Frederic T Chong, and Ronghui Gu. Gleipnir: toward practical error analysis for quantum programs. In *Proceedings of the 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation*, pages 48–64, 2021.

[24] Fredrik Dahlqvist and Renato Neves. The syntactic side of autonomous categories enriched over generalised metric spaces. *Logical Methods in Computer Science*, 19, 2023.

[25] Jean-Yves Girard, Yves Lafont, and Laurent Regnier. *Advances in linear logic*, volume 222. Cambridge University Press, 1995.

[26] P Nick Benton. A mixed linear and non-linear logic: Proofs, terms and models. In *International Workshop on Computer Science Logic*, pages 121–135. Springer, 1994.

[27] Hendrik P Barendregt et al. *The lambda calculus*, volume 3. North-Holland Amsterdam, 1984.

[28] Paul Bernays. Alonzo church. an unsolvable problem of elementary number theory. american journal of mathematics, vol. 58 (1936), pp. 345–363. *The Journal of Symbolic Logic*, 1(2):73–74, 1936.

[29] John W Backus, Friedrich L Bauer, Julien Green, Charles Katz, John McCarthy, Alan J Perlis, Heinz Rutishauser, Klaus Samelson, Bernard Vauquois, Joseph Henry Wegstein, et al. Report on the algorithmic language algol 60. *Communications of the ACM*, 3(5):299–311, 1960.

[30] Michael Shulman. A practical type theory for symmetric monoidal categories. *Theory and Applications of Categories*, 37(5):863–907, 2021.

[31] Radu Mardare, Prakash Panangaden, and Gordon Plotkin. Quantitative algebraic reasoning. In *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 700–709, 2016.

[32] Radu Mardare, Prakash Panangaden, and Gordon Plotkin. On the axiomatizability of quantitative algebras. In *2017 32nd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–12. IEEE, 2017.

[33] Peter Selinger and Benoît Valiron. A lambda calculus for quantum computation with classical control. *Mathematical Structures in Computer Science*, 16(3):527–552, 2006.

[34] Peter Selinger, Benoıt Valiron, et al. Quantum lambda calculus. *Semantic techniques in quantum computation*, pages 135–172, 2009.

[35] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[36] Walter Rudin. *Functional Analysis*. McGraw-Hill, 1991.

[37] A Hitchhiker's Guide. *Infinite dimensional analysis*. Springer, 2006.

[38] Simon Perdrix. Quantum entanglement analysis based on abstract interpretation. In *International Static Analysis Symposium*, pages 270–282. Springer, 2008.

[39] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[40] John S Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

[41] Alain Aspect, Jean Dalibard, and Gérard Roger. Experimental test of bell's inequalities using time-varying analyzers. *Physical review letters*, 49(25):1804, 1982.

[42] Wolfgang Tittel, Jürgen Brendel, Bernard Gisin, Thomas Herzog, Hugo Zbinden, and Nicolas Gisin. Experimental demonstration of quantum correlations over more than 10 km. *Physical Review A*, 57(5):3229, 1998.

[43] Jian-Wei Pan, Dik Bouwmeester, Harald Weinfurter, and Anton Zeilinger. Experimental entanglement swapping: entangling photons that never interacted. *Physical review letters*, 80(18):3891, 1998.

[44] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, et al. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[45] Daniel A Lidar. Lecture notes on the theory of open quantum systems. *arXiv preprint arXiv:1902.00967*, 2019.

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

[47] David Deutsch. Quantum theory, the church–turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985.

[48] Swamit S Tannu and Moinuddin K Qureshi. Mitigating measurement errors in quantum computers by exploiting state-dependent bias. In *Proceedings of the 52nd annual IEEE/ACM international symposium on microarchitecture*, pages 279–290, 2019.

[49] Roy L Crole. *Categories for types*. Cambridge University Press, 1993.

[50] Peter Selinger. Lecture notes on the lambda calculus, 2013.

[51] Peter Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, 2004.

[52] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical review letters*, 70(13):1895, 1993.

[53] H-J Briegel, Wolfgang Dür, Juan I Cirac, and Peter Zoller. Quantum repeaters: the role of imperfect local operations in quantum communication. *Physical Review Letters*, 81(26):5932, 1998.

[54] Daniel Gottesman and Isaac L Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390–393, 1999.

[55] H Jeff Kimble. The quantum internet. *Nature*, 453(7198):1023–1030, 2008.

[56] Maximilian Schlosshauer. Decoherence, the measurement problem, and interpretations of quantum mechanics. *Reviews of Modern physics*, 76(4):1267, 2005.

[57] Alejo Salles, Fernando de Melo, MP Almeida, Malena Hor-Meyll, SP Walborn, PH Souto Ribeiro, and Luiz Davidovich. Experimental investigation of the dynamics of entanglement: Sudden death, complementarity, and continuous monitoring of the environment. *Physical Review A*, 78(2):022322, 2008.

[58] Jing Wang, Li Jiang, Han Zhang, Hanzhuang Zhang, and Liquan Zhang. Fidelity of structured amplitude-damping channels. *Physica Scripta*, 83(4):045008, mar 2011.

[59] Fredrik Dahlqvist and Renato Neves. A complete v-equational system for graded lambda-calculus. *Electronic Notes in Theoretical Informatics and Computer Science*, 3, 2023.

Place here information about funding, FCT project, etc. in which the work is framed. Leave empty otherwise.